A guide to field theory

For the last part of the course we will be studying fields and some classical applications of field theory, such as to prove that that it is not possible to trisect an arbitrary angle with straightedge and compass, and that there is no formula for the roots of a polynomial of degree five or more, analogous to the familiar formula for the roots of a quadratic polynomial.

Most of the theory that we will need is covered in Goodman's text, although I will add a few things, mainly about finite fields (see the separate set of notes on this subject) and the impossibility of angle trisection. Goodman treats the subject more comprehensively than we will have need or time for. In these notes, I will outline the parts of the subject that I would like you to learn, and where to find them in Goodman.

Here and there I will also mention simplifications or alternative approaches to what you will find in the text.

1. Vector spaces

All the familiar operations of vector and matrix algebra, such as solving a system of linear equations $A\,\mathbf{x} = \mathbf{0}$ by row-reducing the matrix A, work for matrices and vectors with entries in any *field* K.

We do require that K be a field, and not just a commutative ring with identity, because it is essential to be able to divide by non-zero scalars. For example, just to solve a single linear equation $a\,x = b$ in one variable x, you need to be able to divide by a.

For a review of vector and matrix algebra you might want to read Goodman Appendix E.1-2.

The definition of an abstract *vector space* V over any field K and some fundamental examples are given in Goodman 3.3.1-3 and 3.3.6-7.

The definition and properties of a *basis* of V, and the *dimension* $\dim(V)$ if V is finite-dimensional, are in Goodman 3.3.15-28.

You will notice that Goodman proves Proposition 3.3.25 using the fact that if C is a matrix with more columns than rows, then the vector equation $C\,\mathbf{a} = \mathbf{0}$ has non-zero solutions $\mathbf{a}$. This should be familiar to you in the case when K is the field of real numbers, but it is equally valid for other fields.

One important point which Goodman skips over is that a subset S of V is a basis if and only if every element of V can be expressed *uniquely* as a linear combination of elements of S. Exercise: prove this.

The above is all that we will need from linear algebra.

2. Field extensions

Carefully read all of Goodman 7.3 for the definition and basic properties of field extensions $K \subseteq L$. We will be studying the theory of *finite* extensions, which are always algebraic.

The dimension $\dim_K(L)$ and the formula $\dim_K(M) = \dim_K(L)\dim_L(M)$ for $K \subseteq L \subseteq M$ (Goodman 7.3.1) will be important for us.

The *minimal polynomial* $f(x) \in K[x]$ of an element $\alpha \in L$, and the description of the subfield $K(\alpha) \subseteq L$, isomorphic to $K[x]/(f(x))$, will also be especially important (Goodman 7.3.5-8).

3. Solution of the cubic, and splitting fields of polynomials in $\mathbb{C}$

In 7.2, Goodman explains how to solve a cubic equation, after reducing it to the special form $x^3 + px + q = 0$.

In 7.4, he works out the description of field extensions $K \subseteq L$, where K is a subfield of $\mathbb{C}$ containing the coefficients of a cubic $f(x) = x^3 + px + q = 0$, and $L = K(\alpha_1, \alpha_2, \alpha_3)$ is the extension of K generated by the three complex roots α_i of $f(x)$, called the *splitting field* of $f(x)$ over K.

In 7.5, he outlines the general picture for the splitting field in $\mathbb{C}$ of a polynomial $f(x)$ with coefficients in a subfield K of $\mathbb{C}$.

In class I will go over the example of the cubic equation, as discussed in Goodman 7.2 and 7.4, along with other examples, to motivate and illustrate the theory we will be developing.

You should read 7.2 and 7.4 in full.

You can skip all proofs and many of the intermediate results in 7.5. It will be enough to understand the statements of Theorem 7.5.1, 7.5.7-9, and 7.5.11, and how they apply in examples 7.5.12-14 and any others we might discuss in class.

4. Impossibility of angle trisection

This topic is not in Goodman, so I will explain it briefly here (and in class). We will only need the material in Goodman 7.3 for this.

