Lie Groups

Richard Borcherds

May 25, 2012

Abstract

These are preliminary rather scrappy notes that have not yet been proofread. Many of the sections, especially the latter ones, are still incomplete, contain many errors, and need a lot of further work. You have been warned. For updated versions go to `http://math.berkeley.edu/~reb`.

These are notes for a Lie Groups course Math 261AB, 2011-2012. The course philosophy is that this is a service course, so I will emphasize applications of Lie groups to other areas, and will concentrate more on discussing examples than on giving complete proofs. Some of the sections are based on some lectures I gave a few years ago, and I have used the TeX files of notes for these lectures written by Hanh Duc Do, An Huang, Santiago Canez, Lilit Martirosyan, Emily Peters, Martin Vito-Cruz, Anton Geraschenko (many of whose TeX macros I have reused), and Sevak Mkrtchyan.

Contents

1 Examples

A typical example of a Lie group is the group $GL_2(\mathbb{R})$ of invertible 2 by 2 matrices, and a Lie group is defined to be something that resembles this. Its key properties are that it is a smooth manifold and a group and these structures are compatible. So we define a Lie group to be a smooth manifold that is also a group, such that the product and inverse are smooth maps. All manifolds will be smooth and metrizable unless otherwise stated.

We start by trying to list all Lie groups.

Example 1 Any discrete group is a 0-dimensional Lie group.

This already shows that listing all Lie groups is hopeless, as there are too many discrete groups. However we can split a Lie group into two: the component of the identity is a connected normal subgroup, and the quotient is discrete. Although a complete description of the discrete part is hopeless, we can go quite far towards classifying the connected Lie groups.

Example 2 The real numbers under addition are a 1-dimensional commutative Lie group. Similarly so is any finite dimensional real vector space under addition.

Example 3 The circle group S^1 of all complex numbers of absolute value 1 is a Lie group, also abelian.

We have essentially found all the connected abelian Lie groups: they are products of copies of the circle and the real numbers. For example, the non-zero complex numbers form a Lie group, which (via the exponential map and polar decomposition) is isomorphic to the product of a circle and the reals.

Example 4 The general linear group $GL_n(\mathbb{R})$ is the archetypal example of a non-commutative Lie group. This has 2 components as the determinant can be positive or negative. Similarly we can take the complex general linear group.

The classical groups are roughly the subgroups of general linear groups that preserve bilinear or hermitian forms. The compact orthogonal groups $O_n(\mathbb{R})$ preserve a positive definite symmetric bilinear form on a real vector space. We do not have to restrict to positiver definite forms: in special relativity we get the Lorentz group $O_{1,3}(\mathbb{R})$ preserving an indefinite form. The symplectic group $Sp_{2n}(\mathbb{R})$ preserves a symplectic form and is not compact. The unitary group U_n preserves a hermitian form on C^n and is compact as it is a closed subgroup of the orthogonal group on $\mathbb{R}^{2n}$. Again we do not have to restrict to positive definite Hermitian forms, and there are non-compact groups $U_{m,n}$ preserving $|z_1|^2 + \cdots + |z_m|^2 - z_{m+1}^2 - \cdots$.

There are many variations of these groups obtained by tweaking abelian groups at the top and bottom. We can kill off the abelian group at the top of many of them by taking matrices of determinant 1: this gives special linear, special orthogonal r groups and so on. ("Special" usually means determinant 1). Alternatively we can make the abelian group at the top bigger: the general symplectic group GSp is the group of matrices that multiply a symplectic form by a non-zero constant. We can also kill off the abelian group at the bottom (often the center) by quotienting out by it: this gives projective general linear groups and so on. (The word "projective" usually means quotient out by the center, and comes from the fact that the projective general linear group acts on projective space.) Finally we can make the center bigger by taking a central extension. For example, the spin groups are double covers of the special orthogonal groups. The spin group double cover of $SO_3(\mathbb{R})$ can be constructed using quaternions.

Exercise 5 If $z = a + bi + cj + dk$ is a quaternion show that $z\overline{z}$ is real, where $\overline{z} = a - bi - cj - dk$. Show that $z \mapsto |z| = \sqrt{z\overline{z}}$ is a homomorphism of groups from non-zero quaternions to positive reals. Show that the quaternions form a division ring; in other words check that every non-zero quaternion has an inverse.

Exercise 6 Identify $\mathbb{R}^3$ with the set of imaginary quaternions $bi + cj + dk$. Show that the group of unit quaternions S^3 acts on this by conjugation, and gives a homomorphism $S^3 \mapsto SO_3(\mathbb{R})$ whose kernel has order 2.

A typical example of a solvable Lie group is the group of upper triangular matrices with nonzero determinant. (Recall that solvable means the group can be split into abelian groups.) It has a subgroup consisting of matrices with 1s on the diagonal: this is a typical example of a nilpotent Lie group. (Nilpotent means that if we keep killing the center we eventually kill the whole group. We will see later that a connected Lie group is nilpotent if all elements of its lie algebra are nilpotent matrices: this is where the name “nilpotent” comes from.)

$$G_{\rm sol} \subseteq \left\{ \begin{pmatrix} * & & & * \\ & \ddots & & \\ & & * & \\ 0 & & & * \end{pmatrix} \right\} \qquad G_{\rm nil} \subseteq \left\{ \begin{pmatrix} 1 & & & * \\ & \ddots & & \\ & & 1 & \\ 0 & & & 1 \end{pmatrix} \right\}$$

Exercise 7 Check that these groups are indeed solvable and nilpotent.

Exercise 8 Show that any finite group of prime-power order p^n is nilpotent, and find a non-abelian example of order p^3 for any prime p. (Hint: show that any conjugacy class not in the center has order divisible by p, and deduce that the center has order divisible by p unless the group is trivial.)

Exercise 9 The Moebius group consists of all isomorphisms from the complex unit disk to itself: $z \mapsto (az+b)/(cz+d)$ with $ad - bc = 1$, $a = \bar{d}$, $b = \bar{c}$. Show that this is the group $PSU_{1,1}$. Similarly show that the group of conformal transformations of the upper half plane is $PSL_2(\mathbb{R})$. Since the upper half plane is isomorphic to the unit disc, we see that the groups $PSU_{1,1}$ and $PSL_2(\mathbb{R})$ are isomorphic. This illustrates one of the confusing things about Lie groups: there are a bewildering number of unexpected isomorphisms between them in small dimensions.

Exercise 10 Show that there is a (nontrivial!) homomorphism from $SL_2(\mathbb{R})$ to the group $O_{2,1}(\mathbb{R})$, and find the image and kernel. (Consider the action of the group $SL_2(\mathbb{R})$ on the 3-dimensional symmetric square $S^2(\mathbb{R}^2)$ and show that this action preserves a quadratic form of signature $(2,1)$.)

Klein claimed at one point that geometry should be identified with group theory: a geometry is determined by its group of symmetries. (This fails for Riemannian geometry.) For example, affine geometry consists of the properties of space invariant under the group of affine transformations, projective geometry is properties of projective space invariant under projective transformations, and so on. The group of affine transformations in n dimensions is a semidirect product $\mathbb{R}^n.GL_n(\mathbb{R})$. This can be identified with the subgroup of GL_{n+1} fixing a vector (sometimes called the mirabolic subgroup). For example, in 1-dimension we get a non-abelian 2-dimensional Lie group of transformations $x \mapsto ax + b$ with $a \neq 0$.

What does a general Lie group look like? In general, a Lie group G can be broken up into a number of pieces as follows.

As we mentioned earlier,the connected component of the identity, $G_{\rm conn} \subseteq G$, is a normal subgroup, and $G/G_{\rm conn}$ is a discrete group.

$$1 \longrightarrow G_{\rm conn} \longrightarrow G \longrightarrow G_{\rm discrete} \longrightarrow 1$$

so this breaks up a Lie group into a connected subgroup and a discrete quotient.

The maximal connected normal solvable subgroup of $G_{\rm conn}$ is called the solvable radical $G_{\rm sol}$. Recall that a group is *solvable* if there is a chain of subgroups

$G_{\text{sol}} \supseteq \cdots \supseteq 1$, where consecutive quotients are abelian. Lie's theorem tells us that some cover of G_{sol} is isomorphic to a subgroup of the group of upper triangular matrices.

Since G_{sol} is solvable, $G_{\text{nil}} := [G_{\text{sol}}, G_{\text{sol}}]$ is nilpotent, i.e. there is a chain of subgroups $G_{\text{nil}} \supseteq G_1 \supseteq \cdots \supseteq G_k = 1$ such that G_i/G_{i+1} is in the center of G_{nil}/G_{i+1}. In fact, G_{nil} must be isomorphic to a subgroup of the group of upper triangular matrices with ones on the diagonal. Such a group is called *unipotent*.

Every normal solvable subgroup of $G_{\text{conn}}/G_{\text{sol}}$ is discrete, and therefore in the center (which is itself discrete). We call the pre-image of the center G_*. Then G/G_* is a product of simple groups (groups with no normal subgroups).

So a general Lie group has a chain of normal subgroups that are trivial,nilpotent, solvable, connected, or the whole group, such that the quotients are nilpotent, abelian, almost a product of simple groups, and discrete.

Example 11 Let G be the group of all shape-preserving transformations of $\mathbb{R}^4$ (i.e. translations, reflections, rotations, and scaling). It is sometimes called $\mathbb{R}^4 \cdot GO_4(\mathbb{R})$. The $\mathbb{R}^4$ stands for translations, the G means that we can multiply by scalars, and the O means that we can reflect and rotate. The $\mathbb{R}^4$ is a normal subgroup. In this case, we have

$$\begin{array}{rrl}
 & \mathbb{R}^4 \cdot GO_4(\mathbb{R}) = G & \\
 & & G/G_{\text{conn}} = \mathbb{Z}/2\mathbb{Z} \\
\begin{array}{r} G_{\text{conn}}/G_{\text{sol}} \\ = SO_4(\mathbb{R}) \end{array} \left\{ \begin{array}{r} \\ \\ \\ \\ \end{array} \right. & \begin{array}{r} \mathbb{R}^4 \cdot GO_4^+(\mathbb{R}) = G_{\text{conn}} \\ \\ \mathbb{R}^4 \cdot \mathbb{R}^\times = G_* \\ \\ \mathbb{R}^4 \cdot \mathbb{R}^+ = G_{\text{sol}} \end{array} & \begin{array}{l} \\ G_{\text{conn}}/G_* = PSO_4(\mathbb{R}) \\ \qquad\qquad \big(\simeq SO_3(\mathbb{R}) \times SO_3(\mathbb{R})\big) \\ G_*/G_{\text{sol}} = \mathbb{Z}/2\mathbb{Z} \\ \end{array} \\
 & & G_{\text{sol}}/G_{\text{nil}} = \mathbb{R}^+ \\
 & \mathbb{R}^4 = G_{\text{nil}} &
\end{array}$$

where $GO_4^+(\mathbb{R})$ is the connected component of the identity (those transformations that preserve orientation), $\mathbb{R}^\times$ is scaling by something other than zero, and $\mathbb{R}^+$ is scaling by something positive. Note that $SO_3(\mathbb{R}) = PSO_3(\mathbb{R})$ is simple.

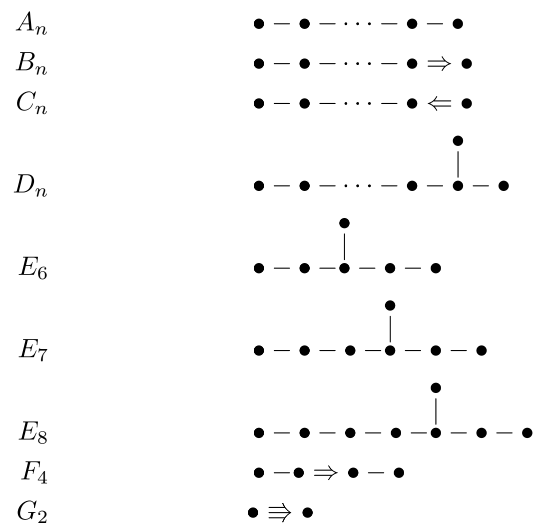
$SO_4(\mathbb{R})$ is "almost" the product $SO_3(\mathbb{R}) \times SO_3(\mathbb{R})$. To see this, consider the associative (but not commutative) algebra of quaternions, $\mathbb{H}$. Since $q\bar{q} = a^2 + b^2 + c^2 + d^2 > 0$ whenever $q \neq 0$, any non-zero quaternion has an inverse (namely, $\bar{q}/q\bar{q}$). Thus, $\mathbb{H}$ is a division algebra. Think of $\mathbb{H}$ as $\mathbb{R}^4$ and let S^3 be the unit sphere, consisting of the quaternions such that $\|q\| = q\bar{q} = 1$. It is easy to check that $\|pq\| = \|p\| \cdot \|q\|$, from which we get that left (right) multiplication by an element of S^3 is a norm-preserving transformation of $\mathbb{R}^4$. So we have a map $S^3 \times S^3 \to O_4(\mathbb{R})$. Since $S^3 \times S^3$ is connected, the image must lie in $SO_4(\mathbb{R})$. It is not hard to check that $SO_4(\mathbb{R})$ is the image. The kernel is $\{(1,1), (-1,-1)\}$. So we have $S^3 \times S^3/\{(1,1),(-1,-1)\} \simeq SO_4(\mathbb{R})$.

Conjugating a purely imaginary quaternion by some $q \in S^3$ yields a purely imaginary quaternion of the same norm as the original, so we have a homomorphism $S^3 \to O_3(\mathbb{R})$. Again, it is easy to check that the image is $SO_3(\mathbb{R})$ and that the kernel is ± 1, so $S^3/\{\pm 1\} \simeq SO_3(\mathbb{R})$.

So the universal cover of $SO_4(\mathbb{R})$ (a double cover) is the Cartesian square of the universal cover of $SO_3(\mathbb{R})$ (also a double cover). Orthogonal groups in dimension 4 have a strong tendency to split up like this. Orthogonal groups tend to have these double covers.

Exercise 12 Let G be the (parabolic) subgroup of $GL_4(\mathbb{R})$ of matrices whose lower left 2 by 2 block of elements are all zero. Decompose G in an analogous way to the example above.

So to classify all connected Lie groups we need to find the simple ones, the unipotent ones, and find how the simple ones can act on the unipotent ones. One might guess that the easiest part of this will be to find the unipotent ones, as these are just built from abelian ones by taking central extensions. However this turns out to be the hardest part, and there seems to be no good solution. The simple ones can be classified with some effort: we will more or less do this in the course. Over the complex numbers the complete list is given by the following Dynkin diagrams (where the subscript in the name is the number of nodes):



These Dynkin diagrams are pictures of the Lie groups with the following meaning. Each dot is a copy of SL_2. Two dots are disconnected if the corresponding SL_2s commute, and are joined by a single line if they "overlap by one matrix element". Double and triple lines describe more complicated ways they can interact. For each complex simple Lie group there are a finite number of simple real Lie groups whose complexification is the complex Lie group, and we will later use this to find the simple Lie groups.

For example, $\mathfrak{sl}_2(\mathbb{R}) \not\simeq \mathfrak{su}_2(\mathbb{R})$, but $\mathfrak{sl}_2(\mathbb{R}) \otimes \mathbb{C} \simeq \mathfrak{su}_2(\mathbb{R}) \otimes \mathbb{C} \simeq \mathfrak{sl}_2(\mathbb{C})$. By the way, $\mathfrak{sl}_2(\mathbb{C})$ is simple as a *real* Lie algebra, but its complexification is $\mathfrak{sl}_2(\mathbb{C}) \oplus \mathfrak{sl}_2(\mathbb{C})$, which is not simple.

Dynkin diagrams also classify lots of other things: 3-dimensional rotation groups, finite crystallographic reflection groups, du Val singularities, Macdonald polynomials, singular fibers of elliptic surfaces or elliptic curves over the integers,...

Exercise 13 Find out what all the things mentioned above are, and find some more examples of mathematical objects classified by these Dynkin diagrams. (Hint: wikipedia.)

We also need to know the actions of simple Lie groups on unipotent ones. We can at least describe the actions on abelian ones: this is called representation theory.

1.1 Infinite dimensional Lie groups

Examples of infinite dimensional Lie groups are diffeomorphisms of manifolds, or gauge groups, or infinite dimensional classical groups. There is not much general theory of infinite dimensional Lie groups: they are just too complicated.

1.2 Lie groups and finite groups

1. The classification of finite simple groups resembles the classification of connected simple Lie groups.

   For example, $PSL_n(\mathbb{R})$ is a simple Lie group, and $PSL_n(\mathbb{F}_q)$ is a finite simple group except when $n = q = 2$ or $n = 2, q = 3$. Simple finite groups form about 18 series similar to Lie groups, and 26 or 27 exceptions, called sporadic groups, which don't seem to have any analogues for Lie groups.

   Exercise 14 Show that the projective special linear groups $PSL_2(\mathbb{F}_4)$ and $PSL_2(\mathbb{F}_5)$ are isomorphic (or if this is too hard, show they have the same order). This gives a first hint of some of the complications of finite simple groups: there are many accidental isomorphisms similar to this.

2. Finite groups and Lie groups are both built up from simple and abelian groups. However, the way that finite groups are built is much more complicated than the way Lie groups are built. Finite groups can contain simple subgroups in very complicated ways; not just as direct factors.

   For example, there are *wreath products*. Let G and H be finite simple groups with an action of H on a set of n points. Then H acts on G^n by permuting the factors. We can form the semi-direct product $G^n \ltimes H$, sometimes denoted $G \wr H$. There is no analogue for (finite dimensional) Lie groups. There is an analogue for infinite dimensional Lie groups, which is one reason why the theory becomes hard in infinite dimensions.

3. The commutator subgroup of a connected solvable Lie group is nilpotent, but the commutator subgroup of a solvable finite group need not be a nilpotent group.

   Exercise 15 Show that the symmetric group S_4 is solvable but its derived subgroup is not nilpotent. Show that it cannot be represented as a group of upper triangular matrices over any field.

4 Non-trivial nilpotent finite groups are never subgroups of real upper triangular matrices (with ones on the diagonal).

1.3 Lie groups and algebraic groups

By algebraic group, we mean an algebraic variety which is also a group, such as $GL_n(\mathbb{R})$. Any real algebraic group is a Lie group. Most of the connected Lie groups we have seen so far are real algebraic groups. Since they are so similar, we'll list some differences.

1. Unipotent and semisimple abelian algebraic groups are totally different, but for Lie groups they are nearly the same. For example $\mathbb{R} \simeq \{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)\}$ is unipotent and $\mathbb{R}^\times \simeq \left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)\right\}$ is semisimple. As Lie groups, they are closely related (nearly the same), but the Lie group homomorphism $\exp : \mathbb{R} \to \mathbb{R}^\times$ is not algebraic (polynomial), so they look quite different as algebraic groups.

2. Abelian varieties are different from affine algebraic groups. For example, consider the (projective) elliptic curve $y^2 = x^3 + x$ with its usual group operation and the group of matrices of the form $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$ with $a^2 + b^2 = 1$. Both are isomorphic to S^1 as Lie groups, but they are completely different as algebraic groups; one is projective and the other is affine.

3. Some Lie groups do not correspond to ANY algebraic group. We give two examples here.

   The *Heisenberg group* is the subgroup of symmetries of $L^2(\mathbb{R})$ generated by translations $(f(t) \mapsto f(t+x))$, multiplication by $e^{2\pi i t y}$ $(f(t) \mapsto e^{2\pi i t y} f(t))$, and multiplication by $e^{2\pi i z}$ $(f(t) \mapsto e^{2\pi i z} f(t))$. The general element is of the form $f(t) \mapsto e^{2\pi i (yt+z)} f(t+x)$. This can also be modeled as

$$\left\{\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}\right\} \Big/ \left\{\begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\middle| n \in \mathbb{Z}\right\}$$

   It has the property that in any finite dimensional representation, the center (elements with $x = y = 0$) acts trivially, so it cannot be isomorphic to any algebraic group.

   The *metaplectic group*. Let's try to find all connected groups with Lie algebra $\mathfrak{sl}_2(\mathbb{R}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) | a + d = 0\}$. There are two obvious ones: $SL_2(\mathbb{R})$ and $PSL_2(\mathbb{R})$. There aren't any other ones that can be represented as groups of finite dimensional matrices. However, if you look at $SL_2(\mathbb{R})$, you'll find that it is not simply connected. To see this, we will use Iwasawa decomposition (which we will only prove in some special cases).

   Theorem 16 (Iwasawa decomposition) *If G is a connected semisimple Lie group, then there are closed subgroups K, A, and N, with K compact, A abelian, and N unipotent, such that the multiplication map $K \times A \times N \to G$ is a surjective diffeomorphism. Moreover, A and N are simply connected.*

   In the case of SL_n, this is the statement that any basis can be obtained uniquely by taking an orthonormal basis ($K = SO_n$), scaling by positive reals (A is the group of diagonal matrices with positive real entries), and shearing (N is the group $\begin{pmatrix} 1 & \ddots & * \\ 0 & \ddots & 1 \end{pmatrix}$). This is exactly the result of the Gram-Schmidt process.

The upshot is that $G \simeq K \times A \times N$ (topologically), and A and N do not contribute to the fundamental group, so the fundamental group of G is the same as that of K. In our case, $K = SO_2(\mathbb{R})$ is isomorphic to a circle, so the fundamental group of $SL_2(\mathbb{R})$ is $\mathbb{Z}$.

So the universal cover $\widetilde{SL_2(\mathbb{R})}$ has center $\mathbb{Z}$. Any finite dimensional representation of $\widetilde{SL_2(\mathbb{R})}$ factors through $SL_2(\mathbb{R})$, so none of the covers of $SL_2(\mathbb{R})$ can be written as a group of finite dimensional matrices. Representing such groups is a pain.

(This seems to be repeated later....) Most of the examples of Lie groups so far are algebraic: this means roughly that they are algebraic varieties over the reals. Much of the theory of algebraic groups is similar to that of Lie groups, but there are some differences. In particular some Lie groups are not algebraic. One example is the group of upper triangular 3 by 3 unipotent matrices modulo $\mathbb{Z}$. This is the Heisenberg or Weyl group: it has a nice infinite dimensional representation generated by translations and multiplication by e^{iyx} acting on L^2 functions on the reals. it is somewhat easier to study the representations of its Lie algebra, which has a basis of 3 elements X, Y, Z with $[X, Y] = Z$. We can represent this in infinite dimensions by putting $X = x$, $Y = d/dx$, $Z = 1$ acting on polynomials (this is Leibniz's rule!) In quantum mechanics this algebra turns up a lot where X is the position operator and Y the momentum operator. But it has not finite dimensional representations with Z acting as 1 because the trace of Z must be 0.

Also abelian algebraic groups are much more subtle than abelian Lie groups. For example, over the complex numbers, the Lie groups $\mathbb{C}$, $\mathbb{C}^*$, and an elliptic curve are all quite similar: they differ by quotienting out copies of $\mathbb{Z}$ so look the same locally. However as algebraic groups they are totally different and have nothing to do with each other: the first is unipotent, the second is semisimple, and the third is a (complete) variety. The point is that the maps between the corresponding Lie groups that make them similar are transcendental functions (exponentials or elliptic functions) that do not exist in the algebraic setting. Rather oddly, non-abelian algebraic groups are easier to handle than abelian ones. The reason is that non-abelian ones can be studied using the adjoint representation on their Lie algebras, while for abelian ones this representation is trivial and gives no useful information: abelian varieties are abelian algebraic groups, and are VERY hard to understand over the rationals.

The most important case is the metaplectic group $Mp_2(\mathbb{R})$, which is the connected double cover of $SL_2(\mathbb{R})$. It turns up in the theory of modular forms of half-integral weight and has a representation called the metaplectic representation.

p-adic Lie groups are defined in a similar way to Lie groups using p-adic manifolds rather than smooth manifolds. They turn up a lot in number theory and algebraic geometry. For example, Galois groups act on varieties defined over number fields, and therefore act on their (etale) cohomology groups, which are vector spaces over p-adic fields, So we get representations of Galois groups into p-adic Lie groups. These see much more of the Galois group than representations into real Lie groups, which tend to have finite images.

1.4 Lie groups and Lie algebras

Lie groups can have a rather complicated global structure. For example, what does $GL_n(\mathbb{R})$ look like as a topological space, and what are its homology groups? Lie algebras are a way to linearize Lie groups. The Lie algebra is just the tangent space to the identity, with a Lie bracket $[,]$ which is a sort of ghost of the commutator in the Lie group. The Lie algebra is almost enough to determine the connected component of the Lie group. (Obviously it cannot see any of the components other than the identity.)

Exercise 17 The Lie algebra of $GL_n(\mathbb{R})$ is $M_n(\mathbb{R})$, with Lie bracket $[A, B] = AB - BA$, corresponding to the fact that if A and B are small then the commutator $(1 + A)(1 + B)(1 + A)^{-1}(1 + B)^{-1} = 1 + [A, B]+$ higher order terms. Show that $[A, B] = -[B, A]$ and prove the Jacobi identity

$$[[A, B], C] + [[B, C], A] + [[C, A], B] = 0$$

An abstract Lie algebra over a field is a vector space with a bracket satisfying these two identities.

We have an equivalence of categories between simply connected Lie groups and Lie algebras. The correspondence cannot detect

- Non-trivial components of G. For example, SO_n and O_n have the same Lie algebra.
- Discrete normal (therefore central) subgroups of G. If $Z \subseteq G$ is any discrete normal subgroup, then G and G/Z have the same Lie algebra. For example, $SU(2)$ has the same Lie algebra as $PSU(2) \simeq SO_3(\mathbb{R})$.

If $\tilde{G}$ is a connected and simply connected Lie group with Lie algebra $\mathfrak{g}$, then any other connected group G with Lie algebra $\mathfrak{g}$ must be isomorphic to $\tilde{G}/Z$, where Z is some discrete subgroup of the center. Thus, if you know all the discrete subgroups of the center of $\tilde{G}$, we can read off all the connected Lie groups with the given Lie algebra.

Let's find all the groups with the algebra $\mathfrak{so}_4(\mathbb{R})$. First let's find a simply connected group with this Lie algebra. You might guess $SO_4(\mathbb{R})$, but that isn't simply connected. The simply connected one is $S^3 \times S^3$ as we saw earlier (it is a product of two simply connected groups, so it is simply connected). The center of S^3 is generated by -1, so the center of $S^3 \times S^3$ is $(\mathbb{Z}/2\mathbb{Z})^2$, the Klein four group. There are three subgroups of order 2

Therefore, there are 5 groups with Lie algebra $\mathfrak{so}_4$.

Formal groups are intermediate between Lie algebras and Lie groups: We get maps (Lie groups) to (Formal groups) to (Lie algebras). In characteristic 0 there is little difference between formal groups and Lie algebras, but over more general rings there is a big difference. Roughly speaking, Lie algebras seem to be the "wrong" objects in this case as they do not see enough of the group, and formal groups seem to be a good replacement.

A 1-dimensional formal group is a power series $F(x, y) = x + y + \cdots$ that is associative in the obvious sense $F(x, F(y, z)) = F(F(x, y), z)$. For example $F(x, y) = x + y$ is a formal group called the additive formal group.

Exercise 18 Show that $F(x, y) = x + y + xy$ is a formal group, and check that over the rationals it is isomorphic to the additive formal group (in other words there is a power series with rational coefficients such that $F(f(x), f(y)) = f(x + y)$). These formal groups are not isomorphic over the integers.

Higher dimensional formal groups are defined similarly, except they are given by several power series in several variables.

1.5 Important Lie groups

Dimension 1: There are just $\mathbb{R}$ and $S^1 = \mathbb{R}/\mathbb{Z}$.

Dimension 2: The abelian groups are quotients of $\mathbb{R}^2$ by some discrete subgroup; there are three cases: $\mathbb{R}^2$, $\mathbb{R}^2/\mathbb{Z} = \mathbb{R} \times S^1$, and $\mathbb{R}^2/\mathbb{Z}^2 = S^1 \times S^1$.

There is also a non-abelian group, the group of all matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & a^{-1} \end{smallmatrix}\right)$, where $a > 0$. The Lie algebra is the subalgebra of 2×2 matrices of the form $\left(\begin{smallmatrix} h & x \\ 0 & -h \end{smallmatrix}\right)$, which is generated by two elements H and X, with $[H, X] = 2X$.

Dimension 3: There are some abelian and solvable groups, such as $\mathbb{R}^2 \ltimes \mathbb{R}^1$, or the direct sum of $\mathbb{R}^1$ with one of the two dimensional groups. As the dimension increases, the number of solvable groups gets huge, so we ignore them from here on.

You get the group $SL_2(\mathbb{R})$, which is the most important Lie group of all. We saw earlier that $SL_2(\mathbb{R})$ has fundamental group $\mathbb{Z}$. The double cover $Mp_2(\mathbb{R})$ is important. The quotient $PSL_2(\mathbb{R})$ is simple, and acts on the open upper half plane by linear fractional transformations

Closely related to $SL_2(\mathbb{R})$ is the compact group SU_2. We know that $SU_2 \simeq S^3$, and it covers $SO_3(\mathbb{R})$, with kernel ± 1. After we learn about Spin groups, we will see that $SU_2 \cong \mathrm{Spin}_3(\mathbb{R})$. The Lie algebra $\mathfrak{su}_2$ is generated by three elements X, Y, and Z with relations $[X, Y] = 2Z$, $[Y, Z] = 2X$, and $[Z, X] = 2Y$.[1]

The Lie algebras $\mathfrak{sl}_2(\mathbb{R})$ and $\mathfrak{su}_2$ are non-isomorphic, but when we complexify, they both become isomorphic to $\mathfrak{sl}_2(\mathbb{C})$.

There is another interesting 3 dimensional algebra. The Heisenberg algebra is the Lie algebra of the Heisenberg group. It is generated by X, Y, Z, with $[X, Y] = Z$ and Z central. You can think of this as strictly upper triangular matrices.

Dimension 6: (nothing interesting happens in dimensions 4,5) We get the group $SL_2(\mathbb{C})$. Later, we will see that it is also called $\mathrm{Spin}_{1,3}(\mathbb{R})$.

Dimension 8: We have $SU_3(\mathbb{R})$ and $SL_3(\mathbb{R})$. This is the first time we get a 2-dimensional root system.

Dimension 14: G_2, which we will discuss a little.

Dimension 248: E_8, which we will discuss in detail.

This class is mostly about finite dimensional algebras, but let's mention some infinite dimensional Lie groups or Lie algebras.

[1]An explicit representation is given by $X = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, $Y = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$, and $Z = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$. The cross product on $\mathbb{R}^3$ gives it the structure of this Lie algebra.

1. Automorphisms of a Hilbert space form a Lie group.

2. Diffeomorphisms of a manifold form a Lie group. There is some physics stuff related to this.

3. *Gauge groups* are (continuous, smooth, analytic, or whatever) maps from a manifold M to a group G.

4. The *Virasoro algebra* is generated by L_n for $n \in \mathbb{Z}$ and c, with relations $[L_n, L_m] = (n-m)L_{n+m} + \delta_{n+m,0}\frac{n^3-n}{12}c$, where c is central (called the *central charge*). If we set $c = 0$, we get (complexified) vector fields on S^1, where we think of L_n as $ie^{in\theta}\frac{\partial}{\partial\theta}$. Thus, the Virasoro algebra is a central extension
$$0 \to c\mathbb{C} \to \text{Virasoro} \to \text{Vect}(S^1) \to 0.$$

5. Affine Kac-Moody algebras, which are more or less central extensions of certain gauge groups over the circle.

2 Lie algebras

Lie groups such as $GL_n(\mathbb{R})$ are quite complicated nonlinear objects. A Lie algebra is a way of linearizing a Lie group, which is often easier to handle. Roughly speaking, the addition and Lie bracket of the Lie algebra are given by the lowest order terms in the product and commutator of the Lie group. By a minor miracle (the Campbell-Baker-Hausdorff formula) we do not need any higher order terms: the Lie algebra is enough to determine the group product locally. We first recall some background about vector fields and differential operators on a manifold. We will then define the Lie algebra of a Lie group to be the left invariant vector fields on the group.

For any algebra over a ring we define the Lie bracket $[a, b]$ to be $ab - ba$. It satisfies the identities

- $[a, b]$ is bilinear
- $[a, b] = -[b, a]$
- $[[a, b], c] + [[b, c], a] + [[c, a], b] = 0$ (Jacobi identity)

Definition 19 *A Lie algebra over a ring is a module with a bracket satisfying the conditions above, in other words it is bilinear, skew symmetric, and satisfies the Jacobi identity.*

These conditions make sense in any additive tensor category, so for example we can define Lie algebras of sheaves, or graded Lie algebras. An interesting variation is Lie superalgebras, where we use the tensor category of supermodules over a ring or field. Some authors add the non-linear condition that $[a, a] = 0$.

Example 20 The basic example of a Lie algebra is given by taking V to be an associative algebra and defining $[a, b]$ to be $ab - ba$.

The Lie algebra of a Lie group can be defined as its tangent space at the identity, with the Lie bracket given by the lowest order part of the commutator. The lowest-order terms of the group law are just given by addition on the Lie algebra, as can be seen in $GL_n(\mathbb{R})$: the product of $1+\epsilon A$ and $1+\epsilon B$ is $1+\epsilon(A+B)$ to first order. However defining the Lie bracket in terms of the commutator is a little messy, and it is technically more convenient to define the Lie algebra as the left invariant vector fields on the manifold.

There are several different ways to think of vector fields:

- Informally, a vector field is a little tangent vector at each point.
- A vector field is informally an infinitesimal diffeomorphism, where we get an infinitesimal diffeomorphism from a vector field by pushing each point slightly in the direction of the vector field.
- More formally, a vector field is a section of the tangent bundle or sheaf.
- A vector field is a normalized differential operator of order at most 1
- A vector field is a derivation of the ring of smooth functions.

The last two seem less intuitive but turn out to be the easiest definitions to work with.

Suppose we have a manifold M, with its ring R of smooth functions. A differential operator on M should be something that in local coordinates looks like a partial differential operator times a smooth function. It is easier to forget about local coordinates, and just use the following key property of differential operators: the commutator of an nth order operator with a smooth function is a differential operator of smaller order. This is really just a form of Leibniz's rule for differentiating a product. We will use this to DEFINE differential operators as follows.

Definition 21 *A differential operator of order less than 0 is 0. A differential operator of order at most $n \geq 0$ is an operator on R whose commutator with elements of R is a differential operator of order at most $n-1$.*

Differential operators on R form a filtered ring $D^0 \subset D^1 \subset D^2 \cdots$, where D^n is the differential operators of order at most n. The differential operators of order at most 0 can be identified with the ring R (look at their action on 1), and any differential operator can be normalized by adding a function so that it kills 1. So a differential operator can be written canonically as a function (order 0 operator) plus a normalized differential operator.

The product of differential operators of orders at most m, n has order at most $m+n$. Differential operators do not quite commute with each other; however the commutator or Lie bracket $[D_1, D_2]$ of operators of orders at most m, n has order at most $m+n-1$; in other words differential operators commute "up to lower order terms". This means that the associated graded ring $D^0 \oplus D^1/D^0 \oplus D^2/D^1 \oplus \cdots$ is a commutative graded ring (whose elements are sometimes called symbols).

We will call a differential operator normalized if it kills the function 1. Differential operators of order at most 1 can be written canonically as the sum of an order 0 differential operator and a normalized differential operator. (However there is no canonical way to write an operator of order $n > 1$ as an operator of order less than n and something "homogeneous" of order n.) A vector field on a manifold is the same as a normalized differential operator of order at most 1. Vector fields are closed under the Lie bracket, and in particular form a Lie algebra. It is useful to think of a vector field as a sort of infinitesimal diffeomorphism of the manifold: each point is moved an infinitesimal distance in the direction of the vector at that point. Since the Lie algebra of a group can be thought of as the "infinitesimal" elements of the group, this means that the vector fields on a manifold are more or less the Lie algebra of the group of diffeomorphisms.

The Lie algebra of vector fields is an infinite dimensional Lie algebra, which is too big for this course, so we cut it down.

Definition 22 *The Lie algebra of a Lie group is the Lie algebra of left-invariant vector fields on the group.*

We explain what this means. The group is a manifold, so we have the Lie algebra of all vector fields on it forming an infinite dimensional lie algebra. The group acts on itself by left translation, and so acts on everything constructed from the manifold, such as vector fields. We just take the vector fields fixed by this action of left translation. It is automatically a subalgebra of the lie algebra of all vector fields, as the group action preserves the Lie bracket.

We can also identify the Lie algebra of the group with the tangent space at the origin. The reason is that if we pick a tangent vector at the origin, there is a unique vector field on G given by left translating this vector everywhere. We could have defined the Lie algebra to be the tangent space at the origin, but then it would not have been so clear how (or why) we can define the Lie bracket.

Now we will calculate the left invariant vector fields on the group $GL_n(R)$ and find the Lie bracket. We will then be able to find the Lie algebras of other groups by mapping them to $GL_n(R)$. There are obvious coordinates x_{ij} for $GL_n(R) \subset R^{n\times n}$, and corresponding vector fields $\partial/\partial x_{ij}$. Of course they are not left invariant under $GL_n(R)$: they are left invariant vector fields on the abelian group R^{n^2}, and have zero Lie bracket.

We let $x = (x_{ij})$ be the matrix whose entries are the coordinate functions. We can think of x as the identity function from R^{n^2} to itself, so might guess that G acts trivially on it, but this is wrong: the point is that the two copies of R^{n^2} are not really the same as the domain is acted on by G by translations, while the range is acted on trivially by G. This is very confusing. The action of an element g on x is given by right multiplying it by g^{-1}. Next if $a = (a_{ij})$ is a matrix we can consider the matrix of differential operators with entries a_{ij} We consider the matrix D of differential operators $x_{ik}\partial/\partial x_{jk}$ (using the Einstein summation convention). This acts on x as left multiplication by the matrix e_{ij} (with a 1 in position i, j, other entries 0). Since left multiplication by a matrix commutes with right multiplication we see that these differential operators all commute with left translation on the entries of x, and therefore are left invariant differential operators.

So we get a natural correspondence between n by n matrices and these left invariant differential operators. Finally we can work out the Lie bracket of two such differential operators

$$[x_{ik}\frac{\partial}{\partial x_{jk}}, x_{i'k'}\frac{\partial}{\partial x_{j'k'}}] = [j = i']x_{ij}\frac{\partial}{\partial x_{j'k}} - [i = j']x_{i'j}\frac{\partial}{\partial x_{j'k}}$$

, and we see that it just corresponds to the Lie bracket

$$[e_{ij}, e_{i'j'}] = [j = i']e_{ij'} - [i = j']e_{i'j}$$

of n by n matrices e_{ij} that have a one in position (i, j) and are zero elsewhere.

To summarize, the Lie algebra of $GL_n(R)$ is just $M_n(R)$, with the Lie bracket given by $[A, B] = AB - BA$.

To find the Lie algebras of subgroups of general linear groups, which covers most practical cases, we just have to find the tangent space at the identity. The easy way to do this to to find the matrices A such that $1 + \epsilon A$ satisfies the equations defining the Lie group, where $\epsilon^2 = 0$.

Example 23 The orthogonal group consists of matrices g such that $gg^T = I$. So its Lie algebra consists of matrices a such that $(1 + \epsilon a)(1 + \epsilon a^T) = 1$ to first order in ϵ, in other words $a + a^T = 0$, so that a s skew-symmetric.

Example 24 The special linear group consists of matrices g such that $\det g = 1$. So its Lie algebra consists of matrices a such that $\det(1 + \epsilon a) = 1$ to first order in ϵ. Since $\det(1 + a\epsilon) = 1 + \mathrm{Trace}(a)\epsilon$ to first order in epsilon, the Lie algebra consists of the matrices of trace 0.

Exercise 25 Show that the Lie algebra of the unitary group consists of skew Hermitian matrices, which are Hermitian matrices multiplied by i.

Identifying skew hermitian matrices with hermitian matrices by multiplication by i shows that defining $[a, b] = i(ab - ba)$ makes Hermitian matrices into a Lie algebra. This Lie bracket is not the only interesting algebraic structure one can put on Hermitian matrices.

Exercise 26 Show that if a and b are Hermitian then so is their Jordan product $a \circ b = (ab+ba)/2$. Show that this is a commutative but non-associative product, satisfying the Jordan identity $(x \circ y) \circ (x \circ x) = x \circ (y \circ (x \circ x))$. Algebras with these properties are called Jordan algebras.

In the early days of quantum mechanics it was hoped that a suitable Jordan algebra would explain the universe, but this hope was abandoned when the simple finite dimensional Jordan algebras were classified: they are mostly algebras of Hermitian matrices, and none of them explain the known elementary particles.

Exercise 27 Find the Lie algebra of the group $Sp_{2n}(\mathbb{R})$ of symplectic matrices.

As we mentioned before, the Lie algebra cannot detect other components of the Lie group, or discrete normal subgroups. It is often useful to note that discrete normal subgroups of a connected group are always in the center (proof: the image of an element under conjugation is connected and discrete, so is just one point). So for example, O_n, SO_n and PO_n all have the same Lie algebra.

Subalgebras of Lie algebras B are defined in the obvious way and are analogues of subgroups. The analogues of normal subgroups are subalgebras A such that $[A, B] \subseteq A$ (corresponding to the fact that a subgroup is normal if and only, if $aba^{-1}b^{-1}$ is in A for all $a \in A$ and $b \in B$) so that B/A is a Lie algebra in the obvious way. Much of the terminology for groups is extended to Lie algebras in the most obvious way. For example a Lie algebra is called abelian if the bracket is always 0, and is called solvable if there is a chain of ideals with abelian quotients. Unfortunately the definition of simple Lie algebras and simple Lie groups is not completely standardized and is not consistent with the definition of a simple abstract group. The definition of a simple lie algebra has a trap: a Lie algebra is called simple if it has no ideals other than 0 and itself, and if the Lie algebra is NON-ABELIAN. In particular the 1-dimensional Lie algebra is NOT usually considered to be simple. The definition of simple is sometimes modified slightly for Lie groups: a connected Lie group is called simple if its Lie algebra is simple. This corresponds to the Lie group being non-abelian having no normal subgroups other than itself and discrete subgroups of its center, so for example $SL_2(\mathbb{R})$ is considered to be a simple Lie group even though it is not simple as an abstract group.

Subgroups of Lie groups are closely related to subgroups of the Lie algebra. Informally, we can get a subalgebra by taking the tangent space of the subgroup, and can get a subgroup by taking the elements "generated" by the infinitesimal group elements of the Lie algebra. However it is rather tricky to make this rigorous, as the following examples show.

Example 28 The rational numbers and the integers are subgroups of the reals, but these do not correspond to subgroups of the Lie algebra of the reals. It is clear why not: the integers are not connected so cannot be detected by looking near the identity, and the rationals are not a closed subset.

This suggests that subalgebras should correspond to closed connected subgroups, but this fails for more subtle reasons:

Example 29 Consider the compact abelian group $G = \mathbb{R}^2/\mathbb{Z}^2$, a 2-dimensional torus. For any element (a, b) of its Lie algebra $\mathbb{R}^2$ we get a homomorphism of $\mathbb{R}$ to G, whose image is a subgroup. If the ratio a/b is rational we get a closed subgroup isomorphic to S^1 as the image. However if the ratio is irrational the image is a copy of $\mathbb{R}$ that is dense in G, and in particular is not a closed subgroup. You might think this problem has something to do with the fact that G is not simply connected, because it disappears if we replace G by its universal cover. However G is a subgroup of the simple connected group $SU(3)$ so we run into exactly the same problem even for simply connected compact groups.

In infinite dimensions the correspondence between subgroups and subalgebras is even more subtle, as the following examples show.

Example 30 Let us try to find a Lie algebra of the unitary group in infinite dimensions. One possible choice is the Lie algebra of bounded skew Hermitian operators. This is a perfectly good Lie algebra, but its elements do not correspond to all the 1-parameter subgroups of the unitary group. We recall from Hilbert space theory that 1-parameter subgroups of the unitary group correspond to unbounded skew Hermitian operators (typical example: translation on $L^2(\mathbb{R})$ corresponds to d/dx, which is not defined everywhere.) So if we define the Lie algebra like this, then 1-dimensional subgroups need not correspond to 1-dimensional subalgebras. So instead we might try to define the Lie algebra to be unbounded skew hermitian operators. But these are not even closed under addition, never mind the Lie bracket, because two such operators might have no non-zero vectors in their domains of definition.

Example 31 It is reasonable to regard the Lie algebra of smooth vector fields as something like the Lie algebra of diffeomorphisms of the manifold. However elements of this Lie algebra need not correspond to 1-parameter subgroups. To see what can go wrong, consider the vector field $x^2 d/dx$ on the real line. If we try to find the flow corresponding to this we have to solve $dx/dt = x^2$ with solution $x = x_0/(1 - x_0 t)$. However this blows up at finite time t. so we do not get a 1-parameter group of diffeomorphisms. A similar example is the vector field d/dx on the positive real line: it corresponds to translations, but translations are not diffeomorphisms of the positive line because we fall off the edge.

So in infinite dimensions 1-parameter subgroups need not correspond to 1-dimensional subalgebras of the Lie algebra, and 1-dimensional subalgebras need not correspond to 1-parameter subgroups.

3 The Poincaré-Birkhoff-Witt theorem

We defined the Lie algebra of a Lie group as the left-invariant normalized differential operators of order at most 1, and simply threw away the higher order operators. This turns out to lose no information, because we can reconstruct these higher order differential operators from the Lie algebra by taking the "universal enveloping algebra", which partly justifies the claim that the Lie algebra captures the Lie group locally.

The universal enveloping algebra Ug of a Lie algebra g is the associative algebra generated by the module g, with the relations $[A, B] = AB - BA$. A module over a Lie algebra g is a vector space together with a linear map f from g to operators on the space such that $f([a, b]) = f(a)f(b) - f(b)f(a)$.

Exercise 32 Show that modules over the algebra Ug are the same as modules over the Lie algebra g, and show that Ug is universal in the sense that any map from the Lie algebra to an associative algebra such that $[A, B] = AB - BA$ factors through it. (Category theorists would say that the universal enveloping algebra is a functor that is left adjoint to the functor taking an associative algebra to its underlying Lie algebra.)

The universal enveloping algebra of a Lie algebra can be thought of as the ring of all left invariant differential operators on the group (while the Lie algebra consists of the normalized ones of order at most 1). Actually this is only correct in characteristic 0: over fields of prime characteristic it breaks down because not all left invariant differential operators can be generated by left invariant vector fields. We can see this even in the case of the 1-dimensional abelian Lie algebra over the integers.

Exercise 33 Show that the space of translation-invariant differential operators on $Z[x]$ has a basis of elements $\frac{1}{n!}\frac{d^n}{dx^n}$

So these are definitely not generated by $\frac{d}{dx}$. If we reduce mod p we get similar problems over fields of characteristic p. This is really a sign that in characteristic $p > 0$ the Lie algebra is not the right object (and does NOT capture the Lie group locally): the correct replacement is the algebra of all left invariant differential operators, or something closely related such as a formal group.

We need some control over the size of the universal enveloping algebra. Suppose that g is a free module over a ring. It is easy to find a good upper bound on the size of Ug. We can filter Ug by $U_0 \subset U_1 \subset U_2 \cdots$ where U_n is spanned by monomials that are products of at most n elements of g.

Exercise 34 The associated graded ring $U_0 \oplus U_1/U_0 \oplus \cdots$ has the following properties: is is generated by U_1, and is commutative.

Commutativity follows using $AB - BA = [A, B]$. So this graded algebra is a quotient of the polynomial ring on g, which gives an upper bound on the size of Ug.

Theorem 35 *The Poincaré-Birkhoff-Witt theorem says that the map from the polynomial ring $S(g)$ to this graded algebra $G(Ug)$ of $U(g)$ is an isomorphism, in other words there is no further collapse.*

In particular the map from the Lie algebra to the UEA is injective, or in other words we can find faithful representations of the Lie algebra.

The universal enveloping algebra is given by "generators and relations", and when objects are given in this way it is usually easy to find upper bounds for the size of such objects by algebraic manipulation, but harder to show they do not collapse further. A good way to find a lower bound on the size is to find an explicit representation on something. Some cases of the PBW theorem are easy: for example, if our Lie algebra is known to be the Lie algebra of a Lie group, then the UEA should be differential operators, which come with a natural representation on smooth functions, or we can even restrict to formal power series expansions of smooth functions at the identity. There are enough such functions to see that the elements $g_1^{n_1} g_2^{n_2}...$ of the UEA are linearly independent as they have linearly independent actions on smooth functions.

If we want to prove the PBW theorem more generally we have to work harder: even over the reals it is not at all obvious that any Lie algebra is the Lie algebra of a Lie group. (At first sight this seems easy: all one has to do is find a faithful representation on a vector space, and exponentiate this to a group action. For abelian Lie algebras this is trivial, and at the opposite extreme when the algebra has no center it is also trivial as we can use the adjoint representation. Every Lie algebra can be obtained by starting with these two type and taking extensions, but it the trouble is that it is hard to show that one can find a faithful representation of an extension of two algebras with faithful representations.)

In general we have to build a suitable representation from the Lie algebra. We will do this by building something that "ought" to be Ug, and then defining an action of g on this by left multiplication and checking that it works.

Step 1: Construction of V. We choose a well-ordered basis of g and define V to have a basis of monomials that are formal products $abc...$ of elements of the basis with $a \le b \le c \le \cdots$. (There is an obvious map from V onto Ug; our aim is to prove that it is an isomorphism.)

Step 2: Construction of the action of g on V. Suppose a is a basis element of g and $bc\cdots$ is in V. We define $a(bc\cdots)$ to be $abc\cdots$ if $a \le b$, and $[ab](c\cdots) + b(a(c\cdots)$ if $a > b$. This is well defined by induction on the length of an element of V and by using the fact that the basis is well ordered.

Step 3. Check that this action of g on V satisfies $[a,b] = ab - ba$. This holds on $c\cdots$ whenever $b \le c$ by definition of the action, and similarly it holds whenever $a \le c$, so we can assume that both a and b are greater than c. We can also assume by induction that $[x,y](z) = x(y(z)) - y(x(z)$ for any elements x, y of the Lie algebra and any element z of V of length less than that of $c\cdots$. We calculate both sides of the identity we have to prove, pushing c to the left, as follows:

$$
\begin{aligned}
a(b(c\cdots)) &= a(c(b(\cdots)) + a([b,c](\cdots)) &(1)\\
&= c(a(b(\cdots))) + [a,c](b(\cdots) + [a,[b,c]](\cdots) + [b,c](a(\cdots)) &(2)
\end{aligned}
$$

and similarly

$$b(a(c\cdots)) = c(b(a(\cdots))) + [b,c](a(\cdots) + [b,[a,c]](\cdots) + [a,c](b(\cdots))$$

$$[a,b](c\cdots) = c([a,b](\cdots)) + [[a,b],c](\cdots)$$

Comparing everything we see that

$$a(b(c\cdots)) - b(a(c\cdots)) - [a,b](c\cdots)$$

is equal to

$$[[a,b],c](\cdots) + [[b,c],a](\cdots) + [[c,a],b](\cdots)$$

We finally use the Jacobi identity for g to see that this vanishes, thus showing that we indeed have an action of g on V.

This completes the proof of the PBW theorem.

The PBW theorem shows that we have found "all" identities satisfied by the Lie bracket, at least over fields, because any Lie algebra is a subalgebra of the Lie algebra of some associative algebra. For Jordan algebras the analogous result is not true. Jordan algebras are analogous to Lie algebras except that the Jordan product $a \circ b$ is $ab + ba$ rather than $ab - ba$. This satisfies identities $a \circ b = b \circ a$ and the Jordan identity. However these identities are not enough to force the Jordan algebra to be a subalgebra of the Jordan algebra of an associative ring: the Jordan algebras with this property are called special, and satisfy further independent identities (the smallest of which has degree 8). There is a 27-dimensional Jordan algebra (Hermitian matrices over the Cayley numbers) that is not special. Another example is Lie superalgebras: here we need the extra identity $[a,[a,a]] = 0$ for a odd in order to get a faithful representation in a ring.

The PBW theorem underlies the later calculations of characters of irreducible representations of Lie algebras. These representations can be written in terms of "Verma modules", an Verma modules in turn can be identified with the universal enveloping algebras of Lie algebras. The PBW theorem gives complete control over the "size" of the Verma module, in other words its character, which in turn leads to character formulas for the irreducible representations. A related application is the construction of exceptional simple Lie algebras (and Kac–Moody Lie algebras): the hard part of the construction is to show that these algebras are non-zero, which ultimately reduces to showing that certain universal enveloping algebras are non-zero.

The UEA of a Lie algebra is not just an associative algebra; it is also a Hopf algebra.

Definition 36 *A Hopf algebra is a group.*

In order to understand this, we need to explain what a group is. It is a set G with an associative product, identity, and inverse. However it also has further structure as follows. Given a group action on sets X, Y, there is an action on $X \times Y$ given by $g(x \times y) = g(x) \times g(y)$. This action is given by the diagonal map $g \mapsto g \times g$ from G to $G \times G$. Similarly there is an action of G on a 1-point set, induced by a map $g \mapsto *$ from G to a 1-point set. These extra maps are not usually mentioned in the definition of a group, because they are uniquely determined. There is a unique diagonal map from G to $G \times G$ so that the maps $G \mapsto G \times G \mapsto G$ are identities. So we have a coassociative coproduct map $G \mapsto G \times G$ and a counit $G \mapsto 1$ making G into a "cogroup", but this structure is boring because it is uniquely determined for any set. The reason it is unique is that we define the product of a group using the categorical product of sets. Similarly we can define groups in any category with products, and again the "coalgebra" structure is uniquely determined.

Now suppose that we have a category with some sort of product operation that is not the categorical product; for example, the tensor product of modules over a ring. If we copy the naive definition of a group, we get the concept of an associative algebra. However these do not behave like groups: for example, there is not natural action on tensor products of modules, corresponding to an action of a group on a product of sets. To get this we need to put in the "costructure" explicitly. In other words, we need a coassociative product with a counit, so that the coproduct is an automorphism of algebras. The inverse of a group gives an antipode on the Hopf algebra.

So we can defined groups/Hopf algebras in any symmetric monoidal category. In the category of sets, these are just the usual groups, while in the category of modules over a ring we get the usual Hopf algebras.

Example 37 If G is a group, then its group ring $R[G]$ over a commutative ring is a Hopf algebra, with the coproduct given by $g \mapsto g \otimes g$ and the counit given by $g \mapsto 1$.

We can ask if the group is determined by the group ring. The answer is "no" if the group ring is considered as an associative algebra: for example, the complex group ring of a finite abelian group is just a sum of copies of $\mathbb{C}$ corresponding to the irreducible representations, so two finite abelian groups have isomorphic group rings if and only if they have the same order. However the group can be recovered from the Hopf algebra as the group-like elements:

Definition 38 *An element of a Hopf algebra is called group-like if* $\Delta(a) = a \otimes a$ *and* $(a) = 1$.

Exercise 39 Show that the group-like elements of a Hopf algebra form a group. Show that the group-like elements of a group ring of G form a group that can be naturally identified with the group G. What is the group of group-like elements of the universal enveloping algebra of a Lie algebra?

The universal enveloping algebra is not the only analogue of the group ring for a Lie group. Another analogue, often used in analysis, is the algebra of continuous (or smooth) functions of compact support (or L^1 functions, or finite measures...) under convolution. For p-adic groups one can take the locally constant functions with compact support. These algebras look more like the group algebra of a finite group, but is less convenient in some ways as they need not have a coproduct.

Example 40 The main point of all this is that the UEA of a Lie algebra is a Hopf algebra. In other words it behaves as if it were a group or group ring, which is of course an approximation to the Lie group of the Lie algebra. The map from Ug to $Ug \otimes Ug$ is given by the Leibniz formula $g \mapsto 1 \otimes g + g \times 1$ from calculus. This is really just the formula telling you how to differentiate a product: $\frac{d}{dx}(fg) = \frac{d}{dx}(f)g + f\frac{d}{dx}(g)$, where we can see the map $\frac{d}{dx} \mapsto \frac{d}{dx} \otimes 1 + 1 \otimes \frac{d}{dx}$.

The fact that the map Δ extends to a ring homomorphism follows from the universal property of the UEA.

We would like to reconstruct the Lie algebra from its universal enveloping algebra in the same way we reconstructed a group from its group algebra.

Definition 41 *An element of a Hopf algebra is called primitive if it satisfies the Leibniz identity* $\Delta(a) = a \otimes 1 + 1 \otimes a$.

Exercise 42 Show that the primitive elements of a Hopf algebra form a Lie algebra.

A natural guess is that the Lie algebra consists of the primitive elements of the universal enveloping algebra. This fails over fields of positive characteristic p:

Exercise 43 If a is primitive in a Hopf algebra of prime characteristic $p > 0$, so is a^p. Find the Lie algebra of primitive elements of the universal enveloping algebra of a 1-dimensional Lie algebra over the finite field $\mathbb{F}_p$.

Sometimes in characteristic p one works with restricted Lie algebras: these are Lie algebras together with a ""p"th power operation" $a \mapsto a^[p]$ behaving like the p-th power of derivations.

Lemma 44 *Over a field of characteristic 0, an element of the UEA is primitive if and only if it is in the Lie algebra.*

Proof It is obvious that elements of the Lie algebra are primitive, so we need to show that primitive elements are in the Lie algebra. By the PBW theorem, the coalgebra structures on any two Lie algebras of the same dimension are isomorphic, so we can just the lemma for one Lie algebra of any dimension, say the abelian one.

Exercise 45 Show that over a field of characteristic 0, the dual of a polynomial ring generated by primitive elements is a ring of formal power series. Show that this is false in positive characteristic.

Primitive elements satisfy $\Delta(a) = 1\otimes a+a\times 1$, so $a(fg) = a(f)\eta(g)+\eta(f)a(g) = 0$ whenever f and g are power series with constant term 0 (in other words in the kernel of the counit η), so have to vanish on all decomposable elements, those that are products of two power series with constant term 0. The decomposable elements span all elements whose terms of degrees less than 2 vanish, so primitive elements have degree 1 and are therefore in the Lie algebra. □ The proof fails

in positive characteristic because the dual algebra of the coalgebra of a UEA is no longer a power series ring. If the coalgebra is $Z[D]$ then the dual algebra is $Z[\{x^i/i!\}]$, so reducing mod p we get an algebra generated by elements of degrees p^n each of which has p'th power 0. This is another indication that the UEA is the wrong object if we are not working over fields of char 0.

There is a second way to associate a Hopf algebra to a Lie group, which is in some sense dual to the UEA, which is to take the ring of polynomial functions on an (algebraic) Lie group. The UEA consists of (left invariant) differential operators and is cocommutative but not usually commutative, while the ring of (polynomial) functions is commutative but not usually cocommutative. It works as follows: suppose that G is an algebraic group contained in R^n. Then it has a coordinate ring $O(G) = R[x_1.\cdots,x_n]/(I)$ where the ideal I is the polynomials vanishing on R. The product map $G\times G \mapsto G$ induces a dual map $O(G)\mapsto O(G)\otimes O(G)$, and similarly the unit of G induces a map $O(G)\mapsto R$, so we have all the data for a commutative Hopf algebra.

Example 46 Suppose G is the general linear group $SL_2(R)$. Then the coordinate ring is $O(G) = R[a,b,c,d]/(ad - bc - 1)$. The coproduct is given by the group product:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$$

so $\Delta(a) = a\otimes a+b\otimes c$, $\Delta(b) = a\otimes b+b\otimes d$, $\Delta(c) = c\otimes a+d\otimes b$, $\Delta(d) = c\otimes b+d\otimes d$. The counit is given by $\eta(a) = 1$, $\eta(b) = 0$, $\eta(c) = 0$, $\eta(d) = 1$. The antipode is $S(a) = d$, $S(b) = -b$, $S(c) = -c$, $S(d) = a$.

Example 47 Following Quillen and Milnor, we will show that the Steenrod algebra in algebraic topology is a sort of infinite dimensional Lie group.

First recall the original definition of the Steenrod algebra. The Steenrod algebra is the algebra of stable cohomology operations mod 2, so can be found by calculating the cohomology of Eilenberg–Maclane spaces, which was originally done by H. Cartan and Serre. They showed that the Steenrod algebra is the algebra over F_2 generated by elements Sq^q for $q = 1,2,3\cdots$ modulo the Adem relations

$$Sq^iSq^j = \sum_{k=0}^{[i/2]} \binom{j-k-1}{i-2k} Sq^{i+j-k}Sq^k$$

which not even algebraic topologists are able to remember. Cartan also gave a formula for the action of Steenrod squares on a cup product

$$Sq^n(x\cup y) = \sum_{i+j=n} (Sq^ix)\cup(Sq^jy)$$

which we know should be interpreted as a coproduct on the Steenrod algebra

$$\Delta Sq^n = \sum_{i+j=n} Sq^i \otimes Sq^j$$

In other words the Steenrod algebra is a cocommutative Hopf algebra over the field with 2 elements. A cocommutative Hopf algebra should be thought of as something like a (universal enveloping algebra of a Lie) group, so should be related to the automorphisms of something. We will show that the Steenrod algebra is in some sense the automorphism group of the 1-dimensional additive group.

At first sight this makes no sense. The automorphism group of the additive Lie group R is just R^* which looks nothing like the Steenrod algebra. This is because we need to look more closely at this group, where by "more closely" we mean infinitesimally.

So first look at infinitesimal automorphisms of the real line fixing 0. These can be written as formal power series

$$x \mapsto a_0 x + a_1 x^2 + \cdots$$

with a_0 invertible. The product of this group is by composition of power series (which accounts for the funny grading of the coefficients). We can do this all over the integers Z. Then this group is represented by the ring $Z[a_0, a_0^{-1}, a_1, a_2, \ldots]$, which has a complicated coproduct map describing the group product.

Exercise 48 Find the image of a_0, a_1, and a_2 under the coproduct map.

To get the Steenrod algebra, we restrict to the subgroup of automorphisms of the line preserving the additive group structure, in other words we want the power series f with $f(x+y) = f(x) + f(y)$. The problem is that there are non (except for multiplication by constants). This is because we forgot to reduce mod p. If we work mod a prime p there are now plenty of additive homomorphisms, in particular the Frobenius map $x \mapsto x^p$ and its powers $x \mapsto x^{p^n}$. So the group of infinitesimal automorphisms of the additive group consists of the maps

$$x \mapsto a_0 x + a_{p-1} x^p + a_{p^2-1} x^{p^2} + \cdots$$

. (with a_0 invertible). So the coordinate ring of the corresponding group is $F_p[x_0, x_0^{-1}, a_{p-1}, a_{p^2-1}, \cdots]$. Now we need to find the coproduct on this corresponding to composition of functions. Suppose we have two group elements

$$x \mapsto f(x) = a_0 x + a_{p-1} x^p + a_{p^2-1} x^{p^2} + \cdots$$

and

$$x \mapsto g(x) = b_0 x + b_{p-1} x^p + b_{p^2-1} x^{p^2} + \cdots$$

. We want to calculate $f(g(x))$. This is given by

$$f(g(x)) = \sum a_{p^i-1} (\sum b_{p^j-1} x^{p^j})^{p^i} \quad (3)$$

$$= \sum a_{p^i-1} b_{p^j-1}^{p^i} x^{p^{i+j}} \quad (4)$$

so the coproduct is given by Milnor's formula

$$\Delta(a_{p^n-1}) = \sum_{i+j=n} a_{p^i-1} \otimes a_{p^j-1}^{p^i}.$$

or

$$\Delta(a_0) = a_0 \otimes a_0$$
$$\Delta(a_1) = a_0 \otimes a_1 + a_1 \otimes a_0^2$$
$$\Delta(a_3) = a_0 \otimes a_3 + a_1 \otimes a_1^2 + a_3 \otimes a_0^4$$
$$\Delta(a_7) = a_0 \otimes a_7 + a_1 \otimes a_3^2 + a_3 \otimes a_1^4 + a_7 \otimes a_0^8$$

We get the classical Steenrod algebra from this (for $p = 2$) by making 2 minor changes: we identify a_0 with 1, and (following Milnor) we take the graded dual (so that the Steenrod algebra is cocommutative rather than commutative). So, as Quillen pointed out, the mysterious Adem relations turn out to be a disguised form of the rule for composing two formal power series.

We can try to understand the structure of the Steenrod algebra by pretending that it is a Lie group. So we should ask if it is solvable/nilpotent/simple. It is graded by the non-negative integers, so it has an abelian degree 0 piece on the top, and then the rest of it is almost nilpotent: more precisely it is pro-nilpotent, a projective limit of nilpotent objects. So the Steenrod algebra itself should be thought of as a pro-solvable infinite dimensional Lie group. (The correct terminology is affine group scheme.) For any commutative R ring the group $S(R)$ has a decreasing filtration $S_0 \subset S_{p-1} \subseteq S_{p^2-1} \subseteq \cdots$, where S_{p^n-1} for $n > 0$ consists of the automorphisms $x \mapsto x + a_{p^n-1}x^{p^n} + \cdots$. So S_0/S_{p-1} is the multiplicative group of R, and $S_{p^n-1}/S_{p^{n+1}-1}$ is the additive group of R.

4 The exponential map

If A is a matrix, we can define $\exp(A)$ by the usual power series. We should check this converges: this follows if we define the norm of a matrix to be $\sup_{x\neq 0}(|Ax|)/|x|$. Then $|AB| \leq |A||B|$ and $|A+B| \leq |A|+|B|$ so the usual estimates show that the exponential series of a matrix converges. The exponential is a map from the Lie algebra $M_n(R)$ of the Lie group $GL_n(R)$ to $GL_n(R)$. (The same proof shows that the exponential map converges for bounded operators on a Banach space. The exponential map also exists for unbounded self-adjoint operators on a Hilbert space, but this is harder to prove and uses the spectral theorem.) The exponential map satisfies $\exp(A+B) = \exp(A)\exp(B)$ whenever A and B commute (same proof as for reals) but this does NOT usually hold if A and B do not commute. Another useful identity is $\det(\exp(A)) = \exp(\mathrm{trace}(A))$ (conjugate A to an upper triangular matrix).

To calculate the exponential of a matrix explicitly one can use the Lagrange interpolation formula as in the following exercises.

Exercise 49 Show that if the numbers λ_i are n distinct numbers, and B_i are numbers, then

$$B_1\frac{(A-\lambda_2)(A-\lambda_3)\cdots}{(\lambda_1-\lambda_2)(\lambda_1-\lambda_3)\cdots} + B_2\frac{(A-\lambda_1)(A-\lambda_3)\cdots}{(\lambda_2-\lambda_1)(\lambda_2-\lambda_3)\cdots} + \cdots$$

is a polynomial of degree less than n taking values B_i at λ_i.

Exercise 50 Show that if the matrix A has distinct eigenvalues λ_1,λ_2,... then $\exp(A)$ is given by

$$\exp(\lambda_1)\frac{(A-\lambda_2)(A-\lambda_3)\cdots}{(\lambda_1-\lambda_2)(\lambda_1-\lambda_3)\cdots}+\exp(\lambda_2)\frac{(A-\lambda_1)(A-\lambda_3)\cdots}{(\lambda_2-\lambda_1)(\lambda_2-\lambda_3)\cdots}+\cdots$$

(In this formula exp can be replaced by any holomorphic function.)

Exercise 51 Find $\exp\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The work can be reduced a little by writing the matrix as a sum of a multiple of the identity and a matrix of trace 0.

In particular for every element of the Lie algebra we get a 1-parameter subgroup $\exp(tA)$ of the Lie group. We look at some examples of 1-parameter subgroups.

Example 52 If A is nilpotent, then $\exp(tA)$ is a copy of the real line, and its elements consist of unipotent matrices. In this case the exponential series is just a polynomial, as is its inverse $\log(1+x)$, so the exponential map is an isomorphism between nilpotent matrices and unipotent ones.

Example 53 If the matrix A is semisimple with all eigenvalues real, then it can be diagonalized, and the image of the exponential map is a copy of the positive real numbers. In particular it is again injective.

Example 54 If the matrix A is $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (semisimple with imaginary eigenvalues) then the image of the exponential map is the circle group of rotations. In particular the exponential map is no longer injective.

Example 55 A 1-parameter subgroup need not have closed image: consider an irrational line in the torus $S^1 \times S^1$, considered as (say) diagonal matrices in $GL_2(\mathbb{C})$.)

In general a 1-parameter subgroup may combine features of all the examples above.

Exercise 56 Show that if A is in the Lie algebra of the orthogonal group (so $A + A^t = 0$) then $\exp(A)$ is in the orthogonal group.

One way to construct a Lie group from a Lie algebra is to fix a representation of the Lie algebra on a vector space V, and define the Lie group to be the group generated by the elements $\exp(a)$ for a in the Lie algebra. It is useful to do this over fields other than the real numbers; for example, we might want to do it over finite fields to construct the finite simple groups of Lie type. The problem is that the exponential series does not seem to make sense. We can get around this in two steps as follows. First of all, if we work over (say) the rational numbers, the exponential series still makes sense on nilpotent elements of the Lie algebra, as the series is then just a finite polynomial. The other problem is that the exponential series contains coefficients of $1/n!$, that make no sense if $n \le p$ for p the characteristic of the field. Chevalley solved this problem as follows. The elements $a^n/n!$ are elements of the universal enveloping algebra over the rationals. If we take the universal enveloping algebra over the integers and reduce it mod p we cannot then divide a^n by $n!$. However we can first do the division by $n!$ and then reduce mod p: in other words we take the subring of the universal enveloping algebra over the rationals generated by the elements $a^n/n!$ for a nilpotent, and then reduce this subring mod p. Then this has well defined exponential maps for nilpotent elements of the Lie algebra.

Another way to define exponentials without dividing by a prime p is to use the Artin-Hasse exponential

$$\exp\left(\frac{x}{1}+\frac{x^p}{p}+\frac{x^{p^2}}{p^2}+\cdots\right)$$

Exercise 57 Show that a formal power series $f(x) = 1 + \cdots$ with rational coefficients has coefficients with denominators prime to p if and only if $f(x^p)/f(x)^p \equiv 1 \bmod p$. Use this to show that the Artin-Hasse power series has coefficients with denominators prime to p.

Example 58 The exponential map need not be onto, even if the Lie group is connected. As an example, we will work out the image of the exponential map for the connected group $SL_2(R)$. The Lie algebra is the 2 by 2 matrices of trace 0, so the eigenvalues are of the form $\lambda, -\lambda$ for $\lambda > 0$, or $i\lambda, -i\lambda$ for $\lambda > 0$, or $0, 0$. In the first case $\exp(A)$ is diagonalizable with two positive distinct eigenvalue with product 1. In the second case A is diagonalizable with two eigenvalues of absolute value 1 and product 1. In the third case A is unipotent (both eigenvalues 1) but need not be diagonalizable. If we check through the conjugacy classes of $SL_2(R)$ we see that we are missing the following classes: matrices with two distinct negative eigenvalues (in other words trace less than -2), and non-diagonalizable matrices with both eigenvalues -1. So the image of the exponential map is not even dense (or open or closed): it omits all matrices of trace less than -2.

