Group Theory (Math 113), Summer 2016

James McIvor and George Melvin
University of California, Berkeley
(Updated July 16, 2016)

Abstract

These are notes for the first half of the upper division course 'Abstract Algebra' (Math 113) taught at the University of California, Berkeley, during the summer session 2016. Students are assumed to have attended a first course in linear algebra (equivalent to UCB Math 54). The aim of these notes is to provide an introduction to group theory with a particular emphasis on finite groups: topics to be covered include basic definitions and concepts, Lagrange's Theorem, Sylow's Theorems and the structure theorem of finitely generated abelian groups, and there will be a strong focus on group actions and realising groups through symmetry. The notes are a slightly modified version of those used in summer 2014.

Contents

1 Lecture 1 - Examples

Further Reading: Goodman 1.1-1.3, Appendices A,B,D

Groups should be understood as symmetries of a certain object. We begin by ignoring definitions and jargon, etc., and building some intuition for what symmetries are and how we can work with them and write down statements about them. It will be a rather "hands-on" class, and as such there are not many notes online here.

1. Symmetries of a square
2. The famous "mattress group"
3. Symmetries of a tetrahedron - on HW.

Please refer to the separate notes entitled "preliminary materials" and/or the appendices in Goodman's book, for a review of basic concepts about sets and functions.

2 Lecture 2 - Basic arithmetic properties of $\mathbb{Z}$. Equivalence relations.

Previous lecture - Next lecture

Keywords: Fundamental Theorem of Arithmetic, division algorithm, gcd**, Euclid algorithm. Equivalence relation, equivalence class, class representative, natural mapping.**

Further Reading: Goodman 1.6, 2.6

In this lecture we will collect some basic arithmetic properties of the integers that will be used repeatedly throughout the course - they will appear frequently in both Group Theory and Ring Theory - and introduce the notion of an equivalence relation on a set.

2.1 Arithmetic properties of $\mathbb{Z}$

The set of integers

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, ...\},$$

is a fundamental object in both group theory and ring theory. Many of its abstract algebraic properties were explained to us as children. Here we record some of the basic (algebraic) facts about this set:

Theorem 2.1.1 (Fundamental Theorem of Arithmetic)**.** *Let $n \in \mathbb{Z}_{>0}$. Then, there exist primes $p_1, \dots, p_r$ and integers $n_1, \dots, n_r \geq 1$ such that $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$. Moreover, if we order $p_1 < p_2 < \dots < p_r$, then the above product is unique.*[1]

Theorem 2.1.2 (Division algorithm in $\mathbb{Z}$)**.** *Let $x, a \in \mathbb{Z}$, $a \neq 0$. Then, there exists $b, r \in \mathbb{Z}$, with $0 \leq r < a$, such that $x = ba + r$.*

Definition 2.1.3. Let $a, b \in \mathbb{Z}$. Then, the **greatest common divisor of** a, b, denoted $\gcd(a, b)$, is the largest (positive) integer c such that c divides a and c divides b. If $\gcd(a, b) = 1$ then we say that a, b are **coprime**.

Theorem 2.1.4 (Euclid's algorithm)**.** *Let $a, b \in \mathbb{Z}$. Then, there exist $u, v \in \mathbb{Z}$ such that*

$$\gcd(a, b) = ua + bv.$$

2.2 Equivalence relations

Let A be an arbitrary nonempty set. There are many ways that we can *partition* a set into collections of similar objects - in this context, the term '*partition*' means that A is 'broken up' into disjoint nonempty subsets.

For example,

- if A is the set of people in this classroom then we could partition A by hair colour or height or country of birth.
- if $A = \mathbb{Z}$ then we can partition A into three subsets A_0, A_1, A_2, where A_i consists of all those integers that have remainder i when divided by 3.

In mathematics we embody this process - of breaking up a set into disjoint nonempty subsets - using equivalence relations.

Definition 2.2.1 (Equivalence Relation)**.** Let A be a (nonempty) set. We say that $R \subset A \times A = \{(a, b) \mid a, b \in A\}$ is an **equivalence relation on** A if the following properties hold:

(ER1) R contains the diagonal subset $\Delta_A = \{(a, a) \mid a \in A\}$; **(reflexive)**

(ER2) if $(a, b) \in R$ then $(b, a) \in R$; **(symmetric)**

[1] Recall that a prime number is an integer p, $p > 1$, such that the only divisors of p are 1 and p.

(ER3) if $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$. **(transitive)**

This definition seems to be quite different from our notions of similarity that we introduced above. For example, why should we care about a subset of the product $A \times A$? Let's see how the definition of an equivalence relation just given does actually embody 'similarity': first, let us write

$$a \sim_R b \quad \Leftrightarrow \quad (a,b) \in R,$$

and say

$$a \sim_R b \quad \Leftrightarrow \quad a \text{ is equivalent to } b.$$

Note that the order in which we write $a \sim_R b$ (and say 'a is equivalent to b') must respect the order of the ordered pair (a,b).