We define a real number to be *constructible* if it is the x or y coordinate of a point in the plane constructible by straightedge and compass, starting with nothing but two marked points: one at the origin $(0, 0)$ and one on the x axis at $(1, 0)$, which serve to establish a unit of length.

For example, since we can construct a unit square, and mark off a segment on the x-axis congruent to its diagonal, the number $\sqrt{2}$ is constructible.

There are only three ways to construct new points: intersect two lines, a line and a circle, or two circles. The only lines we can construct are those passing through two constructible points, and the only circles are those centered on a constructible point and having constructible radius. You can verify, by working out the equations for the intersection points of two lines, or a line and a circle, or two circles, that every new number produced by these constructions is a solution of a quadratic equation whose coefficients are previously constructed real numbers.

This shows that every constructible real number is contained in a finite iterated quadratic extension of $\mathbb{Q}$, that is, a subfield $K \subseteq \mathbb{R}$ such that there is a tower of intermediate fields

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = K$$

in which each K_{i+1} has the form $K_i(\alpha_i)$, where α_i is a root of a quadratic equation with coefficients in K_i. Then $\dim_{K_i}(K_{i+1}) = 2$ for all i, so $\dim_{\mathbb{Q}}(K) = 2^m$. If β is a constructible real number, then $\mathbb{Q}(\beta)$ is a subfield of a field K as above. Hence $\dim_{\mathbb{Q}}(\mathbb{Q}(\beta))$, which is the degree of the minimal polynomial of β over $\mathbb{Q}$, divides 2^m, and so is itself a power of 2.

(It can be shown, conversely, that all elements of any iterated quadratic extension of $\mathbb{Q}$ in $\mathbb{R}$ are constructible. For this one has to exhibit geometric constructions for the arithmetic operations and square roots. We won't need this.)

Since we can construct an equilateral triangle, we can construct two lines meeting at at angle of $2\pi/3 = 120°$. If there were a construction to trisect an angle, we could then use it to construct an angle of $2\pi/9$, which would imply that the real number $2\cos 2\pi/9$ is constructible.

To prove that angle trisection is impossible, it will therefore suffice to show that the minimial polynomial of $2\cos 2\pi/9$ over $\mathbb{Q}$ has degree 3.

To this end, let $\omega = e^{2\pi i/9}$, so that $2\cos 2\pi/9 = \omega + \omega^{-1}$. Since $\omega^9 = 1$, we see that ω is a root of $x^9 - 1 = 0$. The latter polynomial factors as

$$x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1).$$

Since $\omega^3 \neq 1$, ω must be a root of the second factor, so it satisfies $\omega^6 + \omega^3 + 1 = 0$. Dividing by ω^3, we get

$$\omega^3 + \omega^{-3} + 1 = 0,$$

or

$$(\omega + \omega^{-1})^3 - 3(\omega + \omega^{-1}) + 1 = 0.$$

This shows that $2\cos 2\pi/9 = \omega + \omega^{-1}$ is a root of the polynomial $x^3 - 3x + 1$. To complete our argument we need only show that this last polynomial is irreducible in $\mathbb{Q}[x]$. Since it is a cubic polynomial, it suffices to show that it has no rational root. By the rational root test, the only possible rational roots are ± 1. But neither of these is a root, so $x^3 - 3x + 1$ is irreducible.

Exercise: Show that $x^3 - 3x + 1$ has three real roots, equal to $2\cos 2\pi/9$, $2\cos 4\pi/9$ and $2\cos 8\pi/9$.

5. Splitting fields, automorphisms, and Galois theory

In Goodman Chapter 7 we encountered the notion of the splitting field in $\mathbb{C}$ of a polynomial $f(x)$ with coefficients in a subfield K of $\mathbb{C}$. These concepts apply in a more general setting.

Given any field K and a polynomial $f(x) \in K[x]$, we can prove that there is an algebraic extension $K \subseteq L$ such that $f(x)$ factors into linear factors in $L[x]$—that is, L contains a complete set of roots of $f(x)$—and the roots of f in L generate L as extension of K. This extension L is called the *splitting field* of $f(x)$ over K.