There is an alternative more abstract definition of the exponential map that goes roughly as follows. For any element a of the Lie algebra of a group G , we show that there is a unique 1-parameter subgroup $\mathbb{R} \mapsto G$ whose derivative at the origin is a. Then $\exp(a)$ is defined to be the value of this 1-parameter subgroup at 1. This definition has the advantage that it works for all Lie groups, and in particular shows that the exponential map does not depend on a choice of representation of the Lie group as a matrix group. The disadvantage is that one has to prove existence and uniqueness of 1-parameter subgroups, which are essentially geodesics for a suitable connection on G.

Theorem 59 *(Campbell-Baker-Hausdorff)*

$$\exp(A)\exp(B) = \exp(A + B + [A, B]/2 + \cdots)$$

where the exponent on the right is an infinite formal series in the free Lie algebra generated by formal variables A and B.

In particular this justifies the claim that Lie algebras capture the local structure of a Lie group, because we can define the product of the Lie group locally in terms of the Lie bracket. The convergence of the Campbell-Baker-Hausdorff formula is a bit subtle: it converges in some neighborhood of 0, and converges for nilpotent Lie algebras, but does not converge everywhere if the simply connected Lie group of the Lie algebra is not homeomorphic to a vector space. For example, if it converged everywhere for the group $SU(2)$ then we would find that R^3 can be given a group structure locally isomorphic to it, which is impossible as the universal cover is not R^3.

In general there is no exponential map from a Lie algebra to its UEA, but we can define one to its completion if the Lie algebra is graded with all pieces of positive degree. In this case the UEA is also graded so we can take its completion, and the exp and log maps are well defined on elements with constant terms 0 and 1 in this completion. We can define group-like elements in the completed UEA in the obvious way (but note that the map Δ has image in the completion of $Ug \otimes Ug$, which is larger than the tensor products of the completions). For nilpotent Lie algebras things are even better as the series are finite as elements of the Lie algebra are nilpotent, so we do not need to take completions.

Lemma 60 *exp is an isomorphism from primitive elements to group-like elements in the completion of the UEA, with inverse given by log*

Proof This is an easy calculation: for example, if a is primitive so that $\Delta(a) = 1 \otimes a + a \otimes 1$, then $\Delta(\exp(a)) = \exp(\Delta(a)) = \exp(1 \otimes a)\exp(a \otimes 1) = \exp(a) \otimes \exp(a)$. □

Proof (of the Baker-Campbell-Hausdorff formula) If we grade the free Lie algebra by giving A and B degree 1 then it is trivial that $\exp(A)\exp(B) = \exp(C)$ for some C in the completion of the UEA: we just take C to be $\log(\exp(A)\exp(B))$. The problem is to prove that C is in the completion of the Lie algebra, in other words can be written in terms of A and B using just the Lie bracket but not the product of the UEA. In other words we have to show that C is primitive. But this follows easily from the remarks above: A and B are primitive, so $\exp(A)$ and $\exp(B)$ are group-like, so their product $\exp(A)\exp(B)$ is also group-like, so the log of the product is primitive. □

One application of this formula is to prove Lie's rather hard theorem that there is a Lie group for every Lie algebra: roughly speaking the CBH formula allows us to define a sort of local chunk of the Lie group near the identity, and we can construct a global Lie group by carefully pasting such chunks together.

This does not quite give an explicit expression for $\exp(a)\exp(b)$; in fact there are many different explicit expressions, because there are many ways to write elements of the free Lie algebra. We will now use the Campbell-Baker-Hausdorff to find an explicit expression.

Dynkin gave an explicit formula for the Campbell-Baker-Hausdorff formula as follows. We can write

$$\log(e^x e^y) = \sum_{m>0} \frac{(-1)^m}{m} \left(\sum_{i+j>0} \frac{x^i}{i!} \frac{y^j}{j!} \right)$$

(remembering that x and y do not commute) which gives an explicit non-commuting power series, though not written in terms of the Lie bracket. However we know the right hand side is primitive by the Baker-Campbell-Hausdorff theorem, so if we apply any linear map Φ from the free associative algebra to the free Lie algebra on x, y that is the identity on primitive elements we will get an explicit expression for $\log(e^x e^y)$ in terms of the Lie bracket. One such linear map ϕ was found by Dynkin as follows. Put

$$\Phi(x_1 x_2 \cdots x_{n-1} x_n) = [x_1, [x_2, \ldots, [x_{n-1}, x_n] \cdots]]$$

if $n \geq 1$. Then by definition of Φ, if $\deg v > 0$ we have $\Phi(uv) = \theta(u)\Phi(v)$, where θ is the algebra homomorphism from the associative algebra to $\mathrm{End}(A)$ taking x_i to $[x_i, *]$ (so $\theta(u)v = [u, v]$ whenever u is primitive). Then $\Phi(u) = \deg(u)u$ for all primitive elements u. This follows by induction on the degree of u as $\Phi([u, v]) = \Phi(uv - vu) = \theta(u)\Phi(v) - \theta(v)\Phi(u) = \deg(v)[u, v] - \deg(u)[v, u] = \deg([u, v])[u, v]$.

So we define ϕ by $\phi(u) = \Phi(u)/\deg(u)$ if $\deg(u) > 0$, giving the desired retraction from the associative algebra to the Lie algebra.

Exercise 61 Work out the terms of Dynkins formula of degree up to 3. (Answer: $x + y + [x, y]/2 + [x, [x, y]]/12 + [y, [y, x]]/12$.)

5 Free things

The free monoid on n generators $a_1, \ldots a_n$ has elements $a_{i_1} a_{i_2}$ corresponding to all finite sequences $i_1, i_2, \ldots$ of $1, \ldots n$ in the obvious way. These elements form a basis of the free algebra on these generators (which is the monoid ring of the free monoid). In particular the free algebra, graded so that all generators have degree 1, and a degree m piece of dimension n^m.

Example 62 The free Lie algebra on n generators $a, b, c, \ldots$ is graded by giving all generators degree 1, and we can ask for the dimension of the piece of degree m; in other words how many independent expressions can we form using the Lie bracket $m - 1$ times. We can solve this using the PBW theorem. The point is that the UEA of a free Lie algebra is the free associative algebra on $a, b, c, \ldots$,whose piece of degree m has dimension n^m. By the PBW theorem the UEA is the "same size" as the polynomial algebra over the free Lie algebra. So if the free Lie algebra has k_m independent elements of degree m, then

$$\frac{1}{(1-t)^{k_1}} \frac{1}{(1-t^2)^{k_2}} \cdots = 1 + nt + n^2 t^2 + \cdots$$

(where the left is the Poincare series of the symmetric algebra of the UEA, and the right is the Poincare series of the free associative algebra). So this gives a recursive way to calculate the numbers k_m, especially if we take logs of both sides:

$$\sum_i k_i t^{ij}/j = \log(1/(1 - nt)) = \sum_i n^i t^i / i$$

The dimension $M(\alpha, n)$ of the degree n piece of the free Lie algebra on α generators is called a necklace polynomial, and by Moebius inversion is given by

$$M(\alpha, n) = \frac{1}{n} \sum_{d|n} \mu(n/d) \alpha^d$$

$$M(\alpha,1)=\alpha$$

$$M(\alpha,2)=\frac{\alpha^2-\alpha}{2}$$

$$M(\alpha,3)=\frac{\alpha^3-\alpha}{3}$$

$$M(\alpha,4)=\frac{\alpha^4-\alpha^2}{4}$$

Exercise 63 Show that the necklace polynomial $M(\alpha, n)$ counts the number of aperiodic necklaces with n beads of α colors. (Aperiodic means that the necklace cannot be obtained by repeating some smaller necklace. Necklaces are the same if one can be obtained by rotating another, but "flipping" is not allowed.) Show that if q is a prime power then $M(q, n)$ is the number of irreducible monic polynomials of degree n over the field of q elements. Show that

$$(1-\alpha z)=\prod_n (1-z^n)^{M(\alpha,n)}.$$

We can construct a totally ordered basis H for the free Lie algebra on a totally ordered set X using Hall sets as follows. The set H is the union of sets H_1, H_2, of degrees 1, 2, ...and if u has length less than v then $u < v$. The set H_1 is just X. The set H_2 is the elements $[u, v]$ with $u, v \in H_1, u < v$. The elements of length at least 3 are those of the form $[u[vw]]$ with $v \le u < [u, v]$ and $v < w$ and $u, v, w, [[vw]$ all in H. We choose any total ordering on H_n. We will not give a proof that this works as we do not use this result later.

Exercise 64 Find the sets H_1, H_2, H_3, H_4, H_5 for a free Lie algebra on 2 generators (for some choice of ordering in H_i).

A useful variation of the free monoid is the free group on generators $a, b, \ldots$, which is the same as the monoid on generators $a, A, b, B, \ldots$ with the relations $aA = Aa = 1$ and so on. We review some basic facts about free groups.

Lemma 65 *Each element of the free group has a unique representative given the product of a sequence of elements $a, A = a^{-1}, b, B = b^{-1}, \ldots$ such that no generator occurs next to its inverse. In other words, there are no "unexpected" relations between generators of a free group.*

Proof It is obvious that any element of the free group can be written in this form, and the problem is to show that this representative is unique. If $X = Y$ then $XY^{-1} = 1$, so this reduces to checking that non-empty representative is not the identity element. This is the usual problem for things given by generators and relations of showing that there is no unexpected collapse, and a good way to show this is to find explicit representations where given elements are obviously nontrivial. We will do this by constructing some explicit finite permutation representations.

Given a product $X = x_n \cdots x_2x_1 \cdots$ of $n > 0$ elements $a, A, b, B, \ldots$ with no generator next to its inverse we will construct an action of the free group on a finite set of $n+1$ points $1, 2, \ldots n+1$ such that X takes 1 to $n+1$. We first decree that $x_1(1) = 2$, $x_2(2) = 3$, and so on. We need to extend this to an action of each generator a on 1, 2, ..., $n+1$. But since a does not occur next to A in X, the conditions on a are consistent so we can extend the action of a to the whole of $1, \ldots, n+1$. So we get an action of the free group on $n+1$ points with X acting nontrivially, which shows that X is not the identity. □

In fact we have shown a little more: free groups are residually finite, meaning that for any nontrivial element we can find a finite index (normal) subgroup containing it. Another way of thinking about this is that elements can be detected by homomorphisms to finite groups. (In general if P is some property of groups, then "residually P" means that any two distinct elements of the group can be separated by a quotient group with property P.)

A useful way of thinking of free groups is that they are the fundamental groups of (connected) graphs with base points. Given such a graph we can obtain an independent set of generators for its free fundamental group by picking a maximal tree. The remaining edges then correspond to generators of the fundamental group as follows: given such an edge, start at the basepoint, travel along the tree to one end of the edge, go along the edge, then go back along the tree to the basepoint.

Lemma 66 *Any subgroup of a free group is free. More precisely, an index m subgroup of a free group on n generators is free on $m(n-1)+1$ generators.*

Proof Represent the free group as the fundamental group of a graph with n loops. Then a subgroup of index m is the fundamental group of the corresponding m-fold connected cover. Since this is also a tree, its fundamental group is also free.

To count the number of generators, observe that the number of generators of the fundamental group of a graph is $1-\chi$ where χ is the Euler characteristic (number of vertices minus number of edges). Since the Euler characteristic gets multiplied by m when we take an m-fold cover, this gives the number of generators of a subgroup. □

Exercise 67 Consider the action of the free group on 2 generators a, b on 3 points 1, 2, 3 such that a and b act as the transposition (12) and (13). Find a set of four generators for the free subgroup fixing 1. (Draw the graph with three vertices 1, 2, 3 and four edges giving the actions of a and b on the vertices, then pick a maximal tree (with 2 edges) then find the four generators by starting at 1, running along the tree, across and edge, and back along the tree.)

Exercise 68 How many subgroups of index 3 does the free group on 2 generators have? (The subgroups correspond to transitive actions on 3 points, one of which is marked.) How many triple covers does a figure 8 have?

Now we show that free Lie algebras and free Lie groups are closely related. This may be a little surprising, because these correspond to connected and discrete groups, which in some sense are opposite to each other. Given a free group F, we can form its descending central series $F_0 \supseteq F_1 \supseteq \cdots$, with $F_{i+1} = [F_i, F]$, the group generated by commutators.

If a group has a descending central series $G_0 \supset G_1 \cdots$ we can construct a graded Lie ring from it as follows. The Lie ring will be $G_0/G_1 \oplus G_1/G_2 \oplus \cdots$.

The additive structure of the ring is just given by the (abelian) group structure on each quotient. The Lie bracket is given by the commutator $[a, b] = a^{-1}b^{-1}ab$. The key point is to check that the Jacobi identity holds. This follows from Philip Hall's identity:

Exercise 69

$$[[x, y^{-1}], z]^y \cdot [[y, z^{-1}], x]^z \cdot [[z, x^{-1}], y]^x = 1$$

Exercise 70 Check that $G_0/G_1 \oplus G_1/G_2 \oplus \cdots$ is a Lie ring.

Theorem 71 *The Lie ring of the descending central series of the free Lie group on n generators is the free Lie ring on these generators.*

Proof First, there is an obvious homomorphism from the free Lie ring to the Lie ring of the free group, by the universal property of the free ring. To prove this is an isomorphism we want to construct a map in the other direction. We do this as follows.

We map each generator A of the free group to $\exp(a)$ in the rational completed universal enveloping algebra of the free Lie ring, where a is the generator of the free Lie ring corresponding to the generator A of the free group. This extends to a homomorphism f of groups by the universal property of a free group. If A is in F_n then $f(A)$ is of the form $1 + a_{n+1} + a_{n+2} + \cdots$ where a_i has degree i in the universal enveloping algebra. We define the image of A to be the element a_{n+1}. We can check that this is primitive (as the log of a group-like element is primitive) and integral, so an element of the free Lie algebra. We can also check that this preserves addition and the Lie bracket and so gives a Lie algebra homomorphism from the Lie ring of the free group. This gives the desired inverse map, so proves that the Lie ring of the free group is the free Lie algebra. □

Exercise 72 Show that free groups are residually nilpotent. Show that free Lie algebras are residually nilpotent.

So the relation between the free group and the free Lie algebra on some generators is given as follows. The Lie ring of the free group is the free Lie ring on the generators. The group generated by the elements $\exp(a)$, as a runs through generators for a free Lie ring, is the free group.

6 Nilpotent Lie groups

The main result about nilpotent Lie algebras is Engel's theorem, due to Friedrich Engel (not to be confused with the philosopher Friedrich Engels).

Theorem 73 *(Engel) Suppose that g is a Lie algebra of nilpotent endomorphisms of a non-zero finite dimensional vector space V. Then V has a nonzero vector fixed by g.*

Proof We use induction on the dimension of g. The main step is to show that g has an ideal h of codimension 1 (unless g is 0). So fix any proper nonzero subalgebra h of g. Then h acts on g by nilpotent endomorphisms, and so acts on the vector space g/h by nilpotent endomorphisms. By induction there is a nonzero element of g/h killed by h, so if h has codimension greater than 1 we can add this to h and repeat until h has codimension 1. In this case h is an ideal of g.

Now look at the subspace W of V fixed by all elements of h, which is nonzero by induction. This is acted on by the 1-dimensional Lie algebra g/h as h is an ideal, and as g/h acts by a nilpotent endomorphism of W there must be a non-trivial fixed vector. □

This theorem shows that if g is a Lie algebra of nilpotent endomorphisms of V, then there is a flag $0 = V_0 \subset V_1 \subset \cdots \subset V_n = V$ such that g acts trivially on each V_i/V_{i-1}. (Take V_1 to be the vectors fixed by g and apply induction to V/V_1). In other words V has a basis so that g is strictly upper triangular. Conversely any strictly upper triangular Lie algebra consists of nilpotent endomorphisms.

We would like to say that a Lie algebra is nilpotent if all elements are represented by nilpotent matrices, but there is a slight problem that this depends on the choice of representation: an 1-dimensional abelian Lie algebra can be represented by either a nilpotent or a non-nilpotent matrix. So instead we use the following definition:

Definition 74 *A Lie algebra g is called nilpotent if it has a central series $0 = g_0 \subset g_1 \subset \cdots \subset g_n = g$. This means that each g_i is an ideal, and g fixes all elements of g_i/g_{i-1} (or equivalently that g_i/g_{i-1} is in the center of g/g_{i-1}).*

There are two obvious ways to construct a central series of a group or Lie algebra: we can start at the bottom, and repeatedly quotient out by the center (g_i/g_{i-1} = center of g/g_{i-1}), or we can start at the top and repeatedly take commutators ($g_i = [g, g_{i+1}]$). The first method produces the "largest" central series and the second produces the "smallest". It is also possible to continue the upper and lower central series "transfinitely" but then they are no longer closely related: for example, for the free group or Lie algebra the descending central series becomes trivial after ω steps, but the ascending one never takes off as the center is trivial.

Exercise 75 Find an example of a nilpotent Lie algebra whose ascending and descending central series are not the same. (The smallest example is 4-dimensional.)

A reasonably typical example of a nilpotent Lie algebra is the Lie algebra of all strictly upper triangular matrices. A Lie algebra is nilpotent if and only if it is isomorphic to a Lie algebra of strictly upper triangular matrices. This follows immediately from Engel's theorem if we can show that it has a finite-dimensional faithful representation in which all elements act nilpotently. We will prove this later as a special case of Ado's theorem.

Similarly we define a group to be nilpotent if it has a central series. There is nothing obviously nilpotent in a nilpotent group: the terminology comes from Lie algebras.

Theorem 76 *For finite groups, the nilpotent ones are just the products of groups of prime power order.*

Proof First we show that any group of prime power order is nilpotent. The key step is to show that it has a nontrivial center (if it is nontrivial). For this, look at the partition into conjugacy classes. Each conjugacy class has order (order of G)/(order of subgroup fixing an element), so has order divisible by p if it is not in the center. If G is nontrivial it also has order divisible by p, so the number of elements in the center is divisible by p. So by repeatedly killing the center we see that G has a central series and is nilpotent.

It is trivial to see that a product of two nilpotent groups is nilpotent, so any finite product of groups of prime power order is nilpotent.

Conversely we want to show that if G is nilpotent then it is a product of its Sylow subgroups, or in other words all its Sylow subgroups are normal. If G is nontrivial then we can find an element of some prime order p in the center generating a subgroup H as G is nilpotent, and by induction G/H is a product of its Sylow subgroups. But if Q is a Sylow q-subgroup of G, then its image in G/H is the unique Sylow q-subgroup of G/H, whose inverse image in G is QH. But since H is in the center of QH there is only one Sylow q-subgroup of QH (either Q or QH depending on whether or not $p = q$) so it must be normalized by G. So all Sylow subgroups of G are normal, so G is a product of its Sylow subgroups. □

For any finite nilpotent group we can construct a finite Lie ring of the same order, as in the previous section. This does not seem to help all that much, as finite Lie rings seem just as messy as finite nilpotent groups.

The naive analogue of Engel's theorem fails for nilpotent groups: for example, the dihedral group of order 8 is nilpotent but has no fixed vectors in its 2-dimensional real representation. However there is an analogue that works: if a p-group acts on a non-zero finite dimensional vector space over a field with p elements then it fixes some vector The proof is similar to the proof that a non-trivial p group has a nontrivial center. There is also a similar analogue for algebraic groups: an algebraic group acting on a nonzero vector space whose elements are unipotent (all eigenvalues 1, or equivalently 1 plus nilpotent) fixes some vector, so is conjugate to a group of upper-triangular matrices with 1's on the diagonal.

There are huge numbers of p-groups of order p^n if n is reasonably large; in fact the number of groups of order less than some number is dominated by groups of order 2^n. In fact we can do this with just 2-step nilpotent groups. Fix two vector spaces V, W over a field (such as the field with p elements). If we are given a skew symmetric bilinear map $[,]$ from $V \times V$ to W then we can make $V \oplus W$ into a nilpotent group by letting the commutator of w_1, w_2 be the element $[w_1, w_2]$ of V. So the number of groups we get is about $p^{\dim(V)^2 \dim(W)/2}$. For groups of order p^n we have $\dim(V) + \dim(W) = n$, so the number of groups is maximized for $\dim(V) = n/3$, $\dim(W) = 2n/3$, and the number of groups is about $p^{2n^3/27}$. Of course we should divide out by groups that are isomorphic, but the number of choices we make is only $p^{\text{something quadratic in } n}$ so this is dominated by the cubic exponent of p and does not reduce the number of groups all that much. The number of groups of order 2^n is 1, 1, 2, 5, 14, 51, 267, 2328, 56092, 10494213, 49487365422, ..., and almost all groups of order less than some large integer are 2-group.

Exercise 77 Classify the groups of order 8. (The 3 abelian ones are obvious; the other two are the dihedral group and the quaternion group. One way to find the non-abelian ones is to start by observing that the center of a nonabelian group has order 2 and the quotient by the center is a Klein 4-group.)

Trying to classify nilpotent Lie algebras or nilpotent Lie groups of given dimension is just as bad: beyond dimension about 6 or so everything just gets horribly messy.

We saw earlier that in some sense Lie groups are commutative to first order. This suggests that maybe discrete subgroups generated by elements close to the identity will be commutative. This is not quite correct: for example, the group of unipotent upper triangular matrices has non-abelian subgroups generated by elements close to the identity. However Zassenhaus showed that it is essentially correct, except that "abelian" has to be replaced by "nilpotent", which is in some sense very close to "abelian".

Theorem 78 *(Zassenhaus) The identity of a Lie group has a neighborhood U with the following property: any discrete subgroup generated by elements of U is nilpotent.*

Proof The idea of the proof is that elements near the identity almost commute with each other. The commutator of two elements is second order. So if U is small enough then then sets $u_1 = U$, $U_2 = [U, U]$, $U_3 = [[U, U], U]$, will tend to 0 in the sense that they will eventually be in any given neighborhood. If a subgroup H of G is discrete this means that its intersection with U_n for n large is the identity element. If in addition H is generated by elements of U, this means that $[...[g_1, g_2], g_3, ...], g_n] = 1$ for any n elements in the generating set, which implies that H is nilpotent of step n. □

For nilpotent Lie algebras $\mathfrak{g}$ over fields of characteristic 0, the Campbell-Baker-Hausdorff formula converges as it only has a finite number of nonzero terms, so can be used to give $\mathfrak{g}$ a group structure. In particular, if G is a nilpotent Lie group then its universal covering space is a vector space and in particular is contractible. This fails completely for general Lie groups: for example the group S^3 is simply connected so has universal covering space a sphere.

We should at least mention Gromov's theorem that a finitely-generated group has polynomial growth if and only if it has a nilpotent subgroup of finite index.

7 Solvable Lie groups

Recall that a solvable group is one all of whose composition factors are abelian. The term comes from Galois theory, where a polynomial is solvable by radicals (and Artin–Schrier extensions in positive characteristic) if and only if its Galois group is solvable. For Lie groups the term solvable has the same meaning, and for Lie algebras it means the obvious variation: the Lie algebra is solvable if all composition factors are abelian Lie algebras.

The main goal of this section is to prove Lie's theorem that a complex solvable Lie algebra of matrices is conjugate to an algebra of upper triangular matrices.

Lie's theorem fails in positive characteristic, so in proving it we need to make use of some property of matrices that holds in characteristic 0 but not in positive characteristic. One such property is that if the trace of λI vanishes then so does λ; this is used in the following lemma.

Lemma 79 *Suppose that the Lie algebra G over a field of characteristic 0 has an ideal H and acts on the finite dimensional vector space V. Then G acts on each eigenspace of H.*

Proof Recall that an eigenvalue of H is given by some linear form λ on H, and the corresponding eigenspace consists of vectors v such that $h(v) = \lambda(h)v$ for all $h \in H$. Pick some eigenvector of H with eigenvalue λ, and pick some $g \in G$. We need to show that $g(v)$ also has eigenvalue λ. Look at the space W spanned by g, gv, g^2v,... which has an increasing filtration $0 = W_0 \subset W_1 \subset \cdots \subset W_n = W$ where W_i is spanned by W_{i-1} and $g^i v$. Then each W_i/W_{i-1} is at most 1-dimensional and is acted on by H with eigenvalue λ, because $[g,h]$ is in H. So on W, any element h of H has trace $n\lambda(h)$. In particular $[g,h]$ has trace $n\lambda([g,h])$, so $\lambda([g,h]) = 0$ because $[g,h]$ has trace 0 and n is invertible (this is where we use the characteristic 0 assumption). But $\lambda([g,h]) = 0$ implies that $hgv = ghv = g\lambda(h)v$, so gv is an eigenvalue of H with eigenvalue λ, which is what we were trying to prove. □

This lemma really does fail in infinite dimensions or in characteristic $p > 0$. For example, we can take the nilpotent Lie algebra spanned by the operators 1, x, d/dx which acts on $k[x]$. Then 1 is an eigenvalue of d/dx, but $x1$ is not. In characteristic p we can take the finite dimensional quotient $k[x]/(x^p)$. It is clear from the proof that it holds in characteristic $p > 0$ provided the vector space V has dimension less than p. this is quite a common phenomenon: results true in characteristic 0 are often true in characteristic $p > 0$ provided we stick to vector spaces of dimension less than p.

Theorem 80 *Lie's theorem. If a solvable Lie algebra G over an algebraically closed field of characteristic 0 acts on a non-zero finite-dimensional vector space, it has an eigenvector.*

Proof If G is nonzero, then as it is solvable we can find an ideal H of codimension 1. By induction on the dimension of G there is an eigenspace W of H for some eigenvalue of H. If g is any element of G not in H then by the previous lemma g acts on W, and as we are working over an algebraically closed field we can find some eigenvector of g on W. This is an eigenvector of G because G is spanned by g and H. □

By repeatedly applying this theorem, we see that the Lie algebra fixes a flag. So solvable Lie subalgebras of $M_n(C)$ are conjugate to subalgebras of the Lie algebra of upper triangular matrices.

Another way of stating Lie's theorem is that any irreducible representation of a finite-dimensional complex solvable Lie algebra is 1-dimensional. This does not mean that their representation theory is trivial. Non-abelian solvable complex Lie algebras have plenty of infinite dimensional irreducible representations. And even finite dimensional representations are hard to study, because there are plenty of indecomposable representations that are not irreducible. In fact, even for abelian Lie algebras of dimension 2, the finite dimensional indecomposable representations are very hard to classify. We will see later that the representation theory of simple Lie algebras is much easier, because we do not have this problem: all indecomposable representations are irreducible.

If we examine the proof, we see that Lie's theorem still holds in positive characteristic provided the dimension of the vector space is less than the characteristic.

Example 81 The solvable (in fact nilpotent) Lie algebra spanned by the operators 1, x, d/dx acts on $k[x]$, and has no eigenvectors. In characteristic p is acts on the finite dimensional quotient $k[x]/(x^p)$, but has no eigenvectors; in fact the action is irreducible. So Lie's theorem fails in characteristic $p > 0$ and in infinite dimensions.

Corollary 82 *The derived subalgebra of a finite dimensional solvable Lie algebra over a field of characteristic 0 is nilpotent.*

Proof We can extend the field to be algebraically closed. In this case the corollary follows from Lie's theorem, because the Lie algebra can be assume to be upper triangular, in which case its derived algebra consists of strictly upper triangular matrices and is therefore nilpotent. □

Although Lie's theorem fails in positive characteristic for Lie algebras, it still holds for solvable algebraic groups in any characteristic: this is Kolchin's theorem. (However it fails for solvable connected Lie groups: these are not necessarily isomorphic to groups of (upper triangular) matrices.) More generally still, Borel proved that any solvable algebraic group acting on a projective variety (over an algebraically closed field) has a fixed point. The special case when the projective variety is projective space is Kolchin's theorem.

Example 83 There are obvious analogues of Lie's theorems for connected solvable Lie groups of matrices. However for disconnected solvable groups the conclusions do not hold. For example, the symmetric group S_3 acting on its irreducible 2-dimensional representation has no eigenvectors. And the derived subgroup of a solvable finite group is usually not nilpotent: an example is the solvable symmetric group S_4 whose derived subgroup is the alternating group A_4.

Example 84 Lie's theorem shows that in some sense solvable connected Lie groups are not too far from nilpotent ones: they are given by sticking an abelian group on top of a nilpotent one. For (disconnected) finite groups, the solvable ones can be much more complicated than nilpotent ones. For example, a typical example of a smallish solvable group is $GL_2(\mathbb{F}_3)$ of order 48 with the chain of normal subgroups $1 \supset \mathbb{Z}/2\mathbb{Z} \subset Q_8 \subset SL_2(\mathbb{F}_3) \subset GL_2(F_3)$ with quotients of orders 2, 4, 3, 2. Larger finite solvable groups tend to be a similar but more complicated mess, and are rather hard to work with. The relatively easy structure of solvable connected groups is one of the reasons that connected Lie groups are easier to handle than finite groups.

Exercise 85 Which well-known group is $PGL_2(\mathbb{F}_3)$ isomorphic to?

Exercise 86 Over a field k of characteristic $p > 0$, show that the semidirect product of the 3-dimensional Lie algebra $\{1, x, d/dx\}$ by the p-dimensional abelian Lie algebra $k[x]/(x^p)$ is solvable, but its derived algebra is not nilpotent. This shows that the corollary above fails in positive characteristic.

Although in some ways solvable Lie algebras are not too far from nilpotent ones, their behavior can be much more complicated. For example, for any connected nilpotent Lie algebra, the exponential map to the simply connected group is an isomorphism (of sets). For example, we can use the BCH formula to define a Lie group structure on the Lie algebra.

Exercise 87 Show that if a a Lie group G has a connected central subgroup H, and the exponential map is surjective for G/H, then it is surjective for G. Deduce that the exponential map is surjective for connected nilpotent Lie groups.

It is very plausible that a similar result holds for solvable Lie algebras. For example, if a Lie algebra $\mathfrak{g}$ has a normal subalgebra $\mathfrak{h}$ such that the exponential maps take $\mathfrak{g}$ and $\mathfrak{h}$ onto their simply connected Lie groups then it seems almost obvious that the same is true for $\mathfrak{g}$, which would prove it for all solvable Lie algebras. Rather surprisingly, this is in fact sometimes false: the exponential map for a solvable Lie algebra need not map onto the simply connected group.

Example 88 Let $\mathfrak{g}$ be the Lie algebra of (orientation preserving) isometries of the Euclidean plane. If we identify the Euclidean plane with the complex numbers and rotations with multiplication by complex numbers of absolute value 1, then the group G can be thought of as the matrices $\left(\begin{smallmatrix} e^{it} & z \\ 0 & 1 \end{smallmatrix}\right)$ for t real and z complex. The Lie algebra consists of matrices of the form $\left(\begin{smallmatrix} it & z \\ 0 & 0 \end{smallmatrix}\right)$ and the exponential map takes this to $\left(\begin{smallmatrix} e^{it} & z(e^{it}-1)/(it) \\ 0 & 1 \end{smallmatrix}\right)$. (Recall the fast way to see this: exp of an $n \times n$ matrix is a polynomial of degree less than n in it.) Examining this we see that the exponential map is surjective, but not injective. This is easy to fix: we can make it injective by replacing the Lie group by its universal cover (the fundamental group is just $\mathbb{Z}$). So what is the problem? The problem is that the exponential map is surjective the group G, but is NOT surjective for the universal cover of G. To see this, notice that points of G of the form $\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right)$ are in the image of only 1 point under the exponential map. So only one of their inverse images in the universal cover can be in the image of the exponential map. So there is no group such that the exponential map of $\mathfrak{g}$ is an isomorphism: it fails to be either injective or surjective (or both, if we take a non-trivial finite cover).

This problem is closely related to the fact that the Lie algebra has elements with non-zero purely imaginary eigenvalues in the adjoint representation.

Exercise 89 Show that the universal cover of the group of orientation-preserving isometries of the plane can be represented faithfully as a group of 3 by 3 matrices.

$$\begin{pmatrix} e^{it} & 0 & z \\ 0 & 1 & t \\ 0 & 0 & 1 \end{pmatrix}$$

Use Kolchin's theorem that a solvable algebraic group can be diagonalized (over $\mathbb{C}$) to show that it cannot be represented faithfully as an algebraic group.

There are several other ways in which solvable Lie groups are fundamentally more complicated than nilpotent ones. We will see later that left-invariant Haar measures on nilpotent Lie groups are right-invariant, but this need not be true for solvable Lie groups. Also the representation theory of solvable Lie algebras can be a lot wilder than the representation theory of nilpotent ones, in the sense that von Neumann algebras not of type I can appear. A related fact is that the coadjoint orbit space (the space of orbits of the group on the dual of the Lie algebra) of a solvable Lie algebra can have unpleasant topological properties: it need not be T_0 for example.

8 Picard–Vessiot theory

One of Lie's motivations for studying Lie groups was to extend Galois theory to differential equations, by studying the symmetry groups of differential equations. We will give a very sketchy account of this, missing out most proofs (and for that matter most definitions).

The theorem in Galois theory that a polynomial in characteristic 0 is solvable by radicals if and only if its Galois group is solvable has an analogue for differential equations: roughly speaking, a differential equation is solvable by radicals, integration, and exponentiation if and only if its group of symmetries is a solvable algebraic group. This theory was initiated by Picard and Vessiot but it is sometimes hard to tell exactly what they proved as their definitions are somewhat vague. Kolchin gave a rigorous reformulation of their results using the theory of algebraic groups (which he created for this purpose). In particular one needs to distinguish between nilpotent and semisimple abelian groups (which look the same as Lie groups, but are quite different as algebraic groups). The correct analogue of nilpotent Lie algebras is not nilpotent groups but unipotent groups (those such that all eigenvalues of all elements are 1): for example, the group of diagonal matrices is nilpotent but not unipotent.

In this extension of Galois theory, one replaces fields by differential fields: fields with a derivation D. Just as adjoining a root of a polynomial equation to a field gives an extension of fields, adjoining a root of a differential equation to a field gives an extension of differential fields. As in Galois theory, one can form the differential Galois group of an extension $k \subset K$of differential fields as the group of automorphisms of the differential field K fixing all elements of k. Much of the theory of differential Galois groups is quite similar to usual Galois theory: for example, one gets a Galois correspondence between algebraic subgroups of the differential Galois group of an extension and sub differential fields.

Example 90 Suppose we adjoin a root of the equation $df/dx = p(x)$ to the field $k = \mathbb{Q}(x)$ of rational functions over $\mathbb{Q}$. This extension has a group of automorphisms given by the additive group of $\mathbb{Q}$, because we can change f to $f + c$ for some constant of integration c to get an automorphism.

Example 91 Suppose we adjoin a root of the equation $df/dx = p(x)f$ (with solution $\exp(\int p)$) to the field $k = \mathbb{Q}(x)$ of rational functions over $\mathbb{Q}$. This extension has a group of automorphisms given by the multiplicative group of $\mathbb{Q}$, because we can change f to cf for some nonzero constant c to get an automorphism.

The theory applies to homogeneous linear differential equations, so that the set of solutions is a finite-dimensional vector space acted on by the differential Galois group. Equations such as $df/dx = 1/x$ with solutions $\log x$ are not homogeneous so the theory does not apply directly to them, but we can easily turn them into homogeneous equations such as $(d/dx)x(d/df)f = 0$, at the expense of making the space of solutions 2-dimensional rather than 1-dimensional.

Exercise 92 Find the Lie group of automorphisms of the solutions of

$$(d/dx)x(d/df)f = 0$$

and describe its action on the space of solutions.

We will sketch the proof of one of the results of Picard-Vessiot theory, which says roughly that a linear homogeneous differential equation can be solved by radicals, exponentials, and integration if and only if its differential Galois group is solvable.

In one direction this follows by calculating the differential Galois group: each time we take radicals we get a finite cyclic group, each time we take an integral we get a differential Galois group isomorphic to the additive group, and each time we take an exponential we get a differential Galois group isomorphic to the multiplicative group. So by repeating such extensions we get a group built out of additive groups, which is solvable.

Conversely, suppose the differential Galois group is solvable. The quotient by the connected component is a finite solvable group, which corresponds to repeatedly taking radicals just as in ordinary Galois theory, so we can assume that the differential Galois group is connected and solvable. Now we apply Lie's theorem on solvable Lie algebras (or more precisely Kolchin's version of it for solvable algebraic groups) so see that the differential Galois group has an eigenvector f in the space of solutions of the differential equation. Also Df has the same eigenvalue as D commutes with the differential Galois group, so Df/f is fixed by the differential Galois group and so is in the base field. So f satisfies the differential equation $Df = af$ for some a, which can be solved by exponentials and integration.

Example 93 A typical application of differential Galois theory is that Bessel's equation $x^2d^2y/dx^2+xdy/dx+(x^2-\nu^2)y = 0$ cannot be solved using integration and elementary functions unless $\nu - 1/2$ is integral. Except for these special values, the differential Galois group is SL_2 which is not solvable. Finding the differential Galois group is rather too much of a digression, but we can at least get non-trivial upper and lower bounds for it as follows. First, we can show that it lies in SL_2 (rather than just GL_2) by using the Wronskian of the equation, given by $W = \begin{pmatrix} f & g \\ f' & g' \end{pmatrix}$ for two independent solutions f and g. The Wronskian get multiplied by the determinant of a matrix of the differential Galois group, so the elements of the differential Galois group have determinant 1 if and only if the Wronskian is in the base field.

Exercise 94 Show that the Wronskian of $d^2y/dx^2 + p(x)dy/dx + q(x)y = 0$ satisfies the differential equation $dW/dx + p(x)W = 0$. Use this to find the Wronskian of Bessel's equation, and deduce that the differential Galois group lies in the special linear group.

To find a lower bound for the differential Galois group, we observe that monodromy gives elements of this group. (Monodromy means go around a branch point.) Bessel's equation has a branch point at 0, and the two solutions $J_\nu = x^\nu \times$(something holomorphic) and $J_{-\nu} = x^{-\nu} \times \cdots$ for ν not an integer are multiplied by $e^{\pm 2\pi i\nu}$ by the monodromy, so the differential Galois group contains the diagonal matrix with these entries. When ν is an integer the monodromy is unipotent instead of semisimple: in this case the solutions are J_ν with trivial monodromy, and $Y_\nu =$ (something holomorphic)$+J_\nu\times$(something holomorphic)$\times$ log that has a logarithmic singularity and is changed by a multiple of J_ν by monodromy. So in this case the differential Galois group has a unipotent element of the form $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ generated by monodromy.

For proofs of most of the results discussed here, see Kolchin's papers on differential Galois theory.

9 Lie groups of dimension at most 3

We will find all (real, connected) Lie groups and Lie algebras of dimension at most 3.

Dimension 0: This is the hardest case, as it involves classifying all discrete groups, which is hopeless. Even if we restrict to compact simple groups, the 0-dimensional case is the classification of finite simple groups, which is about a thousand times longer than the classification of compact simple Lie groups of positive dimension. In general any Lie group has a normal closed subgroup consisting of the connected component of the identity, and the quotient is a discrete group. So we just give up on the discrete part, and from now on try to find the connected Lie groups of small dimension.

Dimension 1: The only 1-dimensional Lie algebra is the abelian one. The corresponding simply connected group is just the reals under addition. Other groups come by quotienting by a discrete subgroup of the center: up to equivalence, the only way to do this is to take R/Z. So there are just two 1-dimensional connected Lie groups: The reals and the circle group.

Dimension 2: First we find the Lie algebras. One possibility is that the algebra is abelian. Otherwise the derived algebra has dimension 1 (spanned by $[a, b]$ for any two independent vectors), so we take one element a of a basis to span the derived algebra. For any other vector we have $[a, b]$ is a multiple of a, so by multiplying b by a constant we can assume that $[a, b] = a$. So there is just one non-abelian Lie algebra.

The abelian groups correspond to quotients of R^2 by discrete subgroups (or lattices) in R^2. There are 3 possibilities: the lattice can have rank 0, 1, or 2, giving 3 groups R^2, $R^1 \times S^1$, and $S^1 \times S^1$ (the torus).

Exercise 95 Find the automorphism groups of the 3 connected 2-dimensional abelian Lie groups.

The non-abelian simply connected group is the $ax+b$ group that can be represented as the orientation preserving affine transformations of the real line of the form $x \mapsto ax+b$ for a positive. It also appears acting on the upper half plane by the same formula, and as 2 by 2 matrices of the form $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ with $a > 0$. The center is trivial, so this is the only non-abelian 2-dimensional Lie group. It is solvable but not nilpotent.

This group has analogues over finite fields that are semidirect products of the additive group of order q by the multiplicative group of order $q-1$. More generally, we can form the semidirect product of the additive group of order q by any subgroup of the multiplicative group, which can be a cyclic group of any order dividing $q-1$. These groups account for many of the small non-abelian finite groups.

Exercise 96 Show that any nonabelian group of order pq for $p < q$ primes is of this form: more precisely, there are no such groups unless p divides $q-1$, in which case there is a unique such group, given by a subgroup of the $ax+b$ group.

Dimension 3: This is where things start to get hairy. We find the connected groups by first finding the Lie algebras, and then finding the corresponding simply connected Lie group, and then finding the discrete subgroups of its center. The algebras were classified by Bianchi.

We first assume that G is solvable. We start by showing that G has a normal abelian subalgebra of dimension 2. It certainly has some normal subalgebra of dimension 2 (codimension 1) as G is not perfect. If this is not abelian then it must be the unique non-abelian Lie algebra of dimension 2, so G is a semidirect product of this by a 1-dimensional algebra acting on it. However this 2-dimensional non-abelian Lie algebra has no outer derivations, so the Lie algebra is just a product of the 2-dimensional non-abelian Lie algebra with a 1-dimensional Lie algebra, in which case it has a normal 2-dimensional abelian Lie algebra.

So we see that G can be given as follows: it has a normal 2-dimensional abelian subalgebra, and is a semidirect product by a 1-dimensional algebra acting on it by some transformation A. So G is determined by the 2 by 2 real matrix A. Changing A by conjugation or multiplying it by a non-zero constant does not change the isomorphism class of the Lie algebra. So to classify the solvable Lie algebra of dimension 3, we just have to run through all possible types of 2 by 2 matrices as follows.

- A is zero. The Lie algebra is abelian. (Bianchi type I). There are now 4 possibilities, all products of copies of the circle and the real line.

- A is nilpotent but not zero. The Lie algebra is the Heisenberg algebra (Bianchi type II), which can be represented as strictly upper triangular 3 by 3 matrices.

  The corresponding simply connected group is the group of unipotent upper triangular 3 by 3 matrices: the exponential map is a bijection because the exponential and logarithm maps are polynomials. The center of the simply connected group is R, and there is an outer automorphism that acts by rescaling the center, so there are two possible groups with this Lie algebra, one simple connected, and one with center S^1. The simply connected one can be represented as upper triangular unipotent matrices, and is the group associated with one of the 8 Thurston geometries (the nilmanifolds: take a quotient of the group by a discrete subgroup, such as the subgroup of matrices with integer coefficients). The other group can be represented as the group of transformations of $L^2(R)$ generated by translations and multiplication by e^{ixy}. These satisfy the Weyl commutation relations. The center is multiplication by constants of absolute value 1. This group has no faithful finite dimensional representations: in any finite dimensional representation the center must act trivially. One way to see this is to observe that any element of the center of a characteristic 0 Lie algebra in the derived algebra must act nilpotently in any finite dimensional representation (chop the representation up into generalized eigenspaces, and then look at the trace on any generalized eigenspace. The trace must be zero as the element is in the derived algebra, so the eigenvalue must be zero.) But the only way a nilpotent element can generate a compact group is if it acts trivially. There are several variations and generalizations of these groups. There is a Heisenberg group of dimension $2n+1$ for any positive integer n associated to a symplectic form of dimension $2n$. We can also define Heisenberg groups over finite fields in a similar way.

Exercise 97 Show that over a finite field of prime order p for p odd, every element of the Heisenberg group has order 1 or p, and the exponential map is a bijection. What happens over the field of order 2?

The universal enveloping algebra of the Heisenberg algebra becomes the ring of polynomials in x and d/dx if we take a quotient by identifying the center of the Heisenberg algebra with the real numbers. This gives a representation of the Lie algebra on the ring of polynomials, with the center acting as scalars. The center of this Lie algebra cannot make up its mind whether it is semisimple or nilpotent: in finite dimensional representations it acts nilpotently, but in the infinite dimensional representations we have described its acts semisimply.

- A is not nilpotent and not semisimple. Both eigenvalues must be the same, and we can normalize A so they are both 1. So we can assume A is $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. (Bianchi type IV)

  Exercise 98 Show that there is a unique connected Lie group with this Lie algebra, and represent it by 3 by 3 upper triangular matrices. Find the conjugacy classes of this group that are in the 2-dimensional derived subalgebra, and sketch a picture of them, paying careful attention to what happens near the origin (the answer may be slightly stranger than you expect).

- A is semisimple, nonzero, with one eigenvector zero. The Lie algebra is the product of the 1-dimensional abelian Lie algebra with the 2-dimensional non-abelian Lie algebra (Bianchi type III). There are two corresponding Lie groups.

- A is semisimple, nonzero, with real non-zero eigenvectors (Bianchi type VI if the eigenvalues are distinct, type V if they are the same). Here we get an uncountable infinite family of distinct Lie algebras, as we can change the smallest eigenvalue to anything we want, but then the second is determined. There is only one connected group for each of these Lie algebras. If the eigenvalues have sum 0 the Lie algebra has an extra symmetry (Bianchi type VI_0) This is the Lie algebra of isometries of 2-dimensional Minkowski space. This also appears as the group of one of the 8 Thurston geometries, giving the solv manifolds. For example one can take a quotient of this group by a cocompact discrete subgroup. Some of these manifolds are the mapping cylinder of an Anosov map of the 2-torus (given by an integral matrix A with distinct real nonzero eigenvectors whose product is 1).

  Exercise 99 Find an example of an Anosov map. Show how to construct a cocompact discrete subgroup of the Bianchi group VI_0 from any Anosov map.

  Exercise 100 Show that the outer automorphism group of this connected Lie group is dihedral of order 8. (Some elements correspond to time reversal, parity reversal, and changing the sign of the metric of Minkowski space.)

  When the eigenvalues are the same the group consists of translations and dilations of the plane.

- A is semisimple, nonzero, with non-real eigenvectors. Bianchi type VII. Again we get an infinite family of Lie algebras. The simply connected group has trivial center except for the following special case (Bianchi type VII_0): this is the one with imaginary eigenvalues, and is the Lie algebra of isometries of the plane. It has an extra symmetry. There is an obvious connected group with this Lie algebra: we can take orientation-preserving isometries of the plane. However this group is not simply connected, as it has homotopy type the circle, so we can also take its universal cover, or the cover of any order $1, 2, 3, \ldots$. We came across this group earlier as a solvable connected Lie group whose exponential map is not surjective.

  Exercise 101 Show that the real Lie algebras of type VI_0 and VII_0 are not isomorphic, but become isomorphic when tensored with the complex numbers.

The remaining cases are where G is not solvable, in which case it must be simple as all groups of smaller dimension are solvable. (Similarly the non-solvable finite group of smallest order is necessarily simple.) We will postpone the classification of these as this will be easier when we have developed more theory, and just state the result. There are 2 possible Lie algebras, $su(2)$ (Bianchi type IX) and $sl_2(R)$ (Bianchi type VIII). The first has simply connected group $SU(2)$ with center of order 2, so we get two possible Lie groups (one is $SO_3(R)$). For the other there are two obvious groups $SL_2(R)$ and the quotient by its center $PSL_2(R)$. However there are infinitely many other groups because $SL_2(R)$ is not simply connected: its fundamental group is Z so we can take its universal cover (which also has fundamental group Z) and quotient out by any subgroup of Z. These covers have no faithful finite dimensional representations. The double cover of $SL_2(Z)$ appears in the theory of modular forms of half-integral weight and it called the metaplectic group. It has a representation called he metaplectic representation that we will construct later in the course. The other covers of $PSL_2(R)$ do not seem to appear very often.

The two Lie algebras have the same complexification. This means that the corresponding real Lie algebras or groups are closely related: for example, the finite dimensional complex representation theory of $su(2)$ is essentially the same as that of $sl_2(\mathbb{R})$. However in some ways they are quite different: for example, the irreducible unitary representations of $SU(2)$ are all finite dimensional, while the non-trivial irreducible unitary representations of $SL_2(\mathbb{R})$ are all infinite dimensional.

Exercise 102 Show that the groups $SU(1,1)$, $SL_2(\mathbb{R})$, $Sp_2(\mathbb{R})$ (symplectic group), $SO_{1,2}(\mathbb{R})$ all have the same Lie algebra. Which of the groups are isomorphic?

Exercise 103 The 3-dimensional group of orientation-preserving isometries of 2-dimensional hyperbolic space is one of the groups above. Which one? (One way is to identify hyperbolic space with one of the components of norm 1 vectors in $\mathbb{R}^{1,2}$.)

Exercise 104 Identify the 3-dimensional group of Moebius transformations (invertible conformal transformations of the unit disk in the complex plane) with one of the groups on the list above.

Exercise 105 Show that $\mathbb{R}^3$ with the usual cross-product of vectors is a Lie algebra, and identify it with one of the Bianchi Lie algebras.

Exercise 106 Identify the 3-dimensional Lie algebras of matrices of the forms

$$\begin{pmatrix} 0 & 0 & 0 \\ a & b & c \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} c & 0 & c \\ a & 0 & b \\ 0 & 0 & c \end{pmatrix}$$

with Lie algebras on the list above.

Dimension 4: The classification can be (and has been) pushed beyond dimension 3, but becomes rather tiresome. The problem is that, as suggested by the 3-dimensional case, there are huge numbers of rather uninteresting solvable groups and Lie algebras, which just seem to form a complicated mess. In higher dimensions one just gives up on classifying the solvable ones. We will later prove Levi's theorem that any finite dimensional Lie algebra is a semidirect product of a solvable normal Lie algebra with a product of simple Lie algebras, and will classify the simple ones. So in some sense the finite dimensional Lie algebras can be classified modulo the solvable ones.

Exercise 107 Classify the complex Lie algebras of dimension at most 3. (The Bianchi algebras of types VIII and IX become isomorphic when tensored with the complex numbers.)

Thurston conjectured (and Perelman proved) that 3-manifolds can be cut up in a certain way into 3-manifolds with one of 8 geometries. Five of the eight Thurston geometries in 3 dimensions are the obvious ones: 3-dimensional flat, spherical or hyperbolic space, or the product of 2-dimensional spherical or hyperbolic space with a line. The remaining 3 are those modeled on the 3 groups mentioned above: the nilpotent one, the solvable one related to Minkowski space, and the universal cover of $SL_2(\mathbb{R})$. (Although most of the Thurston geometries can be modeled as left-invariant metrics on 3-dimensional groups this is not true for all of them: there is no 3-dimensional group structure on $S^2 \times \mathbb{R}$.)

10 Killing form and Cartan's criterion

At first sight one might guess that solvable groups are easier to classify than simple ones, and 0-dimensional compact simple groups are easier to classify than ones of higher dimension. This turns out to be completely wrong: the 0 dimensional compact simple groups are far harder to classify than the ones of positive dimension, and the solvable ones seem hopelessly complicated. What is the key reason why the positive dimensional simple Lie groups are so much easier to handle? One answer is Cartan's criterion, which implies that the Killing form on a simple complex Lie algebra (a symmetric invariant bilinear form) is non-degenerate.

We first figure out what it means for a bilinear form (,) on a representation V of a Lie algebra to be invariant. For a group G acting on V, invariance obviously means that $(gu, gv) = (u, v)$. For a Lie algebra, we formally replace g by $1+\epsilon a$ for some a in the Lie algebra (with $\epsilon^2 = 0$), to find that invariance means $(u, v)+\epsilon([a, u], v)+(u, [a, v]) = (u, v)$, or in other words $([a, u], v)+(u, [a, v]) = 0$.

If the Lie algebra G acts on a finite dimensional vector space V, we can define a bilinear form on G by $(a, b)_V = \mathrm{Trace}_V(ab)$.

Exercise 108 Show that this form is invariant, which means $([a, b], c)_V+(b, [a, c])_V = 0$.

A particularly important special case is where we take V to be the adjoint representation of G. In this case the invariant bilinear form on G is called the Killing form $(a, b) = \mathrm{Trace}(Ad(a)Ad(b))$.

Example 109 The Killing form on any abelian Lie algebra is obviously just zero. More generally, the Killing form on any nilpotent Lie algebra is identically zero, as we can put the matrices representing it into strictly upper triangular form, and the product of any two such matrices has trace 0. This does not mean that these algebras cannot have non-zero invariant bilinear forms; for example, any bilinear form on an abelian Lie algebra is invariant.

Exercise 110 Show that the kernel of an invariant symmetric bilinear form on a Lie algebra is an ideal. In particular if the Lie algebra is simple then the bilinear form is either zero or non-degenerate. Show that the orthogonal complement of an ideal is an ideal.

Exercise 111 Find the Killing form on the 2-dimensional non-abelian Lie algebra, and check that it is degenerate but not identically zero.

Exercise 112 Find the Killing form on the Lie algebra $su(2)$, and check that it is negative definite.

Exercise 113 Find the Killing form on the Lie algebra $sl_2(\mathbb{R})$, and check that it is non-degenerate and indefinite.

Exercise 114 If L is the complex Lie algebra spanned by W, X, Y, Z with relations $[X, Y] = Z, [W, X] = X, [W, Y] = -Y, Z \in$ center, find a non-degenerate invariant symmetric bilinear form on L. Show that the bilinear form associated to any finite-dimensional representation of L is degenerate (use Lie's theorem to put L in upper triangular form).

Theorem 115 *(Jordan decomposition) Suppose that a is a linear transformation of a vector space V over a perfect field k. Then there is a unique way to write $a = a_s + a_n$ where a_s is semisimple, a_n is nilpotent, and a_s and a_n commute.*

Proof We can assume k is algebraically closed, as uniqueness of the decomposition implies it is fixed by all elements of the absolute Galois group of k, and therefore in k as k is perfect.

For existence, write V as a direct sum of the generalized eigenspaces V_λ of a with eigenvalues λ. (Recall that v is a generalized eigenvector for eigenvalue λ if $(a - \lambda)^n v = 0$ for some positive integer n.) Then we just put $a_s = \lambda$ on V_λ, $a_n = a - a_s$ and it is easy to check that a_n and a_s have the required properties.

Uniqueness is left as an exercise. □

Exercise 116 (Jordan decomposition can fail over non-perfect fields) Suppose that V is the field $F_p(x)$ and k the subfield $F_p(x^p)$. Show that V is a vector space over k of dimension p, and multiplication by x is a linear transformation of V that cannot be written as the sum $x_s + x_n$ of commuting semisimple and nilpotent endomorphisms.

Exercise 117 (Multiplicative Jordan decomposition) Show that an invertible linear transformation a acting on a finite dimensional vector space over a perfect field can be written uniquely as $a = a_s a_u$ where a_s is semisimple and a_u is unipotent (all eigenvalues 1) and $a_s a_u = a_u a_s$.

Lemma 118 *Suppose that $M \subseteq gl(V)$ is the normalizer of a subspace G of $gl(V)$, for a complex vector space V. If a is in the kernel of the form $(,)_V$ on $M \times M$, then a is nilpotent.*

Proof The semisimple part a_s of a also lies in M because $Ad(a_s) = Ad(a)_s$. If b is in M and $Ad(c)$ is a polynomial in $Ad(b)$ then c is also in M.

Suppose that a has eigenvalues α_i. Suppose that ϕ is any additive (possibly not $\mathbb{R}$-linear) function from the rational vector space spanned by the α_i. The eigenvalues of $Ad(a)$ are $\alpha_i - \alpha_j$, so there is a polynomial p such that $p(\alpha_i - \alpha_j) = \phi(\alpha_i) - \phi(\alpha_j)$, as whenever two of the terms $\alpha_i - \alpha_j$ are equal, so are the corresponding terms $\phi(\alpha_i) - \phi(\alpha_j)$ by linearity of ϕ. So the element c with eigenvalues $\phi(\alpha_i)$ is in M because $Ad(c)$ has eigenvalues $\phi(\alpha_i) - \phi(\alpha_j)$ so is $p(Ad(a)$. But then $\sum \alpha_i \phi(\alpha_i) = (a, c) = \phi(0) = 0$. Taking ϕ to be complex conjugation shows that $\sum |\alpha_i|^2 = 0$, so all the α_i are zero. So $a_s = 0$ and a is nilpotent. □

A little more effort show that the same result holds over fields of characteristic 0, but we will not use or prove this.

Theorem 119 *Cartan's criterion for a faithful representation. Suppose that G is a subalgebra of $gl(V)$ with $(a, b)_V = 0$ for all $a, b \in G$, where V is a finite dimensional complex vector space. Then G is solvable.*

Proof Let M be the normalizer of G. Then $(m, [g_1, g_2]) = ([m, g_1], g_2) = 0$ for $g_i \in G$, so $(M, [G, G]) = 0$. By the previous lemma this implies that all elements of $[G, G]$ are nilpotent. Engel's theorem then implies that $[G, G]$ is nilpotent, so G is solvable.

□

Exercise 120 Suppose that G is a subalgebra of $gl(V)$ where V is a finite dimensional complex vector space. Show that G is solvable if and only if $(a, b)_V = 0$ for all $a, b \in [G, G]$, (Use Cartan's criterion above and Lie's theorem.)

Theorem 121 *Cartan's criterion for the Killing form. If G is a finite dimensional Lie algebra over a field of characteristic 0 whose Killing form is 0, then G is solvable.*

Proof We apply Cartan's criterion for the adjoint representation. There is a slight glitch because G need not act faithfully on the adjoint representation because its center acts trivially on G. However this is not a big deal, because we find that G/center is solvable, which immediately implies that G is also solvable. □

Cartan's criterion as stated above does not give a necessary and sufficient condition for a Lie algebra to be solvable, because the Killing form on a solvable Lie algebra need not be zero. It is often stated as the following variation, which does give a necessary and sufficient condition.

Exercise 122 Cartan's criterion, necessary and sufficient form. If G is a finite dimensional Lie algebra over a field of characteristic 0, then the following conditions are equivalent:

- G is solvable
- $(a, b) = 0$ if a is in $[G, G]$. In other words $[G, G]$ is in the kernel of the Killing form.
- $(a, b) = 0$ if a and b are both in $[G, G]$.

(For one implication use Lie's theorem, and for another use Cartan's criterion and the fact that if $[G, G]$ is solvable then so is G.

Example 123 A nilpotent Lie algebra has a Killing form that is identically zero. The converse is not true. Suppose that V is a finite dimensional vector space with and automorphism A, and we take the Lie algebra G that is a semidirect product of V with a 1-dimensional Lie algebra whose action on V is given by A. Then G is nilpotent if and only if A is a nilpotent endomorphism. The Killing form contains V in its kernel, so vanishes on $G \times G$ if $(A, A) = 0$. But $(A, A) = \mathrm{Trace}(A^2)$, so if we take A to be any endomorphism whose square has trace 0 but is not nilpotent we get a non-nilpotent Lie algebra whose Killing form vanishes.

Exercise 124 Find a non-nilpotent 2 by 2 real matrix A whose square has trace 0.

Exercise 125 Show that for the Lie algebra $gl_n(k)$ with e_i the matrix with just one non-zero entry, a 1 in position i on the diagonal, we have $(e_i, e_j) = 2n - 2$ if $i = j$ and -2 if $i \neq j$. Deduce that the Killing form on $sl_n(k)$ is $2n$ times the symmetric bilinear form associated to the standard representation, but the Killing form on $gl_n(\mathbb{R})$ is not a multiple of the form of the standard representation and has a non-trivial kernel.

Exercise 126 If k is a field of characteristic 2 then the semidirect product $gl_2(k).k^2$ is solvable. The Killing form is not identically zero on its derived algebra $sl_2(k).k^2$.

Exercise 127 Let G be the Lie algebra $sl_p(F_p)$ of 2 by 2 matrices over the field of p elements. Show that G is simple if $p > 2$. Show that the Killing form of G is identically 0. Show that $\mathrm{Trace}(AB)$ is a non-degenerate invariant bilinear form on G.

Exercise 128 Suppose G is the Lie algebra over a field of characteristic $p > 0$ with basis a_i for $i \in Z/pZ$ and bracket $[a_i, a_j] = (i - j)a_{i+j}$. Show that G is a simple Lie algebra but has no non-zero invariant bilinear form.

Lemma 129 *(Dieudonne) Suppose that a finite dimensional Lie algebra over any field of any characteristic has a non-degenerate bilinear form, and no abelian ideals. Then it is a direct sum of simple subalgebras.*

Proof Fix a minimal ideal M. The derived ideal $[M, M]$ is contained in M and cannot be 0 as M is non-abelian, so $M = [M, M]$ is perfect. The orthogonal complement N of M is also an ideal as the bilinear form is invariant. It cannot contain M as otherwise we would have $(x, m) = (x, \sum[a_i, b_i]) = \sum([x, a_i], b_i) = 0$ so M would be in the kernel of $(,)$ which is not possible. So $N \cap M = 0$ as it is a proper ideal of the minimal ideal M. So G splits as the direct sum of M and N, so M is simple, and continuing by induction so is N. □

Exercise 130 Show that if L is a Lie algebra with an invariant symmetric bilinear form $(,)$ then $L[t]/(t^n)$ has an invariant symmetric bilinear form given by the coefficient of t^{n-1} of the bilinear form on $L[t]/(t^n)$ with values that are truncated power series. If the form on L is non-degenerate show that the form on $L[t]/(t^n)$ is also non-degenerate. Find an example of a finite-dimensional complex Lie algebra with a non-degenerate symmetric bilinear form that is not a sum of abelian and simple Lie algebras.

Exercise 131 What is wrong with the following "proof" of the false result that a finite-dimensional complex Lie algebra L with a non-degenerate symmetric bilinear form is a sum of abelian and simple Lie algebras: take any ideal of L, and write L as the sum of the ideal and its orthogonal complement (which is also an ideal). By repeating this we can write L as a sum of ideals with no proper subideals, so L is a sum of abelian and simple Lie algebras.

Corollary 132 *(Cartan's criterion for semisimplicity) For a complex Lie algebra G the following conditions are equivalent:*

1. *G has no nonzero solvable ideals*
2. *G has no non-zero abelian ideals*
3. *G has non-degenerate Killing form*
4. *G is a direct sum of simple Lie algebras (in other words G is semisimple)*

Proof If the Killing form is degenerate, then its kernel is an ideal, and is solvable by one form of Cartan's criterion. So if the algebra has no nonzero solvable ideals then the Killing form is non-degenerate. Conversely if the Killing form is nondegenerate and A is an abelian ideal, then for any $a \in A$ and $g \in G$, $Ad(a)Ad(g)$ has square 0 so has trace 0 and therefore $a = 0$ as the Killing form is non-degenerate. So all Abelian ideals are 0,and therefore all solvable ideals are 0.

We have seen that if the Killing form is non-degenerate then there are no abelian ideals, so if the Killing form is non-degenerate then by the previous lemma the Lie algebra is a sum of simple Lie algebras.

If the algebra is a sum of simple subalgebras, it is obvious that it has no nonzero solvable ideals.

□

11 Cartan subalgebras, Cartan subgroups and maximal tori

The Lie algebra gl_n has a subalgebra H of diagonal matrices, and under the action of this subalgebra gl_n splits as the sum of eigenspaces. The zero eigenspace is just H, while the other eigenspaces just correspond to the off-diagonal entries of gl_n. The subalgebra H is an example of a Cartan subalgebra, and we want to find a similar subalgebra for any Lie algebra. The first guess is to take a maximal abelian subalgebra, but this does not work: the algebra of matrices of block form $\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}$ is abelian but does not act nicely on the rest of the Lie algebra (and has dimension much larger than that of the diagonal matrices).

Definition 133 *A toral subalgebra of a Lie algebra is an abelian subalgebra that acts semisimply on the adjoint representation.*

Definition 134 *A Cartan of a Lie algebra is a self-centralizing nilpotent subalgebra. (Self-centralizing means that it contains its centralizer.)*

For semisimple Lie algebras, maximal toral subalgebras and Cartan subalgebras will turn out to be the same. In general it is really the maximal toral subalgebras that are important. It seems to be a historical accident that Cartan subalgebras have this rather unintuitive definition. The properties of being nilpotent or self normalizing are not really that important or easy to use. The really important property is the semisimplicity, which means that one can decompose the (complex) Lie algebra into eigenspaces.

Exercise 135 Find maximal toral subalgebras for the algebra of all matrices, the algebra of upper triangular matrices, and the algebra of strictly upper triangular matrices (0's on the diagonal).

Theorem 136 *The centralizer of a toral subalgebra of G is a Cartan subalgebra is self normalizing.*

Proof

Take any abelian subalgebra H of the Lie algebra G, and decompose G into a direct sum of generalized eigenspace of H (acting on G by the adjoint representation). The eigenvalues are elements of the dual of H. If G_λ is the generalized eigenspace for some eigenvalue λ, then $[G_\lambda, G_\mu] \subseteq G_{\lambda+\mu}$. In particular G_0 is a self-normalizing subalgebra of G containing H. If in addition all elements of H are semisimple, then H lies in the center of G_0 as generalized eigenvectors (with eigenvalue 0) are honest eigenvectors. □

For semisimple Lie algebras we will later see that a maximal toral subalgebra is its own normalizer (so is a Cartan subalgebra). In general this is not true:

Exercise 137 Show that a subalgebra of a nilpotent Lie algebra is toral if and only if it is contained in the center. So the center is the unique maximal toral subalgebra, and its normalizer is the whole algebra.

This exercise is a bit misleading. There is a subtle problem in that the definition of a maximal toral subgroup of an algebraic group does not quite correspond to maximal toral subalgebras of the Lie algebra. This is because a toral subgroup of an algebraic group has elements that are semisimple. In (say) the group of unipotent upper triangular matrices, the only semisimple element is 1, so the maximal toral subgroup is trivial. However the maximal toral subalgebra of its Lie algebra is the center which is not trivial. This is related to the fact that it is ambiguous whether elements of the center of a Lie algebra or group should be thought of as semisimple or unipotent/nilpotent. For example, in the Heisenberg algebra, the center looks nilpotent in finite dimensional (algebraic) representations, but looks semisimple in its standard infinite dimensional representation. The Heisenberg algebra is trying hard to be semisimple in some sense; in fact it can be thought of as a sort of degeneration of a semisimple algebra. For semisimple lie algebras or groups this problem does not arise: "maximal toral" means the same whether one defines it algebraically or analytically.

Exercise 138 Show that $sl_2(R)$ has two maximal toral subalgebras that are not conjugate under any automorphism. (Take one to correspond to diagonal matrices, and the other to correspond to a compact group of rotations.)

Theorem 139 *If a finite dimensional complex Lie algebra is semisimple, then the normalizers of the maximal toral subalgebras are abelian*

Proof Suppose H is a maximal toral subalgebra, and G_0 its normalizer, so that G_0 is nilpotent. Since G_0 is solvable it can be put into upper triangular form, so the Killing form restricted to G_0 has $[G_0, G_0]$ in its kernel. On the other hand, any invariant bilinear form vanishes on (u, v) if u and v have eigenvalues that do not sum to 0, so G_0 is orthogonal to all other eigenspaces of H. So $[G_0, G_0]$ is in the kernel of the Killing form. By Cartan's criterion, this implies that it vanishes, so G_0 is abelian. □

Remark 140 There is an analogue of Cartan subgroups for finite groups. A subgroup of a finite group is called a Carter subgroup (not a misprint: these are named after Roger Carter) if it is nilpotent and self-normalizing. Any solvable finite group contains Carter subgroups, and any two Carter subgroups of a finite group are conjugate. However anyone with plans to classify the finite simple groups by copying the use of Cartan subgroups in the classification of simple Lie groups should take note of the following exercise:

Exercise 141 Show that the simple group A_5 of order 60 does not have any Carter subgroups.

The analogues of Cartan subgroups for compact Lie groups are maximal tori. In fact these are the subgroups associated to Cartan subalgebras of the Lie algebra. Every element of a compact connected Lie group is contained in a maximal torus, and the maximal tori are all conjugate.

Warning 142 In a compact connected Lie group, maximal tori are maximal abelian subgroups, but the converse is false in general: maximal abelian subgroups of a compact connected Lie group are not necessarily maximal tori. This is a common mistake. In particular, although every element is contained in a torus, it need not be true that every abelian subgroup is contained in a torus.

Exercise 143 Show that the subgroup of diagonal matrices of $SO_n(\mathbb{R})$ for $n \geq 3$ is a maximal abelian subgroup but is not contained in any torus.

12 Unitary and general linear groups

The fundamental example of a Lie group is the general linear group $GL_n(\mathbb{R})$. There are several closely related variations of this:

- The complex general linear group $GL_n(\mathbb{C})$
- The unitary group U_n
- The special linear groups or special unitary groups, where one restricts to matrices of determinant 1

- The projective linear groups, where one quotients out by the center (diagonal matrices)

Exercise 144 Show that the complex Lie algebras $gl_n(\mathbb{R}) \otimes \mathbb{C}$, $gl_n(\mathbb{C})$, and $u_n(\mathbb{R}) \otimes \mathbb{C}$ are all isomorphic. We say that $gl_n(\mathbb{R})$ and $u_n(\mathbb{R})$ are real forms of $gl_n(\mathbb{C})$.

The general linear group has a rather obvious representation on n-dimensional space. Therefore it also acts on the 1-dimensional subspaces of this, in other words $n-1$-dimensional projective space. The center acts trivially, so we get an action of the projective general linear group $PGL_n(\mathbb{R})$ on P^{n-1}. There is nothing special about 1-dimensional subspaces: the general linear group also acts on the Grassmannian $G(m, n-m)$ of m-dimensional subspaces of $\mathbb{R}^n$. The subgroup fixing one such subspace is the subgroup of block matrices $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$, so the Grassmannian is a quotient of these two group.

Exercise 145 Show that the Grassmannian is compact. (This also follows from the Iwasawa decomposition below).

More generally still, we can let the general linear group act on the flag manifolds, consisting of chains of subspaces $0 \subset V_1 \subset V_2 \cdots$, where the subspaces have given dimensions. The extreme case is when V_i has dimension i, in which case the subgroup fixing a flag is the Borel subgroup of upper triangular matrices. In general the subgroups fixing flags are called parabolic subgroups; the corresponding quotient spaces are projective varieties.

The Iwasawa decomposition for the general linear group is $G = GL_n(\mathbb{R}) = KAN$ where $K = O_n(\mathbb{R})$ is a maximal compact subgroup, A is the abelian subgroup of diagonal matrices with positive coefficients, and N is the unipotent subgroup of unipotent upper triangular matrices. For the general linear group, the Iwasawa decomposition is essentially the same as the Gram-Schmidt process for turning a base into an orthonormal base. This works as follows. Pick any base $a_1, a_2, \ldots$ of R^n; this is more or less equivalent to picking an an element of the general linear group. Now we can make the base orthogonal by adding a linear combination of a_1 to a_2, then adding a linear combination of a_1, a_2 to a_3, and so on. This operation corresponds to multiplying the base by an element N of the unipotent upper triangular matrices. Next we can make the elements of the base have norm 1 by multiplying them by positive reals. This corresponds to acting on the base by an element of the subgroup A of diagonal matrices with positive entries. We end up with an orthonormal base, that corresponds to an element of the orthogonal group.