Thus, we can reformulate **ER1**, **ER2**, **ER3** in the following way:

(ER1)' if $a \in A$ then $a \sim_R a$ - 'every $a \in A$ is equivalent to itself';

(ER2)' if $a \sim b$ then $b \sim_R a$ - 'if a is equivalent to b then b is equivalent to a';

(ER3)' if $a \sim_R b$ and $b \sim_R c$ then $a \sim_R c$ - 'if a is equivalent to b and b is equivalent to c then a is equivalent to c'.

It should now feel more plausible that an equivalence relation is capturing the notion of similarity of objects. For example, check (by saying aloud) that if we let A be the set of people in this classroom and

$$R = \{(a,b) \in A \times A \mid \ a \text{ and } b \text{ have the same hair colour}\} \subset A \times A,$$

then R satisfies ER1, ER2, ER3 and so defines an equivalence relation on A.

How does this all relate to partitioning a set A into disjoint nonempty subsets?

Definition 2.2.2 (Equivalence Class)**.** Let A be a (nonempty) set, $R \subset A \times A$ an equivalence relation on A. For $a \in A$ we define the **equivalence class of** a **(with respect to** R**)** to be the subset of A

$$[a] \overset{def}{=} \{b \in A \mid a \sim_R b\} \subset A.$$

So, the equivalence class of a (with respect to R) is the set of all elements in A that are equivalent to a.

We will also refer to $[a]$ as an **equivalence class (of** R**)** (without reference to a) when the context is clear.

If $b \in [a]$ then we say that b is a **(class) representative of** $[a]$. We denote the **set of all equivalence classes of** R by A/R or $A/\sim_R$, or even $A/\sim$ when the equivalence relation R is understood. We will often write the set of all equivalence classes making use of some (nice) choice of class representatives (see Example 2.2.6).

We define the **natural mapping associated to** R **(or** $\sim_R$**, or** $\sim$**)** to be

$$\pi : A \rightarrow A/\sim \ ; \ a \mapsto [a],$$

the function that sends an element of A to its equivalence class.

The main reason we are interested in equivalence classes is that they are precisely the subsets that describe a partition of a set. This will be made precise and proved in the following results.

First, consider the example discussed above: A is the set of people in this classroom and

$$R = \{(a,b) \mid a \text{ and } b \text{ have the same hair colour}\}.$$

Then, we can consider an equivalence class for this equivalence relation as the set of all people in this classroom with the same hair colour. In particular, we can label equivalence classes by a single person in an equivalence class or by the hair colour of that student - thus, we have

$$A/R \longleftrightarrow \{\text{brown, black,...}\}$$

Lemma 2.2.3. *Let A be a nonempty set, $R \subset A \times A$ an equivalence relation on A. Let $a, b \in A$ be such that $b \in [a]$ (so that b is a representative of $[a]$). Then, $[a] = [b]$.*

Proof: Homework/worksheet problem. □

Lemma 2.2.3 states that

$$\boxed{\textbf{if } a \sim b \textbf{ then the equivalence class of } a \textbf{ is equal to the equivalence class of } b.}$$

Theorem 2.2.4. *Let A be a (nonempty) set, $R \subset A \times A$ an equivalence relation on A. Then, A is a disjoint union of the equivalence classes of R*

$$A = \bigsqcup_{X \in A/R} X.$$

Remark 2.2.5. To say that A is a disjoint union of equivalence classes of R means the following: A is a union of equivalence classes and, if $X, X' \in A/R$ are distinct equivalence classes then $X \cap X' = \varnothing$.

Proof: We must prove two statements:

- *A is a union of equivalence classes*: recall that an equivalence class $X \in A/R$ is of the form $X = [a]$, for some $a \in A$. Let $a \in A$. Then, $a \in [a]$, by ER1, so that an arbitrary $a \in A$ is a member of some equivalence class. Hence,

$$A = \bigcup_{a \in A} [a].$$

- *if $X, X' \in A/R$ are distinct equivalence classes then $X \cap X' = \varnothing$*: let $X = [a], X' = [b]$, for some $a, b \in A$. Since $X \neq X'$ then a is not equivalent to b by Lemma 2.2.3. Suppose, for a contradiction, that $X \cap X' \neq \varnothing$. Thus, there is some $c \in X \cap X'$ so that $c \in [a]$ and $c \in [b]$. Hence, $a \sim_R c$ and $b \sim_R c$. By ER2 we know that $c \sim_R b$ which implies, by ER3, that $a \sim_R b$. Hence, by Lemma 2.2.3, $X = [a] = [b] = X'$, which is absurd. Thus, the assumption that $X \cap X' \neq \varnothing$ must be false so that $X \cap X' = \varnothing$.

□

Example 2.2.6. 1. Let $A = \mathbb{Z}$ and fix $n \in \mathbb{Z}$, $n \neq 0$. Consider the following equivalence relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid n \text{ divides } (a - b)\}.$$

That is,

$$a \sim b \quad \Leftrightarrow \quad n \text{ divides } (a - b).$$

Then, the following are examples of equivalence classes

$$[0] = \{\dots, -2n, -n, 0, n, 2n, 3n, \dots\}$$

$$[1] = \{\dots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, 3n + 1, \dots, \}$$

If $n \neq 1$ then $[0] \neq [1]$.[2] The set of equivalence classes correspond to the possible remainders when dividing by n:

$$A/R \longleftrightarrow \{0, 1, \dots, n - 1\}.$$

How do we know that this gives all of the equivalence classes? Suppose that $X \in A/R$ is an equivalence class. Thus, there is some $x \in \mathbb{Z}$ such that $[x] = X$. By Lemma 2.2.3 we have (check!)

$$\dots = [x - 2n] = [x - n] = [x] = [x + n] = \dots$$

[2] What if $n = 1$?