Sections 9.1-5 of Goodman discuss the theory of splitting fields and their automorphism groups, leading to the *fundamental theorem of Galois theory* (Goodman 9.5.4).

We will need much but not all of the material in these sections.

In 9.1, we only need Proposition 9.1.1.

Section 9.2 discusses the existence of splitting fields and how to construct them, their uniqueness up to isomorphism, and the construction of specific isomorphisms and automorphisms in appropriate circumstances. Everything in 9.2 is important for us.

Section 9.3 discusses criteria for a polynomial to have multiple roots. You may already know that a polynomial $f(x)$ with real coefficients has distinct roots (including complex roots) if and only if $f(x)$ and its derivative $f'(x)$ are relatively prime.

In Goodman Exercises 9.3.1-5 you will work out the corresponding criterion for polynomials over any field. (The phrase "if $Df(x)$ is not identically zero, then" in 9.3.5 could be omitted, since if $Df(x) = 0$, then the gcd of $f(x)$ and $Df(x)$ is $f(x)$.)

The rest of 9.3 discusses some applications of the criterion in Exercise 9.3.5. The main point is that if K has characteristic zero, or if K is finite, then an irreducible polynomial over K always has distinct roots in any extension of K. This includes most fields K that will be of interest to us.

Section 9.4 discusses the automorphism group $\mathrm{Aut}_K(L)$ of a splitting field $K \subseteq L$. We will need everything in this section except maybe Corollaries 9.4.18-19.

There is a mistake in Goodman's proof of Proposition 9.4.1: it should refer to Proposition 9.2.4 instead of Corollary 9.2.5. Or, better, study the proof of Proposition 9.4.2 first, and then notice that Proposition 9.4.1 is the special case of 9.4.2 when $M = K(\alpha)$ and $M' = K(\beta)$.

The most subtle, but also the most fundamental, result in 9.4 is Theorem 9.4.13. Here is a slightly different proof which you might find simpler and more conceptual.

The first part is the same as in Goodman: we list the roots $\beta_1, \ldots, \beta_r$ of $f(x)$ in L and consider the tower of subfields

$$K = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_r = L$$

in which $M_i = M_{i-1}(\beta_i)$. We will prove that if β is a root of $f(x)$ in L, then for any subfields $K \subseteq M \subseteq M(\beta) \subseteq L$, every element of $M(\beta)$ fixed by $\mathrm{Aut}_K(L)$ belongs to M. It follows that if $\mathrm{Fix}(\mathrm{Aut}_K(L)) \subseteq M_{i+1}$, then $\mathrm{Fix}(\mathrm{Aut}_K(L)) \subseteq M_i$. Since we obviously have $\mathrm{Fix}(\mathrm{Aut}_K(L)) \subseteq M_r$, we can use this repeatedly to conclude that $\mathrm{Fix}(\mathrm{Aut}_K(L)) \subseteq M_0$. In other words, $\mathrm{Fix}(\mathrm{Aut}_K(L)) = K$, which is what we wanted to prove.

The second part is to prove that every element of $M(\beta)$ fixed by $\mathrm{Aut}_K(L)$ belongs to M. I will do this a bit differently than Goodman does. Since $\mathrm{Aut}_M(L) \subseteq \mathrm{Aut}_K(L)$, it is enough to prove that every element of $M(\beta)$ fixed by $\mathrm{Aut}_M(L)$ belongs to M. In other words, the problem really only concerns the extension $M \subseteq M(\beta) \subseteq L$ and the group $\mathrm{Aut}_M(L)$.

Let $N = M(\beta) \cap \mathrm{Fix}(\mathrm{Aut}_M(L))$. We have $M \subseteq N \subseteq M(\beta)$ and want to show that $M = N$.