Exercise 146 Show that $GL_n(\mathbb{R})$ is homeomorphic as a topological space to $K \times A \times N$ and deduce that it has the same homotopy type as the orthogonal group. Show that $GL_3(\mathbb{R})$ has a fundamental group of order 2. (The corresponding simply connected group is not algebraic.)

Exercise 147 Show that the average of any positive definite inner product on $\mathbb{R}^n$ under a compact subgroup of $GL_n(\mathbb{R})$ is invariant under the compact subgroup. Deduce that the maximal compact subgroups of $GL_n(\mathbb{R})$ are exactly the subgroups conjugate to the orthogonal group. (A similar statement is true for all semisimple Lie groups: the maximal compact subgroups are all conjugate.)

Exercise 148 Show that $GL_n(\mathbb{C}) = KAN$ where K is the unitary group, A is the positive diagonal matrices, and N is the upper triangular complex unipotent matrices. Show that $SL_n(\mathbb{C})$ has a similar decomposition with K the special unitary group. Show that $SL_2(\mathbb{C})$ has the same homotopy type as a 3-sphere.

Exercise 149 Show that the unitary group acts transitively on the full flag manifold of $\mathbb{C}^n$. What is the subgroup of the unitary group fixing a full flag?

The diagonal matrices of $GL_n(\mathbb{R})$ form a Cartan subgroup.

Exercise 150 Find two non-isomorphic Cartan subgroups of $GL_2(\mathbb{R})$.

We recall that a root space is an eigenspace for a non-zero eigenvalue of a Cartan subalgebra. For the general linear group the root spaces just correspond to the off-diagonal matrix entries. If α_i is the value of the ith diagonal element of a matrix, then the roots of $GL_n(\mathbb{R})$ are the linear forms $\alpha_i - \alpha_j$ for $i \neq j$. For example the roots system of $GL_2(\mathbb{R})$ is two opposite points, the roots system of $GL_3(\mathbb{R})$ is a hexagon, and the root system of $GL_4(\mathbb{R})$ is the centers of the edges of a cube. These root systems are very symmetric, and are acted on by S_2, S_3, and S_4. This can be seen by identifying the symmetric groups with the permutation matrices, that normalize the diagonal matrices and therefore act on the root systems. In general the Weyl group is a quotient N/H where H is a Cartan subalgebra and N is a group normalizing it; for the general linear group the group H is the diagonal matrices, the group N is the monomial matrices, and the Weyl group is the symmetric group.

Warning 151 For the general linear group the Weyl group is a subgroup, but this is not always true; in general the Weyl group is only a subquotient. For example, for the group $SL_2(\mathbb{R})$, the Weyl group has order 2 and acts on the diagonal matrices by inversion, but $SL_2(\mathbb{R})$ has no element of order 2 acting in this way (though it does have such an element of order 4).

Exercise 152 Show that the Lie algebra $sl_n(\mathbb{R})$ is simple for $n \geq 2$. (Show that any ideal must contain an eigenvalue of the Cartan subalgebra, then show that a non-zero element of a root space leads to a non-zero element of the Cartan subalgebra, and show that elements of the Cartan subalgebra with 2 distinct entries lead to elements of root spaces. By repeating these operations show that the ideal generated by any non-zero eigenvector is the whole Lie algebra.)

Exercise 153 If k is a field of characteristic p dividing n, show that the Lie algebra $sl_n(k)$ is not simple. Where does the proof in the previous exercise break down? Show that the center is 1-dimensional and the quotient $psl_n(k)$ by the center is simple unless $p = n = 2$.

Exercise 154 Most of the time, one expects an algebraic group over some field to be simple or solvable if and only if the corresponding Lie algebra has the same property. However there are exceptions to this: show that

- The group $PSL_2(\mathbb{F}_2)$ is solvable, and the Lie algebra $psl_2(\mathbb{F}_2)$ is solvable.
- The group $PSL_2(\mathbb{F}_3)$ is solvable, and the Lie algebra $psl_2(\mathbb{F}_3)$ is simple.

- The group $PSL_2(\mathbb{F}_4)$ is simple, and the Lie algebra $psl_2(\mathbb{F}_4)$ is solvable.
- The group $PSL_2(\mathbb{F}_5)$ is simple, and the Lie algebra $psl_2(\mathbb{F}_5)$ is simple.

Exercise 155 Show that the general linear group has the Bruhat decomposition $GL_n(\mathbb{R}) = \uplus_w BwB$ as a disjoint union of double cosets of B, where the union is over the $n!$ elements w of the Weyl group, and B is the Borel subgroup of upper triangular matrices. (If g is an element of $GL_n(\mathbb{R})$, pick the first nonzero entry in the bottom row and multiply on the left and right by elements of B to clear out its row and column. Then pick the first nonzero element on the next to last row, and carry on like this to get a permutation matrix.)

Exercise 156 Show that the Bruhat decomposition induces a decomposition of the full flag manifold G/B is the disjoint union of $n!$ affine spaces of various dimensions. For GL_3 show that these dimensions are 0, 1, 1, 2, 2, 3. Use this to calculate the cohomology groups with compact support of the space of full flags of C^3 if you know what this means.

Example 157 We can calculate the number of elements of $GL_n(\mathbb{F}_q)$ as follows. It is equal to the number of bases of $\mathbb{F}_q^n$, which is just $(q^n - 1)(q^n - q)\cdots(q^n - q^{n-1})$. This is fast but does not generalize in any obvious way to other finite simple groups. A more complicated way to work out the order that does generalize to all other finite groups of Lie type is to use the Bruhat decomposition. For $G = GL_n(\mathbb{F}_q)$, the order is $|G/B||B|$ where B is the Borel subgroup of upper triangular matrices, that has order $(q-1)^n q^{1+2+\cdots+(n-1}$, and G/B is the full flag variety. We can work out the number of points in this by using the Bruhat decomposition to decompose it into a union of $n!$ affine spaces of various dimensions. For example, for GL_3 the affine spaces have dimensions 0, 1, 1, 2, 2, 3, so the flag variety has order $q^0 + q^1 + q^1 + q^2 + q^2 + q^3$. In general these exponents are the lengths of the elements of the symmetric group (or Weyl group) as words in the $n-1$ generators (12), (23), (34), ... (these are not all transposition, but only the “simple” ones exchanging two adjacent numbers).

From these two examples one can see that there is some sort of relation between the compactly generated cohomology of $GL_n(\mathbb{C})$ and the number of points of $GL_n(\mathbb{F}_q)$. This is a special case of the Weil conjectures, which say in particular that the number of points of a variety over a finite field can be expressed in terms of the compactly supported etale cohomology groups, which in turn have the same dimensions as the compactly supported cohomology groups of the corresponding complex variety. In the case of varieties such as flag manifolds or Grassmannians that can be written as a (set theoretic) finite disjoint union of affine spaces the Weil conjectures are trivial to check explicitly, as they just reduce to the case of affine space.

For a semisimple Lie group one can ask what are its “natural” actions on mathematical objects; of course this is a rather vague question. We have seen one answer above: the general linear group acts naturally on projective spaces, Grassmannians, and flag manifolds. These are quotients by parabolic subgroups. Another class of objects acted on by semisimple Lie groups are the symmetric spaces. Symmetric spaces are generalizations of spherical and hyperbolic geometry. Their definition looks a little strange at first: they are connected Riemannian manifolds such that at each point there is an automorphism acting as -1 on the tangent space. Obvious examples are Euclidean space (curvature 0), spheres (positive curvature) and hyperbolic space (negative curvature), and in general symmetric spaces should be thought of as generalizations of these three fundamental geometries. (They account for many of the "natural" geometries but not for all of them: for example, 5 or the 8 Thurston geometries in 3 dimensions are symmetric spaces, but 3 of them are not.) We may as well assume that they are simply connected (by taking a universal cover) and irreducible (not the products of things of smaller dimension). These were classified by Cartan. The first major division is into those of positive, zero, or negative curvature. The only example of zero curvature is the real line. Cartan showed that irreducible simply connected symmetric spaces of negative curvature correspond to the non-compact simple Lie groups: the symmetric space is just the Lie group modulo its maximal compact subgroup. He also showed that the ones of positive curvature correspond to the ones of negative curvature by a duality extending the duality between spherical and hyperbolic geometry. We will look at some examples of symmetric spaces related to general linear groups.

We first examine the symmetric space of the general linear group $GL_n(\mathbb{R})$ (which is neither semisimple nor simply connected, but never mind). We saw above that the maximal compact subgroup is the orthogonal group. The symmetric space $GL_n(\mathbb{R})/O_n(\mathbb{R})$ is the space of all positive definite symmetric bilinear forms on R^n. This is an open convex cone in $R^{n(n+1)/2}$, and is an example of a homogeneous cone. (In dimensions 3 and above it is quite rare for open convex cones to be homogeneous). A minor variation is to replace the general linear group by the special linear group, when the symmetric space becomes positive definite symmetric bilinear forms of discriminant 1.

Exercise 158 Find a similar description of the symmetric space of $GL_n(\mathbb{C})$.

Let us look at the case $n = 2$ in more detail. In this case the space $SL_2(\mathbb{R})/SO_2(\mathbb{R})$ can be identified with the upper half plane, as $SL_2(\mathbb{R})$ acts on this by $z \mapsto (az + b)/(cz + d)$ and $SO_2(\mathbb{R})$ is the subgroup fixing i. This symmetric space has a complex structure preserved by the group, so is called a Hermitian symmetric space. This means that we can construct lots of Riemann surfaces by taking the quotient of the upper half plane by a Fuchsian group (a discrete subgroup of $SL_2(\mathbb{R})$, such as $SL_2\mathbb{Z})$). In fact any Riemann surface of negative Euler characteristic can be constructed like this: this gives all of them except for the Riemann sphere with at most 2 points removed or an elliptic curve. The symmetric spaces of other real general linear or special linear groups do not have complex structures; one reason $SL_2(\mathbb{R})$ does is that $SL_2(\mathbb{R})$ happens to be $Sp_2(\mathbb{R})$, and we will see later that $Sp_{2n}(\mathbb{R})$ has a Hermitian symmetric space. We can spot plausible candidates for Hermitian symmetric spaces as follows: for a Hermitian symmetric space, we can fix some point x and act on its tangent space by multiplying by complex numbers of absolute value 1. This gives a subgroup in the center of the subgroup K fixing x isomorphic to the circle group. This shows that we should look out for Hermitian symmetric space structures whenever the maximal compact subgroup has an S^1 factor.

The upper half plane is also a model of the hyperbolic plane. This does not generalize to $SL_n(\mathbb{R})$ either: the group $PSL_2(\mathbb{R})$ happens to be isomorphic to $PSO^+{}_{1,2}(\mathbb{R})$, and it is the groups $O_{1,n}$ rather than SL_n that correspond to hyperbolic spaces, as we will see when we discuss orthogonal group later on.

Exercise 159 Polar coordinates for symmetric spaces: Show that $GL_n(\mathbb{R}) = KAK$ where $K = O_n(\mathbb{R})$ is the maximal compact subgroup and A is the group of positive diagonal matrices. Show that the element of A in this decomposition need not be uniquely determined, but is uniquely determined up to conjugation by an element of the Weyl group. Find a geometric interpretation of the entries of A in terms of the image of the unit ball under an element of $GL_n(\mathbb{R})$.

The Cartan decomposition of the Lie algebra $g = sl_n(\mathbb{R})$ is $g = k + p$, where k is the subalgebra of orthogonal matrices, and p is the orthogonal complement of k under the Killing form, so is the subspace of symmetric matrices of trace 0. Warning:p is not a subalgebra! There are the $+1$ and -1 eigenspaces of the Cartan involution θ.

Exercise 160 Show that the exponential map is an isomorphism from p to its image P in G, and can be identified with the symmetric space of G. In particular this shows that the symmetric space is contractible. For the special linear group this is easy to see directly by identifying the symmetric space with positive definite symmetric forms of determinant 1, but the argument using the exponential map works for all semisimple Lie groups.

Now we look at the symmetric space of $SL_2(\mathbb{C})$. This turns out slightly surprisingly to be 3-dimensional hyperbolic space. This means that one can construct lots of hyperbolic 3-manifolds and orbifolds by taking a Kleinian group (a discrete subgroup of $SL_2(\mathbb{C})$, such as $SL_2(\mathbb{Z}[i])$, and taking the quotient of hyperbolic space by this subgroup. To see that its symmetric space is 3-dimensional hyperbolic space we first construct a homomorphism from $SL_2(\mathbb{C})$ to $O_{1,3}(\mathbb{R})$ as follows. The group $SL_2(\mathbb{C})$ acts on the space of hermitian matrices x by $g(x) = gx\overline{g}^t$ and preserves the determinant of x. However the determinant on 2 by 2 hermitian matrices is a quadratic form of signature $(1,3)$ so we get a homomorphism from $SL_2(\mathbb{C})$ to $O_{1,3}(\mathbb{R})$. Now the group $O_{1,3}(\mathbb{R})$ acts on the norm 1 vectors of $R^{1,3}$, which form two components, each isometric to 3-dimensional hyperbolic space. The subgroup of $O_{1,3}(\mathbb{R})$ fixing a point of hyperbolic space is a maximal compact subgroup $O_1(\mathbb{R}) \times O_3(\mathbb{R})$.

The group $O_{1,3}(\mathbb{R})$ is the Lorentz group of special relativity, and the local isomorphism with $SL_2(\mathbb{C})$ is used a lot: for example the 2-dimensional representation of $SL_2(\mathbb{C})$ and its complex conjugate are essentially the half-spin representations of a double cover of $SO_{1,3}(\mathbb{R})$. In special relativity the symmetric space appears as the possible values of the momentum of a massive particle.

(Notice by the way that whether a symmetric space has a complex structure has little to do with whether its group has one: the symmetric space of $SL_2(\mathbb{R})$ has a complex structure, but that of $SL_2(\mathbb{C})$ does not.)

There are several other symmetric spaces related to the general linear group. Recall that the group $GL_n(\mathbb{R})$ is not the only real form of $GL_n(\mathbb{C})$; the group $U_n(\mathbb{R})$ of elements preserving the Hermitian form $z_1\overline{z_1} + \cdots$. is also a real form. There is no particular reason why we should restrict to positive definite Hermitian forms: we can also form the group $U_{m,n}(\mathbb{R})$ fixing a Hermitian form on $\mathbb{C}^{m+n}$ of signature (m,n). A maximal compact subgroup of this is $U(m) \times U(n)$. Even if we restrict to elements of determinant 1 this still has an S^1 factor, at least at the Lie algebra level, so we expect the corresponding symmetric spaces to have complex structures.

Exercise 161 Show directly that the symmetric space of $U_{m,n}(\mathbb{R})$ is hermitian, by identifying it with the open subspace of the Grassmannian $G_{m,n}(\mathbb{C})$ consisting of the m-dimensional subspaces on which the Hermitian form is positive definite.

Exercise 162 Show that the symmetric space of $U_{1,n}(\mathbb{R})$ can be identified with the unit ball in $\mathbb{C}^n$ as follows: an element of the Grassmannian represented by the point $z_0, z_1, \ldots, z_n$ is mapped to the point $(z_1/z_0, \ldots, z_n/z_0)$ of the open unit ball in C^n. Show that for $n = 1$ this is essentially the group of Moebius transformations acting on the unit disk of the complex plane.

In particular the open unit ball in $\mathbb{C}^n$ is a bounded homogeneous domain: a bounded open subset of complex affine space such that its group of automorphisms acts transitively. (It is not quite trivial to see that there are any examples of these: the group of affine transformations of $\mathbb{C}^n$ does not act transitively on points of a bounded homogeneous domain!) In 1-dimension the Riemann mapping theorem implies that any simply connected bounded open subset of the complex plane is homogeneous, but in higher dimensions homogeneous domains are quite rare. The non-compact Hermitian symmetric spaces give examples, and for several decades it was an open problem to find any others. This was finally solved by Piatetski-Shapiro in 1959, who found an example of a 4-dimensional homogeneous bounded domain that was not a Hermitian symmetric space.

So far we have seen lots of examples of noncompact symmetric spaces, constructed as G/K where K is a maximal compact subgroup of G. This construction just gives the trivial 1-point space for G compact, so we need a different way of constructing compact symmetric spaces, such as spheres. Cartan discovered a duality between compact and non-compact irreducible symmetric spaces: roughly speaking, for each non-compact symmetric space there is a corresponding compact on (ignoring minor problems about abelian factors and connectedness). A well known special case of this is the duality between spherical and hyperbolic geometry (or even the duality between trigonometric functions and hyperbolic ones). This duality works as follows. Pick a non-compact symmetric space and look at the Cartan decomposition $k+p$ of its Lie algebra. Now change this to the Lie algebra $k+ip \subset g\otimes\mathbb{C}$. Cartan showed that this is the Lie algebra of a compact group, and the quotient of this group by the subgroup K is the dual compact symmetric space. Let us find the dual compact symmetric spaces of some of the symmetric spaces above.

Example 163 The symmetric space of $GL_n(\mathbb{R})$ is $GL_n(\mathbb{R})/O_n(\mathbb{R})$. To find the compact dual, we first look at the Cartan decomposition $gl_n(\mathbb{R}) = k + p$, where k is the Lie algebra of skew symmetric matrices, and p is the space of symmetric matrices. Then we form the Lie algebra $k + ip$. This is the Lie algebra of skew Hermitian matrices, so its Lie group is the unitary group. So the symmetric space should be $U(n)/O_n(\mathbb{R})$. This is the set of real forms on C^n that are compatible with the Hermitian metric (in other words complex conjugation is an isometry).

Example 164 The symmetric space of $U_{m,n}(\mathbb{R})$ is $U_{m,n}(\mathbb{R})/U(m) \times U(n)$. Changing $U_{m,n}(\mathbb{R})$ to its compact form gives $U(m+n)$. So the compact form of the symmetric space is $U(m+n)/U(m)\times U(n)$, in other words the Grassmannian $G_{m,n}(\mathbb{C})$.

Exercise 165 Show that the compact symmetric space dual to the symmetric space of $GL_n(\mathbb{C})$ (the positive definite Hermitian forms) is the unitary group U_n. (Similarly all simply connected compact groups are symmetric spaces, and are the duals of the symmetric spaces of complex Lie groups.)

We can also consider infinite dimensional unitary groups. There are two obvious ways to define the infinite dimensional unitary group: we can either take the union $U(1) \subset U(2) \subset \cdots$, or we can take the group of all unitary automorphisms of an infinite dimensional Hilbert space. It is somewhat surprising (at least to me) that these two groups re quite different. For example, the group of all unitary operators is contractible, while the union of the finite dimensional unitary groups has a complicated topology: its cohomology ring has generators of degrees 1, 3, 5, ... and its odd-dimensional homotopy groups are all $\mathbb{Z}$ by Bott periodicity. For example, if one wants to use the classifying space of the infinite-dimensional unitary group in K-theory, one needs to be careful to use the correct version of this group.

Exercise 166 Show that the union of the finite dimensional unitary groups has a determinant homomorphism onto the circle group, while the group of all unitary operators is perfect.

12.1 Noncommutative determinants

We would like to define an analogue of the special linear group over the quaternions. The general linear group $GL_n(\mathbb{H})$ over the quaternions does not have a determinant map to $\mathbb{H}$, but has one to $\mathbb{R}$. More generally the general linear group over any division algebra D has a determinant map to the abelianization of D^*, called the Dieudonne determinant. This can be constructed as follows.

Take any matrix in $GL_n(D)$ and look at the first column.

$$\begin{pmatrix} \lambda_1 & \cdots \\ \lambda_2 & \cdots \end{pmatrix}$$

Pick some row whose first element λ^i is nonzero. Then make other entries of the first column zero by subtracting multiples of row i from it. Then defined the determinant to be $(-1)^{i-1}\lambda_i$ times the determinant of the matrix formed by eliminating the first column and row i.

We claim that this is a well defined homomorphism to the abelianization $D^*/[D^*, D^*]$.

The key point is to prove that this is a well defined element, in other words independent of which row we pick. To simplify notation, we will just do this for rows 1 and 2, so suppose λ_1 and λ_2 are both nonzero. Then calculating the determinant using these two rows gives the two answers

$$\lambda_1 \times \det \begin{pmatrix} \mathrm{row2} - \lambda_2\lambda_1^{-1}\mathrm{row1} \\ \mathrm{row3} - \lambda_3\lambda_1^{-1}\mathrm{row1} \\ \vdots \end{pmatrix}$$

and

$$\lambda_1 \times \det \begin{pmatrix} \text{row1} - \lambda_1\lambda_2^{-1}\text{row2} \\ \text{row3} - \lambda_3\lambda_2^{-1}\text{row2} \\ \vdots \end{pmatrix}$$

The first matrix can be transformed into the second by multiplying the first row by $-\lambda_1\lambda_2^{-1}$ then subtracting multiples of the first row from the others. So by induction their determinants differ by a factor of $-\lambda_1\lambda_2^{-1}$. This implies that we get the same answer whether we use the first or the second row.

It is now easy to check that the determinant is invariant under elementary row operators, and is multiplied by λ if a row is multiplied by λ. Since these operations generate $GL_n(D)$ the determinant is multiplicative.

Warning 167 The Dieudonne determinant of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is not in general given by $ad - bc$ (this is Cayley's definition of the determinant for non-commutative rings). For example, $\left(\begin{smallmatrix} i & 1 \\ k & j \end{smallmatrix}\right)$ is invertible, but $ij - k1 = 0$. The correct formula (for a invertible) is $ad - aca^{-1}b$.

Exercise 168 If T is an $n \times n$ quaternionic matrix, it can be interpreted as a $4n \times 4n$ real matrix. Show that its determinant as a real matrix is the 4th power of the Dieudonne determinant. How are these related to the Study determinant, defined by regarding T as a $2n \times 2n$ complex matrix?

13 Orthogonal groups

Orthogonal groups are the groups preserving a non-degenerate quadratic form on a vector space. Over the complex numbers there is essentially only one such form on a finite dimensional vector space, so we get the complex orthogonal groups $O_n(\mathbb{C})$ of complex dimension $n(n-1)/2$, whose Lie algebra is the skew symmetric matrices. Over the real numbers there are several different forms. By Sylvester's law of inertia the real nondegenerate quadratic forms are determined by their dimension and signature, so we get groups $O_{m,n}(\mathbb{R})$ preserving the form $x_1^2 + \cdots x_m^2 - x_{m+1}^2 - \cdots - x + m + n^2$. If the form is positive definite the corresponding group is compact. We have the usual variations: special orthogonal groups SO of elements of determinant 1, and projective orthogonal groups where we quotient out by the center ± 1. There are also orthogonal groups over other fields and rings corresponding to quadratic forms, whose classification over the rationals or number fields or the integers is a central part of number theory. For example, the Leech lattice Λ is a 24-dimensional quadratic form over the integers, and the corresponding orthogonal group $O_\Lambda(\mathbb{Z})$ is a double cover of the largest Conway sporadic simple group.

We first look at a few small cases.

Dimension 0 and 1 there is not much to say: the orthogonal groups have orders 1 and 2. They are counterexamples to a surprisingly large number of published theorems whose authors forgot to exclude these cases.

Dimension 2: The special orthogonal group $SO_2(\mathbb{R})$ is the circle group S^1 and is isomorphic to the complex numbers of absolute value 1. To make things more interesting we will look at it over the rationals, in other words looks at the group $SO_2(\mathbb{Q})$. The elements of this group can be identified with Pythagorean triangles: integer solutions of $x^2 + y^2 = z^2$ with no common factor and $z > 0$ (corresponding to the point $x/z, y/z) \in SO_2(\mathbb{Q})$).

Exercise 169 Show that the points can be parametrized by $t \in \mathbb{Q} \sup \infty$ by drawing the line through $(-1, 0)$ and $(x/z, y/z)$ and taking the intersection $(1, t)$ of this with the line $(1, *)$. What is the rational number t corresponding to $3^2 + 4^2 = 5^2$? Find the Pythagorean triangle corresponding to the square of the group element corresponding to the $(3, 4, 5)$ triangle.

Exercise 170 Show that under the action of $SO_2(\mathbb{C})$, the space C^2 splits as the sum of two 1-dimensional representations. What well-known group is $SO_2(\mathbb{C})$ isomorphic to, and what are the two corresponding 1-dimensional representations of this group?

Dimension 3: We have a compact group $O_3(\mathbb{R})$, a complex group $O_3(\mathbb{C})$, and another group $O_{2,1}(\mathbb{R})$ to investigate. We say earlier that $O_{2,1}(\mathbb{R})$ is locally isomorphic to $SL_2(\mathbb{R})$.

Exercise 171 Show that $O_3(\mathbb{C})$ is locally isomorphic to $SL_2(\mathbb{C})$. (Hint: over $\mathbb{C}$ the forms $x^2 + y^2 + z^2$ and $x^2 + y^2 - z^2$ are equivalent!)

The quaternions are a useful way to describe the compact group $SO_3(\mathbb{R})$ in detail. Recall that the quaternions are a 4-dimensional division algebra over the reals with a basis $1, i, j, k$ and products $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. The conjugation is defined by $\overline{a + bi + cj + dk} = a - bi - cj - dk$ and the norm is defined by $N(q) = q\overline{q} = a^2 + b^2 + c^2 + d^2$. Since this is real, any non-zero quaternion has an inverse $\overline{q}/N(q)$. The unit quaternions $q = a + bi + cj + dk$ with $N(q) = q\overline{q} = a^2 + b^2 + c^2 + d^2 = 1$ form a group homeomorphic to the sphere S^3. This is almost the same as the orthogonal group $SO_3(\mathbb{R}$. To see this consider the adjoint action $\gamma(v) = \gamma v \gamma^-1$ of the unit quaternions S^3 on R^3, identified with the space of imaginary quaternions. This preserves norms and is therefore a rotation, so we get a homomorphism $S^3 \mapsto SO_3(R)$.

Exercise 172 Show that this homomorphism is onto, and has kernel of order 2 given by $\{1, -1\}$.

This gives a fast way to multiply two rotations, since multiplying two quaternions takes fewer operations that multiplying two 3 by 3 matrices.

Exercise 173 The quaternions contain a copy of the complex numbers $a + bi$ so can be thought of as a 2-dimensional right vector space over the complex numbers. Show that under this identification, the group S^3 of unit quaternions, acting by left multiplication on $\mathbb{H} = \mathbb{C}^2$, is identified with the group SU_2.

Dimension 4. Here there are 3 real orthogonal groups $O_4(\mathbb{R})$, $O_{3,1}(\mathbb{R})$, and $O_{2,2}(\mathbb{R})$ to look at. We saw earlier that $O_{3,1}(\mathbb{R})$ is locally isomorphic to $SL_2(\mathbb{C})$, so we will mostly ignore it.

We can also use quaternions to do the next case $SO_4(R)$. To do this, be observe that both left multiplication $x \mapsto \gamma x$ and right multiplication $x \mapsto$

$x\gamma$ by unit quaternions γ preserve the norm and therefore give rotations of 4-dimensional space (identified with the quaternions). So we get a homomorphism $S^3 \times S^3 \mapsto SO_4(\mathbb{R})$, taking $(\gamma, \delta) \in S^3 \times S^3$ to the rotation $x \mapsto \gamma x \delta^{-1}$.

Exercise 174 Check that this is a homomorphism onto $SO_4(\mathbb{R})$ with kernel $(-1, -1)$.

The group $SO_{2,2}(\mathbb{R})$, or rather a double cover of it, has a similar splitting. To see this we think of R^4 as the 2 by 2 matrices, with the determinant as a quadratic form of signature (2,2). Then left and right multiplication by elements of $SL_2(\mathbb{R})$ preserve this form, so we get a homomorphism from $SL_2(\mathbb{R}) \times SL_2(\mathbb{R})$ to $O_{2,2}(\mathbb{R})$ with kernel of order 2. We get a similar splitting of the double cover of $O_4(\mathbb{C})$.

Notice that the Lie algebras of $O_4(\mathbb{R})$, $O_{3,1}(\mathbb{R})$, and $O_{2,2}(\mathbb{R})$ are all real forms of $O_4(\mathbb{C})$, but the first and third split as a product of 2 smaller Lie algebras, while the middle one is a simple Lie algebra.

Dimension 5: Orthogonal groups in dimension 5 are sometimes locally isomorphic to symplectic group; we will discuss this later when we cover symplectic groups.

Dimension 6. The orthogonal group $O_6(\mathbb{C})$ is locally isomorphic to $SL_4(\mathbb{C})$. To see this take the alternating square $\Lambda^2(\mathbb{C}^4)$. This is acted on by $SL_4(\mathbb{C})$ with kernel ± 1, and there is a symmetric bilinear form from $\Lambda^2(C^4) \times \Lambda^2(\mathbb{C}^4) \mapsto \Lambda^4(\mathbb{C}^4)$. But $\Lambda^4(\mathbb{C}^4)$ can be identified with $\mathbb{C}$ in a way that is preserved by $SL_4(\mathbb{C})$, as this identification is essentially a determinant. So we get a homomorphism from $SL_4(\mathbb{C})$ to $SO_6(\mathbb{C})$ with kernel ± 1.

Exercise 175 Similarly the group $SL_4(\mathbb{R})$ is locally isomorphic to one of the groups $SO_6(\mathbb{R})$, $SO_{5,1}$, $SO_{4,2}(\mathbb{R})$, or $SO_{3,3}(\mathbb{R})$; which?

Now we will look at some of the symmetric spaces associated to orthogonal groups, which can be thought of as the most natural things they act on. A maximal compact subgroup of $O_{m,n}(\mathbb{R})$ is $O_m(\mathbb{R}) \times O_n(\mathbb{R})$. The symmetric space is easy to identify explicitly: the orthogonal group $O_{m,n}(\mathbb{R})$ acts on $\mathbb{R}^{m+n}$, and the maximal compact subgroup $O_m(\mathbb{R}) \times O_n(\mathbb{R})$ is just the subgroup fixing the positive definite subspace $\mathbb{R}^m$. So the symmetric space is just the Grassmannian of maximal positive definite subspaces of $\mathbb{R}^{m+n}$ (an open subset of the Grassmannian of all m-dimensional subspaces). For small values of m or n this can be described in other ways as follows.

Example 176 The orthogonal group $O_{n+1}(\mathbb{R})$ is the group of isometries of the n sphere, so the projective orthogonal group $PO_{n+1}(\mathbb{R})$ is the group of isometries of elliptic geometry (real projective space) which can be obtained from a sphere by identifying antipodal points. (Recall that P means quotient out by the center, of order 2 in this case.) We will show that the group of isometries of hyperbolic geometry can be described in a similar way.

We construct a model of hyperbolic geometry. Take the indefinite space $R^{1,n}(\mathbb{R})$ with quadratic form $x_1^2 - x_2^2 - x_3^2 - \cdots$. Then the norm 1 vectors form a 2-sheeted hyperboloid, and on this hyperboloid the pseudo-Riemannian metric of $R^{1,n}(\mathbb{R})$ restricts to a Riemannian metric. Then one of these sheets forms a model of hyperbolic space. So just as in the elliptic case, the group of isometries is $PO_{1,n}(\mathbb{R})$. In the indefinite case the orthogonal group $O_{1,n}(\mathbb{R})$ splits as a product of the center $\{1, -1\}$ of order 2 and its index 2 subgroup group $O_{1,n}(\mathbb{R})^+$ of elements that fix the two components of the hyperboloid (these are the elements of spinor norm equal to the determinant).

Exercise 177 In $\mathbb{R}^{1,n}$ there are two sorts of reflection, because we can reflect in the hyperplanes orthogonal to either positive or negative norm vectors. What two sorts of isometries of hyperbolic space do these correspond to?

The symmetric spaces of $O_{m,n}(\mathbb{R})$ for m (or n) equal to 2 also have a special property. In this case the maximal compact subgroup has a factor of $O_2(\mathbb{R})$ which is almost the circle group S^1, which strongly suggests that this symmetric space should be Hermitian. To see this we identify the symmetric space with an open subset of a complex quadric as follows. The quadric is the set of points ω of the projective space $PC^{2,n}$ such that $(\omega, \omega) = 0$. The open subset is the points with $(\omega, \overline{\omega}) > 0$. If ω is represented by $x + iy$ then $x^2 = y^2 > 0$ and $(x, y) = 0$ so x and y form an orthogonal base for a positive definite subspace of $R^{2,n}$. Changing ω by a complex scalar does not change this 2-dimensional subspace (though it changes the basis of course). So this identifies the symmetric space with an open subset of a complex variety in a natural way. These symmetric spaces turn up quite often in moduli space problems: as a typical example, the moduli space of marked Enriques surfaces is the symmetric space of $O_{2,10}(\mathbb{R})$ with a codimension 1 complex submanifold removed.

Exercise 178 Show that this symmetric space can also be identifies with the points of $\mathbb{C}^{1,n-1}$ whose imaginary part lies in the interior of one of the two cones of $\mathbb{R}^{1,n-1}$. This gives a representation of the symmetric space as a "tube domain", generalizing the upper half plane.

Now we will work out the roots of orthogonal groups. We first find a Cartan subgroup of $O_n(\mathbb{R})$. For example, we can take the group generated by rotations in $n/2$ or $(n-1)/2$ orthogonal planes. The problem is that this is rather a mess as it is not diagonal ("split"). So let's start again, this time using the quadratic form $x_1x_2 + x_3x_4 + \cdots + x_{2m-1} + x_{2m}$. This time a Cartan subalgebra is easier to describe: one consists of the diagonal matrices with entries $a_1, 1/a_1, a_2, 1/a_2, \ldots$. The corresponding Cartan subalgebra consists of diagonal matrices with entries $\alpha_1, -\alpha_1, \alpha_2, -\alpha_2, \ldots$. Now let's find the roots, in other words the eigenvalues of the adjoint representation. The Lie algebra consists of matrices A with $AJ = -JA^t$, or in other words AJ is skew symmetric, where J is the matrix of the quadratic form, which in this case has blocks of $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ down the diagonal. For $m = 2$ the elements of the Lie algebra are

$$\begin{pmatrix} \alpha_1 & 0 & a & b \\ 0 & -\alpha_1 & c & d \\ -d & -b & \alpha_2 & 0 \\ -c & -a & 0 & -\alpha_2 \end{pmatrix}$$

so the roots corresponding to the entries a, b, c, d are $\alpha_1 - \alpha_2$, $\alpha_1 + \alpha_2$, $-\alpha_1 - \alpha_2$,$-\alpha_1 + \alpha_2$, so are just $\pm\alpha_1 \pm \alpha_2$. (Notice that in this case the roots split into two orthogonal pairs, corresponding to the fact that $so_4(\mathbb{C})$ is a product of two copies of $sl_2(\mathbb{C})$.) Similarly for arbitrary m the roots are $\pm\alpha_i \pm \alpha_j$. This roots system is called D_m.

Now we find the Weyl group. This consists of reflections in the roots. Such a reflection exchanges two coordinates, and possible changes the sign of both coordinates. So the Weyl group consist of linear transformations that permute the coordinates and then flip the signs of an even number of them, so has order $2^{m-1}.m!$

We will now use the root systems of orthogonal groups to explain most of the local isomorphisms and splittings we observed in low dimensions.

We first the root system to explain why orthogonal groups in 4 dimensions tend to split. Obviously the root system of a product of 2 Lie algebras is the orthogonal direct sum of their root systems. The root system of $O_4(\mathbb{C})$ happens to be a union of 2 orthogonal pairs $\pm(\alpha_1+\alpha_2)$ and $\pm(\alpha_1-\alpha_2)$, each of which is essentially the roots system of $SL_2(\mathbb{C})$, so we expect its Lie algebra to split. We should also explain why some orthogonal Lie algebras in 4 dimensions such as $o_{3,1}(\mathbb{R})$ do not split. For this, we look at the action of the Galois group of $\mathbb{C}/R$, in other words complex conjugation, on the roots. For a complex Lie algebra the roots lie in its dual. For a real lie algebra the roots need not lie in its dual: in general they are in the complexification of its dual, and in particular are acted on by complex conjugation. (For algebraic groups over more general fields such as the rationals we also get actions of the Galois group on the roots.) For the split case $o_{2,2}$ this action is trivial, for the compact group $o_{4,0}$ the action takes each root to its negative, while for $o_{3,1}$ the Galois group flips the two orthogonal pairs of roots. If the Lie algebra splits as a product then the roots system is a union of orthogonal subsystems invariant under complex conjugation, so the reason $o_{3,1}(\mathbb{R})$ does not split is that the decomposition of the root system into two orthogonal pairs cannot be done in a way invariant under complex conjugation.

Exercise 179 For orthogonal groups of odd dimensional spaces, use the quadratic form $x_0^2+x_1x_2+x_3x_4+\cdots+x_{2m-1}+x_{2m}$. Show that the roots are $\pm\alpha_i\pm\alpha_j$ and $\pm\alpha_i$. This root system is called B_m. Show that the Weyl group generated by the reflections of roots has order $2^m.m!$, and is generated by permutations and sign changes of the coordinates.

This explains why $SL_2(\mathbb{C})$ and $SO_3(\mathbb{C})$ are locally isomorphic: they have essentially the same root system consisting of two roots of sum 0.

Exercise 180 Check directly that the root systems A_3 of $SL_4(\mathbb{C})$ and D_3 of $O_6(\mathbb{C})$ are isomorphic (in other words find an isometry between the vector spaces they generate mapping the first roots system onto the second).

We will later see that $SL_5(\mathbb{C})$ and $Sp_4(\mathbb{C})$ also have the same root system, explaining why they are locally isomorphic.

Now we find the automorphism groups of these root systems B_n and D_n.

For B_m this is easy: the roots fall into m orthogonal pairs, so we can permute the m pairs and swap the elements of each pair. this gives an automorphism group $2^m.m!$, which is the same as the Weyl group.

For D_m the Weyl group is not the full automorphism group, because the Weyl group $2^{m-1}.m!$ can only change the sign of an even number of coordinates, but we can also swap the signs of an odd number of coordinates to get a group

$2^m.m!$. In particular the root system has an automorphism of order 2 not in the Weyl group. This corresponds to an outer automorphism of the group $SO_{2m}(\mathbb{C})$, given by any determinant -1 automorphism of $O_{2m}(\mathbb{C})$.

Exercise 181 Why does this only apply for orthogonal groups in even dimensions; in other words why do the determinant -1 elements of $O_{2m+1}(\mathbb{C})$ not give outer automorphisms of $SO_{2m+1}(\mathbb{C})$?

Are there any more automorphisms? The lattice D_m (meaning the lattice generated by the roots) is a lattice of determinant 4 contained in the lattice B_m of determinant 1. If we can show that B_m is unique in some way then this will show that the automorphism group of D_m acts on B_m, so is the automorphism group of B_m. So let's look at the possible integral lattices containing D_4. Any such lattices must be contained in the dual of D_4, which consists of 4 cosets of D_4: all vectors have integral coordinates, or they all have half-integral coordinates. The B_m lattice is formed by taking D_m and adding the coset with integral coordinates whose sum is odd. So we look at the other two cosets, whose minimal norm vectors are $(\pm 1/2, \pm 1/2, ...,)$ with sum either even or odd. The minimal norm is $m/4$, while the minimal norm of the coset used for B_m is 1. So there are no extra automorphisms unless possibly $m/4 = 1$, in other words $m = 4$. In this case there are indeed extra automorphisms: we need to find an automorphisms acting nontrivially on these cosets, and we can find such automorphisms given by reflections in the vectors $(\pm 1/2, \pm 1/2, \pm 1/2, \pm 1/2)$ which ave norm 1 and inner product with each element of D_4 a half integer, so reflection is indeed an automorphism of D_4.

In fact we can extend the root system $D_4 \subset B_4$ to a bigger root system called F_4 by adding in these 16 norm 1 roots. We will see later that this is the root system of an exceptional Lie group. We have essentially worked out the Weyl group of F_4: it is the same as the automorphism group of the root system D_4 and so has order $2^3.4!.6 = 2^7.3^2$.

There is another way to extend D_m to a bigger root system. If we put $m = 8$ then the vectors $(\pm 1/2, \pm 1/2, ...,)$ happen to have norm 2, and all norm 2 vectors of an integral lattice are roots (meaning that their reflections act on the lattice). So if we add one of these cosets to D_8 we get an integral lattice E_8 with $112 + 2^7 = 240$ vectors of norm 2. In other words the roots are the vectors $(\cdots, \pm 1, \cdots, \pm 1, \cdots)$ with two non-zero entries and the vectors $(\pm 1/2, \pm 1/2, ...,)$ with even sum. This root system also corresponds to an exceptional Lie algebra of dimension $8 + 240 = 248$.

Exercise 182 Define the root systems E_7 and E_6 to be the roots of E_8 whose first 2 or 3 coordinates are equal. Show that E_7 has 126 roots and E_6 has 72 roots. (These will turn out to correspond to Lie algebras of dimensions $126 + 7 = 133$ and $72 + 6 = 78$.)

The lattice E_8 is the smallest example of a unimodular integral positive definite lattice that is not a sum of copies of $\mathbb{Z}$. We can form similar unimodular lattices D_m^+ from D_m whenever m is divisible by 4; they are even lattices if m is divisible by 8. However if $m > 8$ they have the same roots as D_m so do not give new Lie algebras or root systems.

The lattice for $m = 16$ was used by Milnor to give a negative answer the question "can you hear the shape of a drum", in other words is a compact Riemannian manifold determined by the spectrum of its Laplacian. The spectrum of a toroidal drum is given by the number of vectors of various norms of the corresponding lattice. The lattices $E_8 + E_8$ and D_{16}^+ are distinct, and the theory of modular forms shows that they have the same theta function, in other words the same number of vectors of every norm, so the corresponding tori are not isomorphic but have the same spectrums.

Exercise 183 Show that the root systems $E_8 + E_8$ and D_{16} in $\mathbb{R}^{16}$ have the same number of roots but are not isomorphic.

14 Clifford algebras

With Lie algebras of small dimensions, we have seen that there are numerous accidental isomorphisms. Almost all of these can be explained with Clifford algebras and Spin groups.

Motivational examples that we'd like to explain:

1. $SO_2(\mathbb{R}) = S^1$: S^1 can double cover S^1 itself.
2. $SO_3(\mathbb{R})$: has a simply connected double cover S^3.
3. $SO_4(\mathbb{R})$: has a simply connected double cover $S^3 \times S^3$.
4. $SO_5(\mathbb{C})$: Look at $Sp_4(\mathbb{C})$, which acts on $\mathbb{C}^4$ and on $\Lambda^2(\mathbb{C}^4)$, which is 6 dimensional, and decomposes as $5 \oplus 1$. $\Lambda^2(\mathbb{C}^4)$ has a symmetric bilinear form given by $\Lambda^2(\mathbb{C}^4) \otimes \Lambda^2(\mathbb{C}^4) \to \Lambda^4(\mathbb{C}^4) \simeq \mathbb{C}$, and $Sp_4(\mathbb{C})$ preserves this form. You get that $Sp_4(\mathbb{C})$ acts on $\mathbb{C}^5$, preserving a symmetric bilinear form, so it maps to $SO_5(\mathbb{C})$. You can check that the kernel is ± 1. So $Sp_4(\mathbb{C})$ is a double cover of $SO_5(\mathbb{C})$.
5. $SO_5(\mathbb{C})$: $SL_4(\mathbb{C})$ acts on $\mathbb{C}^4$, and we still have our 6 dimensional $\Lambda^2(\mathbb{C}^4)$, with a symmetric bilinear form. So we get a homomorphism $SL_4(\mathbb{C}) \to SO_6(\mathbb{C})$, which we can check is surjective, with kernel ± 1.

So we have double covers S^1, S^3, $S^3 \times S^3$, $Sp_4(\mathbb{C})$, $SL_4(\mathbb{C})$ of the orthogonal groups in dimensions 2,3,4,5, and 6, respectively. All of these look completely unrelated. We will give a uniform construction of double covers of all orthogonal groups using Clifford algebras.

Example 184 We have not yet defined Clifford algebras, but to motivate the definition here are some examples of Clifford algebras over $\mathbb{R}$.

- $\mathbb{C}$ is generated by $\mathbb{R}$, together with i, with $i^2 = -1$
- $\mathbb{H}$ is generated by $\mathbb{R}$, together with i, j, each squaring to -1, with $ij + ji = 0$.
- Dirac wanted a square root for the operator $\nabla = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2} - \frac{\partial^2}{\partial t^2}$ (the wave operator in 4 dimensions). He supposed that the square root is of the form $A = \gamma_1 \frac{\partial}{\partial x} + \gamma_2 \frac{\partial}{\partial y} + \gamma_3 \frac{\partial}{\partial z} + \gamma_4 \frac{\partial}{\partial t}$ and compared coefficients in

the equation $A^2 = \nabla$. Doing this yields $\gamma_1^2 = \gamma_2^2 = \gamma_3^2 = 1$, $\gamma_4^2 = -1$, and $\gamma_i\gamma_j + \gamma_j\gamma_i = 0$ for $i \neq j$.

Dirac solved this by taking the γ_i to be 4×4 complex matrices. A operates on vector-valued functions on space-time.

Definition 185 *A* Clifford algebra *over* $\mathbb{R}$ *is generated by elements* $\gamma_1, \ldots, \gamma_n$ *such that* $\gamma_i^2 = \pm 1$*, and* $\gamma_i\gamma_j + \gamma_j\gamma_i = 0$ *for* $i \neq j$*.*

This is a rather clumsy and ad hoc definition. Let's try again:

Definition 186 (better definition) *Suppose* V *is a vector space over a field* K*, with some quadratic form* $N : V \to K$*. (*N *is a* quadratic form *if it is a homogeneous polynomial of degree 2 in the coefficients with respect to some basis.) Then the* Clifford algebra $C_V(K)$ *is the associative algebra generated by the vector space* V*, with relations* $v^2 = N(v)$*.*

Of course this definition also works for quadratic forms on modules over rings, or sheaves over a space, and so on, and much of the basic theory of Clifford algebras can be extended to these cases.

We know that $N(\lambda v) = \lambda^2 N(v)$ and that the expression $(a, b) := N(a+b) - N(a) - N(b)$ is bilinear. If the characteristic of K is not 2, we have $N(a) = \frac{(a,a)}{2}$. Thus, we can work with symmetric bilinear forms instead of quadratic forms so long as the characteristic of K is not 2. We will use quadratic forms so that everything works in characteristic 2. (Characteristic 2 is notoriously tricky for bilinear and quadratic forms and we will not be working in characteristic 2, but if we can pick up this case for free just by using the right definition we may as well.)

Warning 187 Some authors (mainly in index theory) use the opposite sign convention $v^2 = -N(v)$. This is a convention introduced by Atiyah and Bott.

Some people add a factor of 2 somewhere, which usually does not matter, but is wrong in characteristic 2.

Example 188 Take $V = \mathbb{R}^2$ with basis i, j, and with $N(xi + yj) = -x^2 - y^2$. Then the relations are $(xi + yj)^2 = -x^2 - y^2$ are exactly the relations for the quaternions: $i^2 = j^2 = -1$ and $(i+j)^2 = i^2 + ij + ji + j^2 = -2$, so $ij + ji = 0$.

Remark 189 If the characteristic of K is not 2, a "completing the square" argument shows that any quadratic form is isomorphic to $c_1x_1^2 + \cdots + c_nx_n^2$, and if one can be obtained from another other by permuting the c_i and multiplying each c_i by a non-zero square, the two forms are isomorphic.

It follows that every quadratic form on a vector space over $\mathbb{C}$ is isomorphic to $x_1^2 + \cdots + x_n^2$, and that every quadratic form on a vector space over $\mathbb{R}$ is isomorphic to $x_1^2 + \cdots + x_m^2 - x_{m+1}^2 - \cdots - x_{m+n}^2$ (m pluses and n minuses) for some m and n. Sylvester's law of inertia shows that these forms over $\mathbb{R}$ are non-isomorphic (proof: look at the largest possible dimension of a positive definite or negative definite subspace).

We will usually assume that N is non-degenerate (which means that the associated bilinear form is non-degenerate), but one could study Clifford algebras arising from degenerate forms. For example, the Clifford algebra of the zero form is just the exterior algebra.

Remark 190 The tensor algebra TV has a natural $\mathbb{Z}$-grading, and to form the Clifford algebra $C_V(K)$, we quotient by the ideal generated by the even elements $v^2 - N(v)$. Thus, the algebra $C_V(K) = C_V^0(K) \oplus C_V^1(K)$ is $\mathbb{Z}/2\mathbb{Z}$-graded. A $\mathbb{Z}/2\mathbb{Z}$-graded algebra is called a *superalgebra*.

We now want to solve the following problem: Find the structure of $C_{m,n}(\mathbb{R})$, the Clifford algebra over $\mathbb{R}^{n+m}$ with the form $x_1^2+\cdots+x_m^2-x_{m+1}^2-\cdots-x_{m+n}^2$.

Example 191

- $C_{0,0}(\mathbb{R})$ is $\mathbb{R}$.
- $C_{1,0}(\mathbb{R})$ is $\mathbb{R}[\varepsilon]/(\varepsilon^2-1) = \mathbb{R}(1+\varepsilon)\oplus\mathbb{R}(1-\varepsilon) = \mathbb{R}\oplus\mathbb{R}$. In the given basis, this is a direct sum of algebras over $\mathbb{R}$.
- $C_{0,1}(\mathbb{R})$ is $\mathbb{R}[i]/(i^2+1) = \mathbb{C}$, with i odd.
- $C_{2,0}(\mathbb{R})$ is $\mathbb{R}[\alpha,\beta]/(\alpha^2-1,\beta^2-1,\alpha\beta+\beta\alpha)$. We get a homomorphism $C_{2,0}(\mathbb{R}) \to \mathbb{M}_2(\mathbb{R})$, given by $\alpha \mapsto \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ and $\beta \mapsto \left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$. The homomorphism is onto because the two given matrices generate $\mathbb{M}_2(\mathbb{R})$ as an algebra. The dimension of $\mathbb{M}_2(\mathbb{R})$ is 4, and the dimension of $C_{2,0}(\mathbb{R})$ is at most 4 because it is spanned by 1, α, β, and $\alpha\beta$. So we have that $C_{2,0}(\mathbb{R}) \simeq \mathbb{M}_2(\mathbb{R})$.
- $C_{1,1}(\mathbb{R})$ is $\mathbb{R}[\alpha,\beta]/(\alpha^2-1,\beta^2+1,\alpha\beta+\beta\alpha)$. Again, we get an isomorphism with $\mathbb{M}_2(\mathbb{R})$, given by $\alpha \mapsto \left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ and $\beta \mapsto \left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$

So we have computed the Clifford algebras

$m\backslash n$	0	1	2
0	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{H}$
1	$\mathbb{R}\oplus\mathbb{R}$	$\mathbb{M}_2(\mathbb{R})$	
2	$\mathbb{M}_2(\mathbb{R})$		

If $\{v_1,\ldots,v_n\}$ is a basis for V, then $\{v_{i_1}\cdots v_{i_k} | i_1<\cdots<i_k,\ k\le n\}$ spans $C_V(K)$, so the dimension of $C_V(K)$ is less than or equal to $2^{\dim V}$. As usual with objects given by generators and relations, the harder problem is showing that it cannot be smaller.

Now let's try to analyze larger Clifford algebras more systematically. What is $C_{U\oplus V}$ in terms of C_U and C_V? One might guess $C_{U\oplus V}\cong C_U\otimes C_V$. For the usual definition of tensor product, this is false (e.g. $C_{1,1}(\mathbb{R}) \neq C_{1,0}(\mathbb{R})\otimes C_{0,1}(\mathbb{R})$). However, for the *superalgebra* definition of tensor product, this is correct. The superalgebra tensor product is the regular tensor product of vector spaces, with the product given by $(a\otimes b)(c\otimes d) = (-1)^{\deg b\cdot\deg c}ac\otimes bd$ for homogeneous elements a, b, c, and d. For the moment we will forget about superalgebras, and naively calculate with the ordinary tensor product.

Let's specialize to the case $K=\mathbb{R}$ and try to compute $C_{U\oplus V}(K)$. Assume for the moment that $\dim U = m$ is even. Take $\alpha_1, \ldots, \alpha_m$ to be an orthogonal basis for U and let $\beta_1,\ldots,\beta_n$ to be an orthogonal basis for V. Then set $\gamma_i = \alpha_1\alpha_2\cdots\alpha_m\beta_i$. What are the relations between the α_i and the γ_j? We have

$$\alpha_i\gamma_j = \alpha_i\alpha_1\alpha_2\cdots\alpha_m\beta_j = \alpha_1\alpha_2\cdots\alpha_m\beta_i\alpha_i = \gamma_j\alpha_i$$

since $\dim U$ is even, and α_i anti-commutes with everything except itself.

$$\begin{aligned}
\gamma_i\gamma_j &= \gamma_i\alpha_1\cdots\alpha_m\beta_j \\
&= \alpha_1\cdots\alpha_m\gamma_i\beta_j \\
&= \alpha_1\cdots\alpha_m\alpha_1\cdots\alpha_m\underbrace{\beta_i\beta_j}_{-\beta_j\beta_i} \\
&= -\gamma_j\gamma_i \\
\gamma_i^2 &= \alpha_1\cdots\alpha_m\alpha_1\cdots\alpha_m\beta_i\beta_i \\
&= (-1)^{\frac{m(m-1)}{2}}\alpha_1^2\cdots\alpha_m^2\beta_i^2 \\
&= (-1)^{m/2}\alpha_1^2\cdots\alpha_m^2\beta_i^2 && (m \text{ even})
\end{aligned}$$

So the γ_i's commute with the α_i and satisfy the relations of some Clifford algebra. Thus, we've shown that $C_{U\oplus V}(K) \cong C_U(K)\otimes C_W(K)$, where W is V with the quadratic form multiplied by

$$(-1)^{\frac{1}{2}\dim U}\alpha_1^2\cdots\alpha_m^2 = (-1)^{\frac{1}{2}\dim U}\cdot\text{discriminant}(U),$$

and this is the usual tensor product of algebras over $\mathbb{R}$.

Taking $\dim U = 2$, we find that

$$\begin{aligned}
C_{m+2,n}(\mathbb{R}) &\cong \mathbb{M}_2(\mathbb{R})\otimes C_{n,m}(\mathbb{R}) \\
C_{m+1,n+1}(\mathbb{R}) &\cong \mathbb{M}_2(\mathbb{R})\otimes C_{m,n}(\mathbb{R}) \\
C_{m,n+2}(\mathbb{R}) &\cong \mathbb{H}\otimes C_{n,m}(\mathbb{R})
\end{aligned}$$

where the indices switch whenever the discriminant is positive. Using these formulas, we can reduce any Clifford algebra to tensor products of things like $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, and $\mathbb{M}_2(\mathbb{R})$.

Recall the rules for taking tensor products of matrix algebras (all tensor products are over $\mathbb{R}$).

- $\mathbb{R}\otimes X \cong X$.
- $\mathbb{C}\otimes\mathbb{H}\cong\mathbb{M}_2(\mathbb{C})$.

  This follows from the isomorphism $\mathbb{C}\otimes C_{m,n}(\mathbb{R})\cong C_{m+n}(\mathbb{C})$.
- $\mathbb{C}\otimes\mathbb{C}\cong\mathbb{C}\oplus\mathbb{C}$.
- $\mathbb{H}\otimes\mathbb{H}\cong\mathbb{M}_4(\mathbb{R})$.

  This follows by thinking of the action on $\mathbb{H}\cong\mathbb{R}^4$ given by $(x\otimes y)\cdot z = xz\overline{y}$.
- $\mathbb{M}_m\big(\mathbb{M}_n(X)\big)\cong\mathbb{M}_{mn}(X)$.
- $\mathbb{M}_m(X)\otimes\mathbb{M}_n(Y)\cong\mathbb{M}_{mn}(X\otimes Y)$.

Filling in the middle of the table is easy because we can move diagonally by tensoring with $\mathbb{M}_2(\mathbb{R})$. It is easy to see that $C_{8+m,n}(\mathbb{R})\cong C_{m,n+8}(\mathbb{R})\cong C_{m,n}\otimes\mathbb{M}_{16}(\mathbb{R})$, which gives the table a kind of mod 8 periodicity. There is a more precise way to state this: $C_{m,n}(\mathbb{R})$ and $C_{m',n'}(\mathbb{R})$ are *super Morita equivalent* if and only if $m-n\equiv m'-n' \mod 8$.

We found that the structure of a Clifford algebra depends heavily on $m-n$ mod 8. The explanation of this was not all that satisfactory as it seemed to be a fluke coming at the end of a long calculation. There is a hidden cyclic group of order 8 controlling this, given by the super Brauer group of the reals. The usual Brauer group of a field consists of the finite dimensional central division rings, with the group product given by taking tensor products (modulo taking matrix rings). For example, the Brauer group of the reals has order 2, with elements the reals and the quaternions, and the Brauer group of the complex numbers has order 1. The super Brauer group is defined similarly except we use super division algebras: this means every nonzero HOMOGENEOUS element is invertible. The 8 elements are represented by the reals, the quaternions, and the algebras $\mathbb{R}[\epsilon]$, $\mathbb{C}[\epsilon]$, $\mathbb{H}[\epsilon]$, where ϵ is odd, $\epsilon^2 = \pm 1$ and $x\epsilon = \epsilon\overline{x}$ for x in the even part.

Exercise 192 Work out how the super division algebras over $\mathbb{R}$ correspond to elements of a cyclic group of order 8 up to super Morita equivalence, under the super tensor product. Find the 8 algebras underlying them if one forgets the grading and compare these with Clifford algebras.

This mod 8 periodicity turns up in several other places:

1. Real Clifford algebras $C_{m,n}(\mathbb{R})$ and $C_{m',n'}(\mathbb{R})$ are super Morita equivalent if and only if $m-n \equiv m'-n' \mod 8$.

2. *Bott periodicity*, which says that stable homotopy groups of orthogonal groups are periodic mod 8.

3. Real K-theory is periodic with a period of 8.

4. Even unimodular lattices (such as the E_8 lattice) exist in $\mathbb{R}^{m,n}$ if and only if $m-n \equiv 0 \mod 8$. More generally even integral lattices tend to have a strong period 8 behavior: for example $\sum_{\lambda \in L'/L} e^{\pi i \lambda^2} = e^{2\pi i \text{signature}/8}\sqrt{|\text{discriminant}|}$. For 1-dimensional lattices this is more or less Gauss's law of quadratic reciprocity in terms of Gauss sums.

5. The Super Brauer group of $\mathbb{R}$ is $\mathbb{Z}/8\mathbb{Z}$.

Recall that $C_V(\mathbb{R}) = C_V^0(\mathbb{R}) \oplus C_V^1(\mathbb{R})$, where $C_V^1(\mathbb{R})$ is the odd part and $C_V^0(\mathbb{R})$ is the even part. We will need to know the structure of $C_{m,n}^0(\mathbb{R})$, which controls special orthogonal groups in the same way that Clifford algebras control orthogonal groups. Fortunately, this is easy to compute in terms of smaller Clifford algebras. Let $\dim U = 1$, with γ a basis for U and let $\gamma_1, \ldots, \gamma_n$ an orthogonal basis for V. Then $C_{U\oplus V}^0(K)$ is generated by $\gamma\gamma_1, \ldots, \gamma\gamma_n$. We compute the relations

$$\gamma\gamma_i \cdot \gamma\gamma_j = -\gamma\gamma_j \cdot \gamma\gamma_i$$

for $i \neq j$, and

$$(\gamma\gamma_i)^2 = (-\gamma^2)\gamma_i^2$$

So $C_{U\oplus V}^0(K)$ is itself the Clifford algebra $C_W(K)$, where W is V with the quadratic form multiplied by $-\gamma^2 = -\text{disc}(U)$. Over $\mathbb{R}$, this tells us that

$$C_{m+1,n}^0(\mathbb{R}) \cong C_{n,m}(\mathbb{R}) \qquad \text{(mind the indices)}$$
$$C_{m,n+1}^0(\mathbb{R}) \cong C_{m,n}(\mathbb{R}).$$

Remark 193 For complex Clifford algebras, the situation is similar, but easier. One finds that $C_{2m}(\mathbb{C}) \cong \mathbb{M}_{2^m}(\mathbb{C})$ and $C_{2m+1}(\mathbb{C}) \cong \mathbb{M}_{2^m}(\mathbb{C}) \oplus \mathbb{M}_{2^m}(\mathbb{C})$, with $C_n^0(\mathbb{C}) \cong C_{n-1}(\mathbb{C})$. You could figure these out by tensoring the real algebras with $\mathbb{C}$ if you wanted. We see a mod 2 periodicity now. Bott periodicity for the unitary group is mod 2.

Exercise 194 Find the non-trivial finite dimensional super division algebra with center $\mathbb{C}$.

Clifford algebras are analogous to the algebra of differential operators, which are given by generators x_i and D_i with relations that the x_i commute with each other, the D_i commute with each other, and $D_i x_j - x_j D_i = 1$. If we put a skew symmetric form on the vector space spanned by the x_i and D_i so that $\langle x_i, x_j\rangle = 0$, $\langle D_i, D_j\rangle = 0$, $\langle D_i, x_j\rangle = 1$ if $i = j$ and 0 otherwise, then the algebra of differential operators is generated by this space with the relations $ab - ba = \langle a, b\rangle$. This is similar to Clifford algebras which (in characteristic not 2) have relations $ab + ba = (a, b)$ for a symmetric form. If we work with super vector spaces, then these two constructions become special cases of the same construction.

Clifford algebras can also be obtained as a quotient of a Heisenberg superalgebra, in the same way that the algebra of differential operators is a quotient of a Heisenberg algebra. So the study of Clifford algebras and their representations is essentially the study of the Heisenberg superalgebra. This again demonstrates that it is really more natural to work with super vector spaces rather than vector spaces when studying Clifford algebras, but we will mostly just use vector spaces and just point out the changes needed for using superspaces.

14.1 Clifford groups, Spin groups, and Pin groups

In this section, we define Clifford groups of a vector space V with a quadratic form over a field K, denoted $\Gamma_V(K)$. They are central extensions of orthogonal groups that fit into an exact sequence

$$1 \to K^\times \to \Gamma_V(K) \to O_V(K) \to 1.$$

Definition 195 *We define α to be the automorphism of $C_V(K)$ induced by -1 on V (in other words the automorphism which acts by -1 on odd elements and 1 on even elements)). The Clifford group $\Gamma_V(K)$ is the group of homogeneous invertible elements $x \in C_V(K)$ such that $xV\alpha(x)^{-1} \subseteq V$ (recall that $V \subseteq C_V(K)$). This also gives an action of $\Gamma_V(K)$ on V.*

Many authors leave out the α, which is a mistake, though not a serious one, and use xVx^{-1} instead of $xV\alpha(x)^{-1}$. Our definition (introduced by Atiyah, Bott, and Schapiro) is better for the following reasons:

1. It is the correct superalgebra sign. The superalgebra convention says that whenever you exchange two elements of odd degree, you pick up a minus sign, and V is odd.

2. Putting α in makes the theory much cleaner in odd dimensions. For example, we will see that the described action gives a map $\Gamma_V(K) \to O_V(K)$ which is onto if we use α, but not if we do not. (You get $SO_V(K)$ rather

than $O_V(K)$ in odd dimensions without the α, which is not a disaster, but is annoying.)

Lemma 196 *The elements of $\Gamma_V(K)$ that act trivially on V are the elements of $K^\times \subseteq \Gamma_V(K) \subseteq C_V(K)$.*

Proof Suppose $a_0 + a_1 \in \Gamma_V(K)$ acts trivially on V, with a_0 even and a_1 odd. Then $(a_0+a_1)v = v\alpha(a_0+a_1) = v(a_0 - a_1)$. Matching up even and odd parts, we get $a_0 v = v a_0$ and $a_1 v = -v a_1$. Choose an orthogonal basis $\gamma_1, \ldots, \gamma_n$ for V. (All these results are true in characteristic 2, but we have to work harder: we cannot go around choosing orthogonal bases because they may not exist.) We may write

$$a_0 = x + \gamma_1 y$$

where $x \in C_V^0(K)$ and $y \in C_V^1(K)$ and neither x nor y contain a factor of γ_1, so $\gamma_1 x = x\gamma_1$ and $\gamma_1 y = y \gamma_1$. Applying the relation $a_0 v = v a_0$ with $v = \gamma_1$, we see that $y = 0$, so a_0 contains no monomials with a factor γ_1.

Repeat this procedure with v equal to the other basis elements to show that $a_0 \in K^\times$ (since it cannot have any γ's in it). Similarly, write $a_1 = y + \gamma_1 x$, with x and y not containing a factor of γ_1. Then the relation $a_1\gamma_1 = -\gamma_1 a_1$ implies that $x = 0$. Repeating with the other basis vectors, we conclude that $a_1 = 0$.

So $a_0 + a_1 = a_0 \in K \cap \Gamma_V(K) = K^\times$. $\square$ Now we define $-^T$ to be the identity on V, and extend it to an anti-automorphism of $C_V(K)$ ("anti" means that $(ab)^T = b^T a^T$). Do not confuse $a \mapsto \alpha(a)$ (automorphism), $a \mapsto a^T$ (anti-automorphism), and $a \mapsto \alpha(a^T)$ (anti-automorphism).

Now we define the *spinor norm* of $a \in C_V(K)$ by $N(a) = aa^T$. We also define a twisted version: $N^\alpha(a) = a\alpha(a)^T$.

Proposition 197

1. *The restriction of N to $\Gamma_V(K)$ is a homomorphism whose image lies in $K^\times$. (N is a mess on the rest of $C_V(K)$.)*

2. *The action of $\Gamma_V(K)$ on V is orthogonal. That is, we have a homomorphism $\Gamma_V(K) \to O_V(K)$.*

Proof First we show that if $a \in \Gamma_V(K)$, then $N^\alpha(a)$ acts trivially on V.

$$N^\alpha(a)\, v\, \alpha\big(N^\alpha(a)\big)^{-1} = a\alpha(a)^T v \Big(\alpha(a)\underbrace{\alpha\big(\alpha(a)^T\big)}_{=a^T}\Big)^{-1} \tag{5}$$

$$= a\underbrace{\alpha(a)^T v (a^{-1})^T}_{=(a^{-1}v^T\alpha(a))^T}\alpha(a)^{-1} \tag{6}$$

$$= aa^{-1}v\alpha(a)\alpha(a)^{-1} \tag{7}$$

$$= v \tag{8}$$

So by Lemma ???, $N^\alpha(a) \in K^\times$. This implies that N^α is a homomorphism on $\Gamma_V(K)$ because

$$\begin{aligned} N^\alpha(a)N^\alpha(b) &= a\alpha(a)^T N^\alpha(b) && (9)\\ &= aN^\alpha(b)\alpha(a)^T \qquad (N^\alpha(b) \text{ is central}) && (10)\\ &= ab\alpha(b)^T\alpha(a)^T && (11)\\ &= (ab)\alpha(ab)^T = N^\alpha(ab). && (12) \end{aligned}$$

After all this work with N^α, what we're really interested is N. On the even elements of $\Gamma_V(K)$, N agrees with N^α, and on the odd elements, $N = -N^\alpha$. Since $\Gamma_V(K)$ consists of homogeneous elements, N is also a homomorphism from $\Gamma_V(K)$ to $K^\times$. This proves the first statement of the proposition.

Finally, since N is a homomorphism on $\Gamma_V(K)$, the action on V preserves the quadratic form N of V. Thus, we have a homomorphism $\Gamma_V(K) \to O_V(K)$. □

On V, N coincides with the quadratic form N. Some authors seem not to have noticed this, and use different letters for the norm N and the spinor norm N on V. Sometimes they use a poorly chosen sign convention which makes them different.

Now we analyze the homomorphism $\Gamma_V(K) \to O_V(K)$. Lemma ??? says exactly that the kernel is $K^\times$. Next we will show that the image is all of $O_V(K)$. Say $r \in V$ and $N(r) \neq 0$.

$$\begin{aligned} rv\alpha(r)^{-1} &= -rv\frac{r}{N(r)} = v - \frac{vr^2 + rvr}{N(r)} \\ &= v - \frac{(v,r)}{N(r)}r && (13)\\ &= \begin{cases} -r & \text{if } v = r \\ v & \text{if } (v,r) = 0 \end{cases} && (14) \end{aligned}$$

Thus, r is in $\Gamma_V(K)$, and it acts on V by reflection through the hyperplane $r^\perp$. One might deduce that the homomorphism $\Gamma_V(K) \to O_V(K)$ is surjective because $O_V(K)$ is generated by reflections. This is wrong; $O_V(K)$ is *not* always generated by reflections!

Exercise 198 Let $H = \mathbb{F}_2^2$, with the quadratic form $x^2 + y^2 + xy$, and let $V = H \oplus H$. Prove that $O_V(\mathbb{F}_2)$ is not generated by reflections.

Solution 199 *In H, the norm of any non-zero vector is 1. It is immediate to check that the reflection of a non-zero vector v through another non-zero vector u is*

$$r_u(v) = \begin{cases} u & \text{if } u = v \\ v + u & \text{if } u \neq v \end{cases}$$

so reflection through a non-zero vector fixes that vector and swaps the two other non-zero vectors. Thus, the reflection in H generate the symmetric group on three elements S_3, acting on the three non-zero vectors.

If u and v are non-zero vectors, then $(u,v) \in H \oplus H$ has norm $1 + 1 = 0$, so one cannot reflect through it. Thus, every reflection in V is "in one of the

H's," so the group generated by reflections is $S_3 \times S_3$. However, swapping the two H's is clearly an orthogonal transformation, so reflections do not generate $O_V(\mathbb{F}_2)$.

Remark 200 This is the only counterexample. For any other vector space and any other non-degenerate quadratic form on this space, $O_V(K)$ is generated by reflections. The map $\Gamma_V(K) \to O_V(K)$ is surjective even in the example above. Also, in every case except the example above, $\Gamma_V(K)$ is generated as a group by non-zero elements of V (i.e. every element of $\Gamma_V(K)$ is a monomial).

Remark 201 Equation ??? is the definition of the reflection of v through r. It is only possible to reflect through vectors of non-zero norm. Reflections in characteristic 2 are strange; strange enough that people don't call them reflections, they call them *transvections*.

Definition 202

$$Pin_V(K) = \{x \in \Gamma_V(K) | N(x) = 1\}$$

, and

$$Spin_V(K) = Pin_V^0(K)$$

, the even elements of $Pin_V(K)$.

On $K^\times$, the spinor norm is given by $x \mapsto x^2$, so the elements of spinor norm 1 are $= \pm 1$.

$$\begin{pmatrix} 1 & \to & \pm 1 & \to & Pin_V(k) & \to & \Omega_V & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & k^* & \to & \Gamma_V(k) & \to & O_V(k) & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & k^{*2} & \to & k^* & \to & k^*/k^{*2} & \to & 1 \end{pmatrix}$$

where the rows are exact, $K^\times$ is in the center of $\Gamma_V(K)$ (this is obvious, since $K^\times$ is in the center of $C_V(K)$), and $N : O_V(K) \to K^\times/(K^\times)^2$ is the unique homomorphism sending reflection through $r^\perp$ to $N(r)$ modulo $(K^\times)^2$.

To see exactness of the top sequence, note that the kernel of ϕ is $K^\times \cap \mathrm{Pin}_V(K) = \pm 1$, and that the image of $\mathrm{Pin}_V(K)$ in $O_V(K)$ is exactly the elements of norm 1. The bottom sequence is similar, except that the image of $\mathrm{Spin}_V(K)$ is not all of $O_V(K)$, it is only $SO_V(K)$; by Remark **??**, every element of $\Gamma_V(K)$ is a product of elements of V, so every element of $\mathrm{Spin}_V(K)$ is a product of an even number of elements of V. Thus, its image is a product of an even number of reflections, so it is in $SO_V(K)$.

These maps are NOT always onto, but there are many important cases when they are, such as when V has a positive definite quadratic form. The image is the set of elements of $O_V(K)$ or $SO_V(K)$ that have spinor norm 1 in $K^\times/(K^\times)^2$.

What is $N : O_V(K) \to K^\times/(K^\times)^2$? It is the UNIQUE homomorphism such that $N(a) = N(r)$ if a is reflection in $r^\perp$, and r is a vector of norm $N(r)$.

Example 203 Take V to be a positive definite vector space over $\mathbb{R}$. Then N maps to 1 in $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \pm 1$ (because N is positive definite). So the spinor norm on $O_V(\mathbb{R})$ is trivial.

So if V is positive definite, we get double covers

$$1 \to \pm 1 \to \mathrm{Pin}_V(\mathbb{R}) \to O_V(\mathbb{R}) \to 1$$

$$1 \to \pm 1 \to \mathrm{Spin}_V(\mathbb{R}) \to SO_V(\mathbb{R}) \to 1$$

This will account for the weird double covers we saw before.

What if V is negative definite? Every reflection now has image -1 in $\mathbb{R}^\times/(\mathbb{R}^\times)^2$, so the spinor norm N is the same as the determinant map $O_V(\mathbb{R}) \to \pm 1$.

So in order to find interesting examples of the spinor norm, we have to look at cases that are neither positive definite nor negative definite.

Let's look at Lorentz space: $\mathbb{R}^{1,3}$.

Reflection through a vector of norm < 0 (spacelike vector, P: parity reversal) has spinor norm -1, det -1 and reflection through a vector of norm > 0 (timelike vector, T: time reversal) has spinor norm $+1$, det -1. So $O_{1,3}(\mathbb{R})$ has 4 components (it is not hard to check that these are all the components), usually called 1, P, T, and PT.

Example 204 The Weyl group of F_4 is generated by reflections of vectors of norms 1 and 2. It is a subgroup of $O_4(\mathbb{Q})$ so the spinor norm is a homomorphism to Q^*/Q^{*2}. So by combining this with the determinant map, we get a homomorphism of this Weyl group onto the Klein 4-group $(\mathbb{Z}/2\mathbb{Z})^2$, mapping reflections of norm 1 or norm 2 vectors onto two different non-trivial elements. Similarly we see immediately that the Weyl group of B_n has a homomorphism onto the Klein 4-group.

Example 205 The groups $PSO_n(\mathbb{R})$ are simple for $n \geq 5$, so one might guess by analogy that the groups $PSO_n(\mathbb{Q})$ are also simple, but the spinor norm shows immediately that they are not. In fact the spinor norm maps $O_n(\mathbb{Q})$ onto the infinite index 2 subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ represented by positive elements, so the abelianization of $PSO_n(\mathbb{Q})$ is infinite.

Remark 206 In terms of Galois cohomology, there an exact sequence of algebraic groups (over an algebraically closed field)

$$1 \to GL_1 \to \Gamma_V \to O_V \to 1$$

We do not necessarily get an exact sequence when taking values in some subfield.

If

$$1 \to A \to B \to C \to 1$$

is exact,

$$1 \to A(K) \to B(K) \to C(K)$$

is exact, but the map on the right need not be surjective. Instead what we get is

$$\begin{aligned} 1 \to H^0(\mathrm{Gal}(\bar{K}/K), A) \to H^0(\mathrm{Gal}(\bar{K}/K), B) \to H^0(\mathrm{Gal}(\bar{K}/K), C) \to \\ \to H^1(\mathrm{Gal}(\bar{K}/K), A) \to \cdots \end{aligned}$$

It turns out that $H^1(Gal(\bar{K}/K), GL_1) = 1$. However, $H^1(Gal(\bar{K}/K), \pm 1) = K^\times/(K^\times)^2$.

So from

$$1 \to GL_1 \to \Gamma_V \to O_V \to 1$$

we get

$$1 \to K^\times \to \Gamma_V(K) \to O_V(K) \to 1 = H^1(Gal(\bar{K}/K), GL_1)$$

However, taking

$$1 \to \mu_2 \to \mathrm{Spin}_V \to SO_V \to 1$$

we get

$$1 \to \pm 1 \to \mathrm{Spin}_V(K) \to SO_V(K) \xrightarrow{N} K^\times/(K^\times)^2 = H^1(\bar{K}/K, \mu_2)$$

so the non-surjectivity of N is some kind of higher Galois cohomology.

Warning 207 $\mathrm{Spin}_V \to SO_V$ is onto as a map of ALGEBRAIC GROUPS, but $\mathrm{Spin}_V(K) \to SO_V(K)$ need NOT be onto.

Example 208 Take $O_3(\mathbb{R}) \cong SO_3(\mathbb{R}) \times \{\pm 1\}$ as 3 is odd (in general $O_{2n+1}(\mathbb{R}) \cong SO_{2n+1}(\mathbb{R}) \times \{\pm 1\}$). So we have a sequence

$$1 \to \pm 1 \to \mathrm{Spin}_3(\mathbb{R}) \to SO_3(\mathbb{R}) \to 1.$$

Notice that $\mathrm{Spin}_3(\mathbb{R}) \subseteq C_3^0(\mathbb{R}) \cong \mathbb{H}$, so $\mathrm{Spin}_3(\mathbb{R}) \subseteq \mathbb{H}^\times$, and in fact we saw that it is S^3.

14.2 Covers of symmetric and alternating groups

The symmetric group on n letter can be embedded in the obvious way in $O_n(\mathbb{R})$ as permutations of coordinates. Lifting this to the pin group gives a double cover of the symmetric group, which restricts to a perfect double cover of the alternating group if n is at least 5.

Example 209 The alternating group A_5 is isomorphic to the group $PSL_2(\mathbb{F}_5)$ which has a double cover $SL_2(\mathbb{F}_5)$. The alternating group A_6 is isomorphic to the group $PSL_2(\mathbb{F}_9)$, which has a double cover $SL_2(\mathbb{F}_9)$. (This is one way to see the extra outer automorphisms of A_6 since the group $PSL_2(\mathbb{F}_9)$ has an outer automorphism group of order 4: we can either conjugate by elements of determinant not a square, or apply a field automorphism of $\mathbb{F}_9$.)

Exercise 210 Here is another way to see the extra outer automorphisms of S_6. Show that there are 6 ways to divide the 10 edges of the complete graph on 5 points into two disjoint 5-cycles, and deduce from this that there is a homomorphism from S_5 to S_6 not conjugate to the "obvious" embedding. Then use the fact that an index n subgroup of a group gives a homomorphism to S_n to construct an outer automorphism of S_6, taking a "standard" S_5 subgroup to one of these "exceptional" ones.

In most cases this is the universal central extension of the alternating group, but there are two exceptions for $n = 6$ or 7, when the alternating group also has a perfect triple cover.

The triple cover of the alternating group A_6 was found by Valentiner and is called the Valentiner group. He found an action of A_6 on the complex projective plane, in other words a homomorphism from A_6 to $PGL_3(\mathbb{C})$, whose inverse image in the triple cover $GL_3(\mathbb{C})$ is a perfect triple cover of A_6. Here is a variation of his construction:

Exercise 211 Show that the group $PGL_3(\mathbb{F}_4)$ acts transitively on the ovals in the projective plane over F_4, where an oval is a set of 6 points such that no 3 are on a line. Show that the subgroup fixing an oval is isomorphic to A_6, acting on the 6 points of the oval. Show that the inverse image of this group in $GL_3(\mathbb{F}_4)$ is a perfect triple cover of A_6.

15 Spin groups

15.1 Spin representations of Spin and Pin groups

Notice that $\mathrm{Pin}_V(K) \subseteq C_V(K)^\times$, so any module over $C_V(K)$ gives a representation of $\mathrm{Pin}_V(K)$. We already figured out that $C_V(K)$ are direct sums of matrix algebras over $\mathbb{R}, \mathbb{C}$, and $\mathbb{H}$.

What are the representations (modules) of complex Clifford algebras? Recall that $C_{2n}(\mathbb{C}) \cong \mathbb{M}_{2^n}(\mathbb{C})$, which has a representations of dimension 2^n, which is called the spin representation of $\mathrm{Pin}_V(K)$ and $C_{2n+1}(\mathbb{C}) \cong \mathbb{M}_{2^n}(\mathbb{C}) \times \mathbb{M}_{2^n}(\mathbb{C})$, which has 2 representations, called the spin representations of $\mathrm{Pin}_{2n+1}(K)$.

What happens if we restrict these to $\mathrm{Spin}_V(\mathbb{C}) \subseteq \mathrm{Pin}_V(\mathbb{C})$? To do that, we have to recall that $C^0_{2n}(\mathbb{C}) \cong \mathbb{M}_{2^{n-1}}(\mathbb{C}) \times \mathbb{M}_{2^{n-1}}(\mathbb{C})$ and $C^0_{2n+1}(\mathbb{C}) \cong \mathbb{M}_{2^n}(\mathbb{C})$. So in EVEN dimensions $\mathrm{Pin}_{2n}(\mathbb{C})$ has 1 spin representation of dimension 2^n splitting into 2 HALF SPIN representations of dimension 2^{n-1} and in ODD dimensions, $\mathrm{Pin}_{2n+1}(\mathbb{C})$ has 2 spin representations of dimension 2^n which become the same on restriction to $\mathrm{Spin}_V(\mathbb{C})$.

Now we give a second description of spin representations. We will just do the even dimensional case (the odd dimensional case is similar). Suppose $\dim V = 2n$, and work over $\mathbb{C}$. Choose an orthonormal basis $\gamma_1, \ldots, \gamma_{2n}$ for V, so that $\gamma_i^2 = 1$ and $\gamma_i\gamma_j = -\gamma_j\gamma_i$. Now look at the group G generated by $\gamma_1, \ldots, \gamma_{2n}$, which is finite, with order 2^{1+2n}. The representations of $C_V(\mathbb{C})$ correspond to representations of G, with -1 acting as -1 (as opposed to acting as 1). So another way to look at representations of the Clifford algebra, is to look at representations of G.

We look at the structure of G:

(1) The center is ± 1. This uses the fact that we are in even dimensions, otherwise $\gamma_1 \cdots \gamma_{2n}$ is also central.

(2) The conjugacy classes: 2 of size 1 (1 and -1), $2^{2n}-1$ of size 2 ($\pm\gamma_{i_1} \cdots \gamma_{i_n}$), so we have a total of $2^{2n}+1$ conjugacy classes, so we should have that many representations. G/center is abelian, isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{2n}$, which gives us 2^{2n} representations of dimension 1, so there is only one more left to find. We can figure out its dimension by recalling that the sum of the squares of the dimensions of irreducible representations gives us the order of G, which is 2^{2n+1}. So $2^{2n} \times 1^1 + 1 \times d^2 = 2^{2n+1}$, where d is the dimension of the mystery representation. Thus, $d = \pm 2^n$, so $d = 2^n$. Thus, G, and

therefore $C_V(\mathbb{C})$, has an irreducible representation of dimension 2^n (as we found earlier by showing that the Clifford algebra is isomorphic to $M_{2^n}(\mathbb{C})$).

Example 212 Consider $O_{2,1}(\mathbb{R})$. As before, $O_{2,1}(\mathbb{R}) \cong SO_{2,1}(\mathbb{R}) \times (\pm 1)$, and $SO_{2,1}(\mathbb{R})$ is not connected: it has two components, separated by the spinor norm N. We have maps

$$1 \to \pm 1 \to \mathrm{Spin}_{2,1}(\mathbb{R}) \to SO_{2,1}(\mathbb{R}) \xrightarrow{N} \pm 1.$$

$\mathrm{Spin}_{2,1}(\mathbb{R}) \subseteq C^*_{2,1}(\mathbb{R}) \cong \mathbb{M}_2(\mathbb{R})$, so $\mathrm{Spin}_{2,1}(\mathbb{R})$ has one 2 dimensional spin representation. So there is a map $\mathrm{Spin}_{2,1}(\mathbb{R}) \to SL_2(\mathbb{R})$; by counting dimensions and such, we can show it is an isomorphism. So $\mathrm{Spin}_{2,1}(\mathbb{R}) \cong SL_2(\mathbb{R})$.

Now let's look at some 4 dimensional orthogonal groups

Example 213 Look at $SO_4(\mathbb{R})$, which is compact. It has a complex spin representation of dimension $2^{4/2} = 4$, which splits into two half spin representations of dimension 2. We have the sequence

$$1 \to \pm 1 \to \mathrm{Spin}_4(\mathbb{R}) \to SO_4(\mathbb{R}) \to 1 \qquad (N = 1)$$

$\mathrm{Spin}_4(\mathbb{R})$ is also compact, so the image in any complex representation is contained in some unitary group. So we get two maps $\mathrm{Spin}_4(\mathbb{R}) \to SU(2) \times SU(2)$, and both sides have dimension 6 and centers of order 4. Thus, we find that $\mathrm{Spin}_4(\mathbb{R}) \cong SU(2) \times SU(2) \cong S^3 \times S^3$, which give you the two half spin representations.

So now we have done the positive definite case.

Example 214 Look at $SO_{3,1}(\mathbb{R})$. Notice that $O_{3,1}(\mathbb{R})$ has four components distinguished by the maps $\det, N \to \pm 1$. So we get

$$1 \to \pm 1 \to \mathrm{Spin}_{3,1}(\mathbb{R}) \to SO_{3,1}(\mathbb{R}) \xrightarrow{N} \pm 1 \to 1$$

We expect 2 half spin representations, which give us two homomorphisms $\mathrm{Spin}_{3,1}(\mathbb{R}) \to SL_2(\mathbb{C})$. This time, each of these homomorphisms is an isomorphism (I can't think of why right now). The $SL_2(\mathbb{C})$s are double covers of simple groups. Here, we do not get the splitting into a product as in the positive definite case. This isomorphism is heavily used in quantum field theory because $\mathrm{Spin}_{3,1}(\mathbb{R})$ is a double cover of the connected component of the Lorentz group (and $SL_2(\mathbb{C})$ is easy to work with). Note also that the center of $\mathrm{Spin}_{3,1}(\mathbb{R})$ has order 2, not 4, as for $\mathrm{Spin}_{4,0}(\mathbb{R})$. Also note that the group $PSL_2(\mathbb{C})$ acts on the compactified $\mathbb{C} \cup \{\infty\}$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(\tau) = \frac{a\tau+b}{c\tau+d}$. Subgroups of this group are called Kleinian groups. On the other hand, the group $SO_{3,1}(\mathbb{R})^+$ (identity component) acts on $\mathbb{H}^3$ (three dimensional hyperbolic space). To see this, look at the 2-sheeted hyperboloid.

One sheet of norm -1 hyperboloid is isomorphic to $\mathbb{H}^3$ under the induced metric. In fact, we'll define hyperbolic space that way. Topologists are very interested in hyperbolic 3-manifolds, which are $\mathbb{H}^3/(\text{discrete subgroup of } SO_{3,1}(\mathbb{R}))$. If we use the fact that $SO_{3,1}(\mathbb{R}) \cong PSL_2(\mathbb{R})$, then we see that these discrete subgroups are in fact Kleinian groups.

There are lots of exceptional isomorphisms in small dimension, all of which are very interesting, and almost all of them can be explained by spin groups.

Example 215 $O_{2,2}(\mathbb{R})$ has 4 components (given by det, N); $C^0_{2,2}(\mathbb{R}) \cong \mathbb{M}_2(\mathbb{R}) \times \mathbb{M}_2(\mathbb{R})$, which induces an isomorphism $\mathrm{Spin}_{2,2}(\mathbb{R}) \to SL_2(\mathbb{R}) \times SL_2(\mathbb{R})$, which gives the two half spin representations. Both sides have dimension 6 with centers of order 4. So this time we get two non-compact groups. Let us look at the fundamental group of $SL_2(\mathbb{R})$, which is $\mathbb{Z}$, so the fundamental group of $\mathrm{Spin}_{2,2}(\mathbb{R})$ is $\mathbb{Z} \oplus \mathbb{Z}$. As we recall, $\mathrm{Spin}_{4,0}(\mathbb{R})$ and $\mathrm{Spin}_{3,1}(\mathbb{R})$ were both simply connected. This shows that SPIN GROUPS NEED NOT BE SIMPLY CONNECTED. So we can take covers of it. What do the corresponding covers (e.g. the universal cover) of $\mathrm{Spin}_{2,2}(\mathbb{R})$ look like? This is hard to describe because for finite dimensional complex representations, we get finite dimensional representations of the Lie algebra L, which correspond to the finite dimensional representations of $L \otimes \mathbb{C}$, which correspond to the finite dimensional representations of L' = Lie algebra of $\mathrm{Spin}_{4,0}(\mathbb{R})$, which correspond to the finite dimensional representations of $\mathrm{Spin}_{4,0}(\mathbb{R})$, which has no covers because it is simply connected. This means that any finite dimensional representation of a cover of $\mathrm{Spin}_{2,2}(\mathbb{R})$ actually factors through $\mathrm{Spin}_{2,2}(\mathbb{R})$. So there is no way to describe these things with finite matrices, and infinite dimensional representations are hard.

To summarize, the ALGEBRAIC GROUP $\mathrm{Spin}_{2,2}$ is simply connected (as an algebraic group) (think of an algebraic group as a functor from rings to groups), which means that it has no algebraic central extensions. However, the LIE GROUP $\mathrm{Spin}_{2,2}(\mathbb{R})$ is NOT simply connected; it has fundamental group $\mathbb{Z} \oplus \mathbb{Z}$. This problem does not happen for COMPACT Lie groups (where every finite cover is algebraic).

We have done $O_{4,0}, O_{3,1}$, and $O_{2,2}$, from which we can obviously get $O_{1,3}$ and $O_{0,4}$. Note that $O_{4,0}(\mathbb{R}) \cong O_{0,4}(\mathbb{R})$, $SO_{4,0}(\mathbb{R}) \cong SO_{0,4}(\mathbb{R})$, $\mathrm{Spin}_{4,0}(\mathbb{R}) \cong \mathrm{Spin}_{0,4}(\mathbb{R})$. However, $\mathrm{Pin}_{4,0}(\mathbb{R}) \not\cong \mathrm{Pin}_{0,4}(\mathbb{R})$. These two are hard to distinguish. We have

Take a reflection (of order 2) in $O_{4,0}(\mathbb{R})$, and lift it to the Pin groups. What is the order of the lift? The reflection vector v, with $v^2 = \pm 1$ lifts to the element $v \in \Gamma_V(\mathbb{R}) \subseteq C_V^*(\mathbb{R})$. Notice that $v^2 = 1$ in the case of $\mathbb{R}^{4,0}$ and $v^2 = -1$ in the case of $\mathbb{R}^{0,4}$, so in $\mathrm{Pin}_{4,0}(\mathbb{R})$, the reflection lifts to something of order 2, but in $\mathrm{Pin}_{0,4}(\mathbb{R})$, we get an element of order 4!. So these two groups are different.

Two groups are *isoclinic* if they are confusingly similar. A similar phenomenon is common for groups of the form $2 \cdot G \cdot 2$, which means it has a center of order 2, then some group G, and the abelianization has order 2. Watch out.

Exercise 216 $\mathrm{Spin}_{3,3}(\mathbb{R}) \cong SL_4(\mathbb{R})$.

15.2 Triality

This is a special property of 8 dimensional orthogonal groups. Recall that $O_8(\mathbb{C})$ has the root system D_4, which has an extra symmetry of order three.

But $O_8(\mathbb{C})$ and $SO_8(\mathbb{C})$ do NOT have corresponding symmetries of order three. The thing that does have the symmetry of order three is the spin group. The group $\mathrm{Spin}_8(\mathbb{R})$ DOES have "extra" order three symmetry. We can see it as follows. Look at the half spin representations of $\mathrm{Spin}_8(\mathbb{R})$. Since this is a spin group in even dimension, there are two. $C_{8,0}(\mathbb{R}) \cong \mathbb{M}_{2^{8/2-1}}(\mathbb{R}) \times \mathbb{M}_{2^{8/2-1}}(\mathbb{R}) \cong \mathbb{M}_8(\mathbb{R}) \times \mathbb{M}_8(\mathbb{R})$. So $\mathrm{Spin}_8(\mathbb{R})$ has two 8 dimensional real half spin representations. But the spin group is compact, so it preserves some quadratic form, so we get 2 homomorphisms $\mathrm{Spin}_8(\mathbb{R}) \to SO_8(\mathbb{R})$. So $\mathrm{Spin}_8(\mathbb{R})$ has THREE 8 dimensional representations: the half spins, and the one from the map to $SO_8(\mathbb{R})$. These maps $\mathrm{Spin}_8(\mathbb{R}) \to SO_8(\mathbb{R})$ lift to Triality automorphisms $\mathrm{Spin}_8(\mathbb{R}) \to \mathrm{Spin}_8(\mathbb{R})$. The center of $\mathrm{Spin}_8(\mathbb{R})$ is $(\mathbb{Z}/2)+(\mathbb{Z}/2)$ because the center of the Clifford group is $\pm 1, \pm\gamma_1 \cdots \gamma_8$. There are 3 non-trivial elements of the center, and quotienting by any of these gives you something isomorphic to $SO_8(\mathbb{R})$. This is special to 8 dimensions.

15.3 More about Orthogonal groups

Is $O_V(K)$ a simple group? NO, for the following reasons:

(1) There is a determinant map $O_V(K) \to \pm 1$, which is usually onto. (In characteristic 2 there is a similar Dickson invariant map).

(2) There is a spinor norm map $O_V(K) \to K^\times/(K^\times)^2$

(3) $-1 \in$ center of $O_V(K)$.

(4) $SO_V(K)$ tends to split if $\dim V = 4$, is abelian if $\dim V = 2$, and trivial if $\dim V = 1$.

(5) There are a few cases over small finite fields where the orthogonal group is solvable, such as $O_3(\mathbb{F}_3)$.

It turns out that they are simple apart from these reasons why they are not. Take the kernel of the determinant, to get to SO, then take the elements of spinor norm 1, then quotient by the center, and assume that $\dim V \geq 5$. Then this is usually simple, except for a few small cases over small finite fields. If K is a finite field, then this gives many finite simple groups.

Note that $SO_V(K)$ is NOT the subgroup of $O_V(K)$ of elements of determinant 1 in general; it is the image of $\Gamma_V^0(K) \subseteq \Gamma_V(K) \to O_V(K)$, which is the correct definition. Let's look at why this is right and the definition you know is wrong. There is a homomorphism $\Gamma_V(K) \to \mathbb{Z}/2\mathbb{Z}$, which takes $\Gamma_V^0(K)$ to 0 and $\Gamma_V^1(K)$ to 1 (called the Dickson invariant). It is easy to check that $\det(v) = (-1)^{\text{Dickson invariant}(v)}$. So if the characteristic of K is not 2, $\det = 1$ is equivalent to Dickson $= 0$, but in characteristic 2, determinant is a useless invariant (because it is always 1) and the right invariant is the Dickson invariant.

Special properties of $O_{1,n}(\mathbb{R})$ and $O_{2,n}(\mathbb{R})$. $O_{1,n}(\mathbb{R})$ acts on hyperbolic space $\mathbb{H}^n$, which is a component of norm -1 vectors in $\mathbb{R}^{n,1}$. $O_{2,n}(\mathbb{R})$ acts on the "Hermitian symmetric space" (Hermitian means it has a complex structure, and symmetric means really nice). There are three ways to construct this space:

(1) It is the set of positive definite 2 dimensional subspaces of $\mathbb{R}^{2,n}$

(2) It is the norm 0 vectors ω of $\mathbb{PC}^{2,n}$ with $(\omega, \bar{\omega}) = 0$.

(3) It is the vectors $x + iy \in \mathbb{R}^{1,n-1}$ with $y \in C$, where the cone C is the interior of the norm 0 cone.

Exercise 217 Show that these are the same.

15.4 Spin groups in small dimensions

Here we summarize the special properties of orthogonal and spin group is dimensions up to 8.

1. In 1 dimension the groups are discrete.
2. Here the special orthogonal and spin groups are abelian
3. The spin group $Spin_3(\mathbb{R})$ is isomorphic to the special unitary group SU_2. This is because the half-spin representation has dimension 2.
4. Spin groups have a tendency to split. The two half-spin representations have dimension 2, so we get two homomorphisms to SL_2. (Spin groups in this dimension do not always split: for example the spin group $Spin_{1,3}(\mathbb{R})$ of special relativity is locally isomorphic to $SL_2(\mathbb{C})$ which is simple modulo its center.)
5. The spin group is isomorphic to a symplectic group Sp_4. This is because the spin representation has dimension 4 and has a skew symmetric form.
6. The spin group is isomorphic to $SU_4(\mathbb{R})$. This is because the half-spin representation has dimension 4.
7. The spin group $Spin_7(\mathbb{R})$ acts transitively on the sphere S^7 in the spin representation (of dimension 8) and the subgroup fixing a point is the exceptional group G_2.
8. The two half-spin representations of dimension 8 have the same dimension as the vector representation, and have symmetric invariant bilinear forms. The spin group has a triality outer automorphism of order 3, permuting the two half-spin representations and the vector representation.

15.5 String groups

If we start with the orthogonal group (of a finite dimensional positive definite real vector space), it has nontrivial zeroth homotopy group, and we can kill this by taking its connected component, the special orthogonal group. This has non-trivial first homotopy group of order 2, and we can kill this by taking its spin double cover. This process of killing the lowest homotopy group can be continued further as

$$1 \cdots \to \mathrm{String}(n) \to \mathrm{Spin}(n) \to \mathrm{SO}(n) \to \mathrm{O}(n)$$

The first nonvanishing homotopy group of the spin group is the third homotopy group, which is $\mathbb{Z}$. The result of killing the third homotopy group of a spin group is called a string group. At first sight this seems impossible to construct: one problem is that any nonabelian compact Lie group has non-trivial third homotopy group. However it is possible to kill the third homotopy group if one allows non-compact infinite dimensional groups.

Stolz gave the following construction of the string group of a spin group G. Take the PU bundle P over G corresponding to a generator of $\pi_3(G)$, where PU is the projective unitary group of an infinite dimensional separable Hilbert space and is an Eilenberg-Maclane space $K(\mathbb{Z}, 2)$. This follows because the infinite dimensional unitary group U is contractible, and we have a fibration

$$1 \to \text{Circle group} \to U \to PU \to 1$$

so by the long exact sequence of homotopy groups we see that $\pi_n(S^1) = \pi_{n+1}(PU)$. Then the string group is the group of bundle automorphisms that act on the space G as left translations by elements of G. So we have an exact sequence

$$1 \to \text{Gauge group} \to \text{String group} \to \text{Spin group} \to 1$$

A similar construction works if the spin group is replaced by any simply connected simple compact Lie group, since all such groups are 2-connected and have infinite cyclic 3rd homotopy groups.

The construction of the string group from the spin group is similar to the construction of the spin group from the special orthogonal group. In the latter case one takes the $\mathbb{Z}/2\mathbb{Z}$ bundle over $SO_n(\mathbb{R})$, and the spin group is the group of bundle automorphisms lifting translations of the special orthogonal group.

In high dimensions the 4th, 5th, and 6th homotopy groups of the spin group and string group also vanish. One can continue this process further; killing the 7th homotopy group of the string group produces a group called the fivebrane group.

16 Symplectic groups

Symplectic groups are similar to orthogonal groups, but somewhat easier to handle. Over a field there are usually many different non-singular quadratic forms of given dimension, but only 1 alternating form in even dimensions, and none in odd dimensions.

Symplectic groups in dimension $2n$ are easily confused with orthogonal groups in dimension $2n+1$. They have the same dimension $n(2n+1)$, the same Weyl group, and almost the same root system, and they are locally isomorphic for $n \leq 2$. In the early days of Lie group Killing thought at first that they were the same. Over fields of characteristic 2 they do become essentially the same: to see this, consider a quadratic form q in a vector space V of dimension $2n+1$. Its associated symmetric bilinear form is alternating since the characteristic is 2, so has a vector z in its kernel. So any rotation of V induces an linear transformation of the $2n$-dimensional vector space V/z preserving its induced symplectic form. So in characteristic 2 we get a homomorphism from an orthogonal group in dimension $2n+1$ to the symplectic group in dimension $2n$.

We can work out the root system in much the same way that we found the root system of an orthogonal group in even dimensions. We take the symplectic form to be the one with blocks of $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ down the diagonal. The Cartan subalgebra is then the diagonal matrices with $(\alpha_1, -\alpha_1, \alpha_2, -\alpha_2, \ldots)$ down the diagonal, just as for orthogonal groups in even dimensions. We get elements $\pm\alpha_i \pm \alpha_j$ as roots just as for even orthogonal groups, but we also get extra roots $\pm 2\alpha_i$. This root system is called C_n. It is just like B_n except that the roots $\pm\alpha_i$ are doubled to $\pm 2\alpha_i$. In particular the Weyl group is the same in both cases and is just the group $(\mathbb{Z}/2\mathbb{Z})^n S_n$ of order $2^n n!$.

Exercise 218 Show that if n is 1 or 2 then the root system B_n is isomorphic to C_n (up to rescaling) but if $n \geq 3$ they are different.

We recall that $SP_4(\mathbb{C})$ is locally isomorphic to $SO_5(\mathbb{C})$. Form the point of view of $SO_5(\mathbb{C})$ we saw that this is related to the spin double cover of $SO_5(\mathbb{C})$, which is $Sp_4(\mathbb{C})$ as it has a 4-dimensional spin representation with an alternating form. We can see this more easily if we start from $Sp_4(\mathbb{C})$. This has a 4-dimensional representation $\mathbb{C}^4$ with an alternating form. Its alternating square has dimension 6, and has a symmetric bilinear form as the alternating 4th power is $\mathbb{C}$. However the alternating square splits as the sum of 1 and 5 dimensional pieces, as the alternating form gives an invariant 1-dimensional piece. So $Sp_4(\mathbb{C})$ has a 5-dimensional representation with a symmetric bilinear form, and therefore has a map to the orthogonal group $O_5(\mathbb{C})$.

Exercise 219 Which of the three groups $SO_5(\mathbb{R})$, $SO_{4,1}(\mathbb{R})$, $SO_{3,2}(\mathbb{R})$ is $Sp_4(\mathbb{R})$ locally isomorphic to?

There are several ways to distinguish symplectic groups in higher dimensions from orthogonal (or rather spin) groups:

- If we know that Cartan subalgebras are all conjugate, then we can distinguish orthogonal and symplectic groups by the number of long roots in their roots system: the orthogonal groups of dimension $2n+1$ have $2n(n-1)$ long roots, while symplectic groups in dimension $2n$ have $2n$ long roots, so if $n > 2$ the groups are different.
- Another way to distinguish them is to look at the dimension of the non-trivial minuscule representation (the smallest representation on which the center of the simply connected group acts non-trivially). For orthogonal groups in dimension $2n+1$ this is the spin representation of dimension $2^n = 2, 4, 8, 16, \cdots$, while for symplectic groups in dimension $2n$ it is the representation of dimension $2n = 2, 4, 6, 8, \cdots$. Again these are different if $n > 2$.

The symmetric spaces of symplectic groups are generalizations of the upper half plane called Siegel upper half planes. The Siegel upper half plane consists of matrices in $M_n(\mathbb{C})$ whose imaginary part is positive definite (so for $n = 1$ this is the usual upper half plane). We take the symplectic form given by $\left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$ where I is the n by n identity matrix. Then the action of a symplectic matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ on an element τ of the Siegel upper half plane is given by

$$\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)(\tau) = \frac{A\tau + B}{C\tau + D}$$

Exercise 220 Check that this is indeed a well defined action of the symplectic group on the Siegel upper half plane. (One way is to use the fact that the symplectic group is generated by matrices of the form $\left(\begin{smallmatrix} I & B \\ 0 & I \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & I \\ -I & 0 \end{smallmatrix}\right)$).

We have already seen two special cases of this before: if $n = 1$ then the symplectic group Sp_{2n} is just $SL_2(\mathbb{R})$, acting on the usual upper half plane. If $n = 2$ then $Sp_{2n}(\mathbb{R})$ is locally isomorphic to $SO_{3,2}(\mathbb{R})$, and we have seen that groups $SO_{m,2}(\mathbb{R})$ have Hermitian symmetric spaces.

The theory of modular forms on the upper half plane generalizes to Siegel modular forms on the Siegel upper half planes: for example, points of the upper half plane modulo $SL_2(\mathbb{Z}) = Sp_2(\mathbb{Z})$ correspond to complex elliptic curves, while points of the Siegel upper half plane modulo $Sp_{2n}(\mathbb{Z})$ correspond to principally polarized complex abelian varieties. This is of course all a special case of the Langlands program.

The symplectic group is obviously not compact. For orthogonal groups it was easy to find a compact form: just take the orthogonal group of a positive definite quadratic form. For symplectic groups we do not have this option as there is essentially only one symplectic form. Instead we can use the following method of constructing compact forms: take the intersection of the corresponding complex group with the compact subgroup of unitary matrices. For example, if we do this with the complex orthogonal group of matrices with $AA^t = I$ and intersect it with the unitary matrices $A\overline{A}^t = I$ we get the usual real orthogonal group. In this case the intersection with the unitary group just happens to consist of real matrices, but this does not happen in general. For the symplectic group we get the compact group $Sp_{2n}(\mathbb{C}) \cap U_{2n}(\mathbb{C})$. We should check that this is a real form of the symplectic group, which means roughly that the Lie algebras of both groups have the same complexification $sp_{2n}(\mathbb{C})$, and in particular has the right dimension. We show that if V is any †-invariant complex subspace of $M_k(\mathbb{C})$ then the Hermitian matrices of V are a real form of V. This follows because any matrix $v \in V$ can be written as a sum of hermitian and skew hermitian matrices $v = (v + v^\dagger)/2 + (v - v^\dagger)/2$, in the same way that a complex number can be written as a sum of real and imaginary parts. (Of course this argument really has nothing to do with matrices: it works for any antilinear involution † of any complex vector space.) Now we need to check that the Lie algebra of the complex symplectic group is †-invariant. This Lie algebra consists of matrices a such that $aJ + Ja^T = 0$; this is obviously closed under complex conjugation, and is closed under taking transposes if we choose J so that $J^2 = 1$.

For orthogonal groups we can find an index 2 subgroup because the determinant can be positive or negative, and one might guess that one can do something similar for symplectic groups. However for symplectic groups the determinant is always 1:

Lemma 221 *if B is a symplectic matrix preserving the non-degenerate alternating form of A, so that $BAB^t = A$, then* $\det(B) = 1$.

Proof A non-degenerate alternating form on a $2n$-dimensional vector space V gives a 2-form ω in $\Lambda^2(V)$ and $\omega \wedge \cdots \wedge \omega$ is a non-degenerate $2n$-form preserved by B, So B has determinant 1, as the determinant is the amount by which a matrix multiplies a nondegenerate $2n$-form. □

For example, Riemannian manifolds, where the structure group is reduced to the orthogonal group, can be non-orientable, but symplectic manifolds, where the structure group is reduced to the symplectic group, are always orientable.

Definition 222 *An alternating form can be represented by an alternating matrix A. Since this is equivalent to the standard form J with diagonal blocks $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ we can write the matrix as TJT^t for some T. Any two matrices T differ by a symplectic matrix that necessarily has determinant 1, so the determinant of T depends only on A and is called the Pfaffian of the alternating matrix A.*

(More generally, the Pfaffian is really a function of two alternating forms on a vector space, given by the determinant of a map taking one to the other.)

The Pfaffian can also be given as follows: the highest degree part of

$$\exp(\sum A_{ij}\omega_i \wedge \omega_j) = \mathrm{Pf}(A)\omega_1 \wedge \cdots \wedge \omega_{2n}$$

.

Exercise 223 If A is alternating and B is any matrix show that

$$\mathrm{Pf}(BAB^t) = \det(B)\mathrm{Pf}(A)$$

$$\det(A) = \mathrm{Pf}(A)^2$$

We can write the determinant as the square of an explicit polynomial in the entries of A.

Lemma 224 *If A is a skew symmetric matrix over a field of characteristic 0, the Pfaffian of A is given by*

$$\omega^n = 2^n n! Pf(A) e_1 \wedge \cdots \wedge e_n$$

where $\omega = \sum_{i,j} a_{ij} e_i \wedge e_j$.

We can write this as

$$Pf(A) = \frac{1}{2^n n!} \sum_{w \in S_{2n}} \epsilon(w) a_{w(1)w(2)} a_{w(3)w(4)} \cdots$$

and since each term on the right occurs $2^n n!$ times, we get a definition of the Pfaffian over any commutative ring by just summing over the permutations with $w(1) < w(3) < w(5) \cdots$, $w(1) < w(2)$, $w(3) < w(4), \cdots$.

Exercise 225 Find the Pfaffian of

$$\begin{pmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{pmatrix}$$

Example 226 The orthogonal group acts on its Lie algebra, which is the vector space of skew symmetric real matrices. We can ask about the invariants of $O_n(\mathbb{R})$ and its subgroup $SO_n(\mathbb{R})$ for this representation, in other words the polynomials in the entries of A that are invariant under changing A to BAB^{-1} for B an orthogonal or special orthogonal matrix (so $B^{-1} = B^t$). By the formula $\mathrm{Pf}(BAB^t) = \det(B)\mathrm{Pf}(A)$, we see that the Pfaffian is an invariant of the special orthogonal group, but changes sign under reflections. In fact the invariants of the special orthogonal group form a 2-dimensional module over the invariants of the orthogonal group, with a basis given by 1 and the Pfaffian.

16.1 Perfect matchings and domino tilings

The Pfaffian turns up in several problems of statistical mechanics, where it can sometimes be used to give exact solutions in 2 dimensions. As an example we will use it to count the number of perfect matchings of a bipartite planar graph. (Bipartite means that the vertices can be colored black and white such that the two endpoints of any edge have different colors, or equivalently that all cycles have even length.) The idea is to write this number as the Pfaffian of a matrix, and then evaluate the determinant of the matrix by diagonalizing it.

We can form the adjacency matrix of this graph with $a_{ij} = 0, 1$ counting the number of edges from vertex ii to vertex j, and can see that the Pfaffian of this adjacency matrix would b the number of bipartite matchings if it were not for the signs in the Pfaffian. The idea is to cleverly change the signs of some of the entries in the adjacency matrix to nullify the signs in the Pfaffian.

Order the vertices of the graph, and call a cycle odd or even depending on whether as we go around the cycle we have an odd or even number of edges where we go to a larger vertex. (This does not depend on which way we transverse the cycle as the cycle has even length.)

Suppose we label each edge of the graph with a sign. Now we take the adjacency matrix of the graph, and change signs of its entries as follows.

- First change the sign of a_{ij} so that it has the same sign as the corresponding edge of the graph.
- Then make it antisymmetric by changing the sign of a_{ij} if $i < j$.

Lemma 227 *Suppose that for every cycle the product of signs in the cycle of length a is $(-1)^{a/2+1}$ if the cycle is even and minus this if the cycle is odd. Then the Pfaffian of the matrix above is (up to sign) the number of perfect matchings of the graph.*

Proof The non-zero terms of the expansion of the Pfaffian correspond to perfect matchings. The problem is to check that any two terms have the same sign.

Suppose that we have two perfect matchings. Color the edges of one red, and the edges of the other blue. Then we get a collection of even length cycles, whose edges alternate red and blue. (These are allowed to have one double edge colored both red and blue.) We examine a single cycle $v_1v_2 \cdots v_{2k}$ and check that the sign of the term of the Pfaffian does not change if we switch from the red to the blue edges. The sign of the red edges comes from:

- The sign of the permutation $v_1v_2 \cdots v_{2k}$.
- The number of pairs $v_{2i-1}v_{2i}$ that are decreasing (using the order of the vertices)
- The number of pairs $v_{2i-1}v_{2i}$ whose edge has sign -1.

while the sign of the blue permutation comes from

- The sign of the permutation $v_2 \cdots v_{2k}v_1$.
- The number of pairs $v_{2i}v_{2i+1}$ that are decreasing (using the order of the vertices)

- The number of pairs $v_{2i}v_{2i+1}$ whose edge has sign -1.

So we pick up a factor of -1 as the sign of a cycle of length $2n$, and a factor of -1 each time the vertices decrease as we go around the cycle, and a factor of -1 for each edge of the cycle whose edge has sign -1. By assumption the signs of the edges are chosen so that these signs cancel out over every cycle. □

Exercise 228 If we have a planar bipartite graph then we can assign signs to each edge so that the product of signs in a cycle of length a is $(-1)^{a/2+1}$ if the cycle is even and minus this if the cycle is odd. (By induction on the size of the graph we can arrange that this is true for the cycles bounding faces of the planar graph (remove an outer edge, add signs to the remainder of the graph, then add a sign to the removed edge so that its face has the correct number of signs). Then check that all cycles, not just those bounding faces, have the correct parity of signs by induction on the number of faces inside the cycle.)

Example 229 We use this to count the number of domino tilings of a chessboard, or more generally an $m \times n$ rectangle. The number of domino tilings of a chessboard is the number of bipartite matchings of the graph formed by joining all centers of squares to the centers of adjacent squares. We have to choose an ordering of the vertices and signs for the edges satisfying the condition above. We choose lexicographic ordering of vertices. Then every 1 by 1 square has 2 increases as we go around it, so needs an odd number of signs on its edges. We can achieve this by putting signs on the horizontal edges of rows $2, 4, 6, \ldots$. We let Q_n be the $n \times n$ matrix with 1s just above the diagonal, -1 just below it, and 0s elsewhere. We let I_n be the $n \times n$ identity matrix. We let F_n be the diagonal matrix whose entries alternate 1 and -1. Then the matrix whose Pfaffian we want to evaluate is

$$Q_n \otimes I_m + F_n \otimes Q_m$$

Here Q_n comes from the horizontal edges, Q_m from the vertical edges, and F_n comes from the fact that we twiddle the signs of the edges in even rows.

Now we find the determinant of this matrix by (almost) diagonalizing it. First we diagonalize Q_n by finding its eigenvectors. If $(a_1, a_2, \cdots)$ is an eigenvector with eigenvalue λ, then $-a_{k-1} + a_{k+1} = \lambda a_k$ (with $a_0 = a_{n+1} = 0$). This is a difference equation for a_k with solution $a_k = z_1^k - z_2^k$ where $z_1^{n+1} - z_2^{-n-1} = a_{n+1} = 0$, $z_1 z_2 = -1$, $z_1 + z_2 = \lambda$ so $z_1 = e^{(2j+n+1)\pi i/2(n+1)}$ for integers j. The eigenvalue λ is $z_1 + z_2 = 2i\sin((2j+n+1)\pi/2(n+1)) = 2i\cos(j/(n+1))$.

If we replaced F_n by I_n we would be finished, because the vectors $v_i \otimes v_j$ would be a set of eigenvectors for out matrix, where v_i and v_j run through eigenvectors of the matrices Q. We now seem to run into a problem, because the matrices F_n and Q_n do not commute, so we cannot simultaneously diagonalize them. However they are not too far from commuting: in fact $F_nQ_n = -Q_nF_n$. This means that F_n switches the eigenspaces of Q with eigenvalues λ and $-\lambda$, so (at least when λ is nonzero) we can find a basis of eigenvectors of Q_n in which F_n can be written with 2 by 2 blocks $\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ down the diagonal.

What is really going on is that we have a representation of the algebra generated by Q_n, Q_m, and F_n on a space of dimension mn, and the key point is that this representation breaks up as a sum of small representations of dimension at most 2.

So the mn by mn matrix can be written with $mn/2$ diagonal 2 by 2 blocks, each of the form

$$\begin{pmatrix} 2i\cos(j/(n+1)) & 2i\cos(k/(m+1)) \\ 2i\cos(k/(m+1)) & 2i\cos(j/(n+1)) \end{pmatrix}$$

down the diagonal. We could diagonalize this, but there is not much point as all we need is its determinant which is easy to evaluate. The determinant is the product of the determinants of all these 2 by 2 blocks, which is the square root of

$$\prod_{j=1}^{n}\prod_{k=1}^{m}(2i\cos(j/(n+1)))^2+(2i\cos(k/(m+1)))^2$$

So the number of domino tilings is (up to sign) the Pfaffian, in other words the 4th root of the absolute value of this product. For example, there are 12988816 domino tilings of a chessboard.

17 Cayley numbers and G2

Definition 230 *A (possibly nonassociative) algebra is called alternative if for all a and b we have $(aa)b = a(ab)$ and $b(aa) = (ba)a$.*

Alternative algebras have the apparently more general property that the subalgebra generated by any two elements is associative.

The Cayley-Dickson construction turns an algebra into another one of twice the dimension as follows. Suppose that A is a module over some commutative ring with a bilinear product (possibly nonassociative and non-commutative) and an involution $*$ with $(ab)^* = b^*a^*$, $a^{**} = a$. For $\gamma \in R$ we define an involution and product on $A \oplus A$ by

$$(p,q)(r,s) = (pr - \gamma s^*q, sp + qr^*)$$

$$(p,q)^* = (p^*, -q)$$

We will assume that A has an identity 1 and that $a + a^*$ and aa^* are always multiples of 1. Then the same is true of $A \oplus A$. Moreover if A is commutative and $* = 1$ then $A \oplus A$ is commutative, and if A is commutative and associative then $A \oplus A$ is associative, and if A is associative then $A \oplus A$ is alternative.

Starting with the real numbers, and taking γ to be 1 at every step, we get the real numbers, the complex numbers, the quaternions, and the octonions (or Cayley numbers), an 8-dimensional alternative algebra over the reals. We could of course continue further to get algebras of dimension 16, 32, and so on, but it seems to be rather hard to think of anything interesting to say about them.

We define the norm $N(a)$ to be $a^*a = aa^*$. When the algebra A is alternative, we have $N(ab) = N(a)N(b)$, and in particular the norms of elements are closed under multiplication. If $N(a)$ is invertible in R then a has an inverse $a^{-1} = a/N(a)$, with $a^{-1}(ab) = b = (ba)a^{-1}$. In particular the octonions form a nonassociative division algebra.

Exercise 231 In a commutative ring, show that the set of sums of n squares is closed under multiplication if n is 1, 2, 4, or 8. (There are no other positive integers for which this is true for all commutative rings.)

If we apply this construction to the complex numbers we get the quaternions, with a basis $1, i, j, k$ and products $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

Exercise 232 Show that the manifold of octonions of norm 1 and trace 0 has an almost complex structure (in other words each tangent space can be made into a complex vector space in a smooth way) and is diffeomorphic to the sphere S^6. (The spheres S^0, S^2, and S^6 are the only spheres with almost complex structures. It is not known whether the sphere S^6 has a complex structure.)

Now we investigate the automorphism group G of the octonions. It is compact as it is a closed subgroup of the orthogonal group in 8 (or even 7) dimensions. We start finding an upper bound on its dimension. The group G acts on the octonions orthogonal to 1, and preserves norms, so it acts on the sphere S^6 of imaginary octonions of norm 1. Now look at the subgroup H fixing some point i of this sphere. In turn H acts on the sphere of all points of norm 1 orthogonal to 1 and i, which is a 5-sphere S^5. Fix j in this 5-sphere, with i and j generating a copy of the quaternions. Now look at the group fixing i and j. This acts on the sphere S^3 of unit octonions orthogonal to $1, i, j, ij$. Since the octonions are generated by i, j, and a point of this 3-sphere, we see that G has dimension at most $3 + 5 + 6 = 14$.

We want to show that G has exactly dimension 14, so we need to construct enough elements of G to show that the various actions on spheres above are transitive, in other words we need to find some automorphisms of the Cayley numbers. An automorphism is given by mapping (p, q) to (p, rq) for a suitable quaternion: if we look at the formula for multiplication we see that this is an automorphism of the octonions provided that r has norm 1.

The octonions have a basis $e_0 = 1, e_1, \cdots, e^7$ such that $e_1e_2 = e_4$ and cyclic permutations of $(1, 2, 3, 4, 5, 6, 7)$ are automorphisms of the Cayley algebra. We can identify the subspace spanned by $1, e_1, e_2, e_4$ with a copy of the quaternions. We will show that this automorphism of order 7, together with the automorphisms of the form $(p, q) \to (p, rq)$ generate the full automorphism group. In fact we will just use this 3-dimensional group and its 6 conjugates under elements of the cyclic group of order 7. In particular the group of automorphisms fixing e_1, e_2, e_4 acts transitively on the norm 1 vectors that are linear combinations of e_3, e_5, e_6, e_7, and similarly for all cyclic permutations.

We show that the automorphism group acts transitively on the sphere S^6 of norm 1 imaginary octonions. Pick a vector in this sphere. We can first kill off the coefficients of e_5, e_6, e_7. Then by acting with the group fixing e_6, e_7, e_2 we can keep the coefficients of e_6, e_7 zero and kill off the coefficients of e_3, e_4, e^5. Then by acting with the group fixing e_4, e_6, e_7 we can make the vector equal to e_1. So G acts transitively on norm 1 imaginary octonions. .

Now we show that the subgroup fixing e_1 acts transitively on the sphere S^5 of imaginary norm 1 octonions orthogonal to e_1 in a similar way. We first act with the group fixing e_1, e_2, e_4 to kill off the coefficients of e_5, e_6, e_7. Then act with the group fixing e_7, e_1, e_3 to kill off the coefficients of e_4, e_5, e^6, keeping the coefficient of e_7 zero. Finally we act with the group fixing e_5, e_6, e_1 to move the element to e_2.

The subgroup fixing the two vectors e_1 and e_2 (and therefore also $e_1e_2 = e_4$, acts transitively on the sphere S^3 of norm 1 imaginary octonions orthogonal to these three vectors. So we have verified that the group G_2 of automorphisms of the Cayley numbers has dimension exactly 14.

We can read off more information about G_2. We found subgroups A, B with $G/A = S^6$, $A/B = S^5$, $B = S^3$. From this we see that G_2 is connected, simply connected, and (using the exact sequence of homotopy groups of a fibration) the second homotopy group vanishes, and the third is Z.

Obviously any automorphism of the quaternions gives an automorphism of the octonions $H \oplus H$ as the construction of the octonions from the quaternions is functorial.

Exercise 233 There is an obvious guess for a maximal integral form for the octonions, analogous to the Hurwitz quaternions, which is to take the octonions whose coordinates are integers or half integers, such that the set with half integer parts is empty or the image of $(\infty 124)$ under $Z/7Z$ or the complement of one of these sets. However this does not work (and is a common error). Show that this integral form is not closed under multiplication. Show that if we swap ∞ and n in the set of allowed integral parts for some fixed $n \in \mathbb{Z}/7\mathbb{Z}$ (where $1 = e_\infty$) we get an integral form of the octonions that is closed under multiplication. Show that the lattice we get is the E_8 lattice up to rescaling, and there are 240 integral vectors of norm 1.

Exercise 234 Show that the compact group G_2 is the group of automorphisms of R^7 (with basis $x_0, x_1, \ldots, x_6$) preserving the element

$$x_0\wedge x_1\wedge x_3+x_1\wedge x_2\wedge x_4+x_2\wedge x_3\wedge x_5+x_3\wedge x_4\wedge x_6+x_4\wedge x_5\wedge x_0+x_5\wedge x_6\wedge x_1+x_6\wedge x_0\wedge x_2$$

of $\wedge^3(R^7)$. The can be thought of as a sum over the 7 lines of the 7-point projective plane of the field with 2 elements.

Exercise 235 Find a Cartan subalgebra and the root system of G_2. (Start by looking at the subgroup fixing a point of S_6. This is isomorphic to $SU(3)$, of dimension 8, so gives the Cartan subgroup and 6 of the roots arranged as the vertices of a hexagon. If the hexagon is written as 6 triangles, the remaining 6 roots are at the centers of the 6 triangles, so there are 6 short roots and 6 long roots that are $\sqrt{3}$ times as long.)

18 Root systems and reflection groups

We have seen that simple complex Lie algebras have a root system associated to them: this means a finite set of non-zero vectors in Euclidean space, called roots, such that r and s are roots then (r, s) is an integer multiple of $(r, r)/2$ and the reflection $s - 2r(r, s)/(r, r)$ of s in $r^\perp$ is also a root. In particular for every root system we have a Weyl group generated by reflections. The correspondence between semisimple complex Lie algebras and root systems is not quite 1:1 because the root system of a semisimple complex Lie algebra is also reduced: this means that it r is a root then $2r$ is not a root. An example of a non-reduced root system is BC_n, consisting of the vectors $\pm x_i$, $\pm x_i \pm x_j$, and $\pm 2x_i$. In fact these are the only irreducible non-reduced root systems. They are in fact roots systems of finite dimensional simple superalgebras. Most but not all reflection groups in Euclidean space turn up as Weyl groups of Lie groups:

the exceptions are most dihedral groups, the symmetries of an icosahedron, and a group in 4-dimensions.

The classification of root systems and reflection groups is similar. We will do the case of root systems all of whose roots have the same length; the general case uses no essentially new ideas.

The first step is to consider the Coxeter diagram of a reflection group, or the Dynkin diagram of a root system. These are defined as follows. Chop up space by cutting along the reflection hyperplanes. The closed regions bounded by these hyperplanes are called Weyl chambers. Any Weyl chamber is conjugate to its neighbors by a reflection, so all Weyl chambers are conjugate by elements of the reflection group. We pick one Weyl chamber. The Coxeter diagram has a point for each face of the Weyl chamber, and lines between the points according to the angle between faces. If the faces are orthogonal there are no lines, if the faces have an angle of $\pi/3$ there is 1 line, if the faces have an angle of $\pi/4$ there are two lines, and for other angles conventions vary. A Dynkin diagram of a root system is like a Coxeter diagram, with some extra information to indicate the lengths of the roots (which is not defined for arbitrary reflection groups). Usually one draws an inequality sign on the lines to indicate the longest of each pair of roots. (For finite root systems this gives enough information to reconstruct the root system, though for infinite root systems one sometimes needs more information.)

We will work out the Dynkin diagrams of the most of the root systems we have seen.

- A_n: simple roots $\alpha_i - \alpha_{i+1}$
- B_n: simple roots $\alpha_i - \alpha_{i+1}$, α_n
- C_n: simple roots $\alpha_i - \alpha_{i+1}$, $2\alpha_n$
- D_n: simple roots $\alpha_i - \alpha_{i+1}$, $\alpha_{n-1} + \alpha_n$
- E_8 $\alpha_i - \alpha_{i+1}$, $(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 + \alpha_5 - \alpha_6 - \alpha_7 - \alpha_8)/2$

  Exercise 236 what happens if there are 4, 6, 7, or 8 minus signs in this last simple root? Why do these not give Dynkin diagrams for the E_8 root system?

- F_4: $\alpha_1 - \alpha_2$, $\alpha_2 - \alpha_3$, α_3, $-(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)/2$.
- G_2:

A_n, B_n, C_n, D_n, G_2

These Dynkin diagrams explain the numerous local isomorphisms between small simple Lie groups.

- The Dynkin diagrams of A_1, B_1, and C_1 are all points, corresponding to the fact that SL_2, $O_{2,1}$, and Sp_2 are locally isomorphic.
- The Dynkin diagrams of B_2 and C_2 are isomorphic, corresponding to the local isomorphism of SP_4 and $O_{3,2}$.

- The Dynkin diagrams of B_n and C_n are almost the same, explaining why the Lie groups of Sp_{2n} and O_{2n+1} have the same dimension and the same Weyl group.
- The Dynkin diagram of D_2 is two points, corresponding to the fact that $O_{2,2}$ locally splits as $SL_2 \times SL_2$.
- The Dynkin diagram of D_3 is isomorphic to A_3, corresponding to the local isomorphism of SL_4 and $O_{3,3}$.
- The Dynkin diagram of D_4 has an extra automorphism of order 3, corresponding to triality of $Spin_8$.
- The Dynkin diagrams of A_n and D_n have automorphisms of order 2, corresponding to outer automorphisms of SL_{n+1} and O_{2n} given by matrices of determinant -1. (Similarly E_6 has an outer automorphism.)

Coxeter diagrams also make sense for reflection groups not associated to Lie groups, and for infinite reflection groups in Euclidean or hyperbolic space,

Example 237 The Coxeter diagram of the rotations of an icosahedron is

Example 238 The group $GL_2(\mathbb{Z})$ is a reflection group acting on the upper half plane (considered as a quotient of the non-real complex numbers by complex conjugation) and is therefore a hyperbolic reflection group. A Weyl chamber consists of the complex numbers with $0 \leq \Re(z) \leq 1/2$, $|z| \geq 1$, so the Coxeter diagram is (Notice that two of the sides only meet at infinity, so the angle between them is zero.)

Example 239 Conway found the following stunning example of a Dynkin diagram. The 26 dimensional even Lorentzian lattice $II_{1,25}$ is acted on by a hyperbolic reflection group generated by the reflections of its norm -2 vectors. The Dynkin diagram of this reflection group is the affine Leech lattice. The reaction of many mathematicians to this statement is to regard it as nonsense, on groups that a Dynkin digram is a graph, not a lattice in Euclidean space. However the Dynkin diagram is really the set of simple roots of a root system, and in particular is a metric space. (The graph is just a convenient way of describing this metric space). The Leech lattice is also a metric space, and Conway showed these two metric spaces are isometric. The isometry can be described explicitly as follows: the lattice $II_{1,25}$ is isomorphic to $II_{1,1} \oplus \Lambda(-1)$ where $\Lambda(-1)$ is the Leech lattice with norms multiplied by -1, so we can write an element of the lattice as $(m, n, \lambda) \in \mathbb{Z} \oplus \mathbb{Z} \oplus \Lambda$, with norm $2mn - \lambda^2$. The simple roots are the vectors $(1, \lambda^2/2 - 1, \lambda)$ for $\lambda \in \Lambda$. It is straightforward to show that these are some of the simple roots of a Weyl chamber; the hard part of Conway's theorem is to show that there are no further simple roots, which follows easily from the rather deep fact that the Leech lattice has covering radius $\sqrt{2}$.

We will classify the connected Dynkin diagrams X of finite reflection groups such that all roots have the same length 2. The general case is similar but has more cases to check. To do this we look at the affine diagrams of A_n, D_n, and E_n. For each of these there is a positive linear combination of roots with norm 0, so X cannot contain any of these affine diagrams.

Since X does not contain affine A_n it has no cycles, so is a tree.

Since X does not contain affine D_4, all vertices have valence at most 3.

Since X does not contain affine D_n for $n \geq 5$, there is at most one vertex of valence 3.

So either X is a line (in other words A_n) or it has one vertex of valence 3, and 3 branches of lengths a, b, $c \geq 1$.

Since X does not contain affine E_6, not all of a, b, c are at least 2, so one, say a, must be 1.

If another of b, c is also 1 then X is a D_n diagram, so we can assume b and c are both at least 2.

Since X does not contain affine E_7, b and c cannot both be at least 3, so one of them, say b must be 2.

Since X does not contain affine E_8, c must be at most 4. So the only remaining possibilities are $a = 1$, $b = 2$, $c = 2, 3, 4$ which give the E_6, E_7, and E_8 Dynkin diagrams.

Exercise 240 Classify the Dynkin diagrams of finite reflection groups that may contain roots of different lengths. The main change is that there is more than one affine Dynkin diagram associated to a finite Dynkin diagram with roots of different lengths.

There are several generalizations of this classification. First, one can classify the finite reflection groups without worrying about roots. This amalgamates the B_n and C_n cases, and introduces some reflection groups that do not correspond to Lie algebras: the dihedral groups in dimension 2, and two reflection groups H_3 (symmetries of an icosahedron) and H_4 in dimensions 3 and 4. More generally Shephard and Todd classified the finite complex reflection groups, finding 3 infinite series and 34 exceptions. There have been several attempts to find algebraic objects generalizing Lie algebras corresponding to these more general reflection groups, but as far as I know no-one has yet come up with a really compelling answer. One generalization that does correspond to Lie algebras is Euclidean or hyperbolic root systems, which correspond to Kac-Moody algebras.

19 Quivers and tilting

We will describe an unexpected connection between representations of quivers and simple Lie algebras. To summarize, the quivers with a finite number of indecomposable representations correspond to certain semisimple Lie algebras, the indecomposable representations correspond to positive roots, and the irreducible representations correspond to simple roots.

Definition 241 *A quiver is a finite directed graph (possible with multiple edges and loops). A representation of a quiver (over some fixed field) consists of a vector space for each vertex of the graph and a linear map between the corresponding vector spaces for each edge.*

Example 242 Representations of a point are just vector spaces. Representations of a point with a loop are vector spaces with an endomorphism. Over an algebraically closed field the indecomposable representations are classified by Jordan blocks. Representations of 2 points joined by a line are just linear maps of vector spaces. There are 3 indecomposable representations: a map from a 0-dimensional space to a 1-dimensional one, a map from a 1-dimensional space to a 0-dimensional one, and a map from a 1-dimensional space onto a 1-dimensional one. More generally, stars with n incoming arrows correspond to n maps to a vector space. When $n = 2$ there are 6 indecomposable representations, and when $n = 4$ there are 12. When $n = 4$ there is a qualitative change: there are now infinitely many indecomposables. For example we can take 4 1-dimensional subspaces of a 2-dimensional space. The first two determine a base $(0, 1)$ and $(1, 0)$, the third is spanned by $(1, 1)$ and determines the ratio between the two bases, but nor the 4th space can be spanned by $(1, a)$ for any a, so we get a 1-parameter family of indecomposables. Although there are an infinite number of indecomposables, it is not hard to classify them explicitly: it is a "tame" problem. For stars with 5 incoming vertices the indecomposable representations are "wild": there is no neat description of them. We will see that the cases with a finite number of indecomposables correspond to Dynkin diagrams of the finite dimensional semisimple Lie algebras with all roots the same length, and the tame cases correspond to affine Dynkin diagrams.

The representations of a quiver are the same as modules over a certain ring associated with the quiver. This ring has an idempotent for each vertex, with the idempotents commuting and summing to 1. There is also an element for each edge, subject to some obvious relations. The algebra is finite dimensional if the quiver contains no cycles.

There are two titling functors we can apply to modules over quivers:

- If a vertex a is a source, then we can change all the arrows to point into a, and change the vector space of a to be $Coker(V_a \mapsto \oplus_{a \to b} V_b)$.
- If a vertex a is a sink, then we can change all the arrows to point out of a, and change the vector space of a to be $Ker(\oplus_{b \to a} V_b \mapsto V_a)$

The functors take representations of a quiver to representations of a different quiver, with a source changed to a sink or a sink changed to a source. They are almost but not quite inverses of each other. They are inverses provided $V_a \mapsto \oplus_{a \to b} V_b$ is injective, or $\oplus_{b \to a} V_b \mapsto V_a$ is surjective. In particular they are inverses of each other on indecomposable modules, except for the special case of indecomposable modules of total dimension 1.

The idea is that we try to classify irreducible modules by repeated applying tilting functors, trying to make the module vanish. If we succeed then we can recover the original module from a 1-dimensional module by applying the "almost inverse" tilting functors in the opposite order. We will see that we can do this provided the quiver is one of the diagrams A_n, D_n, E_6, E_7, and E_8,

Take a vector space spanned by the vertices of a quiver, and give it an inner product such that the vertices of a quiver have norm 2, and their inner product is minus the number of lines joining them. Then the dimension vector of a quiver can be represented by a point in this space in the obvious way, and the effect of tilting by a source or sink a is just reflection in the hyperplane $a^\perp$ (except on the vector a itself).

We want to find a sequence of tiltings so that the dimension vector has a negative coefficient. It is easy enough to find a sequence of reflections of simple roots that do this: the problem is that we have a constraint that we can only use a reflection of a simple root if it is a source or a sink for the quiver. To do this we will use Coxeter elements.

A Coxeter element of a reflection group is a product of the reflections of simple roots in some order.

Lemma 243 *If a Coxeter element of a reflection group fixes a vector then the vector is orthogonal to all simple roots..*

Proof If a vector $a = \sum a_n v_n$ is fixed by a Coxeter element (for simple roots v_i) then the reflection of v_i is the only one that can change the coefficient of v_i, so it must fix a. So a is fixed by all reflections of simple roots, and is therefore orthogonal to all simple roots, so is 0. □

Corollary 244 *If σ is a Coxeter element of a finite reflection group and a is a non-zero vector, then $\sigma^k(a)$ has a negative coefficient for some k.*

Proof Otherwise we could find a non-zero fixed vector $a + \sigma(a) + \sigma^2(a) + \cdots + \sigma^{h-1}(a)$, where h is the order of the Coxeter element. □

Exercise 245 Show that if a Coxeter diagram of a reflection group is a tree then any two Coxeter elements are conjugate, and in particular have the same order (called the Coxeter number).

Exercise 246 Find the order of the Coxeter elements of A_n.

We now construct a special Coxeter element σ associated to a given quiver as follows. First take the reflection of some source, change the source to a sink, and then mark that vertex as used. Keep repeating this until all vertices have been used. The result is the original quiver, as each edge has had its direction changed twice. So we have found a sequence of reflections of sources that preserves the quiver. This means that we can keep on repeating the sequence of reflections of the Coxeter element, and every time we will be reflecting in some source.

We can now show that the indecomposable representations of any quiver of type A_n, D_n, or E_n correspond to the positive roots of the associated root system: in fact we can apply tiltings until the dimension vector becomes a simple root, when it is trivial to find the unique indecomposable. Take the dimension vector a of any indecomposable representation. As $\sigma^k(a)$ has negative coefficients for some k, we can find a finite sequence of tiltings so that some coefficient of the dimension vector becomes negative, which means that there is some sequence of tiltings reducing the dimension vector to a simple root. In particular the dimension vector must have been a positive root, and there is a unique indecomposable representation with this dimension vector (given by applying the sequence of tiltings in reverse order to the representation corresponding to a simple root).

For affine root systems this argument fails but only just: the inner product space spanned by simple roots has a 1-dimensional subspace that has inner product 0 with all vectors, and the dimension vector of an indecomposable is either conjugate to a simple root by a series of tiltings, or is in this 1-dimensional subspace. We saw an example of the latter for the root system of affine D_4.

Exercise 247 If a quiver contains a cycle show that it has an infinite number of inequivalent indecomposable representations. Show more precisely that there are an infinite number of dimension vectors corresponding to indecomposable representations, and (over infinite fields) there is a dimension vector with an infinite number of corresponding indecomposable representations.

For the affine diagrams of types A_n, D_n, E_6, E_7, E_8 there are an infinite number of indecomposables, but their classification is tame, meaning roughly that it can be described explicitly. The dimension vectors just correspond to the positive roots of affine Kac-Moody algebras. For non-affine diagrams the classification is wild and very hard to describe. For example for a point with two loops the representations are just pairs of matrices acting on a vector space, which are notoriously hard to classify.

20 Representation theory

A representation of a group is an action of a group on something, in other words a homomorphism from the group to the group of automorphisms of something.

The most obvious representations are permutation representations: actions of a group on a (discrete) set. For example the group of rotations of a cube has order 24, and has several obvious permutation representations: it can act on faces, edges, vertices, diagonals, pairs of opposite faces, and so on.

For another example, the group $SL_2(\mathbb{R})$ acts on the real projective line, and on the upper half plane. These sets carry topologies, which we should take into account when defining representations.

Let us try to classify all permutation representations of some group G . First of all, if the group G acts on some set X, then we can write X as the disjoint union of the orbits of G on X, and G is transitive on each of these orbits. So this reduces the classification of all permutation representations to that of transitive permutation representations. Next, given a transitive permutation representation of G on a set X, fix a point $x \in X$ and write G_x for the subgroup fixing x. Then as a permutation representation, X is isomorphic to the action of G on the set of cosets G/G_x. If we choose a different point y, then G_x is conjugate to G_y (using some element of G taking x to y), so we see that transitive permutation representations up to isomorphism correspond to conjugacy classes of subgroups of G.

Exercise 248 Classify the transitive permutation representations of the group S_4 up to isomorphism. (There are such representations on 1, 2, 3, 4, 6, 6, 6, 8, 12, 12, 24 points.)

More generally we can ask for representations on a set preserving some structure, such as a topology, metric, measure, and so on. By far the most important such structure is that of a vector space over a field: such representations are called linear representations, or sometimes just representations. (It was not at all obvious that these were good things to study: people studied permutation representations of finite groups for several decades before Frobenius started the study of linear representations.)

Just as permutation representations can be decomposed into indecomposable (or transitive) ones, we can try to do the same for linear representations.

For finite dimensional representations we can obviously write any representation as a sum of indecomposable ones, where "indecomposable" means that it cannot be written as a sum of two non-zero representations. Unlike the case of permutation representations this decomposition need not be unique, even for the trivial group: a vector space can usually be written as a direct sum of 1-dimensional spaces in more than 1 way. In infinite dimensions a representation cannot always be decomposed into indecomposables: the theory of von Neumann algebras of types II and III is all about this phenomenon.

A linear representation is called irreducible if it is non-zero and has no subrepresentations other than 0 and itself. Obviously any irreducible representation is indecomposable, but the converse need not hold.

Example 249 For quivers, the irreducible representations are those of total dimension 1, while the indecomposables can be much more complicated, as in the previous lecture. The representation of the integers on $\mathbb{R}^2$ taking n to $\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right)$ is indecomposable but not irreducible. The finite group $\mathbb{Z}/p\mathbb{Z}$ acting on the 2-dimensional vector space $\mathbb{F}_2$ by the same formula is indecomposable but not irreducible.

Example 250 Suppose we look at (representations of the trivial group on) finitely generated abelian groups. The indecomposable things are the groups $\mathbb{Z}$ and $\mathbb{Z}/p^n\mathbb{Z}$ for primes p, while the irreducible things are the groups $\mathbb{Z}/p\mathbb{Z}$. In particular there is an indecomposable object that cannot be broken up into irreducibles.

So in general indecomposable things need not be irreducible. The problem is the following: given a subrepresentation $A \to B$ can we always find a complement, in other words a representation C so that B is the sum of A and C?If we can always do this, then obviously indecomposables and irreducibles are the same. There is one very important case when we can always do this: when the representation B is finite dimensional and unitary, in other words the group action preserves a positive definite Hermitian inner product. Then we can just take C to be the orthogonal complement of A. (In infinite dimensions we need to add some further conditions: the space B should be complete, in other words a Hilbert space, and the subspace A should be closed.) This is a major reason why unitary representations are so popular: we do not have to deal with the hard problem of indecomposables that are not irreducible.

In general we say that a representation is completely reducible if it is a sum of irreducible representations.