Let $p(x)$ be the minimal polynomial of β over M, and $q(x)$ its minimal polynomial over N. Since β is a root of $f(x)$, $p(x)$ is an irreducible factor of $f(x)$ in $M[x]$, so $p(x)$ is separable. Let $l = \deg(p(x)) = \dim_M(M(\beta))$. Since L is the splitting field of $f(x)$ over M as well as over K, $p(x)$ has l distinct roots $\alpha_1, \ldots, \alpha_l$ in L, one of which is β. By 9.4.4 (b) (applied to $M \subseteq L$ rather than to $K \subseteq L$), $\mathrm{Aut}_M(L)$ acts transitively on the α_i. Since $q(x)$ has coefficients fixed by $\mathrm{Aut}_M(L)$ and β is a root of $q(x)$, every α_i is a root of $q(x)$. Hence the degree of $q(x)$, which is equal to $\dim_N(M(\beta))$, is at least l. In other words, $\dim_N(M(\beta)) \geq \dim_M(M(\beta))$. But since $\dim_M(M(\beta)) = \dim_M(N)\ \dim_N(M(\beta))$, this implies that $\dim_M(N) = 1$, that is, $M = N$.

In 9.5, we only need 9.5.1-4. Proposition 9.5.1 is known as the *Primitive Element Theorem*. It is used here to prove Proposition 9.5.3, which in turn is used, together with results from Section 9.4, to prove Theorem 9.5.4.

The main results in Galois theory are Theorem 9.4.15, Corollary 9.4.16, Proposition 9.4.17, and Theorem 9.5.4.

6. Unsolvability of the quintic equation

I am more interested in having you appreciate this topic as a demonstration of the power of Galois theory than in your following every technical detail. For this reason, I will first give you an outline of the general ideas before pointing you to the specifics in Goodman.

It will be helpful to begin by thinking about the familiar formula

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

for the roots of a quadratic equation

$$a\,x^2 + b\,x + c = 0.$$

One way to view the symbols a, b and c here is that they stand for complex numbers, which we specify each time we want to use the formula. To address the question of whether such formulas exist for higher degree polynomials, however, it is more useful to take a different point of view, and regard the symblols a, b, c as abstract indeterminates, like the symbol x in a polynomial $p(x)$.

In other words, we consider the field of rational functions $K = \mathbb{C}(a, b, c)$, the fraction field of the polynomial ring $\mathbb{C}[a, b, c]$ in three variables. Then $f(x) = ax^2 + bx + c$ is a polynomial over K, that is, an element of $K[x]$. The expression $\Delta = b^2 - 4ac$ is an element of K, but it is not the square of an element of K. Thus $p(z) = z^2 - \Delta$ has no root in K, and is therefore irreducible (since it has degree 2). We can introduce a square root of Δ by forming the extension $E = K[z]/(p(z)) = K(\sqrt{\Delta})$. The formula

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{-b \pm \sqrt{\Delta}}{2a}$$

now stands for either of two elements (depending on the $\pm$ sign) $\alpha_1, \alpha_2 \in E$, which are, of course, the roots of $f(x)$ in E.

Thus $E = K(\sqrt{\Delta})$ is the splitting field of the *generic quadratic polynomial* $f(x) = ax^2 + bx + c$ over $K = \mathbb{C}(a, b, c)$. Splitting fields always exist, but in this case, the quadratic formula allowed us to construct it in a special way: namely, by adjoining a square root of the element $\Delta \in K$.

We can interpret Cardano's formulas for the roots of a cubic equation, worked out in Goodman 7.2, in a similar manner. We might take the generic cubic to be $ax^3 + bx^2 + cx + d$, but for the problem of finding the roots we can always simplify first, as in Goodman 7.2, to the form

$$f(x) = x^3 + p\,x + q.$$

We now regard this as a polynomial over the field of rational functions $K = \mathbb{C}(p, q)$. Note that this is quite different from the point of view taken in Goodman 7.4, where p and q were complex numbers and K was a subfield of $\mathbb{C}$ containing them. Now $\mathbb{C}$ is a subfield of K instead!