Theorem 251 *Any finite-dimensional complex representation of a finite group is completely reducible.*

Proof The idea is to show that the representation V of the finite group G is unitary. So choose any old positive definite Hermitian inner product. The problem is that this inner product need not be invariant under the group action. However we can make it invariant under the group action by averaging over the group G: we take all images of the inner product under the action of G and take their average. A slightly subtle point is that this average is still positive definite (and in particular non-zero) which follows from positive definiteness. So the representation has an invariant positive definite inner product and is therefore completely reducible. □

We can use this to classify all finite-dimensional complex representations of a finite abelian group. The irreducible representations are easy to find: they are all 1-dimensional because any commuting operators on a finite-dimensional complex vector space have a common eigenvector. The 1-dimensional representations of a group form a group under tensor product, called the character group.

Exercise 252 Show that if a finite abelian group is a direct sum of cyclic groups of orders a, b, c, ... then its character group can also be written in this form. (This result is a bit misleading: although a finite abelian group and its character group are isomorphic, there is usually no natural isomorphism between them.)

So since we know the irreducible finite-dimensional representations of a finite abelian group, and we know that every finite dimensional representation is a sum of irreducibles, this classifies all finite-dimensional representations of a finite abelian group.

Example 253 We find some irreducible representations of the non-abelian finite group S_3 of order 6. There are two obvious 1-dimensional representations: the trivial one, and the "sign representation" where even and odd elements act as 1 and -1. There is also a 2-dimensional (real) representation: think of S_3 acting on the 3 corners of an equilateral triangle with center 0. These are all the irreducible representations, though to see this we need some more theory.

We will need to use duals of representations. These can get rather confusing because there are in fact 8 different natural ways of constructing a new representation from an old one, many of which have been called the dual. The three main ways are as follows:

- The complex conjugate of a representation V: keep the same G-action, but change the action of i to $-i$. If we represent the elements of G by complex matrices, this corresponds to taking the complex conjugate of a matrix.
- Change the left action on V to a right action. If we define $vg = gv$ with does not work (why?) but we get a right action by putting $vg = g^{-1}v$. (This is really using the antipode of the group ring of G thought of as a Hoof algebra: any left module over a Hopf algebra can be turned into a right module in a similar way.) This corresponds to taking inverses of a matrix.
- The usual vector space dual of V is a representation, but we have to be careful how we define the G-action. Putting $(gf)(v) = f(gv)$ fails. However we can make the dual into a right G-module by putting $(fg)(v) = f(gv)$. This operation corresponds to taking transposes of a matrix.

By combining these three operations in various ways we can construct other representations. For example if we want the dual to be a left module, we first construct the dual as a right module, then change it to a left module, so we use the transpose inverse of matrices. If we want the Hermitian dual as a right module we take the complex conjugate of the dual; if we like we can turn this into a left module by taking inverses as well. (Physicists like to leave it as a right module in their bra-ket notation, while mathematician like to make it into a left module.)

For finite (and compact) groups all irreducible complex representations are unitary (or rather can be made unitary in a way that is unique up to multiplication by non-zero scalars). If we work with unitary representations then taking conjugate inverse transpose leaves everything fixed there are only 4 things we can do, and if we stick to left modules this leaves just two things: V and its dual, which can be given by taking complex conjugates. However if we work with non-unitary representations then there are still 4 left modules we can construct from V and taking ordinary or Hermitian duals is no longer the same as taking complex conjugates.

Example 254 The G to be the circle group $\mathbb{R}/2\pi\mathbb{Z}$. Then its irreducible representations are 1-dimensional and are given by $x \mapsto e^{inx}$ for integers n. There functions form an orthonormal base for the L^2 functions on G (using Lebesgue measure divided by 2π), and in particular every L^2 function can be written as a linear combination of them: this is just its Fourier series expansion. In this case the dual of a representation is given by the complex conjugate, as we expect for compact groups.

Exercise 255 Show that the representations of a finite abelian group give an orthonormal basis for the functions on the group in a similar way.

We would like to generalize this to all finite (and compact) groups: in other words find an orthonormal basis for functions on G related to the irreducible representations.

Lemma 256 *(Schur's lemma). Suppose V and W are irreducible representations of a group G over some field k. Then the algebra of linear transformations of V that commute with G is a division algebra over k. The space of linear transformations commuting with G from V to W is 0 if V is not isomorphic to W.*

Proof This is almost trivial: suppose T is any endomorphism commuting with G. Then the image and kernel of T are invariant subspaces, so must be 0 on the whole space. So either T is 0, or it has zero kernel so is an isomorphism and has an inverse. □

For complex representations the only finite dimensional division algebra over $\mathbb{C}$ is $\mathbb{C}$, so the space of linear maps from V to itself is 1-dimensional. Over other fields more interesting things can happen:

Example 257 If G is the group of order 4 acting on the real plane by rotations, then the algebra of endomorphisms commuting with is is the algebra of complex numbers. This also gives an example of a representation that is irreducible but not absolutely irreducible: it becomes reducible over an algebraic closure.

Example 258 If G is the quaternion group of order 8 acting by left multiplication on the quaternions (thought of as a 4-dimensional real vector space) then the algebra commuting with it is the algebra of quaternions (acting by right multiplication in itself).

If G is a finite group we can construct its group ring $\mathbb{C}[G]$: this is the complex algebra with basis G and multiplication given by the product of G. Alternatively we can think of it as functions on G with the product given by convolution: this definition generalizes better to Lie groups. The regular representation of G is the action of G on its group algebra by left multiplication.

The functions $\langle gv, w\rangle$ are called matrix coefficients of the representation: if we choose a basis for V and the dual basis for W they the endomorphisms of V are given by matrices, and the representation of G is given by matrix-valued functions of G. We will now show that these matrix coefficients are mostly orthogonal to each other under the obvious inner product on $\mathbb{C}[G]$ where the elements of G form an orthonormal base.

Lemma 259 *Suppose the representation V does not contain the trivial representation. Then $\sum_g \langle gv, w\rangle = 0$ for any $v \in V$, $w \in V^*$.*

Proof The vector $\sum_g gv$ is fixed by G and is therefore 0, so has bracket 0 with any w. □

Lemma 260 *If the irreducible representations V and W are not dual, then matrix coefficients of V are orthogonal to matrix coefficients of W under the symmetric inner product on $\mathbb{C}[G]$.*

Proof By assumption $V \otimes W$ does not contain the trivial representation (using Schur's lemma) so

$$\sum_{g\in G}\langle g(a), c\rangle\langle g(b), d\rangle = \sum_{g\in G}\langle g(a\times b), c\times d\rangle = 0$$

□

The character of the dual of a unitary representation is given by taking the complex conjugate, so we get:

Lemma 261 *If V and W are irreducible and not isomorphic, then the matrix coefficients of V and W are orthogonal under the hermitian inner product of $\mathbb{C}[G]$.*

Exercise 262 If V is an irreducible complex representation with some basis show that the sum of matrix coefficients $\sum_{g\in G} g_{ij}g^{-1}_{kl}$ is $|G|/\dim(V)$ if $i = l$, $j = k$ and 0 otherwise. (This is similar to the proof when we have two different representations, except that now there is a non-trivial map from V to V that makes some of the inner products of matrix coefficients non-zero.)

We give the group ring the Hermitian scalar product such that the elements of G are orthogonal and have norm $1/|G|$. To summarize: if we take a representative of each irreducible representation of G and take an orthonormal base of each representation, then the matrix coefficients we get form an orthogonal set in the group ring of G. The norms are given by $1/\dim$ (if we normalize the measure on G so that G has measure 1: this generalizes to compact groups).

Definition 263 *The character of a representation is the function from G to $\mathbb{C}$ given by the trace.*

The character is just the sum of the diagonal entries of a matrix, so by the orthogonality for matrix coefficients we see that the characters of irreducible representations form an orthonormal set of irreducible functions on G. Characters are rather spacial functions on G because they are class functions: this means they only depend on the conjugacy class of an element of G (which follows from the fact that matrices $g^{-1}hg$ and h have the same trace).

Exercise 264 If V and W are representations, show that $V \otimes W$ is a representation whose character is the product of the characters of V and W.

Exercise 265 If G acts on a set S, form a representation of G on the vector space with basis S. Show that the character of this representation is given by taking the number of fixed points of an element of G. Show that this representation always contains the trivial 1-dimensional representation as a subrepresentation. How many times does the trivial 1-dimensional representation occur?

Exercise 266 Show that the character of the symmetric square of a representation with character χ is given by $(\chi(g)^2 + \chi(g^2))/2$ and find a formula for the character of the alternating square. (If g has eigenvalues λ_i, then the eigenvalues on the symmetric square or alternating square are $\lambda_i\lambda_j$ for $i \le j$ or $i < j$.)

The character table is almost unitary except that we have to weight the columns by the sizes of the conjugacy classes. The transpose of a unitary matrix is also unitary, so the columns of a character table are orthogonal (for the hermitian inner product) and have norms given by $|G|$/size of conjugacy class which is just the order of the centralizer of an element of the conjugacy class. The orthogonality of characters makes it very easy to work with representations. For example:

- We can count the number of times an irreducible representation occurs in some representation by taking the inner product of their characters.
- A representation is irreducible if and only if its character has norm 1.
- Two representations are isomorphic if and only if they have the same character. (The analogue of this fails in cases when we do not have complete reducibility, such as modular representations of finite groups.)

We can use this to decompose the regular representation: its character is $|G|$ at the identity and 0 elsewhere. So its inner product with the character of any irreducible representation V is $\dim(V)$, so V occurs $\dim(V)$ times. In particular $|G| = \sum \dim(V)^2$, and we can use this to check that a list of irreducibles is complete.

Theorem 267 *The number of irreducible characters of a finite group is equal to the number of conjugacy classes, and the irreducible characters form an orthonormal basis for the class functions.*

Proof The irreducible characters are orthogonal class functions, so it is sufficient to show that the number of conjugacy classes is at most the number of irreducible representations. The key point is to observe that any class function is in the center of the group ring and so by Schur's lemma acts as a scalar on any irreducible representation. If the number of conjugacy classes were greater than the number of irreducibles, we could therefore find a non-zero class function acting as 0 on all irreducibles, and therefore as 0 in the regular representation, which is nonsense. □

It is natural to ask if there is a canonical correspondence between irreducibles and conjugacy classes. At first glance, the answer seems to be obviously no. For example, for infinite compact groups the number of conjugacy classes cane uncountable while the number of irreducibles is countable, and for even the cyclic group of order 3 there is no canonical way to match up the irreducibles with elements of the group. However a close look show that in many cases there does indeed seem to be some sort of natural correspondence. For example, for symmetric groups the conjugacy classes correspond to partitions, and we will later see the same is true for their representations. An even deeper look shows that representations of semisimple Lie groups (and automorphic forms) correspond to conjugacy classes of their "Langlands dual group" though this correspondence need not be 1:1 in general. This is closely related to Langlands functoriality: if the correspondence were 1:1 (which it is not in general) then a homomorphism of Langlands dual groups would induce a map between representations or automorphic forms on different groups. This is expected to hold and is known as Langlands functoriality.

We can describe the irreducible representations of a group most conveniently by giving their character tables: These are just square matrices giving the values of the characters on the conjugacy classes.

One reason why character tables are useful is that they are usually easy to compute. (This only applies to complex character tables: modular character tables are far harder to compute.)

Examples: We compute the character tables of S_3, S_4, S_5 using ad hoc methods. (In fact we will see later how to compute the characters of all symmetric groups in a uniform way.)

We can guess the character table of $SU(2)$. has an obvious 2-dimensional representation. Its conjugacy classes correspond to diagonal matrices with entries u, u^{-1} for u of absolute value 1, except that we can exchange the entries by conjugating by $\left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$ (generating the Weyl group: note that there is no matrix of order 2 in $SU(2)$ swapping the entries). The trace of this on the 2-dimensional representation is just $u + u^{-1}$. We can also take the representation consisting of polynomials of degree n on this 2-dimensional representation. This has a basis $x^n, x^{n-1}y, \ldots, y^n$ on which the trace is $u^n + u^{n-2} + \cdots u^{-n}$, so this is the character of this $n+1$-dimensional representation. So the characters are given by $(u^{n+1} - u^{-n-1})/(u - u^{-1})$, which will turn out to be a special case of the Weyl character formula. We will soon see that these are all the irreducible representations.

What about orthogonality of characters? The characters are orthogonal even functions on the unit circle if we change the measure by a factor of $-(u-u^{-1})^2$. Where has this funny-looking factor come from? The answer is that we should really be integrating over the whole of $SU(2)$, not just over the torus. While the torus does contain a representative of each conjugacy class, we cannot just change integrals of class functions on the group to integrals over the torus, because some conjugacy classes are in some sense bigger than others. The factor $-(u-u^{-1})^2$ accounts for the fact that some conjugacy classes are bigger, and is essentially the Weyl integration formula for $SU(2)$.

Let us check directly that this is indeed the right factor for converting integrals of class functions into integrals over the torus. To see this it is easiest to identify $SU(2)$ with the sphere of unit quaternions, so its maximal torus is the circle of quaternions e^{ix}. Two unit quaternions are conjugate if and only if they have the same real part. So to each element $u = e^{ix}$ of the circle S^1 we get a 2-sphere of unit quaternions conjugate to it. The volume of this 2-sphere is $4\pi\sin(x)^2$, so we see that if f is a class function then

$$\int_{S^3} f(g)dg = \frac{4\pi\sin(x)^2}{2}\int_{x \mod 2\pi} f(e^{ix})dx$$

The factor of 2 in the denominator comes from the fact that there are 2 points in S^1 for most conjugacy classes, and is the order of the Weyl group.

We can now check directly that we have found an orthonormal base for the class functions on S^3, because the functions $u^{n+1} - u^{-n-1}$ form an orthogonal basis for the odd functions on the unit circle.

This shows that the representations we have found are irreducible because their characters have norm 1 (when the measure on the group is normalized to have volume 1). We can also check directly that the representations are irreducible. For example, any nonzero subrepresentation splits as a sum of eigenspaces of the torus S^1, in other words a sum of spaces generated by monomials $x^n y^{n-i}$, and if we are given such a monomial we can recover the other eigenspaces by acting on it with suitable elements of $SU(2)$ and then taking eigenspaces again.

We will restate the relation between representations of S^3 and its torus in a way that generalizes to compact groups:

- Conjugacy classes of S^3 correspond to elements of the torus modulo the action of the Weyl group.
- The irreducible representations of the torus form a lattice acted on by the Weyl group.
- The irreducible representations of the compact group correspond to orbits of the Weyl group on representations of the torus on which the Weyl group acts faithfully.
- There is a fudge factor relating integration of class functions on the group to integration of Weyl-invariant functions on the torus.
- The character of a representation is an alternating sum over the Weyl group divided by the square root of the fudge factor. (It seems to be a lucky coincidence that the fudge factor for S^3 happens to be a square: in

fact this always happens, essentially because the roots of a Lie group come in opposite pairs.)

- Orthogonality for characters of S^3 reduces to orthogonality of characters on the torus. Completeness of characters of S^3 reduces to completeness for functions on the torus that are alternating under the action of the Weyl group.

Example 268 We can decompose tensor products and symmetric squares of representations by calculating characters. For example, the tensor product of the 6 and 3 dimensional representations is the sum of the 4, 6, and 8 dimensional representations, and the symmetric square of the 6-dimensional representation is the sum of the 9, 5, and 1-dimensional representations.

The characters of $SU(2)$ are unimodal. This means the coefficient of q^n is at least that of q^{n+2} whenever $n \geq 0$. They are also symmetric under changing q to q^{-1}. Unimodal polynomials often turn out to be characters of representations of $SU(2)$.

Example 269 Show that the Hopf manifold $C^2/(x, y) = (2x, 2y)$ is not Kaehler. The underlying topological space is $S^1 \times S^3$, so the character of its cohomology ring is $1 + q + q^3 + q^4$ which is not unimodal: there is a gap at q^2. However they theory of Kaehler manifolds shows that the cohomology is a representation of $SU(2)$ with the various cohomology groups corresponding to the eigenspaces of a torus. So the character of the cohomology ring has to be a character of $SU(2)$ (shifted by a power of q).

Exercise 270 The Gaussian binomial coefficients (or q-binomial coefficients) are given by

$$\frac{(1-q)(1-q^2)\cdots(1-q^n)}{(1-q)(1-q^2)\cdots(1-q^k)\times(1-q)(1-q^2)\cdots(1-q^{n-k})}$$

Show that they are (up to a power of q) characters of $SU(2)$ (in fact the k exterior power of the n-dimensional irreducible character), and therefore unimodal.

We show that we can find any irreducible representation V inside the regular representation. For this we pick any nonzero vector w in the dual of V. Then we can map any vector $v \in V$ to the function on G taking g to $w(g(v))$. This embeds the representation V into the group ring, so we can find all irreducible representations by decomposing the regular representation. In fact we can do better than this. Instead of fixing w we can do this simultaneously for all w in the dual, and we get a linear map from $V \otimes V* = \mathrm{End}(V)$ to the group ring. Moreover the group ring is not just a representation of G, but of $G \times G$, because G can act by multiplication on either the left or the right and these two actions commute.

So for each irreducible representation V we can find an image of $\mathrm{End}(V)$ inside the group ring. There are two natural questions: is the map from $\mathrm{End}(V)$ to the group ring injective, and is the group ring the direct sum of these spaces? Over general fields the answer to both questions is no. For example, over the real numbers this fails even for the cyclic group of order 3 which has irreducible representations of dimensions 1 and 2, and over algebraically closed fields of positive characteristic dividing the order of G it fails badly because the group ring of G has a large radical (a nilpotent ideal). However it does hold over the complex numbers: the group ring is the direct sum of matrix rings of irreducible representations.

Example 271 In particular this shows that the sum of the squares of the irreducible complex representations of a finite group is the order of the group. This sometimes gives a quick way to check that we have found all irreducible representations.

Remark 272 This generalizes to compact (Lie) groups when it is called the Peter-Weyl theorem: the space of L^2 functions on a compact group splits as a direct sum of spaces naturally isomorphic to the endomorphism rings of the irreducible representations. In general the representation theory of compact Lie groups is rather similar to the representation theory of finite groups. For non-compact groups the result can fail drastically: there are sometimes irreducible unitary representations that cannot be seen inside the regular representation, and this is one reason why finding the irreducible unitary representations of a non-compact Lie group can be rather hard. (In technical terms the support of the Plancherel measure need not be the whole space of unitary irreducible representations.)

Remark 273 This is all closely related to the Wedderburn structure theorem for finite-dimensional semisimple algebras over a field. This says that such an algebra is a direct sum of matrix algebras over division rings. The group ring of a finite group over a field of characteristic 0 is semisimple so splits as a direct sum of matrix algebras over division rings, where each matrix algebra $M_n(D)$ corresponds to an irreducible representation of dimension $n\dim(D)$ where the algebra of endomorphisms commuting with G is the division algebra D. So the order of the group is the sum of numbers n^2d corresponding to representations of dimension nd. Over the complex numbers the division algebras D are all just the complex numbers and the numbers d are all 1.

21 Schur indicator

Complex representation theory gives a good description of the homomorphisms from a group to a special unitary group. The Schur indicator describes when these are orthogonal or quaternionic, so it is also easy to describe all homomorphisms to the compact orthogonal and symplectic groups (and a little bit of fiddling around with central extensions gives the homomorphisms to compact spin groups). So the homomorphisms to any compact classical group are well understood. However there seems to be no easy way to describe the homomorphisms of a group to the exceptional compact Lie groups.

We have several closely related problems:

- Which irreducible representations have symmetric or alternating forms?
- Classify the homomorphisms to orthogonal and symplectic groups

- Classify the real and quaternionic representations given the complex ones.

Suppose we have an irreducible representation V of a compact group G. We study the space of invariant bilinear forms on V. Obviously the bilinear forms correspond to maps from V to its dual, so the space of such forms is at most 1-dimensional, and is non-zero if and only if V is isomorphic to its dual, in other words if and only if the character of V is real. We also want to know when the bilinear form is symmetric or alternating. These two possibilities correspond to the symmetric or alternating square containing the 1-dimensional irreducible representation. So $(1, \chi_{S^2V} - \chi_{\Lambda^2V})$ is 1, 0, or -1 depending on whether V has a symmetric bilinear form, no bilinear form, or an alternating bilinear form. By the formulas for the symmetric and alternating squares this is given by $\int_G \chi g^2$, and is called the Schur indicator. We have just seen that it vanishes if and only if the character of V has a non-real value.

Exercise 274 If G is a finite group of odd order, show that the map taking g to g^2 is a bijection, and deduce that the Schur indicator of any non-trivial irreducible representation is 0. Using the fact that the degree of an irreducible character divides the order of the group, show that the number of elements of G is equal to the number of conjugacy classes mod 16.

Exercise 275 Find the Schur indicators of the irreducible representations of $SU(2)$.

Lemma 276 *For an irreducible representation V of a compact group the following conditions are equivalent*

- *V has Schur indicator 1*
- *V has has a nonzero invariant symmetric bilinear form*
- *V has an invariant real form*
- *V has an invariant antilinear involution*
- *V is reducible as a real representation.*

Proof It is obvious that real forms correspond to (fixed points of) antilinear involutions. If V has a real form W, then a non-zero invariant symmetric bilinear form of W (which always exists as G is compact: take an average of any positive definite form) gives one on V. Conversely if V has a non-zero invariant bilinear form (a, b) then we can normalize it so that $\Re(a, a) \leq \langle a, a\rangle$ with equality holding for some non-zero a. Then the a for which equality holds form a subspace (as it is the kernel of a positive semidefinite real bilinear form). This subspace is a real form of V. □

Lemma 277 *If V is an irreducible representation of a compact group then the following conditions are equivalent:*

- *V has Schur indicator -1*
- *V has a nonzero invariant skew symmetric form*

- *The underlying real representation of V has a quaternionic structure.*

Proof The existence of a nonzero invariant bilinear form on V is equivalent to the existence of an invariant antilinear map j on V, by putting $(a, b) = \langle a, bj \rangle$. We consider the real algebra generated by i and j. This is either the quaternions or the 2 by 2 matrices over the reals, and the latter case corresponds to V being reducible over the reals. We have seen that the case when V is reducible corresponds exactly to the case when the bilinear form is symmetric, so the case when V is quaternionic corresponds exactly to the case when the bilinear form is antisymmetric. □

To summarize, the real irreducible representation can be read off from the complex ones as follows:

- Complex irreducible representations of complex dimension d with real character and Schur index $+1$ give a real irreducible representation of real dimension d as a real form.

- Complex irreducible representations of complex dimension d with non-real character occur in complex conjugate pairs. The underlying real representations of these two complex representations are isomorphic and give an irreducible real representation of dimension $2d$, with a complex structure (or more precisely two different complex structures).

- Complex irreducible representations of complex dimension d with Schur indicator -1 have d even, and the underlying real vector space is an irreducible real representation with a quaternionic structure or real dimension $2d$ divisible by 4.

  In practice real representations are most common and quaternionic ones tend to be rare.

Example 278 The groups D_8 and Q_8 have the same character table. However the 2-dimensional representations behave differently: one is real and the other is quaternionic.

Example 279 We find the real (orthogonal) representations of $SU(2)$. The Schur indicator of the $n+1$-dimensional irreducible complex representation is $(-1)^n$: we can evaluate this either by decomposing the virtual character $q^n + \cdots q^{-n}$ as a linear combination of characters, or by computing the integral

$$\int_{S^1} (q^{2n} + q^{2n-4} + \cdots)(q - q^{-1})^2 \frac{-1}{2 \times 2\pi} dx$$

where $q = e^{ix}$. So the real representations have dimensions 1, 3, 4, 5, 7, 8, 9,.. and the ones of dimension divisible by 4 are quaternionic.

Exercise 280 Let G be a non-cyclic finite group of rotations in 3-dimensional space (so G is dihedral or the rotations of a Platonic solid). Show that its inverse image in S^3 is a group of order $2|G|$ that has an irreducible 2-dimensional complex representation with Schur index -1.

Exercise 281 By the Wedderburn structure theorem, the real group algebra of G is a sum of matrix algebras over real division algebras, corresponding to the various real irreducible representations of G. Tensoring with $\mathbb{C}$ gives the complex group ring, which decomposes as a sum of matrix algebras over $\mathbb{C}$, corresponding to the complex irreducible representations of $\mathbb{C}$. Show that this is equivalent to the description of the real representations in terms of the Schur indicator.

22 Representations of SL2

Finite dimensional complex representations of the following are much the same: $SL_2(\mathbb{R})$, $\mathfrak{sl}_2\mathbb{R}$, $\mathfrak{sl}_2\mathbb{C}$ (as a complex Lie algebra), $\mathfrak{su}_2\mathbb{R}$, and SU_2. This is because finite dimensional representations of a simply connected Lie group are in bijection with representations of the Lie algebra. Complex representations of a REAL Lie algebra L correspond to complex representations of its complexification $L \otimes \mathbb{C}$ considered as a COMPLEX Lie algebra.

Note that complex representations of a COMPLEX Lie algebra $L\otimes\mathbb{C}$ are not the same as complex representations of the REAL Lie algebra $L\otimes\mathbb{C} \cong L+L$. The representations of the real Lie algebra correspond roughly to (reps of L)$\otimes$(reps of L).

Strictly speaking, $SL_2(\mathbb{R})$ is not simply connected, which is not important for finite dimensional representations.

Set $\Omega = 2EF + 2FE + H^2 \in U(\mathfrak{sl}_2\mathbb{R})$. The main point is that Ω commutes with $\mathfrak{sl}_2\mathbb{R}$. You can check this by brute force:

$$\begin{aligned}
[H,\Omega] &= 2\underbrace{([H,E]F + E[H,F])}_{0} + \cdots \\
[E,\Omega] &= 2[E,E]F + 2E[F,E] + 2[E,F]E \\
&\qquad + 2F[E,E] + [E,H]H + H[E,H] = 0 \\
[F,\Omega] &= \text{Similar}
\end{aligned}$$

Thus, Ω is in the center of $U(\mathfrak{sl}_2\mathbb{R})$. In fact, it generates the center. This does not really explain where Ω comes from. Why does Ω exist? The answer is that it comes from a symmetric invariant bilinear form on the Lie algebra $\mathfrak{sl}_2\mathbb{R}$ given by $(E,F)=1$, $(E,E)=(F,F)=(F,H)=(E,H)=0$, $(H,H)=2$. This bilinear form is an invariant map $L\otimes L \to \mathbb{C}$, where $L=\mathfrak{sl}_2\mathbb{R}$, which by duality gives an invariant element in $L\otimes L$, which turns out to be $2E\otimes F + 2F\otimes E + H\otimes H$. The invariance of this element corresponds to Ω being in the center of $U(\mathfrak{sl}_2\mathbb{R})$.

The bilinear form on $SL_2(\mathbb{R})$ in turn can be constructed as $(a,b) = \mathrm{Trace}_V(ab)$ for some representation V. When V is the adjoint representation this is the Killing form. By a deep theorem of Cartan this form is non-degenerate when the Lie algebra is semisimple, though of course for $SL_2(\mathbb{R})$ this is easy to check directly.

Since Ω is in the center of $U(\mathfrak{sl}_2\mathbb{R})$, it acts on each irreducible representation as multiplication by a constant. We can work out what this constant is for the finite dimensional representations. Apply Ω to the highest vector w_n:

$$\begin{aligned}
(2EF + 2FE + HH)w_n &= (2n + 0 + n^2)w_n \\
&= (2n + n^2)w_n
\end{aligned}$$

So Ω has eigenvalue $2n+n^2$ on the irreducible representation of dimension $n+1$. Thus, Ω has DISTINCT eigenvalues on different irreducible representations, so it can be used to separate different irreducible representations. For more general semisimple Lie groups, the Casimir operator may take the same value on different irreducible representations, though it always distinguishes the trivial 1-dimensional representation from the others.

Theorem 282 *Finite dimensional representations of the complex Lie algebra $sl_2(\mathbb{C})$ are completely reducible.*

This is the key property that makes the representation theory easy. In particular the representation theory of this non-abelian Lie algebra is easier than that of apparently simpler algebras such as the abelian Lie algebra R^2 (classification of 2 commuting matrices is a hard problem).

Proof We will give two proofs of this result, both of which use important ideas.

For the first proof, we use the fact that all finite dimensional representations of compact groups are completely reducible. Since the finite dimensional complex representations of the complex Lie algebra $sl_2(C)$ are "the same" as the finite dimensional complex representations of the real Lie algebra of $SU(2)$, which are in turn the same as the finite-dimensional representations of the compact group $SU(2)$, its finite dimensional representations are completely reducible. (Its infinite dimensional representations are quite unlike those of $SU(2)$, and are not completely reducible.) This is Weyl's famous unitarian trick.

The second proof uses the Casimir operator, and illustrates how to use elements of the center of the UEA. This is an algebraic proof, that also works for some infinite dimensional Lie algebras when the "analytic" proof fails. The key point is that the Casimir operator can be used to separate the different irreducible representations, and in particular can separate the trivial representation from the others.

The key case is to show that if we have an exact sequence of modules

$$0 \to V \to W \to C \to 0$$

with V simple, then it splits. If V is the trivial 1-dimensional module, then this follows because $SL_2(C)$ is prefect: it has no nontrivial 2-dimensional representations that are strictly upper triangular. If V is nontrivial we use the Casimir operator: it has different eigenvalues for V and C, so W can be split as the sum of eigenspaces of the Casimir, and this splitting is invariant under $sl_2(C)$ because the Casimir commutes with $sl_2(C)$.

The general case follows from the key case above by linear algebra as follows. Any exact sequence of the form

$$0 \to V \to W \to C \to 0$$

for a possibly reducible V splits by induction on the length of V: we can split off a top irreducible component of V and work down. Now if we have a general exact sequence of the form

$$0 \to X \to Y \to Z \to 0$$

We want to find a splitting of this sequence, which is given by a $sl_2(C)$-invariant map from Y to X that is the identity on X. we let V be the subspace of

$Hom_C(Y, X)$ of elements that act as a constant on $X \subseteq Y$, and let W be the codimension 1 subspace of elements where this constant is 0, so we have an exact sequence

$$0 \to V \to W \to C \to 0.$$

This splits, in other words we get a map from C to W whose image is fixed by $sl_2(C)$, in other words a $sl_2(C)$ linear map from Y to X that is a (nonzero!) constant on X. This gives the desired splitting of

$$0 \to X \to Y \to Z \to 0.$$

□

There are two properties of $sl_2(C)$ that make the proof of complete reducibility work: first, it is perfect, so extensions of trivial modules split, and second it has a Casimir element that separates the trivial module from others. The proof works for any other Lie algebra with these two properties, which we will later see includes all finite dimensional semisimple complex Lie algebras. For SL_2 the Casimir operator distinguishes any two non-isomorphic finite dimensional representations, but this is no longer true for higher rank Lie algebras: there can be several different irreducible representations with the same eigenvalue for the Casimir operator. However there are "higher Casimir" operators in the center of the universal enveloping algebra that separate all finite dimensional irreducible representations.

Complete reducibility is quite rare: in general it fails for infinite dimensional Lie algebras, or simple Lie algebras in positive characteristic, or infinite dimensional representations of simple complex Lie algebras.

Exercise 283 Find an infinite dimensional representation of $sl_2(C)$ that is not completely reducible. Find a perfect finite dimensional complex Lie algebra whose finite dimensional representations are not completely reducible.

Exercise 284 Show that the adjoint representation of $sl_n(F_p)$ on $gl_n(F_p)$ is not completely reducible if p divides n.

Exercise 285 Show that if the finite dimensional representations of a finite dimensional Lie algebra over some field are completely reducible, then the Lie algebra is a direct sum of simple Lie algebras.

Exercise 286 Classify the finite dimensional indecomposable representations of the 1-dimensional abelian complex Lie algebra. What does this have to do with Jordan blocks of the Jordan normal form of a matrix?

We will now find the irreducible finite dimensional representations of the Lie algebra $\mathfrak{sl}_2\mathbb{R}$, which has basis $H = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $E = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, and $F = \left(\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right)$. H is a basis for the Cartan subalgebra $\left(\begin{smallmatrix} a & 0 \\ 0 & -a \end{smallmatrix}\right)$. E spans the root space of the simple root. F spans the root space of the negative of the simple root. We find that $[H, E] = 2E$, $[H, F] = -2F$ (so E and F are eigenvectors of H), and we can check that $[E, F] = H$.

The Weyl group is generated by $\omega = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $\omega^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

Let V be a finite dimensional irreducible complex representation of $\mathfrak{sl}_2\mathbb{R}$. First decompose V into eigenspaces of the Cartan subalgebra (weight spaces) (i.e. eigenspaces of the element H). Note that eigenspaces of H exist because V is finite dimensional and complex. Look at the LARGEST eigenvalue of H (exists since V is finite dimensional), with eigenvector v. We have that $Hv = nv$ for some n. Compute

$$\begin{aligned} H(Ev) &= [H,E]v + E(Hv) \\ &= 2Ev + Env = (n+2)Ev \end{aligned}$$

So $Ev = 0$ (otherwise it would be an eigenvector of H with higher eigenvalue). $[E,-]$ increases weights by 2 and $[F,-]$ decreases weights by 2, and $[H,-]$ fixes weights.

We have that E kills v, and H multiplies it by n. What does F do to v?

What is $E(Fv)$?

$$\begin{aligned} EFv &= FEv + [E,F]v \\ &= 0 + Hv = nv \end{aligned}$$

In general, we have

$$\begin{aligned} H(F^i v) &= (n-2i)F^i v \\ E(F^i v) &= (ni - i(i-1))F^{i-1}v \\ F(F^i v) &= F^{i+1}v \end{aligned}$$

So the vectors $F^i v$ span V because they span an invariant subspace. This gives us an infinite number of vectors in distinct eigenspaces of H, and V is finite dimensional. Thus, $F^k v = 0$ for some k. Suppose k is the smallest integer such that $F^k v = 0$. Then

$$0 = E(F^k v) = (nk - k(k-1))\underbrace{EF^{k-1}v}_{\neq 0}$$

So $nk - k(k-1) = 0$, and $k \neq 0$, so $n - (k-1) = 0$, so $\boxed{k = n+1}$. So V has a basis consisting of $v, Fv, \ldots, F^n v$. The formulas become a little better if we use the basis $w_n = v, w_{n-2} = Fv, w_{n-4} = \frac{F^2 v}{2!}, \frac{F^3 v}{3!}, \ldots, \frac{F^n v}{n!}$.

This says that $E(w_2) = 5w_4$ for example. So we've found a complete description of all finite dimensional irreducible complex representations of $\mathfrak{sl}_2\mathbb{R}$.

These representations all lift to the group $SL_2(\mathbb{R})$: $SL_2(\mathbb{R})$ acts on homogeneous polynomials of degree n by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) f(x,y) = f(ax+by, cx+dy)$. This is an $n+1$ dimensional space, and we can check that the eigenspaces are $x^i y^{n-i}$.

Corollary 287 *The Cartan subalgebra H acts semisimply on any finite-dimensional representation.*

Proof First notice that this is quite subtle (from an algebraic point of view): for example, the elements E and F which look rather similar to H in the relations for $sl_2(\mathbb{R})$ do not act semisimply: in fact they are nilpotent on any finite-dimensional representation. The fact that H acts semisimply follows from the fact that we have checked this explicitly on the finite dimensional irreducible representations, and any finite dimensional representation is a direct sum of irreducible ones. $\square$

We have implicitly constructed Verma modules. We have a basis

$$w_n, w_{n-2}, \dots, w_{n-2i}, \dots$$

with relations

$$H(w_{n-2i}) = (n-2i)w_{n-2i}$$

,

$$Ew_{n-2i} = (n-i+1)w_{n-2i+2}$$

, and

$$Fw_{n-2i} = (i+1)w_{n-2i-2}$$

. These are obtained by copying the formulas from the finite dimensional case, but allow it to be infinite dimensional. This is the universal representation generated by the highest weight vector w_n with eigenvalue n under H (highest weight just means $E(w_n) = 0$).

For general semisimple groups, a Verma module is the universal module generated by a highest weight vector: a vector that is an eigenvector of the Cartan subalgebra (eigenvalue=weight) and killed by positive root spaces. They are easy to handle because one can start at the highest weight vector and work down. Any finite-dimensional irreducible module has a highest weight, so is a quotient of some Verma module. This suggests that it is useful to study the submodule structure of Verma modules. In general this is quite complicated: the solution involves Kazhdan-Lusztig polynomials, but for $SL_2(\mathbb{R})$ it is much easier and we can do it as follows.

We can start by asking when a Verma module V_λ with some highest weight λ is irreducible. So it has a basis v_λ, $v_{\lambda-2}, \dots$, If we have some submodule W then by decomposing W into eigenspaces of H we may assume that W contains some eigenvector v_μ. Take μ to be as large as possible, so μ is killed by E. So we want to solve the following problem: which vectors v_μ are highest weight vectors? This is easy using the explicit formula $Ew_{\lambda-2i} = (\lambda-i+1)w_{\lambda-2i+2}$ for the action of E: we see that it is only possible if $\lambda - i + 1 = 0$ (or $i = 0$) for some positive integer i. So generically Verma modules are irreducible: the only exceptions are the modules V_λ for λ a non-negative integer, which have a unique nonzero proper submodule isomorphic to $V_{-\lambda-2}$.

There is an alternative argument for testing when one Verma module is in another, which generalizes better to higher rank Lie algebras. For this we observe that the Casimir operator acts on a Verma module as multiplication by a scalar, so one Verma module maps non-trivially to another only if they have the same eigenvalue for the Casimir. To calculate this eigenvalue it is enough to do so for the highest weight vector, as this generates the Verma module and the Casimir commutes with the Lie algebra. To compute the eigenvalue on the highest weight vector it is convenient to rewrite the Casimir as

$$\Omega = 2EF + 2FE + H^2 = 2FE + 2[E,F] + 2FE + H^2 = 4FE + H^2 + 2H$$

because the term FE vanishes on the highest weight vector. So if the highest weight is λ, then the Casimir acts as multiplication by $\lambda^2 + 2\lambda = (\lambda+1)^2 - 1^2$. So if there is a non-zero map between two Verma modules with highest weights λ, μ then $(\lambda+1)^2 = (\mu+1)^2$, in other words $\lambda+1$ and $\mu+1$ are conjugate under the Weyl group $\{\pm 1\}$. For higher rank Lie algebras the analogous theorem says that two Verma modules with highest weights λ and μ have the same eigenvalues for ALL Casimir operators if and only if $\lambda+\rho$ and $\mu+\rho$ are conjugate under the Weyl group, where ρ is a vector called the Weyl vector, equal to half the sum of the positive roots.

The quotient $V_\lambda/V_{-\lambda-2}$ is the finite dimensional module of dimension $\lambda+1$. So we get an exact sequence

$$0 \to V_{-\lambda-2} \to V_\lambda \to (\lambda+1) - \dim \text{rep}$$

Verma modules are rank 1 free modules over the universal enveloping algebra of F, with character $q^\lambda/(1-q^2)$. If we pretend we do not know the character of the finite dimensional modules, we can work it out from this resolution by Verma modules by taking the alternating sum over the characters of the Verma modules, so we get $(q^\lambda - q^{-\lambda-2})/(1-q^2)$. The number of Verma modules appearing in this resolution is the order of the Weyl group. In fact if we look at the character formulas

$$\frac{\sum_w e^{w(\lambda+\rho)}}{\prod_{\alpha>0} e^\rho(1-e^{-\alpha})} = \sum_w \frac{e^{w(\lambda+\rho)-\rho}}{\prod_{\alpha>0}(1-e^{-\alpha})}$$

we see that it is expressing the character of a finite dimensional representation as an alternating sum of characters of Verma modules with highest weights $w(\lambda+\rho)-\rho$, coming from a resolution.

The factor $q-q^{-1}$ in the denominator of the character formula appears for completely different reasons in these two approaches to the representation theory. In the analytic approach where we integrate over compact groups, $q-q^{-1}$ appears as the square root of the fudge factor needed to convert integrals over the group to integrals over the Cartan subgroup. In the algebraic approach, it appears as the inverse of the character of a Verma module.

Some things go wrong in infinite dimensions.

Warning 288 Representations corresponding to the Verma modules with this Cartan subalgebra never lift to representations of $SL_2(\mathbb{R})$, or even to its universal cover. The reason: look at the Weyl group (generated by $\left(\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right)$) of $SL_2(\mathbb{R})$ acting on $\langle H\rangle$; it changes H to $-H$. It maps eigenspaces with eigenvalue m to eigenvalue $-m$. But if we look at the Verma module, it has eigenspaces $n, n-2, n-4, \ldots$, and this set is obviously not invariant under changing sign. The usual proof that representations of the Lie algebra lifts uses the exponential map of matrices, which doesn't converge in infinite dimensions. However, Verma modules using the compact Cartan subalgebra rather than the split one do sometimes lift to representations of the group, called holomorphic discrete series representations.

Remark 289 The universal cover $\widetilde{SL_2(\mathbb{R})}$ of $SL_2(\mathbb{R})$, or even the double cover $Mp_2(\mathbb{R})$, has no faithful finite dimensional representations. **Proof** Any finite dimensional representation comes from a finite dimensional representation of the Lie algebra $\mathfrak{sl}_2\mathbb{R}$. All such finite dimensional representations factor through $SL_2(\mathbb{R})$. □

There is an obvious integral form of the UEA of SL_2, given as the one generated by E, F and H, in other words the UEA of the Lie algebra over the integers. However this is not really a very good integral form: for example, its dual (a commutative ring) ought to be something like a completion of a coordinate ring of the group, but is not. The right integral form was found by Chevalley, and can be motivated by trying to find an integral from that preserves the obvious integral form of the finite-dimensional representations.

Exercise 290 Show that the elements $E^n/n!$, $F^n/n!$ preserve the integral forms of finite dimensional representations and Verma modules given above. (The integral form of Verma modules is not the one generated by the action of F on the highest weight vector!)

So Chevalley's integral form of the universal enveloping algebra is the subalgebra generated by these elements. It has the useful property that coefficients of $\exp(tE)$ and $\exp(tF)$ are in the integral form. Since E and F act nilpotently on finite dimensional representations this means that $\exp(tE)$ and $\exp(tF)$ make sense over any commutative ring.

Exercise 291 Show that $H^n/n!$ does not usually preserve the integral form of finite dimensional representations, but that $\binom{H}{n}$ does. Show that these elements are in the integral form generated by $E^n/n!$ and $F^n/n!$.

Exercise 292 Show that the dual of the integral form above is a power series ring in 3 variables. (The integral form is a cocommutative Hopf algebra, so its dual is a commutative ring.)

23 Infinite dimensional unitary representations

Last lecture, we found the finite dimensional (non-unitary) representations of $SL_2(\mathbb{R})$.

23.1 Background about infinite dimensional representations

(of a Lie group G) What is an infinite dimensional representation?

1st guess Banach space acted on by G?

This is no good for the following reasons: Look at the action of G on the functions on G (by left translation). We could use L^2 functions, or L^1 or L^p. These are completely different Banach spaces, but they are essentially the same representation.

2nd guess Hilbert space acted on by G? This is sort of okay.

The problem is that finite dimensional representations of $SL_2(\mathbb{R})$ are NOT Hilbert space representations, so we are throwing away some interesting representations.

Solution (Harish-Chandra) Take $\mathfrak{g}$ to be the Lie algebra of G, and let K be the maximal compact subgroup. If V is an infinite dimensional representation of G, there is no reason why $\mathfrak{g}$ should act on V.

The simplest example fails. Let $\mathbb{R}$ act on $L^2(\mathbb{R})$ by left translation. Then the Lie algebra is generated by $\frac{d}{dx}$ (or $i\frac{d}{dx}$) acting on $L^2(\mathbb{R})$, but $\frac{d}{dx}$ of an L^2 function is not in L^2 in general.

Let V be a Hilbert space. Set V_ω to be the K-finite vectors of V, which are the vectors contained in a finite dimensional representation of K. The point is that K is compact, so V splits into a Hilbert space direct sum finite dimensional representations of K, at least if V is a Hilbert space. Then V_ω is a representation of the Lie algebra $\mathfrak{g}$, not a representation of G. V_ω is a representation of the group K. It is a $(\mathfrak{g}, K)$-module, which means that it is acted on by $\mathfrak{g}$ and K in a "compatible" way, where compatible means that

1. they give the same representations of the Lie algebra of K.
2. $k(u)v = k(u(k^{-1}v))$ for $k \in K$, $u \in \mathfrak{g}$, and $v \in V$.

The K-finite vectors of an irreducible unitary representation of G is ADMISSIBLE, which means that every representation of K only occurs a *finite* number of times. The GOOD category of representations is the representations of admissible $(\mathfrak{g}, K)$-modules. It turns out that this is a really well behaved category.

We want to find the unitary irreducible representations of G. We will do this in several steps:

1. Classify all irreducible admissible representations of G. This was solved by Langlands, Harish-Chandra et. al.
2. Find which have Hermitian inner products $(\ ,\ )$. This is easy.
3. Find which ones are positive definite. This is very hard, and has not been solved for all simple Lie groups, though it has been done for some infinite series such as general linear groups. We will only do this for the simplest case: $SL_2(\mathbb{R})$, which is much easier than most other cases.

23.2 The group $SL_2(\mathbb{R})$

We found some generators (in $Lie(SL_2(\mathbb{R}))\otimes\mathbb{C}$ last time: E, F, H, with $[H,E] = 2E$, $[H,F] = -2F$, and $[E,F] = H$. We have that $H = -i\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$, $E = \frac{1}{2}\left(\begin{smallmatrix}1&i\\i&-1\end{smallmatrix}\right)$, and $F = \frac{1}{2}\left(\begin{smallmatrix}1&-i\\-i&-1\end{smallmatrix}\right)$. Why not use the old $\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$?

Because $SL_2(\mathbb{R})$ has two different classes of Cartan subgroup: $\left(\begin{smallmatrix}a&0\\0&a^{-1}\end{smallmatrix}\right)$, spanned by $\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}\cos\theta&\sin\theta\\-\sin\theta&\cos\theta\end{smallmatrix}\right)$, spanned by $\left(\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right)$, and the second one is COMPACT. The point is that non-compact (abelian) groups need not have eigenvectors on infinite dimensional spaces. An eigenvector is the same as a weight space. The first thing you do is split it into weight spaces, and if your Cartan subgroup is not compact, you cannot get started. We work with the compact subalgebra so that the weight spaces exist.

Given the representation V, we can write it as some direct sum of eigenspaces of H, as the Lie group H generates is compact (isomorphic to S^1). In the finite dimensional case, we found a HIGHEST weight, which gave us complete control over the representation. The trouble is that in infinite dimensions, there is no reason for the highest weight to exist, and in general they do not as there may be an infinite number of eigenvalues.

A good substituted for the highest weight vector: Look at the Casimir operator $\Omega = 2EF + 2FE + H^2 + 1$. The key point is that Ω is in the center of the universal enveloping algebra. As V is assumed admissible, we can conclude that Ω has eigenvectors (because we can find a finite dimensional space acted on by Ω). As V is irreducible and Ω commutes with G, all of V is an eigenspace of Ω. We will see that this gives us about as much information as a highest weight vector.

Let the eigenvalue of Ω on V be λ^2 (the square will make the most interesting representations have integral λ; the $+1$ in Ω is for the same reason).

Suppose $v \in V_n$, where V_n is the space of vectors where H has eigenvalue n. In the finite dimensional case, we looked at Ev, and saw that $HEv = (n+2)Ev$. What is FEv? If v was a highest weight vector, we could control this. Notice that $\Omega = 4FE + H^2 + 2H + 1$ (using $[E, F] = H$), and $\Omega v = \lambda^2 v$. This says that $4FEv + n^2 v + 2nv + v = \lambda^2 v$. This shows that FEv is a multiple of v.

Now we can draw a picture of what the representation looks like: There is a basis $\ldots v_{n-2}, v_n, v_{n+2}, \ldots$, with

- $Hv_n = nv_n$
- $Ev_n =$ some multiple of v_{n+2}
- $Fv_n =$ some multiple of v_{n-2}

Thus, V_ω is spanned by V_{n+2k}, where k is an integer. The non-zero elements among the V_{n+2k} are linearly independent as they have different eigenvalues. The only question remaining is whether any of the V_{n+2k} vanish.

There are four possible shapes for an irreducible representation

- infinite in both directions:
- a lowest weight, and infinite in the other direction:
- a highest weight, and infinite in the other direction:
- we have a highest weight and a lowest weight, in which case it is finite dimensional

We will see that all these show up. We also see that an irreducible representation is completely determined once we know λ and some n for which $V_n \neq 0$. The remaining question is to construct representations with all possible values of $\lambda \in \mathbb{C}$ and $n \in \mathbb{Z}$. n is an integer because it must be a representations of the circle group.

We can write down explicit representations as follows, by copying the formulas for Verma modules and not cutting them off at the highest weight. We get a representation with basis v_i where i runs through either all even integers or all odd integers, and the action is given by

- $Hv_n = nv_n$
- $Ev_n = \frac{\lambda+n+1}{2} v_{n+2}$

- $Fv_n = \frac{\lambda-n-1}{2}v_{n-2}$

It is easy to check that these maps satisfy $[E,F] = H$, $[H,E] = 2E$, and $[H,F] = -2F$

Problem: These may not be irreducible, and we want to decompose them into irreducible representations. The only way they can fail to be irreducible if if $Ev_n = 0$ of $Fv_n = 0$ for some n (otherwise, from any vector, we can generate the whole space). The only ways that can happen is if

$$\begin{aligned} &n \text{ even: } \lambda \text{ an odd integer} \\ &n \text{ odd: } \lambda \text{ an even integer.} \end{aligned}$$

What happens in these cases? The easiest thing is probably just to write out an example.

Example 293 Take n even, and $\lambda = 3$, so we have two submodules: one with basis $v_4, v_6, \cdots$, and the other with basis $v_{-4}, v_{-6}, \ldots$. So V has two irreducible subrepresentations V_- and V_+, and $V/(V_- \oplus V_+)$ is an irreducible 3 dimensional representation with basis v_{-2}, v_0, v_2.

Example 294 If n is even, but λ is negative, say $\lambda = -3$, we get a subrepresentation with basis v_{-2}, v_0, v_2.

Here we have an irreducible finite dimensional representation. If we quotient out by that subrepresentation, we get $V_+ \oplus V_-$. So this is like the previous example, except that it has been turned upside down.

In particular we can see that the representations are not completely reducible in general.

There is one case when something slightly different happens:

Exercise 295 Show that for n odd, and $\lambda = 0$, then V splits are a direct sum of two irreducible submodules: $V = V_+ \oplus V_-$. (These are called limits of discrete series representations.)

So we have a complete list of all irreducible admissible representations:

1. if $\lambda \notin \mathbb{Z}$, we get one representation (remember $\lambda \equiv -\lambda$). This is the bi-infinite case.
2. Finite dimensional representation for each $n \geq 1$ ($\lambda = \pm n$)
3. Discrete series for each $\lambda \in \mathbb{Z} \setminus \{0\}$, which is the half infinite case: we get a lowest weight when $\lambda < 0$ and a highest weight when $\lambda > 0$.
4. two "limits of discrete series" where n is odd and $\lambda = 0$.

Which of these can be made into unitary representations? $H^\dagger = -H$, $E^\dagger = F$, and $F^\dagger = E$. If we have a Hermitian inner product $(\ ,\ )$, we see that

$$\begin{aligned} (v_{j+2}, v_{j+2}) &= \frac{2}{\lambda+j+1}(Ev_j, v_{j+2}) \\ &= \frac{2}{\lambda+j+1}(v_j, -Fv_{j+2}) \\ &= -\frac{2}{\lambda+j+1}\overline{\frac{\lambda-j-1}{2}}(v_j, v_j) > 0 \end{aligned}$$

So we want $-\frac{\overline{\lambda-1-j}}{\lambda+j+1}$ to be real and positive whenever $j, j+2$ are non-zero eigenvectors. So

$$-(\lambda-1-j)(\lambda+1+j) = -\lambda^2+(j+1)^2$$

should be positive for all j. Conversely, when we have this condition, the representations have a positive semi definite Hermitian form.

This condition is satisfied in the following cases:

1. $\lambda^2 \leq 0$. These representations are called PRINCIPAL SERIES representations. These are all irreducible *except* when $\lambda = 0$ and n is odd, in which case it is the sum of two limits of discrete series representations

2. $0 < \lambda < 1$ and j even. These are called COMPLEMENTARY SERIES. They are annoying, and you spend a lot of time trying to show that they don't occur in cases you are interested in, such as the Selberg conjecture.

3. $\lambda^2 = n^2$ for $n \geq 1$ (for some of the irreducible pieces).

   If $\lambda = 1$, we get a 1-dimensional subrepresentation, which is unitary, and the quotient is the sum of two Verma modules (discrete series representations).

   We see that we get two discrete series and a 1 dimensional representation, all of which are unitary

   For $\lambda = 2$ (this is the more generic one), we have a 2-dimensional middle representation (where $(j+1)^2 < \lambda^2 = 4$ that is not unitary, which we already knew. So the discrete series representations are unitary, and the finite dimensional representations of dimension greater than or equal to 2 are not.

Summary: the irreducible unitary representations of $SL_2(\mathbb{R})$ are given by

1. the 1 dimensional representation

2. Discrete series representations for any $\lambda \in \mathbb{Z} \setminus \{0\}$

3. Two limit of discrete series representations for $\lambda = 0$

4. Two series of principal series representations:

   $$\begin{array}{l} j \text{ even: } \lambda \in i\mathbb{R},\ \lambda \geq 0 \\ j \text{ odd: } \lambda \in i\mathbb{R},\ \lambda > 0 \end{array}$$

5. Complementary series: parametrized by λ, with $0 < \lambda < 1$.

There seems to be a puzzle here: the discrete series representations of the group are (completions of) Verma modules, whereas we claimed earlier that Verma modules were never associated to representations of the group. The difference is that we are looking at Verma modules for different Cartan subalgebras. For the split Cartan subalgebra there is a Weyl group element acting as -1 on the Lie algebra, which implies that representations of the group cannot be Verma modules whose weights are not invariant under -1. On the other hand, for the compact Cartan subalgebra there is no element of the group acting as -1 on its Lie algebra, so this argument no longer applies, and we can have Verma modules that are (essentially) representations of the group, at least if we take a completion of them.

The unitary representations have an obvious topology (for general groups there is also such a topology, called the Fell topology). This topology is not Hausdorff: for example, the two limits of discrete series representations are limits of the same continuous series representations, and the two smallest discrete series representations and the trivial representation are all some sort of limit of complementary series representations as λ tens to 1.

The nice stuff that happened for $SL_2(\mathbb{R})$ breaks down for more complicated Lie groups. In particular if the rank is grater than 1 then the Casimir eigenvalue does not unambiguously determine what the analogues of the operators FE and so on do.

Representations of finite covers of $SL_2(\mathbb{R})$ are similar, except j need not be integral. For example, for the double cover $\widehat{SL_2(\mathbb{R})} = Mp_2(\mathbb{R})$, $2j \in \mathbb{Z}$.

Exercise 296 Find the irreducible unitary representations of $Mp_2(\mathbb{R})$.

Random things not covered: Plancherel measure for $SL_2(\mathbb{R})$ (note that 1 is not in the support!), holomorphic modular forms are highest weights for discrete series representations, Maass wave forms are eigenvectors for principal series representations, characters of representations.

24 Serre relations

We now construct all the simple complex Lie algebras using the Serre relations. The Cartan matrix of a root system with simple roots r_i is given by $a_{ij} = 2(r_i, r_j)/(r_i, r_i)$; these numbers are the integers that appear when reflecting r_j in the hyperplane of r_i.

Suppose that a_{ij} is a Cartan matrix. We can recover the Lie algebra with this matrix as the Lie algebra generated by elements h_i, e_i, f_i subject to the following Serre relations:

$$[e_i, f_j] = h_i \text{if } i = j, 0 \text{otherwise} \quad (15)$$

$$[h_i, e_j] = a_{ij} e_j \quad (16)$$

$$[h_i, f_j] = -a_{ij} e_j \quad (17)$$

$$\mathrm{ad}(e_i)^{1-a_{ij}} e_j = 0 \quad (18)$$

$$\mathrm{ad}(f_i)^{1-a_{ij}} f_j = 0 \quad (19)$$

As usual when objects are defined using a presentation it is easy to find an upper bound on the size of the object but harder to find a lower bound on the size. In particular the main problem with the algebra defined by the Serre relations is to show that it does not collapse to zero. We will do this in two steps: first show that in the algebra generated by the first 3 relations the elements h_i are linearly independent by finding some explicit representations of it, then showing that the ideal generated by the last two relations has trivial intersection with the subalgebra H spanned by the h_i.

So we first forget about the last two relations. Suppose that we have a graded lie algebra, and let F, H and E be the pieces of degree $-1, 0, 1$. Then

- H is a Lie algebra
- E and F are representations of H
- we have a map $E \otimes F \mapsto H$ of H-modules.

Typical example: H=diagonal matrices, E=the things just above the diagonal, and F=things just below. In applications, H will be the (abelian) Cartan subalgebra, E with be the sum of the simple root spaces, and F with be the sum of the root spaces of minus the simple roots.

Conversely given the data above, we want to construct a graded Lie algebra G. Obviously we can define a universal such G by generators and relations, and the problem is to see what its structure is: in particular is is not obvious that G is nonzero!

We first bound G from above, which is straightforward.

Lemma 297 *The obvious vector space map from $Free(F) \oplus H \oplus Free(E)$ to G is onto, where $Free$ means "free Lie algebra generated by a vector space".*

Proof This is easy: just check that the image of this map is closed under brackets by elements of E, F, and H, by induction on length. □

Now we have to show that this map is injective, and in particular that G does not collapse to nothing. As usual, the best way to show that something given by generators and relations is non-zero is to construct a representation of it. The idea is to construct representations as some sort of Verma modules: in other words we have a "lowest weight space" V acted on by H and killed by F, where V is any representation of H. This gives the action of F and H, but we have no idea what E does. We try to build a representation by letting the action of E be as free as possible: in other words we take $TE \otimes V$ where TE is the tensor algebra of E (the UEA of the free Lie algebra generated by E). First we need a lemma for constructing operators on TE:

Lemma 298 *Suppose that E is the free associative algebra generated by elements e_i, and we are given operators b_i on E and an element e of E. Then there is a unique operator b such that $b(1) = e$ and $[b, e_i] = b_i$.*

Proof The algebra E has a basis of elements $e_{i_1} e_{i_2} \cdots e_{i_n}$ for $n \geq 0$. We define b by induction on the length n of a basis element by putting

$$b(1) = e$$

for the basis element of length 0, and

$$b(e_i \cdots) = e_i b(\cdots) + b_i(\cdots)$$

on elements of positive length. □

So if we know that action of some operator on V, and we are given its commutators with elements of E (which should of course depend linearly on E), then we get a unique operator on $TE \otimes V$. This immediately gives us operators on $TE \otimes V$ corresponding to elements of H and F, using the fact that we know $[h, e]$ and then $[f, e]$. To finish the proof that we have a representation, we need to check that $[h_1, h_2]$ and $[h, f]$ have the right values. The idea for doing this is that if two operators on $TE \otimes V$ are the same on V and have the same commutators with elements of E, then they are equal. If we write x' for the operator on $TE \otimes V$ corresponding to x, this means we have to check that $[h_1', h_2'] = [h_1, h_2]'$ and $[h, f]' = [h', f']$. For both identities it is immediate that they coincide on V, so we just have to check the commutators with and $e \in E$ are the same. This follows from

$$[e', [h_1', h_2']] = [[e', h_1'], h_2'] + [h_1', [e', h_2']] = [[e, h_1]', h_2'] + [h_1', [e, h_2]'] = [[e, h_1], h_2]' + [h_1, [e, h_2]]' = [e, [h_1, h_2]]' = [e',$$

since we know that $'$ is a homomorphism brackets of type $[E, H]$.

Exercise 299 Do the case of $[h, f]' = [h', f']$ in the same way.

Exercise 300 Where did the proof use the fact that the map from $E \otimes F \mapsto h$ is a homomorphism of H-modules?

In particular we see that $Free(E)$ acts freely on these modules so maps injectively into G, and by taking V to be any faithful representation of H we see that H also maps injectively into G. To summarize, we have proved:

Theorem 301 *Suppose given a Lie algebra H, and H-modules E and F together with a map of H-modules from $E \otimes F$ to H. Then E, F, and H are the pieces of degree 1, -1 and 0 of a graded Lie algebra G, and the positive part of G is the free Lie algebra on E. Moreover if V is any representation of H, we can extend it to a representation of G on $TE \otimes V$ so that F kills V and E acts in the obvious way by left multiplication.*

Lemma 302 *Suppose that $\mathfrak{g}$ is the Lie algebra generated by elements generated by elements h_i, e_i, f_i subject to the following relations:*

$$[e_i, f_j] = h_i if\ i = j, 0 otherwise \tag{20}$$

$$[h_i, e_j] = a_{ij} e_j \tag{21}$$

$$[h_i, f_j] = -a_{ij} e_j \tag{22}$$

Then $\mathfrak{g}$ can be graded as $\mathfrak{g} = \oplus \mathfrak{g}_m$, where $\mathfrak{g}_+ = \oplus_{m>0} \mathfrak{g}_m$ is the subalgebra generated by the e_i, $\mathfrak{g}_- = \oplus_{m>0} \mathfrak{g}_m$ is the subalgebra generated by the f_i, and $\mathfrak{g}_0$ is the subalgebra generated by the h_i and is abelian.

Proof This is a fairly straightforward check.

We define the grading by giving each e_i degree 1, each f_i degree -1, and each h_i degree 0. This defines a grading as all the relations are homogeneous. (More generally, we could give e_i and positive degree d_i provided we give f_i degree $-d_i$, which is occasionally useful.)

The fact that the subalgebra H generated by the elements h_i is abelian follows from

$$[h_i, h_j] = [h_i, [e_j, f_j]] = [[h_i, e_j], f_j] + [e_j, [h_i, f_j]] = [a_{ij} e_j, f_j] + [e_j, [-a_{ij} f_j] = 0$$

so all the elements h_i commute with each other, and in particular H is spanned by the elements h_i.

If we write E, F, and $H = g_0$ for the subalgebras generated by the elements e_i, f_i, and h_i then the defining relations imply $[f_i, E] \subseteq E$, $[f_i, E] \subseteq H \oplus E$, $[f_i, H] \subseteq F$, so the subspace $E \oplus H \oplus F$ is closed under f_i. Similarly it is closed under e_i and is therefore equal to $\mathfrak{g}$ as these elements generate $\mathfrak{g}$. □

Now we come to the first key point, which is showing that the algebra $\mathfrak{g}$ does not collapse.

Lemma 303 *The elements h_i of the Lie algebra $\mathfrak{g}$ are linearly independent.*

Proof This follows from the previous theorem. □

The Lie algebras we get like this are usually infinite dimensional, as they contain free lie algebras on E. The key idea is that if we have a subspace X of $Free(E)$ that is mapped to itself by F and H, then the subspace it generates under the action of E is still acted on by F and H, so is an ideal of G contained in $Free(E)$, and therefore having zero intersection with H. So if we can find such subspaces X we can reduce the size of G. In general there need not be any such subspaces, but for the special case of the Serre relations we can find some.

The final step is to include the relations $\mathrm{ad}(e_i)^{1-a_{ij}} e_j = 0$ $\mathrm{ad}(f_i)^{1-a_{ij}} f_j = 0$ and in particular we need to show that these do not cause the Lie algebra to collapse to 0.

Lemma 304 *If $i \neq j$ then the element $ad(e_i)^{1-a_{ij}} e_j = 0$ of E is is killed by f_k.*

Proof It is obviously killed by f_k if k is not i or j, as then f_k commutes with both e_i and e_j.

To show that it is killed by f_j we have two cases depending on whether a_{ij} is 0 or not.

$$[f_j[e_i, [\cdots [e_i, e_j] \cdots] = [e_i, [\cdots [e_i, [f_j, e_j] \cdots] \tag{23}$$
$$= -[e_i, [\cdots [e_i, h_j] \cdots] = a_{ij}[e_i, \ldots, , e_i] \cdots] \tag{24}$$

If $a_{ij} = 0$ this vanishes as it contains a factor of a_{ij}, while if $a_{ij} > 0$ it vanishes because $1 - a_{ij} \geq 2$ so it contains a term $[e_i, e_i]$.

Finally we show that $\mathrm{ad}(e_i)^{1-a_{ij}} e_j = 0$ is killed by f_i, which is where we need to use the funny-looking exponent $1 - a_{ij}$. For this we look at the subalgebra generated by e_i, f_i, and h_i, which is isomorphic to $\mathfrak{sl}_2$. Moreover the element e_j is killed by f_i so generates a Verma module for $\mathfrak{sl}_2$. The lowest weight e_j of this Verma module has eigenvalue a_{ij} for h_i, so by the theory of $\mathfrak{sl}_2$ Verma modules, the element $\mathrm{ad}(e_i)^n e_j = 0$ for $n > 0$ is killed by f_j if (and only if) $n = 1 - a_{ij}$. □

Theorem 305 *In the Lie algebra defined by the Serre relations, the elements h_i, e_i, and f_i are linearly independent.*

Corollary 306 *Each of the copies of sl_2 spanned by e_i, f_i, h_i act on the Lie algebra as a sum of finite dimensional representations.*

Proof This follows by first checking that each generator of the Lie algebra lies in a finite dimensional representation (using the extra Serre relations) then showing that the elements of the Lie algebra with this property are closed under the Lie bracket. □

Corollary 307 *The action of each Lie algebra sl_2 spanned by e_i, f_i, h_i lifts to an action of the Lie group SL_2. In particular the Weyl group element $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ acts on the Lie algebra, and acts on the Cartan subalgebra as the reflection of the corresponding simple root, so we get an action of the Weyl group on the roots.*

This is enough to show that the Lie algebra is finite dimensional: more precisely every root is conjugate to a simple root under the Weyl group and therefore has multiplicity 1. (This fails for infinite root systems: for general Kac-Moody algebras there are more roots that are not conjugate to simple roots, called imaginary roots, and they can have multiplicity greater than 1.)

Example 308 We can work this out explicitly for the rank 2 algebras, and write down explicit bases.

Theorem 309 *Every root is conjugate to a simple root under the Weyl group.*

Proof We need to use the fact that to root system and Weyl group are finite: the theorem fails for infinite dimensional Kac-Moody algebras, which have "imaginary" roots not conjugate to simple roots. In particular there is a positive definite quadratic form preserved by the Weyl group. Look at the Weyl chamber W of the simple roots, and its dual convex cone C generated by the simple roots. Any positive root is contained in C, and its orthogonal complement has codimension at least 2 in W unless the root is simple. The conjugates of the Weyl chamber W under the Weyl group cover the whole space, so if a root is not conjugate to a simple root under the Weyl group, its orthogonal complement has codimension at least 2 in the whole space , which is impossible. □

To summarize, we have an explicit description of the Lie algebra: it is a sum of the Cartan subalgebra H (with basis h_i), and a 1-dimensional root space for each root of the root system, for which we can easily write down an explicit basis element if we want to.

Exercise 310 Show that the Lie algebra constructed from an irreducible finite crystallographic root system is simple. (Irreducible means that it is not the sum of two orthogonal root systems: in the case the Lie algebra splits as the direct sum of corresponding Lie algebras.) The idea is to look at eigenvectors of the Cartan subalgebra. If α is some eigenvalue of some element in an ideal, then show that so is β for and β not orthogonal to α.

Much, but not all, of this theory works for infinite root systems, and the corresponding Lie algebras are called Kac-Moody algebras. We still get an action of the Weyl group on the roots, but as mentioned above roots need not be conjugate to simple roots: the proof above fails because the union of Weyl chambers need not cover space when the Weyl group is infinite.

25 The Weyl groups of exceptional groups

We use a vector notation in which powers represent repetitions: so $(1^8) = (1,1,1,1,1,1,1,1)$ and $(\pm\frac{1}{2}^2, 0^6) = (\pm\frac{1}{2}, \pm\frac{1}{2}, 0,0,0,0,0,0)$.

Recall that E_8 has the Dynkin diagram where each vertex is a root r with $(r, r) = 2$; $(r, s) = 0$ when r and s are not joined, and $(r, s) = -1$ when r and s are joined. We choose an orthonormal basis $e_1, \ldots, e_8$, in which the roots are as given.

We want to figure out what the root lattice L of E_8 is (this is the lattice generated by the roots). If we take $\{e_i - e_{i+1}\} \cup (-1^5, 1^3)$ (all the A_7 vectors plus twice the strange vector), they generate the D_8 lattice $= \{(x_1, \ldots, x_8) | x_i \in \mathbb{Z}, \quad \sum x_i \text{ even}\}$. So the E_8 lattice consists of two cosets of this lattice, where the other coset is $\{(x_1, \ldots, x_8) | x_i \in \mathbb{Z} + \frac{1}{2}, \quad \sum x_i \text{ odd}\}$.

Alternative version: If we reflect this lattice through the hyperplane $e_1^\perp$, then we get the same thing except that $\sum x_i$ is always even. We will freely use both characterizations, depending on which is more convenient for the calculation at hand.

We should also work out the weight lattice, which is the vectors s such that $(r, r)/2$ divides (r, s) for all roots r. Notice that the weight lattice of E_8 is contained in the weight lattice of D_8, which is the union of four cosets of D_8: D_8, $D_8 + (1, 0^7)$, $D_8 + (\frac{1}{2}^8)$ and $D_8 + (-\frac{1}{2}, \frac{1}{2}^7)$. Which of these have integral inner product with the vector $(-\frac{1}{2}^5, \frac{1}{2}^3)$? They are the first and the last, so the weight lattice of E_8 is $D_8 \cup D_8 + (-\frac{1}{2}, \frac{1}{2}^7)$, which is equal to the root lattice of E_8.

In other words, the E_8 lattice L is unimodular (equal to its dual L'), where the dual is the lattice of vectors having integral inner product with all lattice vectors. This is also true of G_2 and F_4, but is not in general true of Lie algebra lattices.

The E_8 lattice is even, which means that the inner product of any vector with itself is always even.

Even unimodular lattices in $\mathbb{R}^n$ only exist if $8|n$ (this 8 is the same 8 that shows up in the periodicity of Clifford groups). The E_8 lattice is the only example in dimension equal to 8 (up to isomorphism, of course). There are two in dimension 16 (one of which is $L \oplus L$, the other is $D_{16} \cup$ some coset). There are 24 in dimension 24, which are the Niemeier lattices. In 32 dimensions, there are more than a billion!

The Weyl group of E_8 is generated by the reflections through $s^\perp$ where $s \in L$ and $(s, s) = 2$ (these are called roots). First, let's find all the roots: $(x_1, \ldots, x_8)$ such that $\sum x_i^2 = 2$ with $x_i \in \mathbb{Z}$ or $\mathbb{Z} + \frac{1}{2}$ and $\sum x_i$ even. If $x_i \in \mathbb{Z}$, obviously the only solutions are permutations of $(\pm 1, \pm 1, 0^6)$, of which there are $\binom{8}{2} \times 2^2 = 112$ choices. In the $\mathbb{Z} + \frac{1}{2}$ case, we can choose the first 7 places to be $\pm\frac{1}{2}$, and the last coordinate is forced, so there are 2^7 choices. Thus, we get 240 roots.

Let's find the orbits of the roots under the action of the Weyl group. We don't yet know what the Weyl group looks like, but we can find a large subgroup that is easy to work with. Let's use the Weyl group of D_8, which consists of the following: we can apply all permutations of the coordinates, or we can change the sign of an even number of coordinates (e.g., reflection in $(1, -1, 0^6)$ swaps the first two coordinates, and reflection in $(1, -1, 0^6)$ followed by reflection in $(1, 1, 0^6)$ changes the sign of the first two coordinates.)

Notice that under the Weyl group of D_8, the roots form two orbits: the set which is all permutations of $(\pm 1^2, 0^6)$, and the set $(\pm\frac{1}{2}^8)$. Do these become the same orbit under the Weyl group of E_8? Yes; to show this, we just need one element of the Weyl group of E_8 taking some element of the first orbit to the second orbit. Take reflection in $(\frac{1}{2}^8)^\perp$ and apply it to $(1^2, 0^6)$: you get

$(\frac{1}{2}^2, -\frac{1}{2}^6)$, which is in the second orbit. So there is just one orbit of roots under the Weyl group.

What do orbits of $W(E_8)$ on other vectors look like? We're interested in this because we might want to do representation theory. The character of a representation is a map from weights to integers, which is $W(E_8)$-invariant. Let's look at vectors of norm 4 for example. So $\sum x_i^2 = 4$, $\sum x_i$ even, and $x_i \in \mathbb{Z}$ or $x_i \in \mathbb{Z} + \frac{1}{2}$. There are 8×2 possibilities which are permutations of $(\pm 2, 0^7)$. There are $\binom{8}{4} \times 2^4$ permutations of $(\pm 1^4, 0^4)$, and there are 8×2^7 permutations of $(\pm\frac{3}{2}, \pm\frac{1}{2}^7)$. So there are a total of 240×9 of these vectors. There are 3 orbits under $W(D_8)$, and as before, they are all one orbit under the action of $W(E_8)$. Just reflect $(2, 0^7)$ and $(1^3, -1, 0^4)$ through $(\frac{1}{2}^8)$.

Exercise 311 Show that the number of norm 6 vectors is 240×28, and they form one orbit

(If you've seen a course on modular forms, you'll know that the number of vectors of norm $2n$ is given by $240 \times \sum_{d|n} d^3$. If we let call these c_n, then $\sum c_n q^n$ is a modular form of level 1 (E_8 even, unimodular), weight 4 ($\dim E_8/2$).)

For norm 8 there are two orbits, because we have vectors that are twice a norm 2 vector, and vectors that are not. As the norm gets bigger, there are a large number of orbits.

What is the order of the Weyl group of E_8? We'll do this by 4 different methods, which illustrate the different techniques for this kind of thing:

(1) This is a good one as a mnemonic. The order of E_8 is given by

$$\begin{aligned}|W(E_8)| &= 8! \times \prod \begin{pmatrix}\text{numbers on the} \\ \text{affine } E_8 \text{ diagram}\end{pmatrix} \times \frac{\text{Weight lattice of } E_8}{\text{Root lattice of } E_8} \\ &= 8! \times (1.2.3.4.5.6.4.2.3) \times 1 \\ &= 2^{14} \times 3^5 \times 5^2 \times 7\end{aligned}$$

These are the numbers giving highest root.

We can do the same thing for any other Lie algebra, for example,

$$\begin{aligned}|W(F_4)| &= 4! \times (1.2.3.4.2) \times 1 \\ &= 2^7 \times 3^2\end{aligned}$$

(2) The order of a reflection group is equal to the products of degrees of the fundamental invariants. For E_8, the fundamental invariants are of degrees 2,8,12,14,18,20,24,30 (primes +1).

(3) This one is actually an honest method (without quoting weird facts). The only fact we will use is the following: suppose G acts transitively on a set X with $H =$ the group fixing some point; then $|G| = |H| \cdot |X|$.

This is a general purpose method for working out the orders of groups. First, we need a set acted on by the Weyl group of E_8. Let's take the root vectors (vectors of norm 2). This set has 240 elements, and the Weyl group of E_8 acts transitively on it. So $|W(E_8)| = 240 \times |\text{subgroup fixing } (1, -1, 0^6)|$. But what is the order of this subgroup (call it G_1)? Let's find a set acted on by this group. It acts on the set of norm 2 vectors, but the action is not transitive. What are the orbits? G_1 fixes $s_1 = (1, -1, 0^6)$. For other roots r, G_1 obviously fixes (r, s). So how many roots are there with a given inner product with s?

(s, r)	number	choices
2	1	s
1	56	$(1, 0, \pm1^6), (0, -1, \pm1^6), (\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}^6)$
0	126	
−1	56	
−2	1	$-s$

So there are at least 5 orbits under G_1. In fact, each of these sets is a single orbit under G_1. How can we see this? Find a large subgroup of G_1. Take $W(D_6)$, which is generated by all permutations of the last 6 coordinates and all even sign changes of the last 6 coordinates. It is generated by reflections associated to the roots orthogonal to e_1 and e_2 (those that start with two 0s). The three cases with inner product 1 are three orbits under $W(D_6)$. To see that there is a single orbit under G_1, we just need some reflections that mess up these orbits. If we take a vector $(\frac{1}{2}, \frac{1}{2}, \pm\frac{1}{2}^6)$ and reflect norm 2 vectors through it, this mixes up the orbits under $W(D_6)$, so we get exactly 5 orbits. So G_1 acts transitively on these orbits.

In fact G_1 is the Weyl group of E_7, as we will see during the calculation. We also obtain the decomposition of the Lie algebra E_8 under the action of E_7: it splits as representations of dimensions 1, 56, 133, 1, 56, 1. If we look a bit more closely we see that in fact there is a subgroup $E7 \times SL_2$, and E_8 decomposes as $133 \otimes 1 \oplus 56 \otimes 2 \oplus 1 \otimes 3$. One can see directly from the roots that the 56 dimensional representation has an invariant bilinear form induced by the Lie bracket of E_8. The 56 dimensional representation of E_7 has the special property that all its weights are conjugate under the Weyl group: such representations are called minuscule, and tend to be rather special: they include spin representations and some vector representations.

We'll use the orbit of the 56 vectors r with $(r, s_1) = -1$. Let G_2 be the generated by reflections of vectors orthogonal to s_1 and s_2 where $S_2 = (0, 1, -1, 0, 0, 0, 0, 0)$.

We have that $|G_1| = |G_2| \cdot 56$.

G_2 is the Weyl group of E_6. We can see that E_7 decomposes under E_6 as $133 = 78 + 1 + 27 + 27$: we get two dual 27 dimensional minuscule representations of E_6. We can also decompose E_8 as a representation of E_6, or better as a representation of $E_6 + sl_2$, and we get $240 = 78 \times 1 + 27 \times 3 + 27 \times 3 + 1 \times 8$.

Our plan is to chose vectors acted on by G_i, fixed by G_{i+1} which give us the Dynkin diagram of E_8. So the next step is to try to find vectors r such that s_1, s_2, r form a Dynkin diagram A_3, in other words r has inner product -1 with s_2 and 0 with s_1. The possibilities for r are $(-1, -1, 0, 0^5)$ (one of these), $(0, 0, 1, \pm1, 0^4)$ and permutations of its last five coordinates (10 of these), and $(-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \pm\frac{1}{2}^5)$ (there are 16 of these), so we get 27 total. Then we should check that they form one orbit, which is boring so we leave it as an exercise.

Next we find vectors r such that s_1, s_2, s_3, r form a Dynkin diagram A_4, where s_3 is of course $0,0,1,-1,0,0,0,0)$,

i.e., whose inner product is -1 with s_3 and zero with s_1, s_2. The possibilities are permutations of the last four coords of $(0,0,0,1,\pm 1,0^3)$ (8 of these) and $(-\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2},\pm\frac{1}{2}^4)$ (8 of these), so there are 16 total. Again we should check transitivity, but ill not bother.

For the next step, we want vectors r such that s_1, s_2, s_3, s_4, r form a Dynkin diagram A_5; the possibilities are $(0^4, 1, \pm 1, 0^2)$ and permutations of the last three coords (6 of these), and $(-\frac{1}{2}^4, \frac{1}{2}, \pm\frac{1}{2}^3)$ (4 of these) for a total of 10 vectors r, and as usual these form a single orbit under G_5.

For the next step, we want vectors r such that $s_1, s_2, s_3, s_4, s_5, r$ form a Dynkin diagram A_6; the possibilities are $(0^5, 1, \pm 1, 0)$ and permutations of the last two coords (4 of these), and $(-\frac{1}{2}^5, \frac{1}{2}, \pm\frac{1}{2}^2)$ (2 of these) for a total of 6 vectors r, and as usual these form a single orbit under G_6.

The next case is tricky: we want vectors r such that $s_1, s_2, s_3, s_4, s_5, s_6, r$ form a Dynkin diagram A_7;, the possibilities are $(0^6, 1, \pm 1)$ (2 of these) and $((-\frac{1}{2})^6, \frac{1}{2}, \frac{1}{2})$ (just 1). The proof of transitivity fails at this point. The group G_7 we are using by now doesn't even act transitively on the pair $(0^6, 1, \pm 1)$ (we can't get between them by changing an even number of signs). What elements of $W(E_8)$ fix all of these first 6 points? We want to find roots perpendicular to all of these vectors, and the only possibility is $((\frac{1}{2})^8)$. How does reflection in this root act on the three vectors above? $(0^6, 1^2) \mapsto ((-\frac{1}{2})^6, \frac{1}{2}^2)$ and $(0^6, 1, -1)$ maps to itself. Is this last vector in the same orbit? In fact they are in different orbits. To see this, look for vectors completing the E_8 diagram. In the $(0^6, 1, 1)$ case, we can take the vector $((-\frac{1}{2})^5, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2})$. But in the other case, we can show that there are no possibilities. So these really are different orbits. In other words, there are 3 possible roots r, but these form two orbits under G_7 of sizes 1 and 2.

We use the orbit with 2 elements, and check that there are no automorphisms fixing s_1 to s_7, so we find

$$|W(E_8)| = 240 \times \underbrace{56 \times \overbrace{27 \times 16 \times 10 \times 6 \times 2 \times 1}^{\text{order of } W(E_6)}}_{\text{order of } W(E_7)}$$

because the group fixing all 8 vectors must be trivial. We also get that

$$|W(\text{“}E_5\text{”})| = 16 \times \underbrace{10 \times \overbrace{6 \times 2 \times 1}^{|W(A_2 \times A_1)|}}_{|W(A_4)|}$$

where “E_5” is the algebra with diagram (that is, D_5). Similarly, E_4 is A_4 and E_3 is $A_2 \times A_1$.

We got some other information. We found that the Weyl group of E_8 acts transitively on all the configurations A_1, A_2, A_3, A_4, A_5, A_6, but not on A_7. Obviously a similar method can be used to find orbits of other reflection groups on other configurations of roots.

The sequence of numbers 1, 2 (or 3), 6, 10, 16, 27, 56, 240 tends to turn up in a few other places, such as the number of exceptional curves on a del Pezzo surface (blow up the plane at some points). In particular the number 27 is the same 27 that appears in the 27 lines on a cubic surface (=plane blown up at 6 points).

(4)

We now give the fourth method of finding the order of $W(E_8)$. Let L be the E_8 lattice. Look at $L/2L$, which has 256 elements. Look at this as a set acted on by $W(E_8)$. There is an orbit of size 1 (represented by 0). There is an orbit of size $240/2 = 120$, which are the roots (a root is congruent mod $2L$ to it's negative). Left over are 135 elements. Let's look at norm 4 vectors. Each norm 4 vector, r, satisfies $r \equiv -r \mod 2$, and there are $240 \cdot 9$ of them, which is a lot, so norm 4 vectors must be congruent mod 2 to other norm 4 vectors. Let's look at $r = (2,0,0,0,0,0,0,0)$. Notice that it is congruent to vectors of the form $(0 \cdots \pm 2 \ldots 0)$, of which there are 16. It is easy to check that these are the only norm 4 vectors congruent to r mod 2. So we can partition the norm 4 vectors into $240 \cdot 9/16 = 135$ subsets of 16 elements. So $L/2L$ has 1+120+135 elements, where 1 is the zero, 120 is represented by 2 elements of norm 2, and 135 is represented by 16 elements of norm 4. A set of 16 elements of norm 4 which are all congruent is called a FRAME. It consists of elements $\pm e_1, \ldots, \pm e_8$, where $e_i^2 = 4$ and $(e_i, e_j) = 1$ for $i \neq j$, so up to sign it is an orthogonal basis.

Then we have

$$|W(E_8)| = (\#\text{ frames}) \times |\text{subgroup fixing a frame}|$$

because we know that $W(E_8)$ acts transitively on frames. So we need to know what the automorphisms of an orthogonal base are. A frame is 8 subsets of the form $(r, -r)$, and isometries of a frame form the group $(\mathbb{Z}/2\mathbb{Z})^8 \cdot S_8$, but these are not all in the Weyl group. In the Weyl group, we found a $(\mathbb{Z}/2\mathbb{Z})^7 \cdot S_8$, where the first part is the group of sign changes of an even number of coordinates. So the subgroup fixing a frame must be in between these two groups, and since these groups differ by a factor of 2, it must be one of them. Observe that changing an odd number of signs doesn't preserve the E_8 lattice, so it must be the group $(\mathbb{Z}/2\mathbb{Z})^7 \cdot S_8$, which has order $2^7 \cdot 8!$. So the order of the Weyl group is

$$135 \cdot 2^7 \cdot 8! = |2^7 \cdot S_8| \times \frac{\#\text{ norm 4 elements}}{2 \times \dim L}$$

Remark 312 Conway used a similar method to calculate the order of his largest simple group. In this case if we take the Leech lattice mod 2, it decomposes rather like E_8 mod 2 except there are 4 orbits: the zero vector, orbits represented by a pair $\pm r$ of norm 4 vectors, orbits represented by a pair $\pm r$ of norm 6 vectors, and orbits represented by a frame of 48 norm 8 vectors. The subgroup fixing a frame is $2^{12}.M_{24}$, If Λ is the Leech lattice, we find the order of its automorphism group is

$$|2^{12} \cdot M_{24}| \cdot \frac{\#\text{ norm 8 elements}}{2 \times \dim \Lambda}$$

where M_{24} is the Mathieu group (one of the sporadic simple groups). Conway's simple group has half this order, as one gets it by quotienting out the center ± 1. The Leech lattice seems very much to be trying to be the root lattice of the monster group, or something like that, with its automorphism group behaving rather like a Weyl group, but no one has really been able to make sense of this idea.

$W(E_8)$ acts on $(\mathbb{Z}/2\mathbb{Z})^8$, which is a vector space over $\mathbb{F}_2$, with quadratic form $N(a) = \frac{(a,a)}{2} \mod 2$, so we get a map

$$\pm 1 \to W(E_8) \to O_8^+(\mathbb{F}_2)$$

which has kernel ± 1 and is surjective, as can be seen by comparing the orders of both sides. O_8^+ is one of the 8 dimensional orthogonal groups over $\mathbb{F}_2$. So the Weyl group of E_8 is a double cover of an orthogonal group of a vector space over $\mathbb{F}_2$.

26 Invariants of reflection groups

The ring of invariants of a Weyl group turns up a lot in representation theory. For example, Harish-Chandra showed that the center of the UEA of a semisimple Lie algebra (the "higher Casimir s") is isomorphic to the ring of invariants of the Weyl group. The rational homology of the compact Lie group can be read off from the ring of invariants of the Weyl group. Fortunately it turns out to have a very easy structure: it is a polynomial ring. (This is unusual: rings of invariants of finite groups are usually very complicated.)

For the reflection group S_n acting on R^n the invariants are just the symmetric functions, which form a polynomial ring generated by the usual elementary symmetric functions.

Exercise 313 Show that the ring of invariants of the reflection group $S_n = A_{n-1}$ acting on $\mathbb{R}^{n-1}$ (identified with the vector space of vectors in $\mathbb{R}^n$ whose sum of coordinates is 0) is the polynomial ring $\mathbb{C}[e_2, \cdots e_n]$ in $n-1$ generators.

Exercise 314 Show that the rings of invariants of the reflection groups B_n and D_n are polynomial rings, and find sets of generators.

Exercise 315 Show that the ring of invariants of the alternating group acting on $x_1, \cdots, x_n$ is generated by the invariants $\mathbb{C}[e_1, \ldots, e_n]$ of the symmetric group together with the invariant $\Delta = \prod_{i<j}(x_i - x_j)$. Show that Δ^2 is a polynomial in $\mathbb{C}[e_1, \ldots, e_n]$ and find this polynomial explicitly when n is 2 or 3. Show that if $n = 3$ the ring of invariants is not a polynomial ring.

Example 316 Suppose G is the dihedral group of order $2n$ acting on R^2. We will find its ring of invariants. The obvious coordinate are x and y, but it is easier to use $z = x + iy$ and $\overline{z} = x - iy$ as coordinates. Then one generator of G takes z to ζz and $\overline{z}$ to $\zeta\overline{z}$, while the other exchanges z and $\overline{z}$. The ring of invariants is generated by $z\overline{z}$ and $z^n + \overline{z}^n$.

The invariants of a finite complex reflection group form a polynomial algebra. This was first proved by Shephard and Todd who classified all complex reflection groups into 3 infinite series and 34 exceptional cases, and found the ring of invariants cases by case. Shortly after Chevalley gave a uniform proof.

Lemma 317 *If H is a homogeneous polynomial in $I_1, \ldots$ and $\frac{\partial H}{\partial I_1}$ is a linear combination of $\frac{\partial H}{\partial I_2}, \ldots$, then $\frac{\partial H}{\partial I_1} = 0$.*

Proof Look at the terms of H containing a smallest power of I_1. This shows that H must contain terms not involving I_1. Moreover we get a linear relation between the terms of $\frac{\partial H}{\partial x_2} \ldots$ that do not involve I_1. Now use induction on $H(0, I_2, \cdots)$. □ Most rings

of invariants are not polynomial rings, so we need to find and use some special property of rings of invariants when the group is generated by reflections. The following is the special property of rings of invariants of groups generated by reflections that implies they are polynomial rings.

Lemma 318 *If $I_1, \ldots$ are homogeneous invariants of a complex reflection group such that I_1 is not in the ideal generated by $I_2, \ldots$, and there is some relations*

$$p_1 I_1 + p_2 I_2 + \cdots = 0$$

for homogeneous polynomials p_i, then p_1 is in the ideal generated by invariants of positive degree.

Proof The special property of reflections that we will use is that if g is a reflection with hyperplane $f = 0$ then $p - gp$ is divisible by f. So we find

$$\frac{gp_1 - p_1}{f} I_1 + \frac{gp_2 - p_2}{f} I_2 + \cdots = 0$$

and by induction on the degree of p_1 we see that $gp_1 - p_1$ is in the ideal generated by invariants of positive degree. So taking an average over $g \in G$ shows that $|G| p_1$ is a linear combination of an invariant and an element in the ideal generated by positive degree invariants. By assumption p_1 cannot have degree 0, so must be in the ideal generated by invariants of positive degree. □

Theorem 319 *(Chevalley-Shepherd-Todd) The ring of invariants of a complex reflection group is a polynomial algebra.*

Proof Pick a minimal set of homogeneous invariants $I_1, I_2, \ldots$ that generate the ideal generated by positive degree invariants (so that by Hilbert's theorem they also generate the ring of invariants), We will show that they are algebraically independent. Suppose that $H(I_1, I_2, \ldots) = 0$ for some homogeneous polynomial H. Then

$$\frac{\partial H}{\partial I_1} \frac{\partial I_1}{\partial x_i} + \frac{\partial H}{\partial I_2} \frac{\partial I_2}{\partial x_i} + \cdots = 0$$

Choose I_1 so that it is degree at least that of $I_2, \cdots$. Then $\frac{\partial H}{\partial I_1}$ is an invariant polynomial in $x_1, \ldots$. It has degree at most equal to that of $\frac{\partial H}{\partial I_2}, \ldots$ so by lemma ??? is is not in the ideal generated by $\frac{\partial H}{\partial I_2}, \ldots$. By lemma ??? this shows that its coefficient $\frac{\partial I_1}{\partial x_i}$ is in the ideal generated by invariants of positive degree. But then

$$\deg(I_1)I_1 = \sum x_i \frac{\partial I_1}{\partial x_i}$$

is also in this ideal, contradicting the fact that I_1 is not in the ideal generated by the other invariants $I_2, \ldots$. This shows that the invariants $I_1, I_2, \ldots$ are algebraically independent, so the ring of invariants is the polynomial ring in these generators. □

Theorem 320 *(Molien) If G is a finite group acting on a vector space V, then the Poincar series of its ring of invariants $S(V)^G$ is*

$$\sum_n t^n \dim((S^n V)^G) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - tg)}$$

Proof A single element g acting on $\oplus t^n S^n(V)$ has trace $\frac{1}{\det(1-tg)}$, as one can see by diagonalizing g. But the dimension of the invariant space of a representation is just the average of the trace of all elements of g. □

In particular if the ring of invariants of a group is polynomial with generators of degrees d_i, we find

$$\prod \frac{1}{1 - t^{d_i}} = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - tg)}$$

because the left hand side is the Poincar series of the polynomial ring. Multiplying both sides by $(1-t)^n$ for $n = \dim(V)$ we find

$$\prod \frac{1}{1 + t + \cdots + t^{d_i} - 1} = \frac{1}{|G|} \sum_{g \in G} \frac{(1-t)^n}{\det(1 - tg)}$$

Setting $t = 1$ we find all terms on the left vanish except for the term corresponding to the identity element of G, so we find

$$\prod d_i = |G|.$$

Exercise 321 By examining the derivative of both sides at $t = 1$ show that

$$\sum (d_i - 1) = \text{half the number of (non-trivial) reflections of } G$$

The degrees d_i of the generating invariants of a Weyl group control the corresponding compact Lie group. For example, the real cohomology of the group is an exterior algebra on generators of degrees $2d_i - 1$, and the center of the UEA is a polynomial algebra generated by elements of degrees d_i and, the order of a "simply connected" Chevalley group is given by $q^{\sum d_i - 1} \prod (q^{d_i} - 1)$.

Example 322 The rings of invariants of groups that are not reflection groups tend to be rather complicated. For example, if we take a cyclic group of order n acting on $\mathbb{C}[x, y]$ where the generator multiplies both x and y by a primitive nth root of 1, then the invariants are generated by the $n + 1$ monomials $x^i y^{n-i}$ which is usually not a polynomial ring. There are many relations between these generators. In general the ring of invariants of a finite group is finitely generated by Hilbert's theorem, but the number of generators can be very large, and is usually much larger than the dimension of the representation.

This still leaves the problem of finding the degrees of the polynomial generators of the Weyl groups of F_4, E_6, E_7, E_8. One way is to use the following fact: count the number of positive roots of given height (where the simple roots have height 1). Then the degrees of the invariants are the heights where the number of roots drops by 1.

Exercise 323 Find the heights of the 24 positive roots of F_4, and use the fact mentioned above to show that the degrees of the fundamental invariants are $2, 6, 8, 12$. If you are feeling ambitious, try E_6, E_7, E_8.

27 Hilbert's finiteness theorem

Given a Lie group acting linearly on a vector space V, a fundamental problem is to find the orbits of G on V, or in other words the quotient space. For example, one might want to find the binary forms of degree n up to equivalence under the action of SL_2. One way to attack this problem is to look at invariants: at least formally, the functions on the quotient space V/G might be the invariant functions $S(V^*)^G$ on V. There are a few problems with this as shown by the following examples:

Example 324 Suppose G is the group of non-zero reals acting on the reals, so there are two orbits. However the ring of invariants is just $\mathbb{R}$, so this does not show both orbits. The problem arises from the fact that one orbit is in the closure of the other, so any invariant function has the same value on both orbits and invariant functions cannot separate them. The quotient space in this case is not even Hausdorff. This problem does not appear if the group is compact, so all orbits are closed. In geometric invariant theory on deals with it by only considering "stable" or "semistable" orbits.

Example 325 Suppose G is the group of order 2 acing on the reals by -1. The ring of invariants is a polynomial ring on 1 variable, suggesting that the quotient space should be the real line. It is not: it is half the real line. What is happening is that there are some orbits $\{ix, -ix\}$ in $\mathbb{C}$ that are invariant under complex conjugation, even though the elements in the orbits are not. In other words the ring of invariants is not really detecting orbits of G on V, but rather orbits of G on $V \otimes C$ that are defined over the reals.

To summarize, we might expect the ring of invariants to tell us what the orbits are, provided the group is compact and its representation is complex. Otherwise the relation between the ring of invariants and the orbits is more subtle.

We can now ask if the space of orbits, or rather the spectrum of the ring of invariants, is an algebraic variety. It is an algebra over the complex numbers with no nilpotents, so it comes from an algebraic variety if and only if it is finitely generated. Hilbert proved that it was finitely generated in many cases.

We start by disposing of the standard myth about Hilbert's finiteness theorem. Gordan is supposed to have said about Hilbert's finiteness proof "this is not math; this is theology" as Hilbert's proof was not constructive. It is not all all clear if he really said this, since there is no written record of it until many years after he died, and in any case it may have been a joking compliment rather than a complaint, as Gordan thought highly of Hilbert's work.

Theorem 326 *If G is a Lie group whose finite dimensional representations are completely reducible, then the ring of invariants of G acting on a finite dimensional vector space is finitely generated.*

Proof We do the case when G is finite. A is graded by degree. Let I be ideal generated by positive degree elements of A^G. Then I is a finitely generated ideal by Hilbert basis theorem, with generators $i_1, \ldots, i_k$ which we can assume are fixed by G. We want to show that these generate A^G as an algebra, which is much stronger than saying they generate the ideal I. (Example: subring of $k[x, y]$ generated by xy^* is NOT finitely generated, even though the corresponding ideal is. We need to use some special property of subrings fixed by a finite group.)

We use the Reynolds operator ρ given by taking average under action of G (which needs char=0, though in fact Hilbert's theorem is still true for finite groups in positive characteristic). Key properties: $\rho(ab) = a\rho(b)$ if a fixed by G, $\rho(1) = 1$. It is not true that $\rho(ab) = \rho(a)\rho(b)$ in general. ρ is a projection of A^G modules from A to A^G but is not a ring homomorphism.

We show by induction on degree of x that if $x \in A^G$ then it is in algebra generated by i's.

We know

$$x = a_1 i_1 + \ldots + a_k i_k$$

for some a's in A as x is in I. Apply Reynolds operator:

$$x = \rho(x) = \rho(a_1) i_1 + \ldots + \rho(a_k) i_k$$

By induction $\rho(a_j)$ is in A^G as it has degree less than that of x, so $x \in A^G$. □

It is astonishing that one of the biggest problems in the 19th century can now be disposed of in a few lines of algebra. This is essentially Hilbert's proof, though his version of it occupied many pages. He had to develop background results that are now standard such as his finite basis theorem, and instead of using integration over compact groups used a more complicated operator called Cayley's omega process.

The simplicity of the proof may be a bit misleading: it is rather difficult in general to find explicit generators for rings of invariants, except for a few special cases such as reflection groups. The invariants tend to be horrendously complicated polynomials, and the number of them needed as generators can be enormous. In other words rings of invariants are usually too complicated to write down explicitly. In turn this suggests that the orbit space of a vector space under a Lie group may in general be rather complicated.

Compact groups: the proof is similar as can still integrate over the group:

Noncompact groups such as $SL_n(\mathbb{C})$: Use Weyl's unitarian trick: invariant vectors (for finite dimensional complex reps of the complex group) same as for compact subgroup SU_n, so still get Reynolds operator. Works for all semisimple or reductive algebraic groups (key point: reps are completely reducible), but NOT for some unipotent groups (Nagata counterexample to Hilbert conjecture). Char p harder as groups need not be completely reducible; e.g. Z/pZ acting on 2-dim space over $\mathbb{F}_p$. Haboush proved Mumford's conjecture giving a sort of nonlinear analogue of Reynolds operator, which can be used to prove finitely generated of invariants for reductive groups as in char 0.

Example 327 Classical invariant theory: $G = SL_2(\mathbb{C})$ acting on

$$a_n x^n + a_{n-1} x^{n-1} y + \ldots + a_0 y^n$$

, $A = \mathbb{C}[a_0, \ldots, a_n]$. A^G is the ring of invariants of binary forms, shown to be finitely generated by Gordan. More complicated examples in more variables shown to be finitely generated by Hilbert. Example of an invariant: the discriminant $b^2 - 4ac$ of $ax^2 + bxy + cy^2$.

Example 328 Hilbert asked if the finiteness theorem still holds for all groups, even if their finite dimensional representations are not completely reducible. Nagata found a counterexample as follows. Take the group R acting on R^2 by $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$. The sum of 16 copies of this gives an action of R^{16} on a vector space R^{32}. Nagata showed that for a generic 13-dimensional subgroup G of the R^{16}, the ring of invariants is not finitely generated. The group G is just an abelian Lie group, showing again that abelian Lie groups are in some ways more complicated than the simple ones.

28 Finite dimensional representations of semisimple Lie groups

We now want to study the finite dimensional representations of the semisimple Lie groups we have constructed. There are several problems to solve:

- Find the irreducible representations.
- Find the dimension, and more generally the characters, of the irreducible representations
- Describe the tensor products, symmetric squares, and so on of representations. In other words find the structure of the lambda-ring generated by representations.
- Find natural geometric realizations of the representations.

We will solve the first problem, of parameterizing the irreducible representations, by showing that they correspond to weights in the fundamental Weyl chamber (Cartan's theorem).

If we have a representation of one of the Lie algebras we constructed from a finite root system, then we can look at eigenvectors of the Cartan subalgebra H. By hitting an eigenvector with elements e_i as much as possible, we can assume that the eigenvalue of the eigenvector is a highest weight, in other words the eigenvalue is killed by all the e_i and is an eigenvector of all the h_i. There is a universal module with these properties called a Verma module. We can construct it as an induced modules

$$U(E, H, F) \otimes_{U(E,H)} V$$

where V is any 1-dimensional module over H, where we let E act trivially on it, so is a module for the UEA $U(E, H)$ of the subalgebra generated by E and

H. By the PBW theorem we can see that the Verma module can be identified with the UEA of F, so is the same size as the symmetric algebra on F.

The Verma module is of course infinite dimensional and we need to cut it down. Look at the action of one of the SL_2 subalgebras e_i, h_i, f_i on the highest weight vector v. This generates a Verma module for SL_2, which is infinite dimensional and usually irreducible. The only way to cut it down to something finite dimensional is to kill off $f^{1+2(\alpha,\alpha_i)/(\alpha_i,\alpha_i)}v$, where α is the weight of v and α_i is the root of e_i. So we get two necessary conditions on α for it to be the highest weight of a finite dimensional module:

1. (α, α_i) must be an integral multiple of $(\alpha_i, \alpha_i)/2$, in other words α must be in the "weight lattice"

2. (α, α_i) must be at least 0, in other words α must be in the fundamental Weyl chamber.

Conversely if α satisfies these conditions then we get a finite dimensional module by killing off all the elements $f^{1+2(\alpha,\alpha_i)/(\alpha_i,\alpha_i)}v$. The proof of this is similar to the proof that the Lie algebras were finite dimensional: the extra relations imply that the highest weight vector is contained in finite dimensional representations of all the sl_2's, which implies that every vector of the representation is contained in finite dimensional sl_2 modules. As before this implies that the representations of the Lie algebras sl_2 lift to representations of the groups SL_2, and therefore the Weyl group acts on the weight spaces. Just as for the case of Lie algebras, this implies that the representation is finite dimensional.

So this gives a complete list of the finite dimensional irreducible representations, though it is not obvious what their dimensions or characters are.

We should figure out what the weight lattices are. The weight lattices all contain the root lattices with finite index, $n+1$ for A_n, 2 for B_n, C_n, 4 for D_n, (though there is a difference for n even or odd, as the quotient may be a Klein 4-group or cyclic), 1 for E_8, F_4, G_2, 2 for E_7, and 3 for E_6.

In general it is not yet clear what the characters or dimensions are: this will later be given by the Weyl character and dimension formulas. However there are some easy cases where we can already write down the answers, where the representation is either minuscule or a representation of SL_3.

28.1 Minuscule representations.

There is one case where it is easy to work out the character of a representation: this is when all weights are conjugate under the Weyl group, so they all have the same multiplicity as the highest weight, which is of course 1. These are called minuscule representations. They tend to turn up a lot as the "smallest" representations of a group: in fact, together with the adjoint representation and the representation with highest weight a "short" root, they account for most of the finite-dimensional representations that people study explicitly.

Minuscule representations correspond to characters of the center of the simply connected compact group. More precisely, for each coset of the weight lattice, pick a vector of smallest norm. This is the highest weight of a minuscule representation.

Some authors do not count the identity representation as a minuscule representation, which is rather like removing the zero element from a vector space.

We can list the minuscule representations as follows:

- A_n: the minuscule representations are the exterior powers of the vector representation.
- B_n: the minuscule representations are the trivial representation and the spin representation. (The vector representation is not minuscule!)
- C_n: the minuscule representations are the trivial one and the vector representation.
- D_n: the minuscule representations are the trivial representation, the vector representation, and the two half spin representations.
- E_6: The minuscule representations are the trivial representation and the two 27-dimensional representations, which we constructed earlier by decomposing E_8
- E_7 The minuscule representations are the trivial representation and the 56 dimensional one.

28.2 Representations of SL3

For SL_3 we already have enough information to find the characters of the irreducible representations. The character of a Verma module is the character of a polynomial algebra on 3 generators, so looks like:

We can also work out the character of $V_\lambda / f^{1+(\lambda,\alpha_1)}$ as:

Using the fact that the character is invariant under the Weyl group, this gives the character of the irreducible representation: it is in the convex hull of a sort of semiregular hexagon, and the weight multiplicities increase by 1 every time one goes 1 step further in, until one gets to the "triangle" in the center when they become constant.

Example 329 The dimensions of the irreducible representations of dimension at most 30 are 1, 3, 3, 6, 6, 8, 10, 10, 15, 15, 15, 15, 21, 21, 24, 24, 27, 28, 28,... In general the dimension of the representation whose highest weight has inner products m, n with the simple roots is $(m+1)(n+1)(m+n+2)$: these factors are the inner products of $\lambda + \rho$ with the simple roots. This is a special case of the Weyl dimension formula.

Exercise 330 Verify that the irreducible representation of SL_3 whose highest weight has inner products m and n with the simple roots has dimension $(m+1)(n+1)(m+n+2)$.

Example 331 We can decompose tensor products of representations of SL_3 by calculating their characters and writing these as linear combinations of irreducible characters. For example, $6 \otimes 6 = 15 \oplus 15 \oplus \overline{6}$, $6 \otimes \overline{6} = 27 \oplus 8 \oplus 1$, $8 \otimes 3 = 15 \oplus 6 \oplus \overline{3}$ and so on,

This graphical method is fine for small representations but becomes cumbersome for larger representations. The Littlewood-Richardson rule is a more efficient method for decomposing larger tensor products.

28.3 Compact Lie algebras

The Lie algebras we have constructed are defined over the reals, but are the split rather than the compact forms. We can get the compact forms by twisting them. If we have any involution ω of a real Lie algebra L, we can construct a new Lie algebra as the fixed points of ω extended as an antilinear involution to $L \otimes \mathbb{C}$. This is using the fact that real forms of a complex vector space correspond to antilinear involutions. The reason why we use involutions rather than elements of some other order is related to the fact that the Galois group of $\mathbb{C}/\mathbb{R}$ has order 2. More generally if we wanted to classify (say) rational Lie algebras, we would get a problem involving non-abelian Galois cohomology groups of the Galois group of the rationals.

Example 332 The Lie algebra of the unitary group is given by the complex matrices A with $A = -\overline{A}^T$, so the involution in this case is $A \mapsto -A^T$.

It is obvious how to generalize this example to the Lie algebras constructed from the Serre relations: the analogue of the transpose swaps e_i and f_i, so the involution ω takes e_i to $-f_i$, f_i to $-e_i$, and h_i to $-h_i$.

To show that the corresponding Lie group is compact, it is enough to find an invariant symmetric bilinear form on the Lie algebra that is definite, as the Lie group is then a subgroup of the orthogonal group. The split algebra has a symmetric bilinear form because the adjoint representation is self dual (minus a root is still a root) and this bilinear form can be normalized so that $(e_i, f_i) = 1$. This bilinear form is not definite: for example $(e_i, e_i) = 0$, but a straightforward calculation shows that its twist by ω is negative definite.

An immediate consequence is that the finite dimensional representations of all the simple Lie algebras we have constructed are completely reducible, by Weyl's unitarian trick: their finite dimensional representations are the same as those of a compact group.

For a compact Lie algebra, there may be several different connected compact Lie groups with different centers. We would like to find the simply connected group (and check it is compact!) so that all others are quotients of it. The key point is that the center of the simply connected compact group can be identified with the dual of the finite group (weight lattice/root lattice).

To see this, pick a finite dimensional representation and look at a Cartan subgroup of the group acting on this representation. Its image is isomorphic to (Cartan subalgebra/dual of lattice generated by the weights of the representation). Except for trivial representations, this lies between (Cartan subalgebra/dual of weight lattice) and (Cartan subalgebra/dual of root lattice). So we see that the Cartan subgroup of the simply connected group is (Cartan subalgebra/dual of root lattice) and its center is (Dual of root lattice/dual of weight lattice), which is the dual of (Weight lattice/root lattice). (Here we use the fact that for a compact group we can finite faithful finite dimensional representations, and in particular can detect anything in the center using finite dimensional representations.)

Actually we need a slight further argument: we have really only found the maximal finite cover of a compact group. However the fundamental group of the universal cover is finitely generated, so if their is a finite bound for the finite covers then the maximal finite cover is the universal cover, as any finitely generated abelian group such that there is a bound on the sizes of its finite quotients must be finite.

So now we can list the compact simple simply connected Lie groups:

- A_n: SU(n+1), center cyclic of order $n+1$.
- B_n: Spin double cover of $SO(2n+1)$: center cyclic of order 2.
- C_n: $Sp_{2n}(\mathbb{C}) \cap U(2n)$: center cyclic of order 2.
- D_n: spin double cover of SO_{2n}: center of order 4, cyclic if n is odd.
- E_6: Center order 3, faithful action on the 27-dimensional representations
- E_7: Center order 2, faithful action on the 56-dimensional representations
- E_8, F_4, G_2: center order 1, faithful action on adjoint representation.

While the group (weight lattice/root lattice) detects elements of the center that act nontrivially in finite dimensional representations, it fails to detect elements that act trivially in all finite dimensional representations. This cannot happen for compact groups, but is common for noncompact groups. We have already seen an example of this for $SL_2(\mathbb{R})$, whose universal cover has an infinite cyclic center, which is not equal to (weight lattice/root lattice). However the calculation of the center in the non-compact case can be reduced to the compact case, because for a real algebraic group the fundamental group is the same as that of its maximal compact subgroup.

29 Schur indicator for compact Lie groups

In this section all representations will be finite dimensional and groups will be compact Lie groups.

Theorem 333 *For a compact simply connected Lie group, every irreducible representation is self dual if and only if the Weyl group contains -1.*

Proof If α is the highest weight of an irreducible representation, then the lowest weight of its dual is $-\alpha$. There is a unique element w of the Weyl group taking the fundamental Weyl chamber W to $-W$, so $-w$ takes α to the highest weight of its dual. So every representation is self dual if and only if $-w = 1$, in other words if W contains -1. □

Exercise 334 The element $-w$ is an automorphism of the Dynkin diagram. Show that it is the nontrivial automorphism for diagrams of types A_n ($n \geq 2$), D_n (n odd), and E_6, and the identity for all other connected Dynkin diagrams. Show that an irreducible representation is self dual if and only if its highest weight is fixed by $-w$.

Next we have to figure out which of the self dual representations are real and which are quaternionic, or in other words find out whether their invariant bilinear forms are symmetric or alternating.

Theorem 335 *If G is a connected quasi-simple compact Lie group, there is an element q such that an irreducible representation is real or quaternionic depending on whether q acts as $+1$ or -1.*

Proof For the group SU_2 we can check this by direct calculation: the irreducible representations of even dimension have an alternating form, and those of odd dimension have an even form. So the element q is the non-trivial element of the center.

The idea of the proof for general compact groups is to reduce to this case by finding a homomorphism from SU_2 to G such that the restriction of any irreducible representation V of G to this SU_2 contains some irreducible representation W with multiplicity exactly 1. Then any alternating or symmetric form on V must restrict to an alternating or symmetric form on W, so we can tell which by examining the action on W of the image $q \in G$ of the nontrivial element of the center of the SU_2 subgroup.

We will find a suitable SU_2 subgroup by constructing a basis E, F, H for its complexified Lie algebra. We take E to be the sum $\sum_\alpha E_\alpha$ where the sum is over the simple roots and E_α is some nonzero element of the simple root space of α. We take H to be the element of the Cartan subalgebra that has inner product 2 with every simple root, which is possible as the simple roots are linearly independent. Finally we choose F_α in the root space of $-\alpha$ so that $\sum [E_\alpha, F_\alpha] = H$. Then we see that $[H, E] = 2E$. $[E, F] = H$, and $[H, F] = -H$, so we have found an $\mathfrak{sl}_2$ subalgebra.

This subalgebra has the property that $(H, \alpha) > 0$ for every simple root α, which implies that if β is the highest weight of the representation V, then β restricted to $\langle E, F, H\rangle$ has multiplicity 1. So this subalgebra has the desired property that the restriction of any irreducible representation of G has some irreducible representation of multiplicity 1 □

The $\mathfrak{sl}_2$ subalgebra constructed above is sometimes called a principal $\mathfrak{sl}_2$ subalgebra.

Exercise 336 If the dual Weyl vector ρ' has inner product 1 with all simple roots, show that a self-dual irreducible representation with highest weight α is real or quaternionic depending on whether it has even or odd inner product with ρ'. (The dual Weyl vector is essentially the Weyl vector of the "dual" root system, whose roots are the coroots of the root system, and is half the sum of the positive coroots. It can be identified with the Weyl vector if all roots have norm 2. It is essentially the same as the element H in the theorem above.)

Exercise 337 Find suitable elements E, F, H of $M_n(\mathbb{C})$ spanning a principal $\mathfrak{sl}_2$ subalgebra for the case when G is SU_n.

We can figure out this special element of order 2 for the various compact simply connected quasi-simple Lie groups as follows.

A_n q is the element of order 2 if $n \equiv 1 \bmod 4$, otherwise q is the identity.

B_n q is the element of order 2 if $n \equiv 1, 2 \bmod 4$, otherwise q is the identity.

C_n The $2n$-dimensional representation has an alternating bilinear form, so q must be the non-trivial element of the center.

D_n q is an element of order 2 if $n \equiv 1, 2 \bmod 4$ otherwise q is the identity.

E_7 The 56-dimensional representation has an alternating bilinear form (coming from the Lie bracket on $E_8 = E_7 \oplus 56 \otimes 2 \oplus sl_2$), so q must be the non-trivial element of the center.

G_2, F_4, E_6, E_8 The center has no elements of order 2, so q is the identity.

Exercise 338 Which compact simply connected Lie groups have the property that all representations have a symmetric invariant bilinear form?

For the compact connected Lie groups, for any quaternionic representation there is an element of order 2 in the center acting as -1. This is no longer true for quaternionic representations of finite simple groups. There are some (rare) examples of simple finite groups (with no center) with irreducible quaternionic representations. For sporadic finite simple groups real representations are most common and quaternionic representations are quite rare.

30 Weyl character formula

For irreducible representations of general linear groups, we have seen that the characters are given by Schur functions, which can be written as a quotient of two alternating sums over the Weyl group. The Weyl character formula is a generalization of this to all semisimple finite-dimensional complex Lie algebras. It also works for the corresponding complex Lie groups, compact Lie groups, and so on.

Theorem 339 *Weyl character formula. If V is an irreducible representation of the complex semisimple Lie algebra $\mathfrak{g}$ with highest weight λ, then the character of V is given by*

$$\frac{\sum_{w\in W}\epsilon(w)e^{w(\lambda+\rho)}}{e^{\rho}\prod_{\alpha>0}(1-e^{-\alpha})}$$

The special case of the trivial representation with highest weight 0 is the Weyl denominator formula:

$$\sum_{w\in W}\epsilon(w)e^{w(\rho} = e^{-\rho}\prod_{\alpha>0}(1-e^{\alpha})$$

In the case of the general linear group, this is just the Vandermonde identity, as the left hand side is the expansion of the Vandermonde determinant, and the right hand side is its expression as a product. We can use the denominator identity to replace the denominator in the Weyl denominator formula by an alternating sum over the Weyl group.

Example 340 For the group $SL_2(\mathbb{C})$, the Weyl group has order 2, and the Weyl character formula says that the characters are given by

$$\frac{q^{n+1}-q^{-n-1}}{q^{-1}(1-q^2)} = q^{-n}+q^{2-n}+\cdots+q^{n-2}+q^n$$

There are several different ways to prove the Weyl character formula:

- Weyl's original method used the Weyl integration formula for compact Lie groups. The denominator appears as the square root of the weight in the Weyl integration formula.
- It can be proved using a resolution of the irreducible representation by Verma modules. In this case the denominator of the Weyl character formula is the character of a Verma module, and the sum in the numerator is a sum over the Verma modules appearing in the resolution. Kac extended this proof to Kac-Moody algebras.
- It can be proved by studying the Lie algebra homology of the nilradical $\mathfrak{n}$ of a Borel subalgebra. The denominator is then the character of the universal enveloping algebra of $\mathfrak{n}$, and the sum in the numerator is a sum over a basis for the homology groups of $\mathfrak{n}$.

Example 341 We calculate the characters of some representations of G_2. We have already found the first few, of dimensions 1, 7, 14. The next has highest weight twice a shortest root. To use the Weyl character formula, observe that it gives a recursive relation for the character multiplicities, because the product of the character and $\sum \epsilon(w)e^{w(\rho)}$ is usually 0. This means that the alternating sum of the multiplicities over the "dodecagons" coming from conjugates of the Weyl vector are 0, unless the dodecagon passes through exactly one weight. Using this we see that the multiplicities of the vectors are 1 (2 times shortest root) 1 (longest root) 2 (shortest root) and 3 (0), for a total dimension of 27.

We will sketch a proof using Verma modules. Recall that we constructed the irreducible representation of a quotient of a Verma module by other Verma modules. We know the character of a Verma module, so we can try to find the character of the irreducible module by subtracting the characters of the Verma modules we quotient out by:

$$\frac{e^{\lambda} - \sum_{\alpha \text{simple}} e^{\lambda-(2(\lambda,\alpha)/(\alpha,\alpha)+1)\alpha}}{\prod_{\alpha>0}(1-e^{-\alpha})}$$

This gives a first approximation to the character, but is obviously wrong if the Verma modules we quotient out by overlap. In this case we have to add back in terms for their intersections, then subtract further terms when three intersect, and so on. More precisely, we can write down a resolution of the irreducible module by Verma modules, and the character will be an alternating sum of the characters of the terms of the resolution. So far we have only found the first two terms of the resolution.

To see how to fix this, first look at the denominator. If we rewrite it as

$$e^{-\rho}\prod_{\alpha>0}(e^{\alpha}/2 - e^{-\alpha/2})$$

we see that it is alternating under the Weyl group apart from the factor of $e^{-\rho}$ where the Weyl vector ρ is half the sum of the positive roots. Since the character is invariant under the Weyl group, the numerator must be antiinvariant under the Weyl group, at least if we multiply by e^{ρ}. The simplest possibility for the numerator is then

$$\sum_{w\in W}\epsilon(w)e^{w(\rho+\lambda}$$

where ϵ is the determinant of an element of the Weyl group. The first few terms of this sum for w trivial or a reflection are the terms corresponding to the Verma module we started with and the ones we quotiented out by. The problem is that we need to rule out the possibility of having other antiinvariant terms in the numerator such as

$$\sum_{w \in W} \epsilon(w) e^{w(\rho+\mu}$$

for some other vector μ. In other words we need to show that a minimal resolution of the irreducible module with highest weight λ only contains Verma modules with highest weights of the form $w(\lambda+\rho)-\rho$.

To do this we use the Casimir element. Recall that we have a symmetric invariant bilinear on the Lie algebra, which gives us an element of the center of the UEA of the form $\sum a_i a_{i'}$ where a_i forms a basis and $a_{i'}$ is the dual basis. In our case the Casimir is given by $\sum_\alpha e_\alpha e_{-\alpha} + \sum h_i h_{i'}$. We want to apply this to a highest weight vector of a Verma module, so we move all the vectors of negative root spaces over to the left, picking up a term $[e_{-\alpha}, e_\alpha]$ for each positive root α. So the eigenvalue on a highest weight vector with highest weight λ is $\lambda^2 + (\lambda, 2\rho) = (\lambda+\rho)^2 - \rho^2$. In particular two Verma modules have the same eigenvalue of the Casimir only if they have the same value of $(\lambda+\rho)^2$.

This is enough to complete the proof of the Weyl character formula, because any possible highest weight μ that is in the fundamental chamber of the Weyl group and is of the form $\lambda -$ sum of positive roots satisfies $(\mu+\rho)^2 < (\lambda+\rho)^2$ unless $\lambda = \mu$ by elementary geometry.

Example 342 We can work out the characters of representations of B_2 using the fact that the alternating sum over an octagon of the root multiplicities is usually zero. We can also decompose representations by writing them as a linear combination of irreducible characters, or more efficiently by observing that the multiplicity of highest weight vectors is given by an alternating sum over octagons. For example, $4 \times 10 = 20 \oplus 16 \oplus 4$.

For rank 2 groups A_1^2, A_2, B_2, G_2, we get the multiplicities of representations by looking at alternating sums over a square, hexagon, octagon, or dodecagon. This polygon is easy to remember, as it starts off with the origin and the two simple roots.

We can also work out the dimension of a representation from the Weyl character formula. Substituting in the identity element of the group direct fails badly, because both the numerator and the denominator have a zero of high order (half the number of roots) at the identity. In fact, from this point of view the identity element is the most complicated element of the group! (It is also the place where the set of unipotent elements has the worst singularity.) So instead we examine the asymptotic behavior of the numerator and denominator of the Weyl character formula on a carefully chosen set of elements that tend to the identity.

For this we use the Weyl denominator formulas

$$\sum_{w \in W} \epsilon(w) e^{w(\rho)} = e^{-\rho} \prod_{\alpha>0} (1 - e^\alpha)$$

which gives

$$\sum_{w\in W}\epsilon(w)e^{(w(\rho),t\beta)}=\prod_{\alpha>0}(e^{(\alpha/2,t\beta)}-e^{(-\alpha/2,t\beta)})$$

for any real t and any β in the dual of the Cartan subalgebra. We rewrite this as

$$\sum_{w\in W}\epsilon(w)e^{(w(\beta),t\rho)}=\prod_{\alpha>0}t\frac{(e^{(\alpha/2,t\beta)}-e^{(-\alpha/2,t\beta)})}{t}$$

and examine the behavior as t tens to 0. The right hand side behaves like

$$t^N\prod_{\alpha>0}(\alpha,\beta)+\text{higher powers of}t$$

so this gives the asymptotic behavior of the numerator and denominator of the Weyl character formula on the elements $t\rho$. We can now cancel out the factors of t^N and take the limit as t tends to 0, to find that the dimension is

$$\prod_{\alpha>0}\frac{\lambda+\rho,\alpha)}{\rho,\alpha}$$

Example 343 We check the Weyl dimension formula on G_2. If α and β are the long and short simple roots of norms 6 and 2 then the positive roots are $\beta,\alpha,\alpha+\beta,\alpha+2\beta,\alpha+3\beta,2\alpha+3\beta$. Suppose the highest weight *lambda* has inner product $3m$ with α and n with β, with m and n non-negative integers. Then the dimension is

$$\frac{n+1}{1}\times\frac{3m+3}{3}\times\frac{3m+n+4}{4}\times\frac{3m+2n+5}{5}\times\frac{3m+3n+6}{6}\times\frac{6m+3n+9}{9}$$

For $m=0$, $n=2$ this gives the dimension 27 that we found earlier.

Example 344 If we take $n\rho$ as a highest weight, we see that there are irreducible representations of dimension n^N where N is the number of positive roots. This is related to the Steinberg representation of a finite group of Lie type over a field of order q, an irreducible representation of dimension q^N.

For higher rank groups the Weyl character formula becomes rather unwieldy for practical calculations because the sums over the Weyl group become large. In this case a variation of it called the Freudenthal multiplicity formula is easier to use. This states

$$(\Lambda+\rho)^2-(\lambda+\rho)^2\text{Mult}(\lambda)=2\sum_{\alpha>0}\sum_{j>0}(\lambda+j\alpha,\alpha)\text{Mult}(\lambda+j\alpha)$$

where the sums are over positive roots α and positive integers j. Moreover the sum over the positive roots can usually be reduced in size by grouping things into orbits under the Weyl group. The Freudenthal formula can be proved by calculating the trace of the Casimir element on a weight space in two different ways. On the one had the trace is given by the dimension of the roots space times the eigenvalue $\Lambda^2+2(\Lambda,\rho)$. On the other hand the trace of each term e_if_i in the Casimir can be calculated explicitly by decomposing the representation into a sum of SL_2 modules and working out the trace on the weight spaces each of these; this gives terms depending on the number of times each SL_2 module occurs, which is in turn determined by the multiplicities of the weights $\lambda + j\alpha$ for various α. Finally the terms $h_i h_{i'}$ and ρ in the Casimir operator are easy to deal with. Putting everything together gives the Freudenthal recursion formula.

Example 345 We will demonstrate that this really does give a practical method by using it to calculate the character and dimension of a representation of E_8 with highest weight of norm 4. There are 3 possible orbits of weights under the Weyl group of norms 4 (2160 vectors), 2 (240 vectors), and 0 (1 vector). The vectors or norm 4 all have multiplicity 1 as they are conjugate to the highest weight vector. (Note that the Freudenthal formula give no information in this case.) We need to know the Weyl vector of E_8. Taking the simple roots to be $(..., 1, -1, ...)$ and $(-1/2, -1/2, -1/2, 1/2, 1/2, 1/2, 1/2, 1/2)$ gives Weyl vector $(12, 11, 10, 9, 8, 7, 6, 5)$ of norm $\rho^2 = 620$. The norm 4 vector in the Weyl chamber is $\Lambda = (3/2, (1/2)^7)$ with $(\Lambda, \rho) = 46$. If $\lambda = ((1/2)^7, -1/2)$ is the norm 2 vector in the Weyl chamber then $(\lambda, \rho) = 29$. There are 63 positive roots having inner product 0 with λ. So the Freudenthal formula becomes

$$(4 + 2 \times 46 - 2 - 2 \times 29)\mathrm{Mult}(\lambda) = 2 \times 2 \times 63$$

so the multiplicity of λ is 7.

Similarly if $\lambda = 0$ we find

$$(4 + 2 \times 46 - 0 - 2 \times 0)\mathrm{Mult}(\lambda) = 2 \times 2 \times 120 \times 7$$

so the multiplicity of 0 is 35. The dimension of this representation is therefore $2160 \times 1 + 240 \times 7 + 1 \times 35 = 3875$.

Notice that for the Weyl character formula the large size of the Weyl group was a disadvantage because we had to sum over it, but for the Freudenthal formula the large size is an advantage, because it means there are only a few orbits we have to sum over.

Exercise 346 Find the character of the irreducible representation with a highest weight vector of norm 6. Find the character of the alternating square of the adjoint representation and find out how it splits into irreducible representations.

Example 347 We can also work out the character values of characters of E_8 on elements of finite order. To show how to do this we will do the simplest case of the character of the adjoint representation on elements of order 2. The elements of order dividing 2 correspond to orbits of the Weyl group on $L/2L$ and we saw there are 3 orbits, represented by half of vectors of norms 0, 2, 4. If β is a vector of norm 2, then the order 2 element corresponding to $\beta/2$ acts as 1 on weight spaces if the weight has even inner product with β and -1 if the weight has odd inner product with β. We saw earlier that there are $1 + 56 + 134 + 56 + 1$ weights having inner products 2, 1, 0,-1, -2, so the trace of the order 2 element is $1 - 56 + 134 - 56 + 1 = 24$. Similarly for the norm 4 vector the corresponding order 2 element has trace $14 - 64 + 92 - 64 + 14 = -8$.

We can use these two elements of order 2 to find the two non-compact real forms of $E8$ by the usual construction: take the points of $\mathbb{C} \otimes E8$ fixed by an antilinear involution. One of these real forms is the split form, with fixed point subalgebra D_8, and the other is a new real form of E_8 with fixed point subalgebra $E7 \times SL2$. So we have found the 4 simple Lie algebras associated with E_8: a complex form (of real dimension 2×248), a compact form, a split form, and another form.

Example 348 What are the maximal compact subgroups of the two non-compact real forms? Their Lie algebras are D_8 and $E_7 \times SL_2$, but there are several different connected groups with these Lie algebras as their centers are different. For the one with compact subalgebra D_8, we look at the action on the Lie algebra of E_8 and see that it splits as (adjoint representation) plus (half spin representation). So the corresponding compact subgroup is the image of the spin group under this representation, which is the quotient of the sing group by an element of order 2 in the center, different from the one giving the special orthogonal group.

Exercise 349 Similarly show that the maximal compact subgroup of the other real form is the quotient of $E7 \times SL_2(\mathbb{R})$ by the element $(-1, -1)$ of the center.

Our method of finding the elements of order 2 in $E8$ was somewhat ad hoc. There is a more systematic way of finding all elements of finite order as follows. To find elements of order dividing n, We want to classify the elements of $\frac{1}{N}L/L$ up to conjugacy by the Weyl group, where L is the $E8$ lattice, as these correspond to orbits of elements of order dividing N in a maximal torus. In particular we can assume such an element is in the Weyl chamber, so has non-negative inner product with all simple roots. Moreover we can assume that 0 is the nearest lattice point. This implies that $(v, \alpha) \leq (\alpha, \alpha)/2 = 1$ where α is the highest root (the root in the Weyl chamber) otherwise this root would be closer. So if the inner products with the simple roots are n_i/N, then $\sum m_i n_i/N \leq 1$ where the m_i are the numbers giving the highest root as a linear combination of the simple roots. This can be written more neatly as $\sum m_i n_i = N$ where we now include $m_0 = 1$ in the sum. This makes it easy to list the conjugacy classes of elements of any given order in E_8. For example, there are 5 classes of order dividing 3, so 4 classes of order 3.

Exercise 350 Find the conjugacy classes of $E8$ of elements of order at most 6.

Example 351 There is an amusing way to calculate the order of the Weyl group of $E8$ by looking at the number of elements of order dividing N for large N. On the one hand, this number is about N^8 times the index of the root lattice in the weight lattice divided by the order of the Weyl group. On the other hand it is the coefficient of x^N in $\prod(1 - x_{m_i})^{-1}$, which is about $N^8/8! \prod m_i$. SO the order of the Weyl group is $8! \times 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 4 \times 3 \times 2$. A similar method works for other Lie algebras.

The Weyl character formula also has infinite dimensional generalizations that we will discuss briefly. It works for some highest weight representations of Kac–Moody algebras: these are constructed from an infinite root system in the same way that we constructed algebras from finite root systems. To prove the Weyl character formula we needed 3 ingredients: Verma modules, the Weyl group,and the Casimir element. Verma modules for infinite dimensional Lie algebras are much the same as for finite dimensional ones. To get an action of the Weyl group we used the fact that the representation was finite dimensional but we did not need the full force of this: all we really needed was that the representation is "integrable", in other words splits as a sum of finite dimensional representations for each $SL2$, which in turn follows if the highest weight has suitable inner product with each simple root. We can do the same if the Lie algebra is infinite dimensional. The Casimir element is more of a problem, since its definition for an infinite dimensional Lie algebra becomes a divergent infinite sum. Kac discovered how to renormalize it to make sense. We first use the form $2\sum e_i f_i + \sum h_i h_{i'} + \sum [e_i, f_i]$. All these terms except the last make sense on a highest weight vector, but $\sum [e_i, f_i]$ is still an infinite sum of elements of the Cartan subalgebra. it is formally a sort of Weyl vector. In finite dimensional the Weyl vector can also be defined by $(\rho, \alpha) = (\alpha, \alpha)/2$ for all simple roots α, and this definition makes sense in infinite dimensions. Using this modified definition of the Casimir element, Kac showed that it behaves like the Casimir element for finite dimensional Lie algebras and in particular commutes with all elements of the Lie algebra. The proof of the Weyl–Kac character formula for integrable highest weight modules now goes through much as in the finite dimensional case.

Example 352 The Weyl denominator formula for the affine A_1 Kac-Moody algebra is the Jacobi triple product identity

$$\prod (1 - zq^{2n-1})(1 - z^{-1}q^{2n-1})(1 - q^n) = \sum_n (-1)^n z^n q^{n^2}$$

The product is over positive roots of the affine algebra $SL_2[t, t^{-1}]$, and the sum on the right hand side is really a sum over its Weyl group, which is the infinite dihedral group. Not all roots are conjugate under the Weyl group to simple roots. The infinite dihedral group is almost the integers, so sums over it can be written as sums over the integers. More generally there is a similar identity for every finite dimensional simple Lie algebra (or super algebra); these are the Macdonald identities.

Example 353 Suppose that $j(\tau) - 744 = q^{-1} + 196884q + \cdots = \sum c(n)q^n$ is the elliptic modular function. Then

$$j(\sigma) - j(\tau) = p^{-1} \prod_{m>0, n\in\mathbb{Z}} (1 - p^m q^n)^{c(mn)}$$

is a denominator formula for an infinite dimensional Lie algebra of rank 2. Here $q = e^{2\pi i\tau}$, $p = e^{2\pi i\sigma}$, and the root multiplicities of the root $(m, n) \neq (0, 0)$ of the Lie algebra is $c(mn)$. The Weyl group has order 2, and p^{-1} is really the term coming from the Weyl vector.

Alternatively one can stick to finite dimensional Lie algebras, but ask for the characters of infinite dimensional irreducible quotients of Verma modules. As in the finite dimensional case, we can take a resolution by Verma modules. The main problem is that we no longer have an action by the Weyl group. We can still write the character as

$$\sum_{w\in W} \frac{c(w)e^{w(\lambda+\rho)}}{e^{\rho}\prod_{\alpha>0}(1 - e^{-\alpha})}$$

by using all the higher Casimirs, which together show that a Verma module with highest weight μ only occurs in a minimal resolution if $\lambda+\rho$ is conjugate to $\mu+\rho$. However the coefficients $c(w)$ need no longer be ± 1 as we do not have antiinvariance under the Weyl group to determine them. They can be quite complicated, and are given by values of Kazhdan–Lusztig polynomials (by the Kazhdan-Lusztig conjecture, now proved).

31 Jacobi triple product identity

The denominator formula for the affine A_1 algebra is the Jacobi triple product identity

$$\prod(1-zq^{2n-1})(1-z^{-1}q^{2n-1})(1-q^{2n}) = \sum_n (-1)^n z^n q^{n^2}$$

This function (and its generalizations for other simple groups) turns up in several other places:

- It is the denominator formula of a Kac-Moody algebra
- It is the simplest example of a Macdonald identity: an infinite product identity associated to a simple Lie algebra, or more generally an affine root system.
- It is closely related to the Boson-Fermion correspondence
- It is an example of a theta function: these can be thought of as either functions that are periodic up to elementary exponential factors, or as sections of line bundles over elliptic curves (or abelian varieties in the higher dimensional case)
- It is a solution of the heat equation; in fact it is essentially the fundamental solution to the heat equation on a circle.
- By restricting to special values of z one gets modular forms.
- It is the archetypal example of a Jacobi form.
- It spans a representation of finite Heisenberg groups. This does not seem very interesting as it is only the 1-dimensional trivial representation, but by taking slightly more general functions one gets higher dimensional representations.

We start by explaining the relation with the Boson-Fermion correspondence. We rewrite it as

$$\prod(1+zq^{n-1/2})(1+z^{-1}q^{n-1/2}) = \sum_m z^m q^{m^2} \prod(1-q^n)^{-1}$$

and find a combinatorial interpretation of both sides. We suppose that we have some fermions that can occupy energy levels $n+1/2$ for any integer n, with at most one fermion occupying each energy level. To avoid having negative energy states we fill up all the negative energy states with a Dirac sea, and take this to be our vacuum. Then we can either add fermions of energy $1/2, 3/2, \ldots$

or we can add antiparticles of energy $1/2, 3/2, ...$ by removing the particles of energy $1/2, 3/2, ..$ from the vacuum. The total energy and particle number are defined in the obvious way, by decreeing that the vacuum has particle number 0 and energy 0, and all other states will be obtained by adding a finite number of fermions of particle number 1 and their antiparticles of particle number -1. Then the total number of states of energy E and particle number N is the coefficient of $z^N q^E$ in

$$\prod(1 + zq^{n-1/2})(1 + z^{-1}q^{n-1/2})$$

Now we count this number in a different way. First do the case of particle number 0. We can obtain any state by of particle number 0 and energy E by starting with the vacuum and lifting the fermions to higher energy states; think of hitting them with photons of integral energy, each of which lifts one boson to a higher state. The number of ways to do this is the number of partitions of E, which is the coefficient of q^E in

$$\prod(1 - q^n)^{-1}$$

So this verifies that the coefficient of z^0 in both sides is the same. What about other powers of z, in other words other particle numbers? For this we use the vacuum for particle number N, where we will the states of energy $1/2, 3/2, ..., N - 1/2$, which has total energy N^2. So we just have to include extra terms $z^N q^{N^2}$ for all integers N to account for the vacuums of non-zero particle number.

The Boson-fermion correspondence comes from two different ways of looking at these sets. We can take the sets as basis elements for vector spaces. Then on the one hand we have an exterior algebra of an infinite dimensional space (which is what you get by quantizing a space of fermions) and on the other side we get a tensor product of a symmetric algebra (from quantizing bosons) tensors with a direct sum of vacuum states.

Notice that for finite exterior algebras is does not really matter which state you start with, but in infinite dimensions you get fundamentally different spaces depending on what you take as the vacuum: for example, some spaces have all states of positive energy, while others have states of arbitrarily large negative energy. This is a well-known problem in quantum field theory, that spaces you might expect to be isomorphic from analogy with finite dimensional spaces in quantum mechanics turn out to be fundamentally different.

32 Symmetric functions and representations of symmetric groups

Schur-Weyl duality gives a correspondence between representations of symmetric and general linear groups. So in order to understand representations of general linear groups we would like to know the representations of symmetric groups. We will describe these using symmetric functions.

32.1 The ring of symmetric functions

Recall that conjugacy classes of symmetric groups S_n correspond to partitions of n. The irreducible representations can also be indexed by partitions. (Although finite groups have the same number of conjugacy classes and irreducible representations, it is not in general true that there is a natural correspondence between them: symmetric groups are unusual in that they do have such a natural correspondence.) We will describe the representation theory in terms of symmetric functions. More precisely, the conjugacy classes of S_n will correspond to Newton's symmetric functions of degree n, irreducible representations of S_n will correspond to Schur polynomials of degree n, and the character table of S_n is just the matrix for expressing Schur functions as linear combinations of Newton's functions.

The symmetric functions of n variables $x_1, \ldots, x_n$ are the polynomials in the elementary symmetric functions $e_1 = \sum x_i$, $e_2 = \sum_{i<j} x_i x_j$, ..., $e_n = \prod x_i$. It is convenient to take a sort of limit as n tends to infinity and define the ring of symmetric functions to be polynomials in an infinite number of variables $e_1, e_2, \ldots$. The point is that formulas involving symmetric functions tend to be independent of the number of variables x_i provided this number is sufficiently large.

The ring of symmetric functions has a lot of structure:

- A commutative product
- A cocommutative coproduct
- An antipode (or involution)
- A partial ordered
- A symmetric bilinear form
- Several different natural bases

The ring of symmetric functions has several useful sets of generators and bases.

- The elementary symmetric functions $e_n = \sum_{i_1<i_2<\cdots<i_n} x_{i_1} x_{i_2} \cdots x_{i_n}$ form a generating set. The symmetric functions e_λ for λ a partition form a base. We put $E(x) = \sum e_i x^i = \prod(1 + x_i x)$, so it is a power series that formally has roots $-1/x_i$.
- The complete symmetric functions $h_n = \sum_{i_1 \le i_2 \le \cdots \le i_n} x_{i_1} x_{i_2} \cdots x_{i_n}$ form a generating set. We have $H(x) = \sum h_i x^i = \prod(1 - x x_i)^{-1} = 1/E(-x)$.
- Newton's symmetric functions $p_n = \sum_{i>0} x_i^n$ form a generating set over the rationals, but not over the integers. We have $P(x) = \sum_{n>0} p_n x^n = \sum_i x_i x/(1 - x_i x) = x \frac{d}{dx} \log(H(x) = x H'(x)/H(x)$.
- The Schur functions s_λ (see later)
- The monomial functions m_λ.
- The forgotten monomial functions

Exercise 354 Show that $E(-x)P(x) = -xE'(-x)$ and use this to prove Newton's identities giving recursive formulas for the sums p_i of the powers of roots of a polynomial $x^n - e_1x^{n-1} + \cdots$ in terms of its coefficients.

This gives at least 6 natural bases for the vector space of symmetric functions. Mathematicians working on symmetric functions spend many happy hours expressing writing the various basis elements as linear combinations or polynomials of other basis elements.

The ring of symmetric functions has a bilinear form $\langle , \rangle$ defined by the property that the symmetric functions p_λ form an orthogonal base or norm z_λ where z_λ is the order of the centralizer of a permutation of shape λ. The reason for this will appear later: when homogeneous symmetric functions are identified with class functions, this inner product becomes the usual inner product of class functions.

Exercise 355 Show that if a permutation has shape $1^{n_1}2^{n_2}\cdots$ then $z_\lambda = 1^{n_1}n_1!2^{n_2}n_2!\cdots$.

Recall that if V is a finite dimensional vector space with a symmetric non-degenerate inner product, then $\sum a_i a_i' \in S^2V$ summed over a basis a_i (with a_i' the dual basis) is independent of the choice of basis. We would like to do this for the space Λ but run into the problem that Λ is infinite dimensional. This is easy to fix because Λ is graded with finite-dimensional piece, so we just use $\sum a_i a_i' t^{\deg a_i} \in S^2V[[t]]$ instead. This element is independent of the choice of homogeneous basis.