In Cardano's formulas, we first introduce the square root

$$\sqrt{\Delta}, \quad \text{where} \quad \Delta = \frac{q^2}{4} + \frac{p^3}{27}.$$

Then we introduce a cube root

$$A = \sqrt[3]{B}, \quad \text{where} \quad B = -\frac{q}{2} + \sqrt{\Delta}.$$

After this, the roots of $f(x)$ are given, as in Goodman 7.2, by

$$\alpha_1 = A - \frac{p}{3A}, \quad \alpha_2 = \omega A - \frac{p}{3\,\omega A}, \quad \alpha_3 = \omega^2 A - \frac{p}{3\,\omega^2 A},$$

where $\omega = e^{2\pi i/3}$ (note that our field K contains the complex number ω to begin with).

In other words, the field $E = K(\sqrt{\Delta})(\sqrt[3]{B})$ is the splitting field of the generic cubic $f(x) = x^3 + px + q$ over $K = \mathbb{C}(p, q)$. Again, the splitting field always exists, but Cardano's formulas have allowed us to construct it by adjoining first a square root and then a cube root to K.

A formula for the roots of a polynomial equation involving only arithmetic operations, radicals (meaning n-th roots), and perhaps some specific complex numbers such as the ω in Cardano's formulas is called a *solution of the equation by radicals*. Besides the familiar formula for the quadratic equation and Cardano's formulas for the cubic equation, there is also a known solution of the general fourth degree equation by radicals.

We shall use Galois theory to prove that there is, however, no solution by radicals of the general quintic (degree 5) equation

$$x^5 + a\,x^4 + b\,x^3 + c\,x^2 + d\,x + e = 0$$

(which we have taken to be monic for simplicity and without loss of generality). In the process we will also see the natural explanation for the fact that 5 is the smallest degree in which no solution by radicals exists.

From our discussion so far we already know how to begin. Take $K = \mathbb{C}(a, b, c, d, e)$, let $f(x) \in K[x]$ be the generic quintic

$$f(x) = x^5 + a\,x^4 + b\,x^3 + c\,x^2 + d\,x + e,$$

and let E be the splitting field of $f(x)$ over K. If the quintic were solvable by radicals, it would mean that E, or maybe some larger extension $K \subseteq E \subseteq L$, can be constructed from K in stages, where at each stage we adjoin an n-th root of some element. In other words, we would have a tower of extensions

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r = L, \tag{1}$$

with $K_{i+1} = K_i(\sqrt[n_i]{\alpha_i})$ for some $\alpha_i \in K_i$ and positive integer n_i, for each i. We have only required $E \subseteq L$, rather than $E = L$, to allow for the possibility that there might be a solution by radicals which gives some extraneous solutions in addition to the roots of $f(x)$. Our conclusions will imply that not even this is possible.

The steps to complete the proof are as follows. By definition, E is the splitting field of a polynomial $f(x)$ over K. Since our fields have characteristic zero, $f(x)$ is separable, so $K \subseteq E$ is a Galois extension.

The first thing to prove is that the Galois group $\mathrm{Aut}_K(E)$ is the full permutation group S_5 acting on the five roots of $f(x)$ in E. More generally, the Galois group of any generic polynomial of degree n is the full permutation group S_n of its n roots in a splitting field.

Goodman proves this in 9.6 and 9.7 (Theorem 9.7.1), but there is an easier way, which I will explain briefly. The idea is to prove by induction that $\dim_K(E) = n!$. Then, since $|\,\mathrm{Aut}_K(E)| = \dim_K(E)$ and $\mathrm{Aut}_K(E)$ is a subgroup of S_n, it will follow that $\mathrm{Aut}_K(E) = S_n$.

The degree n generic polynomial

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

is irreducible in $\mathbb{C}[a_0, \ldots, a_{n-1}, x]$ since it is linear in a_0. By Gauss's Lemma, it follows that $f(x)$ is irreducible over $K = \mathbb{C}(a_0, \ldots, a_{n-1})$. Adjoining a root α of $f(x)$ to K therefore gives an extension $K \subseteq K(\alpha)$ with $\dim_K(K(\alpha)) = n$. The polynomial $f(x)$ factors over $K(\alpha)$ as $f(x) = (x-\alpha)g(x)$, for a polynomial $g(x) = x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$ with coefficients $b_i \in K(\alpha)$. Our splitting field E is also the splitting field of $g(x)$ over $K(\alpha)$. If we verify that $g(x)$ is again a generic polynomial, then we will have $\dim_{K(\alpha)}(E) = (n-1)!$ by induction, and therefore $\dim_K(E) = \dim_K(K(\alpha)) \dim_{K(\alpha)}(E) = n \cdot (n-1)! = n!$.

To prove that $g(x)$ is generic we need to show that $K(\alpha)$ is isomorphic to a field of rational functions $\mathbb{C}(b_0, \ldots, b_{n-1}, \alpha)$. We can construct this isomorphism by working out formulas for the b_i in terms of the a_i and vice versa, as I will do in class.

Next we observe that if M contains $\mathbb{C}$, and $\sqrt[n]{\alpha}$ is an n-th root of some $\alpha \in M$, then all the n-th roots of α are $\sqrt[n]{\alpha}, \omega\sqrt[n]{\alpha}, \ldots, \omega^{n-1}\sqrt[n]{\alpha}$, where $\omega = e^{2\pi i/n}$. The extension $M \subseteq M(\sqrt[n]{\alpha})$ is therefore the splitting field of $x^n - \alpha$ over M, so it is Galois. If $g_k \in \mathrm{Aut}_M(M(\sqrt[n]{\alpha}))$ sends $\sqrt[n]{\alpha}$ to $\omega^k\sqrt[n]{\alpha}$, then $g_k(\omega^j\sqrt[n]{\alpha}) = \omega^{j+k}\sqrt[n]{\alpha}$. This gives $g_k g_j = g_{j+k}$ and shows that the Galois group $\mathrm{Aut}_M(M(\sqrt[n]{\alpha}))$ is abelian.

A more general discussion of radical extensions $M \subseteq M(\sqrt[n]{\alpha})$ can be found in Goodman 10.4-5, but we will not need it. The simpler observations in the paragraph above will do.

The remaining steps are the same as in Goodman 10.1-3 and 10.6.

The extension $K \subseteq L$ is not necessarily Galois, but we can always find a larger extension $K \subseteq L \subseteq L'$ which is Galois, and is still given by a tower of radical extensions as in (1). This is Goodman, Lemma 10.6.3. The basic idea is that every time we want to construct an extension $M(\sqrt[n]{\alpha})$, we should not just adjoin an n-th root of α, but of *every* root of the minimal polynomial $p(x)$ of α over K, which gives the splitting field of the polynomial $p(x^n) \in K[x]$ over M. The resulting extension will then be Galois over K if M was.

Replacing L with L', we can now assume that L is Galois over K. Using the fundamental theorem of Galois theory and the tower of intermediate fields (1), we conclude as in Goodman 10.6.4 that the Galois group $G = \mathrm{Aut}_K(L)$ contains a tower of subgroups

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_r = G$$

with each G_i normal in G_{i+1} and G_{i+1}/G_i abelian for each i. Such a group G is said to be *solvable* (Goodman, Definition 10.1.4). Our original splitting field E of $f(x)$ is an intermediate extension $K \subseteq E \subseteq L$, Galois over K. This implies that its Galois group $\mathrm{Aut}_K(E)$ is a quotient group G/N of G.

In class we will prove Goodman, Exercise 10.2.6: every quotient of a solvable group is solvable. We conclude that *if $f(x)$ is solvable by radicals, then the Galois group* $\mathrm{Aut}_K(E)$ *of its splitting field must be a solvable group.* This is the origin of the term "solvable" for groups.

To complete the proof that the general quintic is not solvable by radicals, it only remains to show that *the symmetric group S_5 is not solvable.* This follows because (i) the only normal subgroups of S_5 are $\{e\}$, A_5 and S_5, and (ii) A_5 is non-abelian and *simple* (has no proper non-trivial normal subgroup). This is Goodman, 10.3.2, 10.3.4, and Exercise 10.3.6.

A final remark: S_2, S_3 and S_4 are solvable (A_4 is non-abelian, but not simple because it has a normal subgroup with four elements). This explains why there are formulas for the solution by radicals of general polynomial equations of degrees 2, 3 and 4, but not 5.