Lemma 356 *For any homogeneous basis of* Λ*, we have*

$$\sum a_i a_i' t^{\deg a_i} = \prod_{i,j}(1 - tx_iy_j)^{-1}$$

Proof We only need to check this for one choice of basis, since the left hand side is independent of the choice of basis. Of course we use the basis $a_i = p_\lambda$, $a_i' = p_\lambda/z_\lambda$. The right hand side is given by

$$\exp(\sum_{i,j}\sum_{n>0} t^n x_i^n y_j^n/n) = \exp(\sum_n t^n p_n(x)p_n(y)/n)$$

The coefficient of t^m on the right is

$$\sum_{|\lambda|=m} p_\lambda(x)\frac{p_\lambda(y)}{z_\lambda}$$

which proves the lemma as by definition p_λ/z_λ is a dual basis to p_λ. □

The ring of symmetric functions is a Hopf algebra. The Hopf algebra structure is defined by making $E(x) = \sum e_i x^i$ grouplike (with $e_0 = 1$), or in other words

$$\Delta(e_n) = \sum e_i \otimes e_{n-i}.$$

Exercise 357 Show that over the rationals, the primitive elements of this Hopf algebra are the linear combinations of p_i, and that the Hopf algebra is the universal enveloping algebra of the abelian Lie algebra spanned by the p_i.

We know that commutative Hopf algebras should be thought of as group schemes, so we can ask what the group scheme corresponding to the Hopf algebra of symmetric functions looks like.

Exercise 358 Show that if G is the group scheme corresponding to the ring of symmetric functions, then for a commutative ring R, $G(R)$ can be identified with the multiplicative group of power series with leading coefficient 1 and coefficients in R.

The antipode of this Hopf algebra is given by $e_n^* = (-1)^n h_n$. This is slightly different from the involution often used on the ring of symmetric functions taking e_n to h_n. The two involutions differ on homogeneous elements of degree n by a factor of $(-1)^n$.

The ring of symmetric functions also turns up in other areas of mathematics in different guises. Here are a few apparently unrelated objects all of which are really the same ring, or rather Hopf algebra.

- The ring of symmetric functions
- Representations of symmetric groups
- Representations of general linear groups
- The homology of BU, the classifying space of the infinite unitary group. (It also turns up in several other related generalized homology rings of spectra.)
- Cohomology of Grassmannians ("Schubert calculus")
- The universal commutative λ-ring on one generator e_1
- The coordinate ring of the group scheme of power series with leading coefficient 1 under multiplication
- The Hall algebra of finite abelian p-groups, specialized to $p = 1$.
- It is the underlying space of a bosonic vertex algebra on 1 variable.
- It is the ring of polynomial functors on vector spaces.

32.2 Representations of the symmetric groups

We can now describe the characters of irreducible representations of symmetric groups in terms of the ring of symmetric functions. The idea is that we identify class functions on S_n with homogeneous functions of degree n by the Frobenius characteristic map taking a permutation of shape λ in S_n to the symmetric function $p_\lambda/n!$. This identifies the rational class functions with rational symmetric functions. Under this identification, the characters of irreducible representations correspond to Schur polynomials, and conjugacy classes of cycle shape λ correspond to p_λ/z_λ, so the character table of S_n is given by expressing the Schur polynomials as linear combinations of the symmetric functions p_λ/z_λ.

We prove this in several steps as follows:

1. Show that h_n corresponds to the trivial representation of S_n

2. Show that all homogeneous symmetric functions correspond to virtual representations, by showing that those that do are closed under products. In particular Schur polynomials correspond to generalized characters.

3. By the orthogonality relations, the characters are, up to sign, just the generalized characters of norm 1. So we show that Schur functions have norm 1, so they are irreducible characters up to sign.

4. Show that Schur polynomials are irreducible characters by showing the sign is positive.

Lemma 359 *The symmetric function h_n is the character of the trivial representation of S_n.*

Proof This is similar to the proof of Newton's identities. We have to show that $h_n = \sum_{|\lambda|=n} p_\lambda/z_\lambda$. This follows from $H(x) = \exp\int P(x)dx/x$. □

Exercise 360 Check this explicitly for $n = 3$.

Lemma 361 *If the symmetric functions a and b correspond to representations V and W of S_m and S_n, then ab corresponds to the representation*

$$\mathrm{Ind}_{S_m\times S_n}^{S_{m+n}} V \otimes W$$

Proof This follows from the Frobenius formula for the character of an induced representation, which states that the character of $Ind_H^G(V)$ is obtained from the character of V by smearing it over G. □

Corollary 362 *Every homogeneous symmetric function is the character of a generalized representation of a symmetric group.*

Proof The symmetric functions for which this is true include h_n and are closed under addition and multiplication. The corollary now follows since the symmetric functions h_n generate the ring of all symmetric functions. □

Lemma 363 *The Cauchy matrix with entries $1/(x_i - y_j)$ has determinant*

$$\frac{\prod_{i<j}(x_i - x_j)(y_i - y_j)}{\prod_{i,j}(x_i - y_j)}$$

Proof If we multiply the Cauchy determinant by $\prod_{i,j}(x_i - y_j)$ we get a polynomial of degree $n(n-1)$. It vanishes whenever two of the x_i or two of the y_i are equal, so must be divisible by the degree $n(n-1)$ polynomial $\prod_{i<j}(x_i - x_j)(y_i - y_j)$. As the degrees are the same, these two polynomials must be the same up to a constant. □

Exercise 364 Evaluate the Hilbert determinant with entries $1/(i + j - 1)$ for $1 \le i, j \le n$ by expressing it in terms of a suitable Cauchy determinant.

Theorem 365 *The Schur polynomials $s_\lambda = a_{\lambda+\rho}/a_\rho$ form an orthonormal basis of the symmetric functions.*

Proof We have to show that

$$\prod (1 - x_i y_i)^{-1} = \sum_\lambda s_\lambda(x) s_\lambda(y).$$

We will do this by evaluating the Cauchy matrix with entries $(1 - x_i y_j)^{-1}$ in two different ways. On one hand, by the previous lemma (changing x_i to $1/x_i$) it is equal to

$$\frac{\prod_{i<j}(x_i - x_j)(y_i - y_j)}{\prod_{i,j}(1 - x_i y_j)}.$$

On the other hand, if we expand $(1 - x_i y_j)^{-1}$ as $\sum_{k\geq 0} x_i^k y_j^k$ we see that the determinant is

$$\sum \pm x_1^{\lambda_1} x_2^{\lambda_2} \cdots y_1^{\mu_1} y_2^{\mu_2} \cdots$$

where the λ_i are a permutation of the μ_i. This is equal to

$$\sum_\lambda a_\lambda(x) a_\lambda(y)$$

where a_λ is the determinant of the matrix with entries $x_i^{\lambda_j}$. Defining $s_\lambda = a_{\lambda+\rho}/a_\rho$ and using the fact that $a_\rho(x) = \prod_{i<j}(x_i - x_j)$ by the Vandermonde identity, putting everything together proves the identity stated in the theorem.

□

We are now almost finished, since the Schur polynomials are generalized characters of norm 1 and are therefore irreducible characters up to sign. So we just have to pin down a the sign. (The reason why there is a sign problem can be understood as follows. The construction of the generalized characters is really a special case of a more general construction where the generalized characters appear in an alternating sum of cohomology groups. At most one of these cohomology groups is nonzero, so the sign depends on whether it is an even or an odd cohomology group.)

Lemma 366

$$\langle s_\lambda, p_1^{|\lambda|} \rangle > 0$$

Proof

□

Example 367 For the symmetric group S_3, the conjugacy classes correspond to $p_1^3/3! = e_1^3/6$, $p_1 p_2/2 = e_1^3/2 - e_1 e_2$, and $p_3/3 = e_1^3/3 - e_1 e_2 + e_3$. The characters correspond to $s_{1^3} = e_1^3 - 2e_1 e_2 + e_3$, $s_{12} = e_1 e_2 - e_3$, and $s_3 = e_3$. The coefficients expressing the Schur functions in terms of the Newton functions are just the coefficients of the character table of S_3

		$p_{1^3}/3!$	$p_{12}/2$	$p_3/3$
		$e_1^3/6$	$e_1^3/2 - e_1 e_2$	$e_1^3/3 - e_1 e_2 + e_3$
s_{1^3}	$e_1^3 - 2e_1 e_2 + e_3$	1	1	1
s_3	e_3	1	−1	1
s_{12}	$e_1 e_2 - e_3$	2	0	−1

The Schur polynomials are also the characters of the special linear groups. In fact the Weyl character formula expresses these characters as a quotient of two sums over the Weyl group. The Weyl group is the symmetric group, so the sums can be written as determinants, and turn out to be $a_{\lambda+\rho}$ and a_ρ for a suitable change in notation. The Schur functions are interpreted differently for the symmetric groups and the special linear groups: for symmetric groups the characters are given by regarding the Schur functions as linear combinations of Newton's symmetric polynomials (with the x_i being complex numbers of absolute value 1), while for the general linear group the Schur functions are regarded as functions on a maximal torus.

33 Schur-Weyl duality

In this section V will be a complex vector space, and we will be studying complex representations of the symmetric group and GL_V.

The simplest case of Schur-Weyl duality is the decomposition of $V \otimes V$ into the sum of the symmetric square S^2V and the alternating square $\Lambda^2 V$. In terms of representation theory this can be interpreted as follows. The space $V \otimes V$ is a representation of $GL_V \times S_2$ where GL_V acts on $V \otimes V$ by acting on each factor, and the symmetric group S_2 acts by permuting the two factors of V. Then V splits up as the sum of two irreducible representations $S^2V \oplus \Lambda^2 V$ of $GL_V \times S_2$. This gives a correspondence between representations of S_2 and GL_V, with the trivial and alternating representations of S_2 corresponding to the symmetric square and alternating square representations of GL_V.

The Schur-Weyl correspondence extends this from S_2 to the symmetric group S_n on n points. This time we use the representation of $GL_V \times S_n$ on the tensor product $V \otimes V \otimes \cdots \otimes V$, where GL_V again acts in the standard way on each factor, and the symmetric group permutes the factors. The key point is that each of GL_V and S_n generate each others commutators. This implies that $V \otimes V \otimes \cdots \otimes V$ is a direct sup of representations $\oplus A_i \otimes B_i$ where A_i is an irreducible representation of GL_V, B_i is an irreducible representation of S_n, and all the A_i are distinct and all the B_i are distinct. So we get a correspondence between some representations A_i of GL_V and some representations B_i of S_n.

For any particular choice of n and V we do not usually get a 1:1 correspondence between representations of GL_V and S_n: one problem is that GL_V has an infinite number of irreducible representations if V is non-trivial, while S_n has only a finite number. Another problem is that we can take inverse powers of the determinant of GL_n. However we almost get a 1:1 correspondence if we stabilize: if we let the dimension of V become large enough we get all representations of S_n, and if we let n become large we get all representations of GL_V up to powers of the determinant.

Example 368 Suppose that V has dimension 2. Then Schur-Weyl duality for the tensor product of n copies of V gives a correspondence between representations of $SL_2(\mathbb{C})$ and S_n, where the trivial representation of S_n corresponds to the $n+1$-dimensional irreducible representation of $SL_2(\mathbb{C})$. So we pick up all irreducible representations of $SL_2(\mathbb{C})$ by just using the trivial representation of the symmetric group and letting n tend to infinity.

Exercise 369 If W is a complex vector space, show that the space of elements of $W \otimes W \otimes \cdots \otimes W$ fixed by the symmetric group S_n is spanned by elements of the form $w \otimes w \otimes \cdots \otimes w$.

The key result needed for Schur-Weyl duality is the following:

Theorem 370 *Any endomorphism of $V \otimes V \otimes \cdots \otimes V$ that commutes with S_n is a linear combination of endomorphisms given by elements of $GL_n(V)$.*

Proof We want to show that the space of elements of $\mathrm{End}(V^{\otimes n})$ fixed by the symmetric group is spanned by GL_V. But $\mathrm{End}(V^{\otimes n}) = \mathrm{End}(V)^{\otimes n}$ so by the previous exercise the space of elements fixed by S_n is spanned by elements of the form $w \otimes w \otimes \cdots \otimes w$ for $w \in \mathrm{End}(V)$, or in other words any endomorphism of $V^{\otimes n}$ commuting with S_n is a linear combination of elements of $\mathrm{End}(V)$ acting on it. Since GL_V is dense in $\mathrm{End}(V)$ this proves the theorem. □

Theorem 371 *Suppose that M is an algebra of endomorphisms of $H = \mathbb{C}^n$ containing 1 and closed under taking adjoints. Then $M = M''$*

Proof Suppose $v \in H$. Then Mv is fixed by M'. Also we can write H as a direct sum $H = Mv \oplus Mv^{\perp}$, and the orthogonal projection e onto Mv is in M' as M is closed under adjoints. So M'' maps Mv to Mv as it commutes with e. So $M''v = Mv$. (It is obvious that $M''v \subseteq Mv$ because $1 \in M$.)

Now look at the action of M on $H \oplus H \cdots \oplus H$ (n copies of H). The things commuting with M are just n by n matrices with coefficients in M', so the double commutant M'' is the same as for M acting on H. So $M(v_1 \oplus \cdots \oplus v_n) = M''(v_1 \oplus \cdots \oplus v_n)$. In other words, for any finite number of vectors, and any element of M, we can find an element of M'' having the same effect on these vectors. Since H is finite-dimensional this proves that $M'' = M$.

□

Exercise 372 Find a subalgebra A of $M_2(\mathbb{C})$ containing 1 such that A'' is not equal to A.

Exercise 373 Suppose that M is a von Neumann algebra on a Hilbert space H (possibly infinite dimensional). This means that M is an algebra of bounded operators containing 1 that is weakly closed and closed under taking adjoints. Show that $M'' = M$.

Exercise 374 Suppose that M is any collection of functions from a set H to itself. Show that $M \subseteq M''$ and $M' = M'''$.

Two algebras acting on a vector space each of which is the centralizer of the other occurs quite often, and can be a very powerful technique for constructing representations of groups. For example, a von Neumann algebra M can be defined as a *-algebra of endomorphisms of a Hilbert space such that $M = M''$, where $'$ means take the commutant. The theory of dual reductive pairs depends on finding two subgroups of a metaplectic group each of which generates the commutant of the other acting on the metaplectic representation. Some of the work on the Langlands program that tries to associate a representation of a reductive group to a representation of a Galois group tries to do this by finding a representation of (reductive group) times (Galois group) such that each generates the commutator of the other, in which case one can hope to get a suitable correspondence between their representations.

34 Littlewood-Richardson rule

Given two representations of $U(n)$ we would like to decompose their tensor product into a sum of irreducible representations. This is solved by the Littlewood-Richardson rule. Irreducible polynomial representations correspond to partitions λ with at most n rows, and the tensor product of partitions corresponds to taking products of the Schur functions (which are essentially the characters of the representations). So we want to write the product $S_\lambda S_\mu$ of any two Schur polynomials explicitly as a linear combination $\sum_\nu c^\nu_{\lambda\mu} S_\nu$ of Schur polynomials. The numbers $c^\nu_{\lambda\mu}$ are called Littlewood-Richardson coefficients, and the Littlewood-Richardson rule is a combinatorial rule for calculating them.

The following proof of the Littlewood-Richardson rule (from Stembridge) is short but rather mysterious. It is really a special case of a more general result proved using crystal graphs. It may give a misleading idea of how hard the Littlewood Richardson rule was to prove: it took four decades to find the first complete proof, and several further decades for find some of the more recently short proofs. Altogether more than a dozen mathematicians contributed significantly to finding the proof given here.

Recall that a semistandard tableau is an assignment of positive integers to a Young diagram such that all rows are non-strictly increasing and all columns are strictly increasing.

The Bender-Knuth involution is an involution depending on a pair of consecutive integers $(k, k+1)$ that acts on the semistandard tableaux, and exchanges the numbers of ks and $(k+1)$s. It acts as follows. First pair off as many ks as possible with a $k+1$ below them. The leftover k s and $(k+1)$s form several disjoint rows of the form $kkk\cdots k(k+1)\cdots(k+1)$. If such a row has a copies of k and b copies of $k+1$, change some entries so it has b copies of k and a copies of $k+1$. This produces another semistandard tableau where the number of copies of k and $k+1$ has been exchanged.

Definition 375 *The Schur function s_λ is defined to be $\sum_T x^{\omega(T)}$, where the sum is over all semistandard tableaux of weight λ.*

Lemma 376 *The Schur functions are symmetric polynomials.*

Proof The Bender-Knuth involutions show that the number of tableaux of some weight is invariant under permutations of the weight. □

We write $T_{\geq j}$ for the tableau formed by the columns $j, j+1, \ldots$ of T, and defined $T_{>j}$, $T_{<j}$, and so on in a similar way. The weight $\omega(T)$ of a tableau T is (number of 1's in T, number of 2's, ...)$\in \mathbb{Z}^n$. So the Young diagram $\lambda+\omega(T)$ is formed by adding a box to the first row for every 1 in T, a box to the second row for every 2 in T, and so on. The Weyl vector ρ is $(n-1, n-2, \cdots, 0) \in \mathbb{Z}^n$. We think of partitions into at most n parts as non-increasing sequences in $\mathbb{Z}^n$.

We define a_λ to be $\sum_{w\in S_n}\epsilon(w)x^{w(\lambda)}$, where $\epsilon=\pm 1$ is the sign of the permutation w. In particular a_λ is alternating under permutations of λ and vanishes if two elements of λ are equal.

The Littlewood-Richardson rule will follow easily from the following result:

Theorem 377

$$a_{\lambda+\rho}s_\mu=\sum_T a_{\lambda+\omega(T)+\rho}$$

where the sum is over all semistandard tableaux T of shape μ such that for all j, $\lambda+\omega(T_{\geq j})$ is a partition.

Proof Since s_μ is symmetric, we have

$$a_{\lambda+\rho}s_\mu=\sum_T a_{\lambda+\omega(T)+\rho}$$

where the sum is over all semistandard tableaux T. The core part of the proof is to show that the terms such that for some j, $\lambda+\omega(T_{\geq j})$ is not a partition cancel out in pairs or are zero, which we will do using Bender-Knuth involutions to pair them off.

Fix some j and k. We concentrate on the tableaux T such that $\lambda+\omega(T_{\geq j})$ is not a partition and $\lambda+\omega(T_{\geq i})$ is a partition for any $i>j$. We further restrict to the set X of T such that k is the smallest number with $\lambda_k+\omega_k(T_{\geq j} > \lambda_{k+1}+\omega_{k+1}(T_{\geq j}$. This implies that column j of T contains a $k+1$ and does not contain a k, and that $T_{>j}$ has the same number of ks and $(k+1)$s.

We define an involution $*$ on this set of T by fixing $T_{\geq j}$ and acting as a Bender-Knuth involution $(k,k+1)$ on $T_{<j}$. This takes elements of X to elements of X because $*$ does not change $T_{\geq j}$, and row j of T does not contain k (so that $*$ keeps the rows monotonic).

We check that the term corresponding to T cancels out with the term corresponding to $*T$. The transposition $(k,k+1)$ of S_n fixes $\lambda+\omega(T_{\geq j}+\rho$. It also maps $\omega(T_{<j}$ to $\omega_(*T_{<j})$, so maps $\lambda+\omega(T)+\rho$ to $\lambda+\omega(T)+\rho$. Also $a_{\lambda+\omega(T)+\rho}=-a_{\lambda+\omega(*T)+\rho}$ as a is alternating under permutations of S_n, so the terms corresponding to T and $*T$ cancel (it is possible that $*T=T$ in which case the term is 0). □

Corollary 378

$$s_\mu=a_{\mu+\rho}/a_\rho$$

Proof This is just the special case $\lambda=0$. □

Corollary 379 *(The Littlewood-Richardson rule)*

$$s_\lambda s_\mu=\sum_\nu c^\nu_{\lambda\mu}s_\nu$$

where $c^\nu_{\lambda\mu}$ is the number semistandard tableaux T of shape μ such that $\nu=\lambda+\omega(T)$ and for all j, $\lambda+\omega(T_{\geq j})$ is a partition.

Proof This follows by combining theorem ?? with corollary ??. □

Warning 380 It is hard to avoid errors when doing hand calculations with the Littlewood-Richardson rule. An easy error to make is forgetting to include some tableaux. As a check, one can do the calculation for the product in reverse order, or for the transpose of the permutations (or better still use a computer).

As the proof shows, it is rather easy to find an expression for $S_\lambda S_\mu$ as a sum of terms S_ν possibly with negative coefficients. The tricky part of the proof of the Littlewood-Richardson rule is to pair off the terms with negative coefficients with terms with positive coefficients, so that the final sum has only positive coefficients.

Example 381 We work out $S_{21}S_{21}$. There are 8 tableaux in the sum, given by $\begin{smallmatrix}1&1\\2&\end{smallmatrix}$ $\begin{smallmatrix}1&1\\3&\end{smallmatrix}$ $\begin{smallmatrix}1&2\\2&\end{smallmatrix}$ $\begin{smallmatrix}1&2\\3&\end{smallmatrix}$ $\begin{smallmatrix}1&3\\2&\end{smallmatrix}$ $\begin{smallmatrix}1&3\\4&\end{smallmatrix}$ $\begin{smallmatrix}2&3\\3&\end{smallmatrix}$ $\begin{smallmatrix}2&3\\4&\end{smallmatrix}$. So $S_{21}S_{21} = S_{42} + S_{411} + S_{33} + 2S_{321} + S_{3111} + S_{222} + S_{2211}$.

Example 382 We use the Littlewood-Richardson rule to work out the decomposition of $V \otimes V$ into irreducible representations, where V is the 8-dimensional adjoint representation of SU_3. The partition corresponding to V is 21, which in general for GL_n corresponds to the non-trivial component of the tensor product of the n-dimensional representation and its alternating square. By the previous example, $V \otimes V$ decomposes into 8 irreducible representations if $n \geq 4$. We have to make two changes to find the decomposition for SU_3. First of all, any Young diagram with more than 3 rows corresponds to the zero representation, which eliminates 3111 and 2211. Second, since we are working with SU rather than U, any diagram with exactly 3 rows abc is equivalent to $(a-1)(b-1)(c-1)$, so 411 becomes 3, 321 becomes 21, and 222 becomes the empty Young diagram. So $V \otimes V$ decomposes into a sum of 6 irreducible representations corresponding to the partitions (42), (3), (33), (21), (21), (0).

Exercise 383 Show that the Littlewood-Richardson rule implies Pieri's formula: $S_\lambda S_n = \sum_\nu S_\nu$, where the sum is over all partitions ν obtained from λ by adding n elements with at most 1 in each column.

Exercise 384 Check the (corrected) example given by Littlewood and Richardson: $S_{431}S_{221} = S_{652} + S_{6511} + S_{643} + 2S_{6421} + S_{64111} + S_{6331} + S_{6322} + S_{63211} + S_{553} + 2S_{5521} + S_{55111} + 2S_{5431} + 2S_{5422} + 3S_{54211} + S_{541111} + S_{5332} + S_{53311} + 2S_{53221} + S_{532111} + S_{4432} + S_{44311} + 2S_{44221} + S_{442111} + S_{43321} + S_{43222} + S_{432211}$

Exercise 385 If $\mu \leq \lambda$ we define the skew Schur polynomial $S_{\lambda/\mu}$ as the sum $\sum_T x^{\omega(T)}$ over all semistandard Tableaux of shape λ/μ (the Young diagram of λ with the boxes in μ removed). Prove that this is a symmetric polynomial. Prove that

Hook formula??

35 Combinatorics of Young diagrams

RSK, Jeu de taquin, Plactic monoid, Knuth equivalence

The plactic monoid is generated by a totally ordered set, usually taken to be the positive integers, subject to the Knuth relations:

- $acb = cab$ if $a \leq b < c$
- $bac = bca$ if $a < b \leq c$

The Knuth relations say roughly that the exchange of two adjacent elements a and c is catalyzed by an element next to them that is between a and c under the total order. The relations when equality holds between two of the letters are harder to remember: the relations have the property that the triple on either side of the equality is never an increasing sequence.

For any semistandard tableau we can get an element of the plactic monoid by listing its rows starting with the lowest (in the English convention); for example the tableau $\begin{smallmatrix}1&1&2&3&3&4\\2&3&5\\3&7\end{smallmatrix}$ corresponds to the word 37235112334.

The key result is the following theorem, which identifies elements of the plactic monoid with semistandard tableaux, and in particular shows that the semistandard tableaux form a monoid.

Theorem 386 *Every element of the plactic monoid is represented by a unique semistandard tableau.*

Proof We first show that every word is Knuth equivalent to the word of a semistandard tableau. For this it is sufficient to show that if we multiply a semistandard tableau on the right by a generator x we still get a semistandard tableau. This operation is called Schensted insertion and works as follows. If x is at least as large as the rightmost element of the first row we just add it to the end. Otherwise we move it to the left in the first row using a Knuth relation until it reaches yz with $y \leq x$, $z > x$ (so z is the leftmost element greater than x). Now we can move z to the left of the first row using Knuth relations. If z is at least the rightmost element of the second row we leave it there, otherwise we repeat what we did on the first row with z instead of x. Continuing in this way we obtain a semistandard tableau whose word is Knuth equivalent to the original word.

Now we have to show that any word is equivalent to at most one semistandard tableau. We start by observing that Knuth equivalence preserves the length of the longest increasing sequence. Since in a semistandard tableau the length of the longest increasing sequence is the first row, this shows that the length of the first row of the tableau is determined. More generally, Knuth equivalence preserves the maximum of the sum of the lengths of k disjoint increasing sequences for any k. For a semistandard tableau, this is the sum of the lengths of the first k rows (as there cannot be more than k elements from any column) so the shape of the tableau is determined bu the word.

To complete the proof we have to show that position of each letter of the word in the tableau is determined. Consider the rightmost largest element x in the word. It can never catalyze the exchange of two letters, so the word with x removed is Knuth equivalent to the tableau with x removed. By induction on length the partition of the tableau with x removed is uniquely determined, and is the partition of the word with one box removed, which must therefore be the place where x has to be inserted. □

Exercise 387 Show that there is a polynomial-time algorithm to find the maximal total length of k disjoint increasing subsequences of a given finite sequence.

Exercise 388 Prove the ErdsSzekeres theorem that a sequence of length $mn+1$ contains an increasing sequence of length $m+1$ or a decreasing sequence of length $n+1$. (Let a_i and b_i be the lengths of maximal increasing and decreasing sequences ending at position i. Show that the $mn+1$ pairs (a_i, b_i) are all distinct.)

The distribution of the length of the longest increasing sequence of a long random sequence approaches the TracyWidom distribution, which can be expressed in terms of Painleve functions.

36 Construction of Lie algebras from a root lattice

The root space decomposition of a Lie algebra suggests the following construction of a Lie algebra from its root system. Take the direct sum of the (dual of the) root lattice with a 1-dimensional vector space generated by a special element for each root. However when we try to write down the Lie bracket for this algebra we run into the following sign problem: suppose that α, β, and $\alpha+\beta$ are roots, with corresponding elements e_α, e_β, $e_{\alpha+\beta}$. It seems natural to define $[e_\alpha, e_\beta] = e_{\alpha+\beta}$ The problem is that the left hand side changes sign when α and β are switched, while the right hand side does not. In fact there is in general no functorial way to define a Lie algebra from its root lattice. One way to see this is that if we had such a functor, then the automorphism group, and the Weyl group, of the root lattice would act on the Lie algebra. However in general the Weyl group does not have a nice action on the Lie algebra: it is a subquotient of the Lie group, not a subgroup. This can be seen even for $SL_n(R)$, where order 2 reflections of the Weyl group lift to order 4 elements of the Lie group. The best we can do is find a subgroup of the form $2^n.W$ inside the Lie group.

We can see this going wrong even in the case of $\mathfrak{sl}_2(\mathbb{R})$. Remember that the Weyl group is $N(T)/T$ where $T = \left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right)$ and $N(T) = T \cup \left(\begin{smallmatrix} 0 & b \\ -b^{-1} & 0 \end{smallmatrix}\right)$, and this second part is stuff having order 4, so we cannot possibly write this as a semi-direct product of T and the Weyl group.

So the Weyl group is not usually a subgroup of $N(T)$. The best we can do is to find a group of the form $2^n \cdot W \subseteq N(T)$ where n is the rank. For example, let's do it for $SL(n+1, \mathbb{R})$ Then $T = diag(a_1, \ldots, a_n)$ with $a_1 \cdots a_n = 1$. Then we take the normalizer of the torus to be $N(T)$ =all permutation matrices with ± 1's with determinant 1, so this is $2^n \cdot S_n$, and it does not split. The problem we had with signs can be traced back to the fact that this group doesn't split.

We can construct the Lie algebra from something acted on by $2^n \cdot W$ (but not from something acted on by W). We take a central extension of the lattice by a group of order 2. Notation is a pain because the lattice is written additively and the extension is nonabelian, so we want it to be written multiplicatively. Write elements of the lattice in the form e^α formally, so we have converted the lattice operation to multiplication. We will use the central extension

$$1 \to \pm 1 \to \hat{e}^L \to \underbrace{e^L}_{\cong L} \to 1$$

We want $\hat{e}^L$ to have the property that $\hat{e}^\alpha \hat{e}^\beta = (-1)^{(\alpha,\beta)} \hat{e}^\beta \hat{e}^\alpha$, where $\hat{e}^\alpha$ is something mapping to e^α. What do the automorphisms of $\hat{e}^L$ look like? We get

$$1 \to \underbrace{(L/2L)}_{(\mathbb{Z}/2)^{\mathrm{rank}(L)}} \to \mathrm{Aut}(\hat{e}^L) \to \mathrm{Aut}(e^L)$$

for $\alpha \in L/2L$, we get the map $\hat{e}^\beta \to (-1)^{(\alpha,\beta)} \hat{e}^\beta$. The map turns out to be onto, and the group $\mathrm{Aut}(e^L)$ contains the reflection group of the lattice. This extension is usually non-split.

Now the Lie algebra is $L \oplus \{1$ dimensional spaces spanned by $(\hat{e}^\alpha, -\hat{e}^\alpha)\}$ for $\alpha^2 = 2$ with the convention that $-\hat{e}^\alpha$ (-1 in the vector space) is $-\hat{e}^\alpha$ (-1 in the group $\hat{e}^L$). Now define a Lie bracket by the "obvious rules" $[\alpha, \beta] = 0$ for $\alpha, \beta \in L$ (the Cartan subalgebra is abelian), $[\alpha, \hat{e}^\beta] = (\alpha, \beta)\hat{e}^\beta$ ($\hat{e}^\beta$ is in the root space of β), and $[\hat{e}^\alpha, \hat{e}^\beta] = 0$ if $(\alpha, \beta) \geq 0$ (since $(\alpha + \beta)^2 > 2$), $[\hat{e}^\alpha, \hat{e}^\beta] = \hat{e}^\alpha \hat{e}^\beta$ if $(\alpha, \beta) < 0$ (product in the group $\hat{e}^L$), and $[\hat{e}^\alpha, (\hat{e}^\alpha)^{-1}] = \alpha$.

Theorem 389 *Assume L is positive definite. Then this Lie bracket forms a Lie algebra (so it is skew and satisfies Jacobi).*

Proof The proof is easy but tiresome, because there are a lot of cases.

We check the Jacobi identity: We want $[[a, b], c] + [[b, c], a] + [[c, a], b] = 0$

1. all of a, b, c in L. Trivial because all brackets are zero.
2. two of a, b, c in L. Say α, β, e^γ

$$\underbrace{[[\alpha, \beta], e^\gamma]}_{0} + \underbrace{[[\beta, e^\gamma], \alpha]}_{(\beta,\alpha)(-\alpha,\beta)e^\gamma} + [[e^\gamma, \alpha], \beta]$$

   and similar for the third term, giving a sum of 0.

3. one of a, b, c in L. $\alpha, e^\beta, e^\gamma$. e^β has weight β and e^γ has weight γ and $e^\beta e^\gamma$ has weight $\beta + \gamma$. So check the cases, and we get Jacobi:

$$\begin{aligned} &[[\alpha, e^\beta], e^\gamma] = (\alpha, \beta)[e^\beta, e^\gamma] \\ &[[e^\beta, e^\gamma], \alpha] = -[\alpha, [e^\beta, e^\gamma]] = -(\alpha, \beta + \gamma)[e^\beta, e^\gamma] \\ &[[e^\gamma, \alpha], e^\beta] = -[[\alpha, e^\gamma], e^\beta] = (\alpha, \gamma)[e^\beta, e^\gamma], \end{aligned}$$

   so the sum is zero.

4. none of a, b, c in L. This is the most tedious case, $e^\alpha, e^\beta, e^\gamma$. We can reduce it to two or three cases. We make our cases depending on (α, β), (α, γ), (β, γ).
   (a) if 2 of these are 0, then all the $[[*, *], *]$ are zero.
   (b) $\alpha = -\beta$. By case a, γ cannot be orthogonal to them, so say $(\alpha, \gamma) = 1$ $(\gamma, \beta) = -1$; adjust so that $e^\alpha e^\beta = 1$, then calculate

$$\begin{aligned} [[e^\gamma, e^\beta], e^\alpha] - [[e^\alpha, e^\beta], e^\gamma] + [[e^\alpha, e^\gamma], e^\beta] &= e^\alpha e^\beta e^\gamma - (\alpha, \gamma)e^\gamma + 0 \\ &= e^\gamma - e^\gamma = 0. \end{aligned}$$

(c) $\alpha = -\beta = \gamma$, which is easy because $[e^\alpha, e^\gamma] = 0$ and $[[e^\alpha, e^\beta], e^\gamma] = -[[e^\gamma, e^\beta], e^\alpha]$

(d) We have that each of the inner products is 1, 0 or -1. If some $(\alpha, \beta) = 1$, all brackets are 0.

□

We had two cases left:

$$[[e^\alpha, e^\beta], e^\gamma] + [[e^\beta, e^\gamma], e^\alpha] + [[e^\gamma, e^\alpha], e^\beta] = 0$$

– $(\alpha, \beta) = (\beta, \gamma) = (\gamma, \alpha) = -1$, in which case $\alpha + \beta + \gamma = 0$. then $[[e^\alpha, e^\beta], e^\gamma] = [e^\alpha e^\beta, e^\gamma] = \alpha + \beta$. By symmetry, the other two terms are $\beta + \gamma$ and $\gamma + \alpha$;the sum of all three terms is $2(\alpha + \beta + \gamma) = 0$.

– $(\alpha, \beta) = (\beta, \gamma) = -1$, $(\alpha, \gamma) = 0$, in which case $[e^\alpha, e^\gamma] = 0$. We check that $[[e^\alpha, e^\beta], e^\alpha] = [e^\alpha e^\beta, e^\gamma] = e^\alpha e^\beta e^\gamma$ (since $(\alpha + \beta, \gamma) = -1$). Similarly, we have $[[e^\beta, e^\gamma], e^\alpha] = [e^\beta e^\gamma, e^\alpha] = e^\beta e^\gamma e^\alpha$. We notice that $e^\alpha e^\beta = -e^\beta e^\alpha$ and $e^\gamma e^\alpha = e^\alpha e^\gamma$ so $e^\alpha e^\beta e^\gamma = -e^\beta e^\gamma e^\alpha$; again, the sum of all three terms in the Jacobi identity is 0.

This concludes the verification of the Jacobi identity, so we have a Lie algebra.

Is there a proof avoiding case-by-case check? Yes, but it is actually more work. We really have functors from double covers of lattices to vertex algebras, and from vertex algebras to Lie algebras. However it takes several weeks to define vertex algebras, though it you do you get constructions for a lot more Lie algebras because this works even if the lattice is not positive definite. In fact, the construction we did was the vertex algebra approach, with all the vertex algebras removed. So there is a more general construction which gives a much larger class of infinite dimensional Lie algebras.

Now we should study the double cover $\hat{L}$, and in particular prove its existence. Given a Dynkin diagram, we can construct $\hat{L}$ as generated by the elements e^{α_i} for α_i simple roots with the given relations. It is easy to check that we get a surjective homomorphism $\hat{L} \to L$ with kernel generated by z with $z^2 = 1$. What's a little harder to show is that $z \neq 1$ (i.e., show that $\hat{L} \neq L$). The easiest way to do it is to use cohomology of groups, but since we have such an explicit case, we'll do it bare hands:

Problem: Given Z, H groups with Z abelian, construct central extensions

$$1 \to Z \to G \to H \to 1$$

(where Z lands in the center of G). Let G be the set of pairs (z, h), and set the product $(z_1, h_1)(z_2, h_2) = (z_1 z_2 c(h_1, h_2), h_1 h_2)$, where $c(h_1, h_2) \in Z$ ($c(h_1, h_2)$ will be a cocycle in group cohomology). We obviously get a homomorphism by mapping $(z, h) \mapsto h$. If $c(1, h) = c(h, 1) = 1$ (normalization), then $z \mapsto (z, 1)$ is a homomorphism mapping Z to the center of G. In particular, $(1, 1)$ is the identity. We'll leave it as an exercise to figure out what the inverses are. When is this thing *associative*? Let's just write everything out:

$$\big((z_1, h_1)(z_2, h_2)\big)(z_3, h_3) = (z_1 z_2 z_3 c(h_1, h_2) c(h_1 h_2, h_3), h_1 h_2 h_3)$$
$$(z_1, h_1)\big((z_2, h_2)(z_3, h_3)\big) = (z_1 z_2 z_3 c(h_1, h_2 h_3) c(h_2, h_3), h_1 h_2 h_3)$$

so we must have

$$c(h_1, h_2)c(h_1h_2, h_3) = c(h_1h_2, h_3)c(h_2, h_3).$$

This identity is actually very easy to satisfy in one particular case: when c is bimultiplicative:

$$c(h_1, h_2h_3) = c(h_1, h_2)c(h_1, h_3)$$

and

$$c(h_1h_2, h_3) = c(h_1, h_3)c(h_2, h_3)$$

. That is, we have a map $H \times H \to Z$. Not all cocycles come from such maps, but this is the case we care about.

To construct the double cover, let $Z = \pm 1$ and $H = L$ (free abelian). If we write H additively, we want c to be a bilinear map $L \times L \to \pm 1$. It is really easy to construct bilinear maps on free abelian groups. Just take any basis $\alpha_1, \ldots, \alpha_n$ of L, choose $c(\alpha_1, \alpha_j)$ arbitrarily for each i, j and extend c via bilinearity to $L \times L$. In our case, we want to find a double cover $\hat{L}$ satisfying $\hat{e}^\alpha \hat{e}^\beta = (-1)^{(\alpha,\beta)} \hat{e}^\beta \hat{e}^\alpha$ where $\hat{e}^\alpha$ is a lift of e^α. This just means that $c(\alpha, \beta) = (-1)^{(\alpha,\beta)} c(\beta, \alpha)$. To satisfy this, just choose $c(\alpha_i, \alpha_j)$ on the basis $\{\alpha_i\}$ so that $c(\alpha_i, \alpha_j) = (-1)^{(\alpha_i,\alpha_j)} c(\alpha_j, \alpha_i)$. This is trivial to do as $(-1)^{(\alpha_i,\alpha_i)} = 1$. Notice that this uses the fact that the lattice is even. There is no canonical way to choose this 2-cocycle (otherwise, the central extension would split as a product), but all the different double covers are isomorphic because we can specify $\hat{L}$ by generators and relations. Thus, we have constructed $\hat{L}$ (or rather, verified that the kernel of $\hat{L} \to L$ has order 2, not 1).

Let's now look at lifts of automorphisms of L to $\hat{L}$.

Exercise 390 Any automorphism of L preserving $(\, , \,)$ lifts to an automorphism of $\hat{L}$

There are two special cases:

1. -1 is an automorphism of L, and we want to lift it to $\hat{L}$ explicitly. First attempt: try sending $\hat{e}^\alpha$ to $\hat{e}^{-\alpha} := (\hat{e}^\alpha)^{-1}$, which doesn't work because $a \mapsto a^{-1}$ is not an automorphism on non-abelian groups.

   Better: $\omega : \hat{e}^\alpha \mapsto (-1)^{\alpha^2/2} (\hat{e}^\alpha)^{-1}$ is an automorphism of $\hat{L}$. To see this, check

   $$\omega(\hat{e}^\alpha)\omega(\hat{e}^\beta) = (-1)^{(\alpha^2+\beta^2)/2} (\hat{e}^\alpha)^{-1} (\hat{e}^\beta)^{-1}$$
   $$\omega(\hat{e}^\alpha \hat{e}^\beta) = (-1)^{(\alpha+\beta)^2/2} (\hat{e}^\beta)^{-1} (\hat{e}^\alpha)^{-1}$$

   which work out just right

2. If $r^2 = 2$, then $\alpha \mapsto \alpha - (\alpha, r)r$ is an automorphism of L (reflection through $r^\perp$). You can lift this by $\hat{e}^\alpha \mapsto \hat{e}^\alpha (\hat{e}^r)^{-(\alpha,r)} \times (-1)^{\binom{(\alpha,r)}{2}}$. This is a homomorphism (check it!) of order (usually) 4!

   Remark 391 Although automorphisms of L lift to automorphisms of $\hat{L}$, the lift might have larger order.

This construction works for the root lattices of A_n, D_n, E_6, E_7, and E_8; these are the lattices which are even, positive definite, and generated by vectors of norm 2 (in fact, all such lattices are sums of the given ones). What about B_n, C_n, F_4 and G_2? The reason the construction doesn't work for these cases is because there are roots of different lengths. These all occur as fixed points of diagram automorphisms of A_n, D_n and E_6. In fact, we have a *functor* from Dynkin diagrams to Lie algebras, so and automorphism of the diagram gives an automorphism of the algebra

A_{2n} doesn't really give you a new algebra: it corresponds to some superalgebra stuff.

36.1 Construction of the Lie group of a Lie algebra

It is the group of automorphisms of the Lie algebra generated by the elements $\exp(\lambda Ad(\hat{e}^\alpha))$, where λ is some real number, $\hat{e}^\alpha$ is one of the basis elements of the Lie algebra corresponding to the root α, and $Ad(\hat{e}^\alpha)(a) = [\hat{e}^\alpha, a]$. In other words,

$$\exp(\lambda Ad(\hat{e}^\alpha))(a) = 1 + \lambda[\hat{e}^\alpha, a] + \frac{\lambda^2}{2}[\hat{e}^\alpha, [\hat{e}^\alpha, a]].$$

and all the higher terms are zero. To see that $Ad(\hat{e}^\alpha)^3 = 0$, note that if β is a root, then $\beta + 3\alpha$ is not a root (or 0).

Warning 392 In general, the group generated by these automorphisms is not the whole automorphism group of the Lie algebra. There can be extra diagram (or graph) automorphisms, field automorphisms induced (obviously) by automorphism of the field, and "diagonal" automorphisms, such as the automorphisms of $SL_n(\mathbb{Q})$ induced by conjugation by diagonal matrices of $GL_n(\mathbb{Q})$. Moreover there are some strange extra diagram automorphisms of B_2 and F_4 in characteristic 2, and of G_2 in characteristic 3. (Informally, one can ignore the arrow on a bond of a Dynkin diagram if the characteristic of the field is the number of bonds.)

We get some other things from this construction. We can get simple groups over finite fields: note that the construction of a Lie algebra above works over any commutative ring (e.g. over $\mathbb{Z}$). The only place we used division is in $\exp(\lambda Ad(\hat{e}^\alpha))$ (where we divided by 2). The only time this term is non-zero is when we apply $\exp(\lambda Ad(\hat{e}^\alpha))$ to $\hat{e}^{-\alpha}$, in which case we find that $[\hat{e}^\alpha, [\hat{e}^\alpha, \hat{e}^{-\alpha}]] = [\hat{e}^\alpha, \alpha] = -(\alpha, \alpha)\hat{e}^\alpha$, and the fact that $(\alpha, \alpha) = 2$ cancels the division by 2. So we can in fact construct the E_8 group over *any* commutative ring. With more effort we in fact get group schemes over $\mathbb{Z}$.See Steinberg's notes or the book by Carter on Finite Simple Groups for more details.

37 Simple real Lie algebras

37.1 Real forms

(The stuff about E8 is duplicate and needs to be removed)

In general, suppose L is a Lie algebra with complexification $L \otimes \mathbb{C}$. How can we find another Lie algebra M with the same complexification? $L \otimes \mathbb{C}$ has an anti-linear involution $\omega_L : l \otimes z \mapsto l \otimes \bar{z}$. Similarly, it has an anti-linear involution ω_M. Notice that $\omega_L \omega_M$ is a linear involution of $L \otimes \mathbb{C}$. Conversely, if we know this involution, we can reconstruct M from it. Given an involution ω of $L \otimes \mathbb{C}$, we can get M as the fixed points of the map $a \mapsto \omega_L \omega(a)$"=" $\overline{\omega(a)}$. Another way is to put $L = L^+ \oplus L^-$, which are the $+1$ and -1 eigenspaces, then $M = L^+ \oplus iL^-$.

Thus, to find other real forms, we have to study the involutions of the complexification of L. The exact relation is subtle, but this is a good way to go.

Example 393 Let $L = \mathfrak{sl}_2(\mathbb{R})$. It has an involution $\omega(m) = -m^T$. $\mathfrak{su}_2(\mathbb{R})$ is the set of fixed points of the involution ω times complex conjugation on $\mathfrak{sl}_2(\mathbb{C})$, by definition.

So to construct real forms of E_8, we want some involutions of the Lie algebra E_8 which we constructed. What involutions do we know about? There are two obvious ways to construct involutions:

1. Lift -1 on L to $\hat{e}^\alpha \mapsto (-1)^{\alpha^2/2}(\hat{e}^\alpha)^{-1}$, which induces an involution on the Lie algebra.

2. Take $\beta \in L/2L$, and look at the involution $\hat{e}^\alpha \mapsto (-1)^{(\alpha,\beta)}\hat{e}^\alpha$.

(2) gives nothing new: we get the Lie algebra we started with. (1) only gives one real form. To get all real forms, we multiply these two kinds of involutions together.

Recall that $L/2L$ has 3 orbits under the action of the Weyl group, of size 1, 120, and 135. These will correspond to the three real forms of E_8. How do we distinguish different real forms? The answer was found by Cartan: look at the signature of an invariant quadratic form on the Lie algebra.

A bilinear form (,) on a Lie algebra is called *invariant* if $([a, b], c)+(b[a, c]) = 0$ for all a, b, c. This is called invariant because it corresponds to the form being invariant under the corresponding group action. Now we can construct an invariant bilinear form on E_8 as follows:

1. $(\alpha, \beta)_{\text{in the Lie algebra}} = (\alpha, \beta)_{\text{in the lattice}}$

2. $(\hat{e}^\alpha, (\hat{e}^\alpha)^{-1}) = 1$

3. $(a, b) = 0$ if a and b are in root spaces α and β with $\alpha + \beta \neq 0$.

This gives an invariant inner product on E_8, which we prove by case-by-case check

Exercise 394 do these checks

We constructed a Lie algebra of type E_8, which was $L \oplus \bigoplus \hat{e}^\alpha$, where L is the root lattice and $\alpha^2 = 2$. This gives a double cover of the root lattice:

$$1 \to \pm 1 \to \hat{e}^L \to e^L \to 1.$$

We had a lift for $\omega(\alpha) = -\alpha$, given by $\omega(\hat{e}^\alpha) = (-1)^{(\alpha^2/2)}(\hat{e}^\alpha)^{-1}$. So ω becomes an automorphism of order 2 on the Lie algebra. $e^\alpha \mapsto (-1)^{(\alpha,\beta)}e^\alpha$ is also an automorphism of the Lie algebra.

Suppose σ is an automorphism of order 2 of the real Lie algebra $L = L^+ + L^-$ (eigenspaces of σ). We saw that you can construct another real form given by $L^+ + iL^-$. Thus, we have a map from conjugacy classes of automorphisms with $\sigma^2 = 1$ to real forms of L. This is not in general in isomorphism.

E_8 has an invariant symmetric bilinear form $(e^\alpha, (e^\alpha)^{-1}) = 1$, $(\alpha, \beta) = (\beta, \alpha)$. The form is unique up to multiplication by a constant since E_8 is an irreducible representation of E_8. So the *absolute value of the signature* is an invariant of the Lie algebra.

For the split form of E_8, what is the signature of the invariant bilinear form (the split form is the one we just constructed)? On the Cartan subalgebra L, $(\ ,\ )$ is positive definite, so we get $+8$ contribution to the signature. On $\{e^\alpha, (e^\alpha)^{-1}\}$, the form is $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, so it has signature $0 \cdot 120$. Thus, the signature is 8. So if we find any real form with a different signature, we will have found a new Lie algebra.

We first try involutions $e^\alpha \mapsto (-1)^{(\alpha,\beta)} e^\alpha$. But this does not change the signature. L is still positive definite, and we still have $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right)$ on the other parts. These Lie algebras actually turn out to be isomorphic to what we started with (though we have not shown that they are isomorphic).

Now try $\omega : e^\alpha \mapsto (-1)^{\alpha^2/2} (e^\alpha)^{-1}$, $\alpha \mapsto -\alpha$. What is the signature of the form? We write down the $+$ and $-$ eigenspaces of ω. The $+$ eigenspace will be spanned by $e^\alpha - e^{-\alpha}$, and these vectors have norm -2 and are orthogonal. The $-$ eigenspace will be spanned by $e^\alpha + e^{-\alpha}$ and L, which have norm 2 and are orthogonal, and L is positive definite. What is the Lie algebra corresponding to the involution ω? It will be spanned by $e^\alpha - e^{-\alpha}$ where $\alpha^2 = 2$ (norm -2), and $i(e^\alpha + e^{-\alpha})$ (norm -2), and iL (which is now negative definite). So the bilinear form is *negative definite*, with signature $-248 (\neq \pm 8)$.

With some more work, we can actually show that this is the Lie algebra of the *compact* form of E_8. This is because the automorphism group of E_8 preserves the invariant bilinear form, so it is contained in $O_{0,248}(\mathbb{R})$, which is compact.

Now we look at involutions of the form $e^\alpha \mapsto (-1)^{(\alpha,\beta)} \omega(e^\alpha)$. Notice that ω commutes with $e^\alpha \mapsto (-1)^{(\alpha,\beta)} e^\alpha$. The β's in (α, β) correspond to $L/2L$ modulo the action of the Weyl group $W(E_8)$. Remember this has three orbits, with 1 norm 0 vector, 120 norm 2 vectors, and 135 norm 4 vectors. The norm 0 vector gives us the compact form. Let's look at the other cases and see what we get.

Suppose V has a negative definite symmetric inner product $(\ ,\ )$, and suppose σ is an involution of $V = V_+ \oplus V_-$ (eigenspaces of σ). What is the signature of the invariant inner product on $V_+ \oplus iV_-$? On V_+, it is negative definite, and on iV_- it is positive definite. Thus, the signature is $\dim V_- - \dim V_+ = -\mathrm{tr}(\sigma)$. So we want to work out the traces of these involutions.

Given some $\beta \in L/2L$, what is $\mathrm{tr}(e^\alpha \mapsto (-1)^{(\alpha,\beta)} e^\alpha)$? If $\beta = 0$, the traces is obviously 248 because we just have the identity map. If $\beta^2 = 2$, we need to figure how many roots have a given inner product with β. Recall that this was determined before:

(α,β)	# of roots α with given inner product	eigenvalue
2	1	1
1	56	-1
0	126	1
-1	56	-1
-2	1	1

Thus, the trace is $1-56+126-56+1+8=24$ (the 8 is from the Cartan subalgebra). So the signature of the corresponding form on the Lie algebra is -24. We've found a third Lie algebra.

If we also look at the case when $\beta^2=4$, what happens? How many α with $\alpha^2=2$ and with given (α,β) are there? In this case, we have:

(α,β)	# of roots α with given inner product	eigenvalue
2	14	1
1	64	-1
0	84	1
-1	64	-1
-2	14	1

The trace will be $14-64+84-64+14+8=-8$. This is just the split form again.

Summary: We've found 3 forms of E_8, corresponding to 3 classes in $L/2L$, with signatures 8, -24, -248, corresponding to involutions $e^\alpha \mapsto (-1)^{(\alpha,\beta)}e^{-\alpha}$ of the *compact* form. If L is the *compact* form of a simple Lie algebra, then Cartan showed that the other forms correspond exactly to the conjugacy classes of involutions in the automorphism group of L (this doesn't work if we don't start with the compact form — so always start with the compact form).

In fact, these three are the *only* forms of E_8, but we won't prove that.

Example 395 Let's go back to various forms of E_8 and figure out (guess) the fundamental groups. We need to know the maximal compact subgroups.

1. One of them is easy: the compact form is its own maximal compact subgroup. What is the fundamental group? Remember or quote the fact that for compact simple groups, $\pi_1 \cong \frac{\text{weight lattice}}{\text{root lattice}}$, which is 1. So this form is simply connected.

2. $\beta^2=2$ case (signature -24). Recall that there were 1, 56, 126, 56, and 1 roots α with $(\alpha,\beta)=2,1,0,-1$, and -2 respectively, and there are another 8 dimensions for the Cartan subalgebra. On the $1,126,1,8$ parts, the form is negative definite. The sum of these root spaces gives a Lie algebra of type E_7A_1 with a negative definite bilinear form (the 126 gives you the roots of an E_7, and the 1s are the roots of an A_1). So it a reasonable guess that the maximal compact subgroup has something to do with E_7A_1. E_7 and A_1 are not simply connected: the compact form of E_7 has $\pi_1=\mathbb{Z}/2$ and the compact form of A_1 also has $\pi_1=\mathbb{Z}/2$. So the universal cover of E_7A_1 has center $(\mathbb{Z}/2)^2$. Which part of this acts trivially on E_8? We look at the E_8 Lie algebra as a representation of $E_7\times A_1$. You can read off how it splits form the picture above: $E_8\cong E_7\oplus A_1\oplus 56\otimes 2$, where 56 and 2 are irreducible, and the centers of E_7 and A_1 both act as -1 on them. So

the maximal compact subgroup of this form of E_8 is the simply connected compact form of $E_7 \times A_1/(-1,-1)$. This means that $\pi_1(E_8)$ is the same as π_1 of the compact subgroup, which is $(\mathbb{Z}/2)^2/(-1,-1) \cong \mathbb{Z}/2$. So this simple group has a nontrivial double cover (which is non-algebraic).

3. For the other (split) form of E_8 with signature 8, the maximal compact subgroup is $\mathrm{Spin}_{16}(\mathbb{R})/(\mathbb{Z}/2)$, and $\pi_1(E_8)$ is $\mathbb{Z}/2$.

You can compute any other homotopy invariants with this method.

Let's look at the 56 dimensional representation of E_7 in more detail. We had the picture

(α,β)	# of α's
2	1
1	56
0	126
-1	56
-2	1

The Lie algebra E_7 fixes these 5 spaces of E_8 of dimensions $1, 56, 126+8, 56, 1$. From this we can get some representations of E_7. The $126+8$ splits as $1+(126+7)$. But we also get a 56 dimensional representation of E_7. Let's show that this is actually an irreducible representation. Recall that in calculating $W(E_8)$, we showed that $W(E_7)$ acts transitively on this set of 56 roots of E_8, which can be considered as weights of E_7.

An irreducible representation is called *minuscule* if the Weyl group acts transitively on the weights. This kind of representation is particularly easy to work with. It is really easy to work out the character for example: just translate the 1 at the highest weight around, so every weight has multiplicity 1.

So the 56 dimensional representation of E_7 must actually be the irreducible representation with whatever highest weight corresponds to one of the vectors.

37.2 Every possible simple Lie group

We will construct them as follows: Take an involution σ of the compact form $L = L^+ + L^-$ of the Lie algebra, and form $L^+ + iL^-$. The way we constructed these was to first construct A_n, D_n, E_6, and E_7 as for E_8. Then construct the involution $\omega : e^\alpha \mapsto -e^{-\alpha}$. We get B_n, C_n, F_4, and G_2 as fixed points of the involution ω.

Kac classified all automorphisms of finite order of any compact simple Lie group. The method we'll use to classify involutions is extracted from his method. We can construct lots of involutions as follows:

1. Take any Dynkin diagram, say E_8, and select some of its verticals, corresponding to simple roots. Get an involution by taking $e^\alpha \mapsto \pm e^\alpha$ where the sign depends on whether α is one of the simple roots we've selected. However, this is not a great method. For one thing, we get a lot of repeats (recall that there are only 3, and we've found 2^8 this way).

2. Take any diagram automorphism of order 2, such as

   This gives you more involutions.

Next time, we'll see how to cut down this set of involutions. Split form of Lie algebra (we did this for A_n, D_n, E_6, E_7, E_8): $A = \bigoplus \hat{e}^\alpha \oplus L$. Compact form $A^+ + iA^-$, where $A^\pm$ eigenspaces of $\omega : \hat{e}^\alpha \mapsto (-1)^{\alpha^2/2}\hat{e}^{-\alpha}$.

We talked about other involutions of the compact form. You get all the other forms this way.

The idea now is to find ALL real simple Lie algebras by listing all involutions of the compact form. We will construct all of them, but we won't prove that we have all of them.

We'll use Kac's method for classifying all automorphisms of order N of a compact Lie algebra (and we'll only use the case $N = 2$). First let's look at inner automorphisms. Write down the AFFINE Dynkin diagram

Choose n_i with $\sum n_i m_i = N$ where the m_i are the numbers on the diagram. We have an automorphism $e^{\alpha_j} \mapsto e^{2\pi i n_j/N}e^{\alpha_j}$ induces an automorphism of order dividing N. This is obvious. The point of Kac's theorem is that all inner automorphisms of order dividing N are obtained this way and are conjugate if and only if they are conjugate by an automorphism of the Dynkin diagram. We won't actually prove Kac's theorem because we just want to get a bunch of examples.

Example 396 Real forms of E_8. We've already found three, and it took us a long time. We can now do it fast. We need to solve $\sum n_i m_i = 2$ where $n_i \geq 0$; there are only a few possibilities:

The points NOT crossed off form the Dynkin diagram of the maximal compact subgroup. Thus, by just looking at the diagram, we can see what all the real forms are!

Example 397 Let's do E_7. Write down the affine diagram:

We get the possibilities

(*) The number of ways is counted up to automorphisms of the diagram.

(**) In the split real form, the maximal compact subgroup has dimension equal to half the number of roots. The roots of A_7 look like $\varepsilon_i - \varepsilon_j$ for $i, j \leq 8$ and $i \neq j$, so the dimension is $8 \cdot 7 + 7 = 56 = \frac{112}{2}$.

(***) The maximal compact subgroup is $E_6 \oplus \mathbb{R}$ because the fixed subalgebra contains the whole Cartan subalgebra, and the E_6 only accounts for 6 of the 7 dimensions. You can use this to construct some interesting representations of E_6 (the minuscule ones). How does the algebra E_7 decompose as a representation of the algebra $E_6 \oplus \mathbb{R}$?

We can decompose it according to the eigenvalues of $\mathbb{R}$. The $E_6 \oplus \mathbb{R}$ is the zero eigenvalue of $\mathbb{R}$ [why?], and the rest is 54 dimensional. The easy way to see the decomposition is to look at the roots. Remember when we computed the Weyl group we looked for vectors like

The 27 possibilities (for each) form the weights of a 27 dimensional representation of E_6. The orthogonal complement of the two nodes is an E_6 root system whose Weyl group acts transitively on these 27 vectors (we showed that these form a single orbit, remember?). Vectors of the E_7 root system are the vectors of the E_6 root system plus these 27 vectors plus the other 27 vectors. This splits up the E_7 explicitly. The two 27s form single orbits, so they are irreducible. Thus, $E_7 \cong E_6 \oplus \mathbb{R} \oplus 27 \oplus 27$, and the 27s are minuscule.

Let K be a maximal compact subgroup, with Lie algebra $\mathbb{R} + E_6$. The factor of $\mathbb{R}$ means that K has an S^1 in its center. Now look at the space G/K, where G is the Lie group of type E_7, and K is the maximal compact subgroup. It is a *Hermitian symmetric space*. Symmetric space means that it is a (simply connected) Riemannian manifold M such that for each point $p \in M$, there is an automorphism fixing p and acting as -1 on the tangent space. This looks weird, but it turns out that all kinds of nice objects you know about are symmetric spaces. Typical examples you may have seen: spheres S^n, hyperbolic space $\mathbb{H}^n$, and Euclidean space $\mathbb{R}^n$. Roughly speaking, symmetric spaces have nice properties of these spaces. Cartan classified all symmetric spaces: they are non-compact simple Lie groups modulo the maximal compact subgroup (more or less ... depending on simply connectedness hypotheses 'n such). Historically, Cartan classified simple Lie groups, and then later classified symmetric spaces, and was surprised to find the same result. Hermitian symmetric spaces are just symmetric spaces with a complex structure. A standard example of this is the upper half plane $\{x + iy | y > 0\}$. It is acted on by $SL_2(\mathbb{R})$, which acts by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \tau = \frac{a\tau+b}{c\tau+d}$.

Let's go back to this G/K and try to explain why we get a Hermitian symmetric space from it. We'll be rather sketchy here. First of all, to make it a symmetric space, we have to find a nice invariant Riemannian metric on it. It is sufficient to find a positive definite bilinear form on the tangent space at p which is invariant under K ... then we can translate it around. We can do this as K is compact (so you have the averaging trick). Why is it Hermitian? We'll show that there is an almost complex structure. We have S^1 acting on the tangent space of each point because we have an S^1 in the center of the stabilizer of any given point. Identify this S^1 with complex numbers of absolute value 1. This gives an invariant almost complex structure on G/K. That is, each tangent space is a complex vector space. Almost complex structures don't always come from complex structures, but this one does (it is integrable). Notice that it is a little unexpected that G/K has a complex structure (G and K are odd dimensional in the case of $G = E_7$, $K = E_6 \oplus \mathbb{R}$, so they have no hope of having a complex structure).

Example 398 Let's look at E_6, with affine Dynkin diagram

We get the possibilities

In the last one, the maximal compact subalgebra is $D_5 \oplus \mathbb{R}$. Just as before, we get a Hermitian symmetric space. Let's compute its dimension (over $\mathbb{C}$). The dimension will be the dimension of E_6 minus the dimension of $D_5 \oplus \mathbb{R}$, all divided by 2 (because we want complex dimension), which is $(78 - 46)/2 = 16$.

So we have found two non-compact simply connected Hermitian symmetric spaces of dimensions 16 and 27. These are the only "exceptional" cases; all the others fall into infinite families!

There are also some OUTER automorphisms of E_6 coming from the diagram automorphism

The fixed point subalgebra has Dynkin diagram obtained by folding the E_6 on itself. This is the F_4 Dynkin diagram. The fixed points of E_6 under the diagram automorphism is an F_4 Lie algebra. So we get a real form of E_6 with maximal compact subgroup F_4. This is probably the easiest way to construct F_4, by the way. Moreover, we can decompose E_6 as a representation of F_4. $\dim E_6 = 78$ and $\dim F_4 = 52$, so $E_6 = F_4 \oplus 26$, where 26 turns out to be irreducible (the smallest non-trivial representation of F_4 ... the only one anybody actually works with). The roots of F_4 look like $(\dots, \pm 1, \pm 1 \dots)$ (24 of these) and $(\pm\frac{1}{2} \cdots \pm \frac{1}{2})$ (16 of these), and $(\dots, \pm 1 \dots)$ (8 of them) ... the last two types are in the same orbit of the Weyl group.

The 26 dimensional representation has the following character: it has all norm 1 roots with multiplicity 1 and 0 with multiplicity 2 (note that this is not minuscule).

There is one other real form of E_6. To get at it, we have to talk about Kac's description of non-inner automorphisms of order N. The non-inner automorphisms all turn out to be related to diagram automorphisms. Choose a diagram automorphism of order r, which divides N. Let's take the standard thing on E_6. Fold the diagram (take the fixed points), and form a TWISTED affine Dynkin diagram (note that the arrow goes the wrong way from the affine F_4)

There are also numbers on the twisted diagram, but never mind them. Find n_i so that $r \sum n_i m_i = N$. This is Kac's general rule. We'll only use the case $N = 2$.

If $r > 1$, the only possibility is $r = 2$ and one n_1 is 1 and the corresponding m_i is 1. So we just have to find points of weight 1 in the twisted affine Dynkin diagram. There are just two ways of doing this in the case of E_6

one of these gives us F_4, and the other has maximal compact subalgebra C_4, which is the split form since $\dim C_4 = \#\text{roots of } F_4/2 = 24$.

Example 399 F_4. The affine Dynkin is

We can cross out one node of weight 1, giving the compact form (split form), or a node of weight 2 (in two ways), giving maximal compacts A_1C_3 or B_4. This gives us three real forms.

Example 400 G_2. We can actually draw this root system ... UCB won't supply me with a four dimensional board. The construction is to take the D_4 algebra and look at the fixed points of:

We want to find the fixed point subalgebra.

Fixed points on Cartan subalgebra: ρ fixes a two dimensional space, and has 1 dimensional eigenspaces corresponding to ω and $\bar{\omega}$, where $\omega^3 = 1$. The 2 dimensional space will be the Cartan subalgebra of G_2.

Positive roots of D_4 as linear combinations of simple roots (not fundamental weights):

There are six orbits under ρ, grouped above. It obviously acts on the negative roots in exactly the same way. What we have is a root system with six roots of norm 2 and six roots of norm 2/3. Thus, the root system is G_2:

One of the only root systems to appear on a country's national flag. Now let's work out the real forms. Look at the affine:

we can delete the node of weight 1, giving the compact form:

. We can delete the node of weight 2, giving A_1A_1 as the compact subalgebra:

... this must be the split form because there is nothing else the split form can be.

Let's say some more about the split form. What does the Lie algebra of G_2 look like as a representation of the maximal compact subalgebra $A_1 \times A_1$? In this case, it is small enough that we can just draw a picture:

We have two orthogonal A_1s, and we have leftover the stuff on the right. This thing on the right is a tensor product of the 4 dimensional irreducible representation of the horizontal and the 2 dimensional of the vertical. Thus, $G_2 = 3\times 1 + 1\otimes 3 + 4\otimes 2$ as irreducible representations of $A_1^{(\text{horizontal})} \otimes A_1^{(\text{vertical})}$.

Let's use this to determine exactly what the maximal compact subgroup is. It is a quotient of the simply connected compact group $SU(2)\times SU(2)$, with Lie algebra $A_1 \times A_1$. Just as for E_8, we need to identify which elements of the center act trivially on G_2. The center is $\mathbb{Z}/2\times\mathbb{Z}/2$. Since we've decomposed G_2, we can compute this easily. A non-trivial element of the center of $SU(2)$ acts as 1 (on odd dimensional representations) or -1 (on even dimensional representations). So the element $z \times z \in SU(2) \times SU(2)$ acts trivially on $3 \otimes 1 + 1 \otimes 3 + 4 \times 2$. Thus the maximal compact subgroup of the non-compact simple G_2 is $SU(2) \times SU(2)/(z \times z) \cong SO_4(\mathbb{R})$, where z is the non-trivial element of $\mathbb{Z}/2$.

So we have constructed $3 + 4 + 5 + 3 + 2$ (from E_8, E_7, E_6, F_4, G_2) real forms of exceptional simple Lie groups.

There are another 5 exceptional real Lie groups: Take COMPLEX groups $E_8(\mathbb{C})$, $E_7(\mathbb{C})$, $E_6(\mathbb{C})$, $F_4(\mathbb{C})$, and $G_2(\mathbb{C})$, and consider them as REAL. These give simple real Lie groups of dimensions 248×2, 133×2, 78×2, 52×2, and 14×2.

38 Discrete subgroups of Lie groups

We will show how to classify the finite subgroups G of $O_3(R)$ using Thurston's theory of orbifolds. The key idea it to look at the orbit space S^2/G. This is not usually a manifold (unless G happens to act freely) but is a more general sort of object called an orbifold, which is a sort of manifold with mild singularities. Two-dimensional orbifolds turn out to be easy to classify as there are only a limited number of possible singularities, so we can use this to classify finite rotation and reflection groups.

We first look at the possible singularities of a smooth surface by a finite group. The singularity is going to look locally like R^2/G where G is some finite group acting on the vector space R^2. There are not too many of these, as they have to be subgroups of $O_2(R)$: G is either cyclic, acting as rotations or dihedral, acting as rotations and reflections. The corresponding singularities are either conical points with angle $2\pi/n$ (for G cyclic of order n) or a sector of angle $2\pi/2n$, for G dihedral of order $2n$.

The Euler characteristic of the orbifold is (Euler characteristic of 2-sphere)/(Order of group), which must be positive as the 2-sphere has positive Euler characteristic. This is also equal to the number of points-lines plus faces of the orbifold. However we must be careful to count points and lines properly: a point that is a quotient singularity by a group of order n is really only $1/n$ of a point. Similarly a boundary edge is really only half a line. In other words whenever we have a point that is a quotient singularity we need to adjust the Euler characteristic by $1 - 1/n$.

So in the orientable case when the quotient orbifold is a topological sphere with quotient singularities of orders n_i the Euler characteristic is

$$\text{Euler characteristic of sphere} - \text{corrections} = 2 - \sum(1 - 1/n_i)$$

and this is equal to (Euler characteristic of 2-sphere)/(Order of group) $= 2/|G| >$

0. So we want to solve the equation

$$\sum(1-1/n_i) < 2$$

for integers $n_i > 1$. There is an extra condition: there cannot be just one integer, and if we have just two integers they must be the same, otherwise we get a bad orbifold which has no cover that is a manifold. It is easy to find the solutions: they are (), (n,n), $(2,2,n)$, $(2,3,3)$, $(2,3,4)$, $(2,3,5)$. These correspond to quotients of the sphere by the trivial group, cyclic groups of order n, dihedral groups of order $2n$, and the rotations of a tetrahedron, octahedron, or icosahedron.

The unorientable case when the quotient is a disc or projective plane is similar. The correction factors are $1/2$ for each edge and $1-1/2m$ for every sector singularity on the boundary, so we find

$$1-\sum(1-1/n_i)-\sum(1-1/m_i)/2 = 1/|G| > 0.$$

Here the numbers m_i are the orders of the sector singularities, and the 2's are replaced by 1's because we replace the sphere of Euler characteristic 2 by the disc or projective plane which have Euler characteristic 1. (Of course for the projective plane there are no sector singularities because it has no boundary.)

The finite subgroups of $O_4(R)$ can be classified by reducing to the case of $O_3(R)$ using the fact the $O_4(R)$ is almost a product of 2 copies of $O_3(R)$: more precisely the double cover of $SO_4(R)$ is isomorphic to the product of two copies of the double cover of $SO_3(R)$. These groups act on S^3 so give examples of compact 3-dimensional orbifolds. If the finite group acts freely on S^3 then we get compact 3-dimensional manifolds called space forms. These are fairly straightforward to classify, and by Perelman's proof of Thurston's elliptization conjecture they give all closed 3-manifolds with finite fundamental group. For example, lens spaces arise by taking a 2-dimensional complex representation of a cyclic group, which acts on the 3-sphere of vectors of length 1. A particularly famous example is Poincare's homology 3-sphere. Any subgroup of the group S^3 automatically acts fixed point freely on S^3, so any double cover of a finite group of rotations on $SO_3(R)$ is the fundamental group of a compact 3-manifold. The Poincare 3-sphere arises by taking the double cover of the group of rotations of the icosahedron. The fundamental group is the perfect group of order 120. As the fundamental group is perfect, the first homology group of the manifold is trivial, so the manifold is a homology sphere.

Exercise 401 Classify the 17 wallpaper groups (discrete co-compact subgroups of the group $R^2.O_2(R)$ of isometries of the plane R^2) by looking at the quotient orbifolds. This is similar to classifying the finite subgroups of isometries of the sphere, except this time the Euler characteristic of the quotient orbifold is zero rather than positive. There are 4 orbifolds whose underlying topological space is a sphere and 8 whose underlying space is a disk. Also there are 5 more surfaces that can appear: the Klein bottle, torus, Moebius strip, projective plane, and annulus, each of which corresponds to 1 group.

In 3-dimensions the analogues of wallpaper groups are the cocompact subgroups of $R^3.O_3(R)$ and are called space groups. They are of great interest to crystallographers and geologists as they describe the possible symmetries of crystals. There are 230 or 219 classes of them depending on whether one distinguishes mirror images of group, which were independently classified by Fyodorov, Barlow, and Schnflies in the 1890s. Conway and Thurston redid the classification in terms of 3-dimensional orbifolds.

A Fuchsian group is a discrete subgroup of $SL_2(R)$. The group $SL_2(R)$ acts on 2-dimensional hyperbolic space and also on the upper half complex plane, so Fuchsian groups are closely related to 2-dimensional oriented hyperbolic manifolds and to Riemann surfaces. (The correspondence is not quite exact, as Fuchsian groups can have elliptic elements fixing points, so that the quotients have orbifold singularities.) In particular any compact Riemann surface of genus g at least 2 gives a Fuchsian group isomorphic to its fundamental group. The space of (marked) Fuchsian groups obtained like this is called Teichmuller space, and is a complex manifold of dimension $3g-3$ with a very rich geometry. The classical example of a Fuchsian group is $SL_2(Z)$. The quotient of the upper half plane by $SL_2(Z)$ is an orbifold given by the complex sphere with a point missing and with orbifold singularities of orders 2 and 3. The more general case of congruence subgroups such as $\Gamma_0(N)$ (c divisible by N) are of central importance in number theory: Wiles's proof of Fermat's last theorem depended on a deep study of the modular forms for these groups (sections of certain line bundles over the quotient orbifolds).

A Kleinian group is a discrete subgroup of $SL_2(C)$. Like Fuchsian groups, these can be thought of as either complex or hyperbolic transformation groups, because the group $PSL_2(C)$ is both the group of automorphisms of the complex sphere, and also the group of automorphisms of oriented hyperbolic 3-space. In particular if Kleinian group is cocompact and acts freely, we get a closed hyperbolic 3-manifold. Unlike the case of Fuchsian groups, where there are infinite families of cocompact groups, cocompact (and cofinite) Kleinian groups are rigid: the only deformations are given by inner automorphisms. This is a special case of Mostow rigidity, which says in particular that isomorphisms of cofinite Kleinian groups extend to isomorphisms of $PSL_2(C)$. One way of thinking about this is that closed hyperbolic 3-manifolds have an essentially unique hyperbolic metric (quite unlike what happens in 2-dimensions): any invariant of the metric, such as the volume, is an invariant of the underlying topological manifold.

Thurston discovered that all closed 3-manifolds can be built from discrete subgroups of Lie groups. More precisely every closed 3-manifold can be cut up in a canonical way along spheres and tori so that each piece has a geometric structure of finite volume. There are 8 different sorts of geometric structure that appear corresponding to 8 particular Lie groups (modulo a maximal compact subgroup). We have seem 3 of these above: they correspond to spherical, Euclidean, and hyperbolic structures. Two more come from taking the product of 2-dimensional spherical or hyperbolic structures with a line. The remaining 3 structures come from 3 of the Bianchi groups: the Heisenberg group, the universal cover of $SL_2(R)$, and a solvable group that is the Bianchi group of type VI_0 and its identity component is the group of isometries of Minkowski space in 2-dimensions. Of these 8 geometries, the manifolds for all except the hyperbolic geometry are classified (or at least well understood). There seems to be no obvious analogue of Thurston's classification for manifolds of dimension 4 and above.

39 Chevalley groups

Steinberg presentation.

40 Jacobson-Morozov and nilpotent elements

41 Cohomology of Lie groups and algebras

As an example of how to work with simple Lie groups, we will look at the general question: Given a simple Lie group, what is its homotopy type? Answer: G has a unique conjugacy class of maximal compact subgroups K, and G is homotopy equivalent to K. **Proof** [Proof for $GL_n(\mathbb{R})$] First pretend $GL_n(\mathbb{R})$ is simple, even though it isn't; whatever. There is an obvious compact subgroup: $O_n(\mathbb{R})$. Suppose K is *any* compact subgroup of $GL_n(\mathbb{R})$. Choose any positive definite form $(\ ,\ )$ on $\mathbb{R}^n$. This will probably not be invariant under K, but since K is compact, we can average it over K get one that is: define a new form $(a,b)_{\text{new}} = \int_K (ka,kb)\,dk$. This gives an invariant positive definite bilinear form (since integral of something positive definite is positive definite). Thus, any compact subgroup preserves some positive definite form. But the subgroup fixing some positive definite bilinear form is conjugate to a subgroup of $O_n(\mathbb{R})$ (to see this, diagonalize the form). So K is contained in a conjugate of $O_n(\mathbb{R})$.

Next we want to show that $G = GL_n(\mathbb{R})$ is homotopy equivalent to $O_n(\mathbb{R}) = K$. We will show that $G = KAN$, where K is O_n, A is all diagonal matrices with positive coefficients, and N is matrices which are upper triangular with 1s on the diagonal. This is the *Iwasawa decomposition*. In general, we get K compact, A semisimple abelian, and N is unipotent. The proof of this we saw before was called the Gram-Schmidt process for orthonormalizing a basis. Suppose $v_1,\dots,v_n$ is any basis for $\mathbb{R}^n$.

1. Make it orthogonal by subtracting some stuff, you'll get v_1, $v_2 - *v_1$, $v_3 - *v_2 - *v_1$, ...
2. Normalize by multiplying each basis vector so that it has norm 1. Now we have an orthonormal basis.

This is just another way to say that GL_n can be written as KAN. Making things orthogonal is just multiplying by something in N, and normalizing is just multiplication by some diagonal matrix with positive entries. An orthonormal basis is an element of O_n. ! This decomposition is just a topological one, not a decomposition as groups. Uniqueness is easy to check.

Now we can get at the homotopy type of GL_n. $N \cong \mathbb{R}^{n(n-1)/2}$, and $A \cong (\mathbb{R}^+)^n$, which are contractible. Thus, $GL_n(\mathbb{R})$ has the same homotopy type as $O_n(\mathbb{R})$, its maximal compact subgroup. □ If we wanted to know $\pi_1(GL_3(\mathbb{R}))$, we could calculate $\pi_1(O_3(\mathbb{R})) \cong \mathbb{Z}/2\mathbb{Z}$, so $GL_3(\mathbb{R})$ has a double cover. Nobody has shown you this double cover because it is *not algebraic.*

Lie algebra cohomology is a somewhat mysterious but very powerful tool As motivation for its definition, consider the problem of calculating the cohomology of the underlying space of a Lie group. When the group is compact, this is the same as its de Rham cohomology, and Lie algebra cohomology is an algebraic way of calculating this.

Definition 402 *The de Rham cohomology of a smooth manifold is the cohomology of the complex of smooth differential forms, with the differential given by the exterior derivative.*

Exercise 403 Calculate the de Rham cohomology groups of the circle.

The exterior derivative of a differential form ω is given by

$$d\omega(v_0, \ldots, v_n) = \sum (-1)^{i+j} \omega([v_i, v_j], v_1, ..\hat{v_i}, \hat{v_j}, \ldots)$$

where the hat means that the term is omitted.

The cohomology of a compact connected Lie group is acted on by the Lie group since the lie group acts on itself by left translations. Moreover this action must be trivial, because the group is connected and the cohomology has an integral form, and any action of a connected group on a discrete lattice must be trivial. So we can cut down the infinite dimensional space of all differential forms to the finite dimensional space of left-invariant ones. These in turn can be identified with the exterior algebra of the cotangent space at the identity.

We also notice that we really have an unnecessary duality: instead of looking at elements of the dual exterior algebra of the tangent space, we can just directly use the exterior algebra of the tangent space. The exterior derivative induces the following map:

$$d(v_1 \wedge V_2 \wedge \cdots) = \sum_{i<j} (-1)^{i+j} [v_i \wedge v_j] \wedge v_1 \cdots$$

In other words the homology of a compact connected Lie group G is the homology of the exterior algebra of its Lie algebra $\Lambda^* \mathfrak{g}$ with the differential above.

Exercise 404 Find the Lie algebra homology $H_*(\mathfrak{g})$ for $\mathfrak{g}$ the 3-dimensional abelian Lie algebra, the 3-dimensional Heisenberg Lie algebra, and the orthogonal Lie algebra $\mathfrak{so}_3(\mathbb{R})$. Find a 3-dimensional real Lie algebra $\mathfrak{g}$ whose homology groups $H_i(\mathfrak{g})$ are 1-dimensional for $i = 0, 1, 2, 3$.

Exercise 405 If an n-dimensional complex Lie algebra $\mathfrak{g}$ has a non-degenerate invariant bilinear form, show that its homology group $H_n(\mathfrak{g})$ is 1-dimensional. (Calculate $d(g_1 \wedge g_1 \wedge \cdots)$ for an orthogonal base $g_1, g_2, \cdots$.) Find an example of a complex Lie algebra $\mathfrak{g}$ of dimension 2 such that $H_2(\mathfrak{g}) = 0$.

Exercise 406 If $\mathfrak{g}$ is a finite dimensional Lie algebra over a field, show that $\sum_n (-1)^n \dim(H_n(\mathfrak{g})) = 0$.

Definition 407 *We define a bracket* $[,]$ *on* $\Lambda\mathfrak{g}$ *by*

$$[a_1 \wedge a_2 \wedge \cdots a_n, b_1 \wedge b_2 \wedge \cdots] = \sum_{i,j} (-1)^{i+j+n-1} [a_i, b_j] \wedge a_2 \wedge \cdots \wedge b_2 \wedge \cdots$$

This makes $\Lambda\mathfrak{g}$ into a Lie superalgebra, with the grading shifted by 1.

Exercise 408 Show that

$$[a, b] = (-1)^{\deg a + \deg b - 1}[b, a]$$

$$d(ab) = (da)b + (-1)^{\deg a} adb + [ab]$$

$$d[a, b] = [da, b] + (-1)[a, db]$$

Exercise 409 Suppose that $\mathfrak{g}$ is an n-dimensional complex Lie algebra with a non-degenerate bilinear form, and a and b are homogeneous elements in its exterior algebra. Show that $[a, b] = 0$ whenever $\deg a + \deg b = n$. Show that $\wedge$ induces a nondegenerate "Poincaré duality" pairing

$$H_m(\mathfrak{g}) \times H_{n-m}(\mathfrak{g}) \mapsto G_n(\mathfrak{g}) \cong \mathbb{C}$$

.

Obviously the definition above does not require that $\mathfrak{g}$ be the Lie algebra of a compact Lie group: it works for any Lie algebra over any commutative ring.

Warning 410 For compact connected Lie groups, the Lie algebra homology or cohomology is isomorphic to the homology or cohomology of the underlying topological space. This is definitely NOT true for general connected Lie groups. For example, the Lie groups $\mathbb{R}$ and S^1 have the same Lie algebra so the same Lie algebra homology, but have different first homology groups of the underlying topological spaces.

A useful variation is the Lie algebra homology or cohomology of a module M over a Lie algebra $\mathfrak{g}$. To construct this we form the Lie algebra $\mathfrak{g} \oplus M$ given as a semidirect product of the Lie algebra $\mathfrak{g}$ and the abelian Lie algebra M, and grade it by giving $\mathfrak{g}$ degree 0 and M degree 1. Then the Lie algebra homology $H_*(\mathfrak{g}, M)$ of $\mathfrak{g}$ with coefficients in M is defined to be the degree 1 piece of $H_*(\mathfrak{g} \oplus M)$. Unraveling the definition we find that the homology is given by the homology of $M \otimes \Lambda^*(\mathfrak{g})$, with the differential d given by

$$d(m \otimes v_1 \wedge v_2 \wedge \cdots) = \sum_i (-1)^i [v_i, m] \otimes v_1 \wedge \cdots + \sum_{i,j} m \otimes [v_i, v_j] \wedge v_1 \wedge \cdots$$

We work out the first few homology or cohomology groups of a Lie algebra.

The zeroth homology and cohomology groups are just the field k.

The first homology is given by $\mathfrak{g} = \Lambda^1\mathfrak{g}$ modulo the image of $\mathfrak{g} \wedge \mathfrak{g}$ under the map taking $a \wedge b$ to $[a, b]$. In other words $H_1(\mathfrak{g})$ is the abelianization of $\mathfrak{g}$. Similarly $H * 1(\mathfrak{g})$ is the dual of this, which is the characters of $\mathfrak{g}$.

The second cohomology $H^2(\mathfrak{g}, M)$ classifies the extensions $M.\mathfrak{g}$ of $\mathfrak{g}$ by M (with M an abelian ideal) up to equivalence. To see this, write the bracket of the extension as

$$[(g, m), (h, n)] = ([g, h], c(g, h) + [g, n] + [m, h])$$

for some $c(g, h) \in M$. Then anticommutativity implies that

$$c(g, h) = -c(h, g)$$

and the Jacobi identity implies

$$c([g,h],i)+c([h,i],g)+c([i,g],h)+[i,c(g,h)]+[g,c(h,i)]+[h,c(i,g)]=0.$$

which says that c is a 2-cocycle with values in M, so determines an element of $H^2(\mathfrak{g}, M)$. Also adding a 1-cocycle to c corresponds to changing the lift of elements of $\mathfrak{g}$ so gives an equivalent extension.

The second homology $H_2(\mathfrak{g})$ appears in the center of the universal central extension of a perfect Lie algebra $\mathfrak{g}$. Suppose $\mathfrak{g}$ is a Lie algebra. Then there is an obvious 2-cocycle of $\mathfrak{g}$ taking values in $\Lambda^2 g/d\Lambda^3 g$, so we get a central extension $(\Lambda^2\mathfrak{g}/d\Lambda^3\mathfrak{g}).\mathfrak{g}$. By construction this central extension has the following universality property: if $\mathfrak{n}.\mathfrak{g}$ is any central extension, and we are given a linear map from $\mathfrak{g}$ to $\mathfrak{n}.\mathfrak{g}$ lifting the identity map on $\mathfrak{g}$, then this can be extended to a Lie algebra homomorphism from $(\Lambda^2\mathfrak{g}/d\Lambda^3\mathfrak{g}).\mathfrak{g}$ to $\mathfrak{n}.\mathfrak{g}$. If $\mathfrak{g}$ is perfect we can do better than this by eliminating the dependence on the choice of lifting. To do this we look at the derived algebra of $(\Lambda^2\mathfrak{g}/d\Lambda^3\mathfrak{g}).\mathfrak{g}$. This still maps onto $\mathfrak{g}$ as $\mathfrak{g}$ is perfect, but the central subalgebra may become smaller: it is replaced by the elements of $(\Lambda^2\mathfrak{g}/d\Lambda^3\mathfrak{g})$ that can be written in the form $\sum a_i \wedge b_i$ with $\sum[a_i, b_i] = 0$. In other words it is now exactly the second homology group of $\mathfrak{g}$.

Now we want to show that this is a universal central extension in the following sense: if $\mathfrak{n}.\mathfrak{g}$ is a central extension of $\mathfrak{g}$ then there is a unique homomorphism from $H_2(\mathfrak{g}).\mathfrak{g}$ to $\mathfrak{n}.\mathfrak{g}$ lifting the identity map on $\mathfrak{g}$. Existence of such a lifting follows immediately from the remarks above, since we just have to choose a lifting from $\mathfrak{g}$ to $\mathfrak{n}.\mathfrak{g}$. Now we want to show that the map $H_2(\mathfrak{g}).\mathfrak{g}$ to $\mathfrak{n}.\mathfrak{g}$ is unique. If a,b are any two elements of $H_2(\mathfrak{g}).\mathfrak{g}$ then the image of $[a, b]$ in $\mathfrak{n}.\mathfrak{g}$ is uniquely determined as changing a or b by an element of the center does not change $[a, b]$. So the lifting is uniquely determined on the derived algebra of $H_2(\mathfrak{g}).\mathfrak{g}$, but as this is perfect the lifting is uniquely determined.

The restriction to perfect Lie algebras really is necessary: Lie algebras that are not perfect do not have universal central extensions.

41.1 The Koszul complex

The homology and cohomology of Lie algebras can also be defined using the universal enveloping algebra $U\mathfrak{g}$ as follows: $H^n(\mathfrak{g}, M) = Ext^n_{U\mathfrak{g}}(k, M)$ and $H_n(\mathfrak{g}, M) = Tor^{U\mathfrak{g}}_n(k, M)$. This in turn is a special case of the homology of an supplemented algebra, which is a special case of Hochschild homology. To see this we introduce the Koszul complex.

We first construct the Koszul complex for abelian Lie algebras. The enveloping algebra is then a commutative polynomial ring $k[x, y, z, \ldots]$. If a is an element of a commutative ring R then there is a complex

$$0 \to R \xrightarrow{\times a} R$$

which is a free resolution of R/aR. If $a_1, \ldots, a_n$ is a finite set of elements of R then we can tensor together the corresponding length 2 complexes. This is called the Koszul complex.

Exercise 411 Suppose that for each i, the element $a_i \in R$ is not a zero divisor in $R/(a_1, \ldots, a_{i-1})$ (in other words the sequence is a regular sequence). Use induction on i to show that the Koszul complex is a resolution of $R/(a_1, \ldots, a_n)$.

Now we construct the Koszul resolution for a finite-dimensional Lie algebra. The resolution is $U\mathfrak{g} \otimes \Lambda\mathfrak{g}$, with the differential given by

$$d(u \otimes g_1 \wedge \cdots \wedge g_n) \tag{25}$$

$$= \sum_i (-1)^i u g_i \otimes g_1 \wedge \cdots \wedge g_{i-1} \wedge g_{i+1} \wedge \cdots \wedge g_n \tag{26}$$

$$+ \sum_{i<j} (-1)^{i+j} u \otimes [g_i, g_j] \wedge g_1 \wedge \cdots \wedge g_n \tag{27}$$

We wish to show this is a resolution of k. The main problem is to show that the sequence is exact, which we do by reducing to the case when $\mathfrak{g}$ is abelian. To do this we filter $U\mathfrak{g} \otimes \Lambda\mathfrak{g}$ by "number of elements of $\mathfrak{g}$", and observe that the associated graded object is just the Koszul resolution for the abelian algebra underlying $\mathfrak{g}$. But if we have a differential group with a finite filtration such that the differential d is exact on the associated graded group, then d is exact on the original group. So the Koszul complex is a resolution of k.

The Tor group $\mathrm{Tor}_*^{U\mathfrak{g}}(k, k)$ is by definition given by the homology of $k \otimes_{U\mathfrak{g}} U\mathfrak{g} \otimes \Lambda\mathfrak{g} = \Lambda\mathfrak{g}$, which is exactly the complex we originally used to define the homology of $\mathfrak{g}$.

42 Central extensions and covering spaces

Schur multiplier, metaplectic group

A common problem is trying to turn a projective representation of a group into a linear representation. For example, suppose V is an irreducible representation of a groups G (finite to make things easy). If a group H acts on G does one get an action of H on V? One obvious obstruction is that H acts on the set of representations of G and might not even fix V, so suppose it does fix V. Then for every element h of H, Schur's lemma implies that we have a corresponding endomorphism of V, unique up to multiplication by a constant. So we get a well defined homomorphism of H to $GL(V)/\mathbb{C}^* = PGL_V$and the question is whether this lifts to a map from H to GL_V.Sometimes it does, and sometimes it does not. But in any case we always get a map from some central extension of H to GL_V, as we can just take the central extension of pairs $(h, g) \in H \times GL_V$ that have the same image in PGL_V. In other words, we get a linear representation of a central extension of H.

So we would like to understand the central extensions of a group H. When H is perfect (in particular simple) there is a neat answer: H has a universal perfect central extension such that all other perfect central extensions are quotients of it.

Example 412 If G is a connected Lie group, it has a universal covering space $\tilde{G}$, given by homotopy classes of paths in G starting at the identity. The kernel of the natural map from $\tilde{G}$ to G is discrete and normal, so in the center of the connected group $\tilde{G}$.

Lie groups (and other groups) often have "unexpected" central extensions. For example, special orthogonal groups have spin groups as double covers, and symmetric groups have non-obvious double covers.

Any perfect group G has a universal central extension that can be constructed as follows. Take a presentation

$$1 \to R \to F \to G \to 1$$

of G as a quotient of G by a free group F. Then $F/[R, F]$ is a central extension of G, and has a homomorphism to any central extension $\tilde{G}$ of G lifting the identity map of G. In general this lift is not unique, but is unique on $[F, F]$. If G is perfect then $[F, F]$ maps onto G and so $[F, F]/[R, F]$ is a universal central extension of G. The kernel $([F, F] \cap R)/[F, R]$ is called the Schur multiplier of G, and does not depend on the choice of presentation of the perfect group G because any two universal central extensions of G are canonically isomorphic.

Exercise 413 Use the Lyndon-Hochschild-Serre spectral sequence to show that the Schur multiplier

$$([F, F] \cap R)/[F, R]$$

is isomorphic to the second cohomology group $H_2(G, \mathbb{Z})$.

Exercise 414 Suppose that G is the semidirect product of the symplectic group $Sp_{2n}(\mathbb{R})$ by its natural representation $\mathbb{R}^{2n}$ (considered as an abelian Lie group). Show that G is perfect, and has a perfect central extension with a 1-dimensional center. This group turns up in the theory of Jacobi forms.

Warning 415 For Lie groups, the Schur multiplier can be a LOT bigger than one might expect, and in particular can be far larger than the center of the universal covering space. For example, if G is $PSL_2(\mathbb{R})$, the center of the universal covering space is just $\mathbb{Z}$, the fundamental group of G. However the center of the universal central extension is uncountable, because K_2 of the reals (or any uncountable field) is uncountable. However these central extensions do not take the topology of G into account but treat G as a discrete group, and seem somewhat pathological.

Example 416 Groups of Lie type over small finite fields have a bewildering number of exceptional Schur multipliers. For example, most of the time $SL_n(\mathbb{F}_q)$ has a trivial Schur multiplier. but the simple group $SL_2(\mathbb{F}_4)$ of order 60 happens to be isomorphic to $PSL_2(\mathbb{F}_5)$ so has Schur multiplier of order 2. The group $PSL_3(\mathbb{F}_4)$ has Schur multiplier of order 48, rather than 3 as one might guess. Several of these exceptional multipliers occur in sporadic simple groups: for example ${}^2E_6(\mathbb{F}_4)$ has an exceptional double cover that appears in the baby monster sporadic group.

Example 417 Suppose that M is a symplectic manifold, with closed non-degenerate 2-form ω. Define the Poisson bracket on smooth functions on M by putting $[f, g] = \langle df, fg \rangle$, where $\langle df, fg \rangle$ is the bilinear form on the cotangenet space induced by ω. If we use ω to identify cotangent vector fields with tangent vector fields, then $f \mapsto df$ is a homomorphism of Lie algebras. The kernel is in the center and consists of locally constant functions. The image consists of the Hamiltonian vector fields, a subalgebra of the vector fields preserving the symplectic form.

43 Levi's theorem and Ado's theorem

Theorem 418 *(Levi) If a finite dimensional Lie algebra $\mathfrak{g}$ over a field of characteristic 0 has radical $\mathfrak{h}$, then $\mathfrak{g}$ splits as a semidirect product of $\mathfrak{h}$ and the semisimple Lie algebra $\mathfrak{g}/\mathfrak{h}$.*

Proof By induction on the length of the derived series for the solvable Lie algebra $\mathfrak{h}$ we can assume that $\mathfrak{h}$ is abelian: in other words we start splitting at the top of $\mathfrak{h}$ and work our way down. Extensions $\mathfrak{h}.(\mathfrak{g}/\mathfrak{h})$ are classified by element of the second cohomology group $H^2(\mathfrak{g}/\mathfrak{h}, \mathfrak{h})$. This group vanishes for $\mathfrak{g}/\mathfrak{h}$ semisimple in characteristic 0 and $\mathfrak{h}$ finite dimensional, so the extension $\mathfrak{h}.(\mathfrak{g}/\mathfrak{h})$ splits. □

Exercise 419 Show that if $\mathfrak{g}$ is a Lie algebra (over a field k) with invariant symmetric bilinear form $(,)$ then $\mathfrak{g}[t, t^{-1}] \oplus k$ is a Lie algebra where the bracket is given by $[gt^m, ht^n] = [g, h]t^{m+n} + (m-n)k]$, and k is in the center. Show that if k has characteristic 0 and g is simple then the Lie algebra is a central extension of a simple Lie algebra but does not split. Find a similar finite-dimensional example in characteristic $p > 0$.

Exercise 420 Show that if $\mathfrak{g}$ is a finite-dimensional complex Lie algebra then $\mathfrak{g}$ splits as the semidirect product of its nilradical and a reductive (abelian plus semisimple) Lie algebra.

Theorem 421 *(Ado) Every finite dimensional Lie algebra over a field of characteristic 0 has a faithful finite-dimensional representation. (Iwasawa showed that this is still true over fields of positive characteristic.*

At first sight this theorem looks as if it ought to be trivial to prove. One the one hand if the center is the whole Lie algebra, in other words if $\mathfrak{g}$ is abelian, the theorem is obvious. At the other extreme if the Lie algebra has no center the theorem is just as obvious because the adjoint representation is faithful. One feels that the general case should follow by somehow combining these two extreme cases, but there seems to be no easy way to do this. **Proof** We first do the case when $\mathfrak{g} = \mathfrak{n}$ is nilpotent. In this case there is a decreasing sequence of ideals $\mathfrak{n} = \mathfrak{n}_1 \supseteq \mathfrak{n}_2 \supseteq \cdots$ with $[\mathfrak{n}_i, \mathfrak{n}_j] \subseteq \mathfrak{n}_{i+j}$. We look at the action of $\mathfrak{n}$ on the universal enveloping algebra $U\mathfrak{n}$, which is faithful by the Poincar-Birkhoff-Witt theorem, but infinite dimensional, and try to find a finite dimensional faithful quotient. If we be $U\mathfrak{n}_i$ be the ideal of $U\mathfrak{n}$ spanned by all products of at least i elements of $\mathfrak{n}$ then $U\mathfrak{n}/U\mathfrak{n}_i$ is a finite dimensional representation, and we want to show it is faithful for i large. Pick a basis $n_1, n_2 \ldots$ for $\mathfrak{n}$ such that $[n_i, n_j]$ is a linear combination of n_k for $k \geq i + j$. Then the subspace spanned by all monomials of total weight greater than $\dim(\mathfrak{n})$ is an ideal containing $\mathfrak{n}_{\dim \mathfrak{n}+1}$ and the quotient by it is a faithful representation of $\mathfrak{n}$. So $U\mathfrak{n}/U\mathfrak{n}_{\dim(\mathfrak{n})+1}$ is a finite dimensional faithful representation of $\mathfrak{n}$.

Now we do the general case. By the Levi decomposition we can split $\mathfrak{g}$ as a semidirect product of a semisimple Lie algebra and its solvable radical, and splitting the solvable radical using Lie's theorem shows that we can split $\mathfrak{g}$ as $\mathfrak{n}.\mathfrak{h}$ where $\mathfrak{n}$ is nilpotent containing the center and $\mathfrak{h}$ is the sum of a semisimple and abelian Lie algebra. We take the induced representation $U\mathfrak{g}\times_{U\mathfrak{h}} k$ of the 1-dimensional trivial representation k of $\mathfrak{h}$. As $U\mathfrak{g} = U\mathfrak{n}\otimes U\mathfrak{h}$ as vector spaces by the Poincar-Birkhoff-Witt theorem, the induced representation can be identified with the universal enveloping algebra $U\mathfrak{n}$ of $\mathfrak{n}$. Moreover all the ideals $U\mathfrak{n}_i$ are preserved by the action of $\mathfrak{h}$. So $U\mathfrak{n}/U\mathfrak{n}_{\dim(\mathfrak{n})+1}$ can be extended to a finite dimensional representation of $\mathfrak{g}$ that is faithful on $\mathfrak{n}$ and therefore faithful on the center the center. So the sum of this representation and the adjoint representation is a faithful finite dimensional representation of $\mathfrak{g}$. □

Corollary 422 *If $\mathfrak{g}$ is a finite-dimensional solvable Lie algebra over a field of characteristic 0, we can grade $\mathfrak{g}$ as $\mathfrak{g} = \oplus_{n\geq 0}\mathfrak{g}_n$ so that $\mathfrak{g}_0$ is abelian and the nilradical is $\oplus_{n>0}\mathfrak{g}_n$.*

Proof By Ado's theorem the Lie algebra has a faithful finite dimensional representation, and looking at the proof we see that we can also find one so that the nilradical acts as nilpotent endomorphisms. We put this representation into upper triangular form using Lie's theorem, and use the height above the main diagonal as the grading. □

Combining the theorems of Ado and Levi gives a picture of an arbitrary finite dimensional Lie algebra in characteristic 0: it is a semidirect product of its nilradical with a reductive Lie algebra acting completely reducibly on it, and the nilradical can be take ans a positively graded Lie algebra. The reductive Lie algebras and their completely reducible representations are well understood in characteristic 0, so the obstruction to understanding all these Lie algebras is that there are rather a lot of nilpotent algebras.

Generalized Fitting subgroups

44 Classification of simple complex Lie algebras

We classify the simple complex Lie algebras by combining the root decomposition of a Cartan subalgebra with the non-degeneracy of the Killing form (which follows from Cartan's criterion) and the representation of SL_2. The first job is to tighten up the root space decomposition $G = \oplus G_\lambda$ for a Cartan subalgebra H, by showing that G_0 is equal to H (and so is abelian), and G_λ is 1-dimensional for $\lambda \neq 0$.

Theorem 423 *Suppose H is a Cartan subalgebra of a semisimple complex Lie algebra G, with root space decomposition $G = \oplus G_\lambda$. Then $G_0 = H$.*

Proof The Killing form is non-degenerate, and since it is invariant we see that (G_λ, G_μ) is zero unless $\lambda+\mu = 0$. So the Killing form must be a non-degenerate pairing between G_λ and $G_{-\lambda}$, and in particular is non-degenerate on G_0.

Since G_0 is nilpotent, and therefore solvable, Lie's theorem shows that for any representation of G_0 we have $\mathrm{Trace}(a, [b, c]) = 0$, so in particular for the Killing form of G we have $(a, [b, c]) = 0$ for all $a, b, c \in G_0$. So $[b, c]$ is in the kernel of the Killing form restricted to G_0, which implies $[b, c] = 0$ as this restriction is non-degenerate. □

45 The Segal-Shale-Weil representation

46 Invariant integration

On any locally compact group, there is a left invariant measure called Haar measure, unique up to multiplication by a constant. For a finite dimensional real vector space this is just Lebesgue measure. Haar measure in general is quite hard to construct, but fortunately for Lie groups there is an easy way to do it. On an n-dimensional oriented manifold, we cannot integrate functions, but we can integrate n-forms. (If the manifold is not oriented, we can integrate sections of the line bundle of n-forms tensored with the line bundle of orientations, but since Lie groups are orientable we do not need to worry about this extra complication.) So to give a left-invariant Haar measure all we have to do is find a left-invariant n-form. But this is easy: just fix any n-form at the identity, and we can then extend it uniquely to all points just by left translating it.

Example 424 If the group G is the non-zero real numbers under multiplication, a left-invariant 1-form is given by dx/x. This is why the Gamma function is shifted by 1: it is given by $\int_0^\infty e^{-t}t^s dt/t$, where we are integrating over the group of positive reals, the expression t^s is a character of this group, and dt/t is the invariant measure.

Example 425 On the group $GL_n(R)$, the invariant measure is given by

$$\prod dx_{ij}/\det(x_{ij})^n$$

. This is because an element of the group multiplies ordinary Lebesgue measure on R^n by the determinant, so multiplies Lebesgue measure $\prod dx_{ij}$ on R^{n^2} by $\det^n$.

We have talked about the measure being left-invariant, so it is natural to wonder if it is also right invariant. There are many cases when it is. First observe that right translation by g multiplies the measure by a constant $\Delta(g)$, and this gives a homomorphism Δ from G to the positive reals.

- For finite groups the measure is counting measure, so is obviously left and right invariant.
- For compact groups the total measure of the group is finite, so must also be invariant under right translation.
- For any simple or perfect group the measure is right invariant, as the only possible homomorphism to the abelian group of positive reals is the identity.
- For any nilpotent group the measure is right invariant.

In spite of all these examples, there are also groups where the Haar measure is not right invariant. To find examples we need to understand the modular function. If we have an element g of a group, we can transfer an n-form at the origin to g using either left translation or right translation, and we want to know if these give the same result. This is so if the adjoint action of g on n-forms at the origin is trivial. So we see that the modular function is just the adjoint action of G on the 1-dimensional vector space given by the highest exterior power of the Lie algebra. For example, nilpotent Lie groups act trivially on the highest exterior power of the Lie algebra, so the modular function is trivial.

Example 426 Suppose G is the 2-dimensional solvable non-abelian Lie group represented by transformations $x \mapsto ax + b$ of the reals. Then $x \mapsto ax$ acts as multiplication by a on the exterior square of the Lie algebra. So the modular function is non-trivial and the left invariant measure is not right invariant.

A Lie group G acts on the homogeneous space G/H for any close subgroup H, and we can also ask if G/H has a G-invariant measure. This depends on the modular functions of G and H. In fact measures correspond to a choice of the highest exterior power of g/h, so for there to be an invariant measure on G/H the action of H on this has to be trivial. In other words the modular function of H has to be the restriction of the modular function of G.

Example 427 Suppose G is the group $x \mapsto ax + b$ acting on the reals. Then there is no invariant measure on the reals, and the modular function of G does not restrict to the modular function of the subgroup $H = R^*$ fixing a point. On the other hand, although there is not invariant measure, there is a measure transforming by a character of G which is almost as good. We see that this happens whenever the modular function of H is the restriction of some character of G (not necessarily the modular character of G).

Example 428 Sometimes we cannot even find a measure transforming like a character of G. For example, take G to be $PSL_2(R)$ acting on the projective line. The subgroup fixing the point ∞ is the group of transformations $x \mapsto ax + b$, and the modular character of this cannot be extended to any character of G as G is simple so has no non-trivial characters. So 1-dimensional projective space does not even have a semi-invariant measure.

Example 429 If G is a compact group acting on a manifold X, we can always find an invariant measure by taking any measure on X and averaging it over G. In fact we can do even better: take any Riemannian metric on X and average it over G to get an invariant Riemannian metric. A rather similar construction gives an invariant positive definite Hermitian form on a representation of G: take any positive definite Hermitian form, and average over G to make it invariant. In particular representations of compact groups G are completely reducible, as we can take the orthogonal complement of a subrepresentation.

Exercise 430 For each of the 3-dimensional Bianchi groups, determine whether or not it has a two-sided invariant measure.

47 Heisenberg groups and algebras

The original Heisenberg algebra come from quantum mechanics as the Lie algebra generated by the position and momentum operators x and d/dx. It has a basis of 3 elements X, Y, Z with $[X, Y] = Z$ and Z in the center. Variations of this algebra are common: they have a center, and the quotient by the center is abelian.

We first look at the analogue for finite groups. These are groups G of prime power order p^n with a center Z of order p such that the quotient G/Z is elementary abelian (all elements of order p) and non-trivial. They are called extra-special groups. We will classify them and find their irreducible representations. First of all, the commutator gives a non-degenerate skew symmetric bilinear form on G/Z taking values in Z, so we can think of G/Z as a vector space with a skew symmetric form, so it breaks up into a direct sum of 2-dimensional spaces. So G is a central product of extraspecial groups of order p^3.

We classify the non-abelian groups of order p^3. When $p = 2$ G must have a cyclic subgroup of order 4 as every group all of whose elements have order 2 is cyclic. So G is generated by elements a, b with $a^4 = 1$, $bab^-1 = a^-1$ as b normalizes (a), and $b^2 = 1$ or a^2. This gives two possibilities: the dihedral group of order 8 or the quaternion group of order 8. When p is odd, one possibility is that there is an element of order p^2. Again we find that it is generated by a and b with $a^{p^2} = 1$, $bab^-1 = a^{p+1}$, b^p is a power of a, but this time we find all such groups are isomorphic (given by a semidirect product of cyclic groups of orders p^2 and p). The other possibility is that all elements have order 1 or p, so if we select two elements not in the center we find that G is generated by a and b with relations $a^p = b^1 = 1$, $aba^{-1}b^-1$ has order p and is in the center. This gives a unique group of order p^3 isomorphic to the upper triangular unipotent matrices of size 3.

Now we can find all extraspecial groups by examining what happens when we take central products. When p is odd, the central product of two groups with elements of order p^2 is isomorphic to the central product of the group with elements of order p^2 and the group with no such elements, so we only get two possibilities for each order p^{1+2n} (which are distinct because one has elements of order p^2 and the other does not). When $p = 2$ things are a little different: this time the central product of two quaternion groups is isomorphic to the central product of two dihedral groups. So again there are at most two possibilities for each order 2^{1+2n}. To see that the two possibilities we get are distinct, we notice that the map $G/Z \mapsto Z$ taking g to g^2 is a quadratic form. Quadratic forms over the field with two elements have an invariant called the Arf invariant, which is given by whichever of the numbers 0 or 1 the form takes most often. So again we get exactly two extraspecial groups of order p^{1+2n}.

Now we find the irreducible representations of G of order p^{1+2n}. The abelianization of G has order p^{2n} so there are p^{2n} irreducible representations of dimension 1. The number of conjugacy classes of G is $p + (p^{1+2n} - p)/p = p^{2n} + p - 1$ so there are exactly $p - 1$ more irreducible representations, or degree dividing the order of G, and the sum of their squares is $p^{1+2n} - p^{2n}$. The only possibility is that there are $p - 1$ further irreducible representations all of degree p^n. They can be distinguished by the action of the center, which can act by one of its $p - 1$ nontrivial characters. So we see that the representation theory can be summarized as follows: for each non-trivial character of the center, there is a unique irreducible representation of the extraspecial group.

Now we study the Heisenberg algebra (over the reals). Recall that there are two groups associated with it, one simply connected (upper triangular unipotent matrices) and one not simply connected. By Lie's theorem, or by observing that

Trace($[X,Y]$) = 0 the only irreducible finite dimensional representations are 1-dimensional so we should look at infinite dimensional representations.

Exercise 431 Show that in characteristic p the Heisenberg algebra has an irreducible representation of dimension p.

We can try to find representations of the Heisenberg algebra by bounded operators on a Hilbert space, but this also fails. So interesting representations necessarily involve unbounded operators, such as x and d/dx. We can get a representation of the corresponding group as the group of transformations of $L^2(R)$ generated by translations, multiplication by e^{ixy}. The Stone-von Neumann theorem says that this representation is essentially unique. In other words, just as for the finite case, we get a unique irreducible representation for non-trivial irreducible representations of the center of the group.

Free field theories in quantum mechanics.

Example 432 The Heisenberg algebra has an action on Young diagrams, or more precisely on the vector space V with basis consisting of Young diagrams as follows. We define two operators D and U on V as follows. The operator U takes a Young diagram to the sum of all Young diagrams that can be obtained by adding a single box. Similarly the operator D takes a Young diagram to the sum of all Young diagrams that can be obtained by removing a single box. Then these operators satisfy the relation

$$DU - UD = 1$$

so give an action of the Heisenberg algebra (with the center acting as 1). This relation follows from two properties of Young diagrams:

1. Given two different Young diagrams X and Y, the number of diagrams that can be obtained by adding a single box to either X or Y is the same as the number that can be obtained by subtracting a single box from X or Y. (This number is always 0 or 1).

2. Given a Young diagram, the number of diagrams that can be obtained by adding a single box to X is 1 more than the number that can be obtained by subtracting a single box from X.

(Young diagrams form a poset called the Young lattice, and a poset with similar properties is called a differential poset.)

Exercise 433 Show that $U^n(\emptyset) = \sum_{|\lambda|=n} f_\lambda \lambda$ where f_λ is the number of standard tableaux of shape λ.

Exercise 434 Show that $\sum_{|\lambda|=n} f_\lambda^2 \emptyset = D^n U^n \emptyset$ and use this to show that $\sum_{|\lambda|=n} f_\lambda^2 = n!$.

The numbers f_λ are the dimensions of the irreducible representations of the symmetric group S_n, so the result in this exercise also follows from the fact that the sum of the dimensions of the irreducible representations of a finite group is the order of the group.

48 Kazhdan-Lusztig polynomials

We construct the Kazhdan-Lusztig polynomials of a Coxeter group. These are rather mysterious polynomials that control the infinite dimensional representation theory of simple Lie algebras: for example, the Kazhdan-Lusztig conjectures (proved by Beilinson and Bernstein and by Brylinski and Kashiwara) express the characters of irreducible quotients of some Verma modules in terms of the values of Kazhdan-Lusztig polynomials at $q = 1$.

Kazhdan-Lusztig polynomials $P_{v,w}(q)$ are polynomials depending on a pair of elements v, w of a Coxeter group W.

The Hecke algebra H of a Coxeter group W is an algebra over $Z[q^{1/2}, q^{-1/2}]$. It is generated by the elements T_s for s a simple reflection, subject to the relations

- $(T_s + 1)(T_s - q) = 0$
- $T_sT_tT_s \cdots = T_tT_sT_t \cdots$ whenever $sts \cdots = tst \cdots$ is one of the relations of the Coxeter (or braid) group.

For any $w \in W$ we define T_w to be $T_{s_1}T_{s_2} \cdots$ whenever $w = s_1s_2 \cdots$ is a reduced expression for w. This is well defined because any two reduced words for w can be connected by a series of relations of the form $sts \cdots = tst \cdots$. The Hecke algebra is a free module over $\mathbb{Z}[q^{1/2}, q^{-1/2}]$ with a basis consisting of the elements T_w. In particular the Hecke algebra is a deformation of the group algebra of W, in the sense that it becomes the group algebra if $q = 1$.

Motivation for the Hecke algebras: the Hecke algebra (at least when W is a Weyl group) is the algebra of double cosets BwB for a finite Chevalley group, with q the order of the finite field. This double coset algebra acts on the induced representation given by inducing 1 from B to G, so representations of the Hecke algebra describe the decomposition of this induced representation. The name Hecke algebra comes from Hecke operators in the theory of modular forms, which also form a basis of an algebra of double cosets. Sometimes Hecke algebra is used as a generic terms for an algebra of double cosets.

We write $(-1)^\ell$ for the linear map on H taking T_w to $(-1)^{\ell(w)}T_w$.

The Hecke algebra has an order 2 antiautomorphism $(-1)^\ell R$ (meaning it reverses multiplication: $(-1)^e llR(ab) = (-1)^\ell R(B)(-1)^\ell R(a))$ with $R(q^{1/2}) = q^{1/2}$, $R(T_s) = qT_s^{-1}$ for simple reflections s. So on the basis elements T_w, R acts as $R(T_w) = q^{\ell(w)}T_{w^{-1}}^{-1}$.

Definition 435 *The R-polynomials $R_{v,w}$ are defined to be the matrix coefficients of R in the basis T_w: more precisely*

$$R(T_w) = \sum_v R_{v,w}T_v.$$

Exercise 436 Show that $R_{v,w}$ vanishes unless $v \leq w$, in which case it has degree $\ell(w) - \ell(v)$ and leading coefficient 1.

Show that

$$R_{x,y}(q^{-1}) = (-q)^{\ell(x)-\ell(y)}R_{x,y}(q)$$

.

Show that

- $R_{x,y} = R_{sx,sy}$ if $sx < x$ and $sy < y$.
- $R_{x,y} = (q-1)R_{sx,y} + qR_{sx,sy}$ if $sx > x$ and $sy < y$.

These relations can be used to compute the polynomials $R_{x,y}$ recursively.

The ring $\mathbb{Z}[q^{1/2}, q^{-1/2}]$ has an order 2 automorphism $*$ taking $q^{1/2}$ to $q^{-1/2}$, and this lifts to a ring homomorphism $(-1)^\ell *$ of H taking the generator T_s to $-q^{-1}T_s$. It takes the basis element T_w to $(-q)^{-\ell(w)}T_w$. The antilinear map $*$ fixes the elements $q^{\ell(w)/2}T_w$, which form an alternative basis for the Hecke algebra, which is more convenient when considering duality properties. Some authors write T_w for $q^{-\ell(w)/2}T_w$, in which case one of the relations for the Hecke algebra is changed to $(T_s + q^{-1/2})(T_s - q^{-1/2}) = 0$.

The two functions $*$ and R commute and their composition $*R = R*$ is an antilinear antiautomorphism taking the generator T_s to $T_s^{-1} = q^{-1}T_s + q^{-1} - 1$ and taking $q^{1/2}$ to $q^{-1/2}$, so it takes the basis element T_w to $T_{w^{-1}}^{-1}$.

We order the basis elements $q^{-\ell(w)/2}T_w$ by the Bruhat ordering. In this basis the linear transformation R is an upper triangular matrix with diagonal entries 1.

Lemma 437 *(Birkhoff factorization) If R is an invertible upper triangular matrix over a ring of Laurent polynomials, there are unique matrices P, Q such that $R = QP^{-1}$, Q has polynomial coefficients, and P is the identity matrix modulo terms of negative degree.*

Proof This follows because we can calculate the entries of P and Q recursively, in order of their distance from the diagonal, in much the same way that we can find the inverse of R. At each step the entries of P and Q are given uniquely by splitting some Laurent polynomial into the sum of a polynomial and something all of whose terms have negative degree. □

Lemma 438 *If the matrix R of the previous lemma satisfies $(*R)^2 = 1$, where $*$ takes q to q^{-1}, then $*RP = P*$, or in other words $*R$ and $*$ are conjugate by P: $*R = P * P^{-1}$.*

Proof By definition of P we know that $RP = *Q*$ for some matrix Q with constant term the identity. We have to show that $P = Q$. Using the facts that $(*R)^2 = 1$ and $*^2 = 1$ we see that $*RP = Q*$ and $*RQ = P*$, so $*RS = -S*$ where $S = P - Q$ has polynomial coefficients. But this last equation implies $S = 0$, because we can solve recursively for the entries s of S in order, and find at each step that $*s = -s$ if all previous entries are 0, which implies $s = 0$ as s the terms of s all have degree ≥ 0 and there is no 2-torsion. So $S = 0$, which implies $P = Q$, so $*RP = P*$. □

Definition 439 *The Kazhdan-Lusztig polynomials $P_{v,w}$ are the matrix entries of P, where $R = QP^{-1}$ is the Birkhoff decomposition with respect to the $*$-invariant basis with elements $q^{-\ell(w)/2}T_w$; in other words*

$$P(T_w) = \sum_v P_{v,w}(q)T_v$$

Lemma 440 *The elements $C\prime_w = Pq^{-\ell(w)/2}T_w$ and $C_w = *Pq^{-\ell(w)/2}T_w$ are fixed by $*R$.*

Proof This follows because $*RP = P*$ and the basis elements $q^{-\ell(w)/2}T_w$ are fixed by $*$. $\square$

Exercise 441 Show that:

- $P_{v,w}$ vanishes unless $v \leq w$, and is 1 if $v = w$, and is a polynomial in q of degree less than $(\ell(w) - \ell(v))/2$ if $v < w$.
- For $v \leq w$ the Kazhdan-Lusztig polynomial $P_{v,w}$ is 1 if $\ell(w) - \ell(v) \leq 2$ or if the Coxeter group has rank at most 2.
- $P_{b,bacb}(q) = 1 + q$ where a, b, c are the usual transpositions generating the symmetric group S_4 (with a and c commuting).

Beyond these simple cases, the Kazhdan-Lusztig polynomials are rather hard to compute by hand, and can get very complicated: for example, Polo showed that any polynomial with constant term 1 and non-negative integer coefficients is a Kazhdan-Lusztig polynomial for some symmetric group.

Exercise 442 Classify vector bundles over P^1. (Birkhoff-Grothendieck theorem) Over A^1 all vector bundles are free (coordinate ring is a PID). So cover P^1 by 2 copies of A^1 on each of which vector bundle is free of rank n. Transition functions are given by an $n \times n$ matrix with coordinates in $k[x, x^{-1}]$. We can multiply on left by an invertible matrix in $k[x]$ and on right by invertible matrix in $k[x^{-1}]$. Using these operations we can make transition matrix M diagonal with entries powers of x as follows. Use operations to make 1 column zero except for one element, necessarily of the form x^r, and choose r as large as possible, and take this element to be in top left corner. (To show that such a maximal r exists, observe that it is bounded above by integers t such that for some nonzero vector v with coefficients in $k[x^{-1}]$, Mv has all coefficients divisible by x^t, and this t is invariant under the matrix operations on the left and right, and is bounded by the highest power of x appearing in M.) Then by induction we can make matrix diagonal except for top row. Then using maximality of r we can clear top row, using column operations to clear out powers of x that are at most r, and row operations to clear out powers that are at least s where x^s is the diagonal power in this column. So if there are any entries left in the top row we must have $r < s$ contradicting maximality of s. So vector bundle splits as the sum of one dimensional bundles of the form $\mathcal{O}(m)$. Number of copies of $\mathcal{O}(k)$ is uniquely determined by looking at dimension of space of sections of bundle twisted by line bundles.

Example 443 Example: If the matrix M is $\begin{pmatrix} 1 & x \\ & x^2 \end{pmatrix}$ then it cannot be turned into the diagonal matrix $\begin{pmatrix} 1 & \\ & x^2 \end{pmatrix}$; instead it gets transformed into $\begin{pmatrix} x & \\ & x \end{pmatrix}$. This shows we need to take r maximal in the above argument.

49 Tits systems and the Bruhat decomposition

Definition 444 *A Tits system consists of the following:*

- *A group G, generated by two subgroups B and N, such that $H = B \cap N$ is a normal subgroup of N.*
- *A set S of involutions generating the (Weyl) group $W = N/H$.*
- *If $s \in S$ and $w \in W$ then $sBw \subseteq BwB \cup BswB$.*
- *If $s \in S$ then $sBs \not\subseteq B$.*

Exercise 445 If $G = GL_n(\mathbb{C})$, N is the subgroup of n by n matrices with exactly one non-zero entry in each row and column, and B the subgroup of invertible upper triangular matrices, and S the involutions obtained from the identity matrix by switching two adjacent rows, show that this is a Tits system.

Example 446 We show that the Lie groups $PSL_n(\mathbb{R})$ and $PSL_n(\mathbb{C})$ are simple for $n \geq 2$. In fact it requires little extra effort to determine which of the groups $PSL_n(F)$ are simple for any field F, so wee will do this. By ?? we just have to check when this group is perfect. Since this group is generated by elements $t_{ij}(\lambda)$ (1s on the diagonal, and a λ in position i, j) we try to write these as commutators. If n is at least 3 we can always do this; for example

$$\begin{pmatrix}1 & \lambda & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & \mu\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & \lambda & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & \mu\\ 0 & 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & 0 & \lambda\mu\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}^{-1}$$

Example 447 For 2 by 2 matrices the commutator of $\left(\begin{smallmatrix}\lambda & 0\\ 0 & \lambda^{-1}\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & \mu\\ 0 & 1\end{smallmatrix}\right)$ is $\left(\begin{smallmatrix}1 & (\lambda^2-1)\mu\\ 0 & 1\end{smallmatrix}\right)$, so we are OK as long as we can find a nonzero element λ of the field with $\lambda^2 \neq 1$. This is possible as long as the field has at least 3 elements, so $PSL_n(F)$ is simple for $n \geq 2$ and any field F, except possibly for the two cases $n = 2$ and $F = \mathbb{F}_2$ or $\mathbb{F}_3$.

We look at these two cases in more detail to see that they are not simple. The group $PSL_2(\mathbb{F}_2)$ has order 6 and is just the symmetric group acting on the 3 points of the projective line over $\mathbb{F}_2$, so in particular is solvable. The group $GL_2(\mathbb{F}_3)$ has order 48. The quotient $PGL_2(\mathbb{F}_3)$ has order 24 and acts faithfully the on projective line over $\mathbb{F}_4$ so must be the group S_4 of all permutations of these 4 points. So $GL_2(\mathbb{F}_3)$ has a chain of normal subgroups, with successive quotients $\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^2$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ and in particular it is solvable. The groups $SL_2(\mathbb{F}_3)$ and $GL_2(\mathbb{F}_3)$ are two of the exceptional finite subgroups of the unit quaternions. (The third is $SL_2(\mathbb{F}_5)$.) One way to see this is to observe that these groups contain a quaternion subgroup containing the center of the group, so the action of this quaternion group by right translations on the group algebra gives a quaternion structure to all representations where the center acts as -1.

50 Casimir elements and the center of the universal enveloping algebra

51 Capelli's identity

52 Verma modules

53 The Weyl integration formula

Suppose that G is a compact connected Lie group with maximal torus T. We would like to integrate functions f over T when looking at orthogonality relations of characters, but this is hard to do directly as G can have quite complicated topology. However every element of G is conjugate to an element of T, so any class function is determined by its restriction to T, and therefore we should be able to work out its integral over all of G using a suitable integral over T, which is much easier as T has the much easier structure $\mathbb{R}^n/\mathbb{Z}^n$. The problem is that we cannot integrate f over T directly, because we need to account for the fact that some elements of T are conjugate to more elements of G than others. For example, if we pretend G is finite, then

$$\sum_{g\in G} f(g) = \sum_{t\in T} f(t) \times \frac{\text{number of elements of } G \text{ conjugate to } g}{\text{number of elements of } T \text{ conjugate to } g}$$

where the weight on the right is a function on T invariant under the normalizer of T. Weyl's integration formula identifies this weight function explicitly, and states

$$\int_{g\in G} f(g) = \int_{t\in T} f(t) \times \prod_\alpha (1-e^\alpha)$$

The square root of this fudge factor is the denominator of the Weyl character formula, because

$$\prod_\alpha (1-e^\alpha) = \prod_{\alpha>0}(1-e^\alpha)e^{-\alpha/2} = e^{-\rho}\prod_{\alpha>0}(1-e^\alpha)$$

where we use the fact that if α is a root then so is $-\alpha$, and where ρ is half the sum of the positive roots. **Proof** (of the Weyl integration formula). Suppose that t is in the maximal torus T. Consider the map from $G/T \times T \mapsto G$ taking $(x,t) \mapsto xtx^{-1}$. The fudge factor at t is given by the determinant of the corresponding map of tangent spaces, since the determinant measures how much the measure is increased.

(Add more)

So the fudge factor is given by $\det(1-t)$ acting on $\mathfrak{g}/\mathfrak{h}$. Since $\mathfrak{g}/\mathfrak{h}$ is a sum of the 1-dimensional weight spaces, the determinant is simply the product of the eigenvalues of $1-t$ on these weight spaces, which is $\prod_\alpha(1-t^\alpha)$. □

Example 448 The Weyl integration formula for integral of a class function f over the unitary group is

$$\frac{1}{(2\pi)^n n!}\int f(\theta_1,\ldots,\theta_N)\prod_{j<k}|e^{i\theta_j}-e^{i\theta_k}|d\theta_1\cdots d\theta_N$$

The Weyl character formula follows from the Weyl integration formula as follows. The characters of highest weight representations are characterized by these properties:

1. They are invariant under the Weyl group

2. They are of the form $e^\alpha +$ terms with lower weights

3. They are orthogonal

The characters of the Weyl character formula obviously satisfy the first two conditions, so the key point is to check the third condition. This follows from the Weyl integration formula because the product of the denominators of two characters cancels out with the fudge factor in the Weyl integration formula:

54 Borel-Weil-Bott theorem

The Borel-Weil-Bott theorem gives a natural geometric realization of all the irreducible finite dimensional representations of a complex semisimple Lie group.

If G is a semisimple complex algebraic group, then the space of polynomial functions on G, as a representation of $G\times G$, breaks up as the sum $R\otimes R$ over the irreducible representations R of G. This is analogous to the decomposition of functions on a finite group G as a representation of $G\times G$. If R is an irreducible representation and U the unipotent subgroup of a Borel subgroup B, then the vectors of R fixed by U are just the highest weight vectors of R, and therefore form a 1-dimensional subspace. So if ω is a 1-dimensional representation of B, corresponding to a representation ω of the torus T, then the subspace of vectors of R transforming like ω under B is either 0 or 1-dimensional, depending on whether R has highest weight ω. So the polynomials on G transforming on the right under B according to ω are either 0 or form a copy of the highest weight representation of G (acting on the left) with highest weight ω. This is the Borel-Weil construction of the irreducible representations of G.

The Borel-Weil construction is usually stated in terms of global sections of line bundles over a projective manifold, so we describe this correspondence. The space G/B is a projective variety. A 1-dimensional representation of B gives a line bundle L on this projective variety. The global sections $H^0(V,L)$ of this line bundle are essentially the same as functions on G transforming on the right according to ω.

In the case when the group G is $GL_n(\mathbb{C})$, the group B is the group of upper triangular matrices, and V is the flag variety of all maximal flags in $\mathbb{C}^n$.

There is an extension of the Borel-Weil theorem due to Bott, where instead of looking at $H^0(V,L)$ one looks at the representation $H^i(V,L)$ for more general i. Bott showed that there is at most one i for which this space is non-zero, and in this case the representation is irreducible.

When G is $SL_2(\mathbb{C})$, the space V is just 1-dimensional projective space. In this case $H^i(V,O(n))$ is the $n+1$-dimensional irreducible representation of $SL_2(\mathbb{C})$ if $i=0$ and $n\geq 0$, and the $-n-1$-dimensional irreducible representation of $SL_2(\mathbb{C})$ if $i=1$ and $n\leq -2$, and 0 otherwise. In particular if $n=-1$ then both cohomology groups vanish.

Bott's theorem is one of the simplest examples of cohomological induction, a powerful way of constructing representations of groups. Roughly speaking, 0-dimensional cohomological induction is a sort of variation of ordinary induction.

Add something on $H^i(\mathfrak{n}, V)$ as an algebraic version of Borel-Weil-Bott.

55 Peter-Weyl theorem

The Peter-Weyl theorem says that irreducible unitary representations of compact groups behave much like irreducible representations of finite groups, except the there may be an infinite number of them. In particular they are all finite dimensional, and the space $L^2(G)$ breaks up into an orthogonal sum $R \otimes R^*$, generalizing the fact that if G is finite then its group ring $\mathbb{C}[G]$ is a sum of matrix algebras corresponding to the irreducible representations of G.

When G is finite, the representation $L^2(G)$ is finite-dimensional, and we can construct the irreducible representations of G by breaking up $L^2(G)$ into irreducibles. The main extra problem that appears when G is compact but infinite is that one has to show that $L^2(G)$ still breaks up into finite-dimensional representations. Once one has done this, the arguments for finite groups mostly generalize easily to all compact groups. In particular one can show that for any compact group there are enough finite dimensional irreducible unitary representations, in the sense that for every nontrivial element of G there is a finite dimensional unitary representation on which it acts nontrivially. (There are compact groups for which this is not immediately obvious: for example, if one defines the spin group to be the double cover of the special orthogonal group, it is not completely trivial to construct a representation where the center acts nontrivially.)

Theorem 449 *(Peter-Weyl). Suppose that G is a compact group. Then $L^2(G)$ splits up as an orthogonal direct sum finite dimensional representations of G.*

Proof

We have a left action of G on $L^2(G)$. We would like to break this up into finite dimensional representations. A good way to break up a representation of G is to find operators commuting with G; then eigenstates of these operators are acted on by G. If these operators are compact then things are even better because the eigenspaces of non-zero eigenvalues are finite dimensional. There are lots of obvious operators commuting with G, consisting of right translations. These are not compact operators in general. However we can make them compact by smoothing them: in other words instead of using right translation by an element of G, we use right convolution by some continuous function on G. These operators are compact as they are just integral operators on a compact space with continuous kernel (this is the main point where we use the fact that G is compact). If we want we can arrange for these operators to be self adjoint by taking a function invariant under inverses.

So for every continuous function on G we can break $L^2(G)$ up into a sum of finite dimensional irreducible representations, and a possibly infinite dimensional zero eigenspace. We need to check that there is nothing nasty hiding in these zero eigenspaces. So suppose f is orthogonal to all finite dimensional irreducible representations in $L^2(G)$. Then $f * \phi = 0$ for any continuous function

ϕ, and we want to show that this forces f to be 0. But if we take a sequence (or net) of functions ϕ_n approaching the "delta" measure at 0, then $f * \phi_n$ approaches f, so if all the $f * \phi_n$ are 0 then f is 0. □

Corollary 450 *Every irreducible unitary representation of a compact group G is finite-dimensional.*

Proof Any unitary representation of any group can be represented as continuous functions on G. As G is compact, continuous functions are in L^2, so all irreducible unitary representations occur in $L^2(G)$. As $L^2(G)$ splits up as a sum of finite-dimensional representations, all irreducible unitary representations must be finite-dimensional. □

In particular, since irreducible unitary representations are finite dimensional, we can define their characters as the traces of elements of G. These are continuous functions on G satisfying orthogonality relations similar to those of finite groups, except of course one replaces sums over the group by integration.

Just as for finite groups, the space $L^2(G)$ splits up as a sum $R \otimes R^*$ of irreducible representations of $G \times G$, where the sum is over the irreducible unitary representations of G.

Example 451 If G is the circle group of complex numbers of absolute value 1, then $L^2(G)$ splits up as the sum of the 1-dimensional spaces spanned by z^n for integers n. The decomposition of an element of $L^2(G)$ as a linear combination of these functions is just the Fourier series of a periodic function.

Example 452 Suppose that G is the group $S^3 \subset \mathbb{R}^4$ of unit quaternions. Then (complex) polynomials of degree n on G form a space of dimension $4 \times 5 \times \cdots \times (n+3)/n! - 4 \times 5 \times \cdots \times (n+1)/(n-1)! = (n+1)^2$. These form the space $R \otimes R$, where R is the $(n+1)$-dimensional irreducible representation of G.

Exercise 453 Show that the representation $R \otimes R$ of $S^3 \subset \mathbb{R}^4$ can be identified with the space of harmonic polynomials on $\mathbb{R}^4$ of some fixed degree.

The Peter-Weyl theorem and its corollaries fail when the group G is not compact. Even the trivial representation is not usually a subrepresentation of $L^2(G)$ as the function 1 is not in L^2. For abelian locally compact groups, the space $L^2(G)$ is still an integral rather than a sum of irreducible representations, but for non-abelian groups things are much more complicated. For example, for $G = SL_2(\mathbb{R})$, the space $L^2(G)$ splits up as a sum of some irreducible representations (the discrete series), an integral of others (the continuous series), and there are some irreducible representations that do not appear in $L^2(G)$ at all (the trivial representation, limits of discrete series, and the complementary series). For semisimple G, the decomposition of $L^2(G)$ into a direct sum and integral of irreducibles was worked out by Harish-Chandra. Even stranger things can happen for groups that are not semisimple. For example, for the infinite symmetric group $G = S_\infty$(the union of S_n over all n), the space $L^2(G)$ cannot be split up into irreducible representations at all. (This gives an example of a von Neumann algebra of type II_1, an essentially infinite-dimensional object that has no analogue for finite-dimensional representations.)

56 Formal groups and Hopf algebras

Just how complicated can the 1-dimensional abelian Lie group get?

57 Lazard's universal ring

Commutative formal group laws are represented by the following universal ring: Take the ring generated by elements $c_{i,j}$ with the relations that if $f(x, y) = \sum c_{i,j}x^i y^j$ then f is a commutative formal group law. These relations are some (rather gruesome) polynomial relations between the coefficients, so define a ring L generated by these coefficients subject to these relations. It is obvious that formal group laws over a commutative ring R are the same as homomorphisms from L to R. The ring L is called Lazard's universal ring. Lazard discovered the amazing fact that in spite of its formidable definition it has a simple structure: it is just a polynomial ring on infinitely many generators of degrees $2, 4, 6, \ldots$. We can grade the ring by letting x and y have degree $= 2$, so that $c_{i,j}$ has degree $2(i + j - 1)$. This grading corresponds to the following action of the multiplicative group: if f is a formal group, so is $\lambda^{-1}f(\lambda x, \lambda y)$. The strange factor of 2 in the grading is put in because of Quillen's theorem that Lazard's ring is the coefficient ring of complex cobordism.

To prove Lazard's theorem we need some preliminary results about binomial coefficients.

Lemma 454

$$\binom{a}{b} \equiv \prod \binom{a_i}{b_i} \bmod p$$

where the product is over the digits of the base p expansions of a and b. In particular $\binom{a}{b}$ is divisible by p if and only if some digit of b is bigger than the corresponding digit of a. Or to put it another way, $\binom{a+b}{a}$ is nonzero mod p exactly when the sum $a + b$ can be computed without carrying.

Proof We want to count the number of b element subsets of a elements mod p. Divide up the a elements into a_0 blocks of size 1, a_1 of size p, and so on, and consider the action of a cyclic p-group acting transitively on each block. This acts on the subsets of size b and all non-trivial orbits on the set of subsets have size a power of p, so $\binom{a}{b}$ is congruent to the number of subsets fixed by this action, in other words subsets that contain an entire block if they contain one element of it. But the number of ways of choosing such a subset is $\prod a_i b_i$. □

Corollary 455 *The highest common factor of the numbers $\binom{a}{b}$ for $0 < b < a$ is p if $a = p^n, n > 1$ is a prime power and 1 otherwise.*

Proof By the previous lemma we see that the highest common factor is divisible by p if and only if $a > 1$ is a power of p. To complete the proof we just have to check that the highest common factor is never divisible by p^2, which follows because $\binom{p^n}{p^{n-1}}$ is not divisible by p^2. □

Exercise 456 Write out the first 10 or so rows of Pascal's triangle modulo 2 and 3, and color in the entries that are 0 to see the "fractal" patterns they form.

The following technical lemma is the key point of the proof of Lazard's theorem.

Lemma 457 *Suppose that $\Gamma(x,y)$ is a homogeneous polynomial in 2 variables of degree n with coefficients in some abelian group A. If the coefficients of x^n and y^n vanish, and $\Gamma(x,y) = \Gamma(y,x)$, and Γ satisfies the 2-cocycle condition*

$$\Gamma(x,y) + \Gamma(x+y,z) = \Gamma(x,y+z) + \Gamma(y,z)$$

then Γ is equal to

$$a((x+y)^n - x^n - y^n)$$

for some $a \in A$ unless n is a power of a prime p, in which case Γ is

$$a\frac{(x+y)^n - x^n - y^n}{p}.$$

Proof It is enough to prove this when A is finitely generated (by the coefficients of Γ). Also if it is true for two abelian groups B and C then it is true for an extension $B.C$ because we can first solve for Γ in C, and subtract a lift of this solution to get a similar problem with coefficients in B, which we can also solve by assumption. So we can assume that A is either the integers Z or Z/p for some prime p because every finitely generated abelian group can be obtained from these by taking extensions.

Write

$$\Gamma(x,y) = \sum_{i+j=n} a_{i,j} x^i y^j$$

Then

$$a_{0,n} = a_{n,0} = 0 \quad (28)$$

$$a_{i,j} = a_{j,i} \quad (29)$$

$$\binom{i+j}{i} a_{i+j,k} = \binom{j+k}{k} a_{i,j+k} \text{ whenever } i \text{ and } k \text{ are nonzero} \quad (30)$$

Also the expressions given in the lemma are all solutions of these equations.

We first do the case when A is the integers. If A is the rational numbers the result is clear, because the binomial coefficients in the identity above are all nonzero, so the space of solutions is at most 1-dimensional, and as we have found one solution all the others must be multiples of it. So when A is the integers all solutions must be some rational multiple of the solution given above, but as the highest common factor of the coefficients of this solution is 1 any integral solution must be an integral multiple of it. This proves the lemma when $A$is the integers.

Next we do the case when A is cyclic of prime order, in which case we can assume that A is the field of order p. As before the solutions form a vector space and we are given one non-zero solution, so it is enough to show that the space of solutions is at most 1-dimensional. This is somewhat trickier than the rational case because some of the binomial coefficients can vanish mod p. The coefficient $a_{i,n-i}$ is determined by $a_{j,n-j}$ for j the largest power of p that is at most i, because the addition $(i-j)+j$ involves no carrying. In particular the coefficients are determined by those of the form $a_{p^i,n-p^i}$. Next we observe that $a_{p^i,n-p^i} = a_{n-p^i,p^i}$ is determined by $a_{p^{i+1},n-p^{i+1}}$ if $p^{i+1} < n$, unless $p^{i+1} + p^i > n$. However in the latter case $a_{p^{i+1},n-p^{i+1}}$ is determined by $a_{p^i,n-p^i}$. So in either case we find a coefficient such that all other coefficients are determined by it. In other words the space of solutions is 1-dimensional.

□

Theorem 458 *(Lazard's theorem) The Lazard ring is a polynomial ring on generators of degrees* $2, 4, 6, \ldots$

Proof We will first bound the size of the Lazard ring from above, which is the tricky part, and then bound it from below, which is easy.

To bound the size of the ring from above, we suppose we have a formal group f over some ring, and ask how much freedom we have to change the part of f of degree n. Since we are just trying to get an upper bound on this freedom, let's throw away everything of degree greater than n, so our new formal group will be $f(x,y) + \Gamma(x,y)$ where Γ is a homogeneous polynomial of degree n, and everything of higher degree is quotiented out. Then Γ satisfies the following three conditions:

1. $\Gamma(1,0) = \Gamma(0,1) = 0$ because $(f + \Gamma)(x,y) = x + y \mod xy$
2. $\Gamma(x,y) = \Gamma(y,x)$ because a group law is commutative
3. $\Gamma(x,y) + \Gamma(x+y,z) = \Gamma(x,y+z) + \Gamma(y,z)$ because $f + \Gamma$ is associative.

By the previous lemma *Gamma* is determined by the choice of a single element of R. In other words the Lazard ring has a set of generators with exactly one generator in each positive even degree.

We now have to bound the Lazard ring from below, by showing that these generators are algebraically independent It is enough to do this over the rationals, as any nontrivial relation between the generators over the integers gives a nontrivial relation over the rationals. But over the rational numbers this is easy because we can write down a lot of explicit formal groups: take any power series $l(x) = x + c_1x^2 + c_2x^3 + \ldots$, and form the formal group $l^{-1}(l(x) + l(y))$. (Here l^{-1} is the function with $l^{-1}(l(x)) = x$, not $1/l(x)$.) In each degree we have complete freedom to choose c_i, and in fact over the rational the c_i can be taken as the generators of the Lazard ring. So there are no relations between the generators of the Lazard ring, and it is a polynomial ring in infinitely many generators. (Note that this argument does not work over the integers: the problem is that the formal group might have integer coefficients even if its logarithm l does not: consider $l(x) = x + x^2/2 + x^3/3 + \cdots$.)

□

So in principle we can write down any one dimensional commutative formal group over a ring just by writing down a sequence of elements of R, given as the images of the generators of the Lazard ring. In practice there is a problem: we have not actually written down a universal formal group over the Lazard ring, and this is not so easy to do. (It is easy to do this over the rationals using the logarithm of the formal group; the problem is to do it over the integers.)

58 Affine Lie algebras

59 Jacobi triple product identity