Now, using the division algorithm for $\mathbb{Z}$ (Theorem 2.1.2) we know that there exists $q, r \in \mathbb{Z}$ with $0 \leq r < n$ such that $x = nq + r$. Hence, we have $[x] = [r]$.

This example will appear again and again throughout this course so that we will write

$$\mathbb{Z}/n\mathbb{Z} \overset{def}{=} A/R = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\},$$

for this particular equivalence relation on $\mathbb{Z}$, where $\overline{i}$ denotes the equivalence class of i. We say 'zee mod n zee'.

2. Let $A = \mathbb{Q}$ and consider the equivalence relation

$$R = \{(a, b) \in \mathbb{Q} \times \mathbb{Q} \mid a - b \in \mathbb{Z}\}.$$

Then, some equivalence classes of this equivalence relation on $\mathbb{Q}$ are

$$[0] = \mathbb{Z}, \quad \left[\frac{1}{2}\right] = \left\{\dots, -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \dots\right\}.$$

We have that

$$A/R \longleftrightarrow \{p \in \mathbb{Q} \mid 0 \leq p < 1\}.$$

3. We can extend the above example to define an equivalence relation on $A = \mathbb{R}$,

$$R = \{(a, b) \in \mathbb{R} \times \mathbb{R} \mid a - b \in \mathbb{Z}\}.$$

The set of equivalence classes corresponds the half-open interval $[0, 1)$

$$A/R \longleftrightarrow \{x \in \mathbb{R} \mid 0 \leq x < 1\}.$$

The set of equivalence classes for this particular equivalence relation on $\mathbb{R}$ is usually denoted

$$\mathbb{R}/\mathbb{Z} \overset{def}{=} A/R.$$

4. Let $A = \mathbb{C}^n$, the complex vector space. Define an equivalence relation on A by declaring

$$u \sim v \;\Leftrightarrow\; \text{there exists invertible } n \times n \text{ matrix } P \text{ with entries in } \mathbb{C} \text{ such that } Pu = v.$$

There are exactly two equivalence classes:

$$[0] = \{0\}, \quad X = \{v \in \mathbb{C}^n \mid v \neq 0\}.$$

Indeed, if $v \neq 0$ then we can extend v to a basis $(v, v_2, \dots, v_n)$ of $\mathbb{C}^n$. The matrix $Q = [v \ v_2 \ \cdots \ v_n]$ is invertible (as the columns are linearly independent) and $Qe_1 = v$, where e_1 is the first standard basis vector. Let $P = Q^{-1}$. Then, we have $Pv = PQe_1 = e_1$, so that $v \sim e_1$. Since v is arbitrary we have just shown that $v \sim e_1$, for any $v \in \mathbb{C}^n$, $v \neq 0$.

5. Fix $n \in \mathbb{Z}_{>0}$. Let $M_n(\mathbb{C})$ be the set of $n \times n$ matrices with complex entries. Consider the following equivalence relation

$$R = \{(A, B) \in M_n(\mathbb{C}) \times M_n(\mathbb{C}) \mid A = P^{-1}BP \text{ for some invertible } P \in M_n(\mathbb{C})\}.$$

For $n = 2$, we have the following examples of some equivalence classes

$$[0] = \{0\}, \quad [\mathbb{I}_n] = \{\mathbb{I}_n\},$$

$$\left[\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right] = \{A \in M_2(\mathbb{C}) \mid A^2 = 0, \ A \neq 0\}.$$

The description of the equivalence class of $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ is a consequence of finding the Jordan form of a linear map.[3] In fact, determining the Jordan form of a matrix is precisely the same problem as determining the equivalence classes of the above equivalence relation on $M_n(\mathbb{C})$.

[3] This is usually covered in Math 110, the upper division course in linear algebra at Berkeley.

3 Lecture 3 - Definitions: group, subgroups, order.

Previous lecture - Next lecture

Keywords: Group, subgroup, order of group, order of element.

Further Reading: Goodman 2.1, 2.2, 2.3, 1.5, 1.7

In today's lecture we will introduce the basic algebraic objects that we are going to be investigating for the next few weeks - groups and their subgroups.

3.1 Groups - basic definitions

> **'Group theory is the study of symmetries.'[1]**

A group is an example of a **set with structure** - we will see more examples of objects of this type when study rings. You have already seen an example of a 'set with structure' when you studied vector spaces in Math 54. A group is simultaneously mathematically simpler and (much!) harder to understand than a vector space. A group encapsulates algebraically the notion of a symmetry of an object, where we consider a symmetry of the object to be an operation that leaves the object (essentially) 'unchanged'.

Definition 3.1.1 (Definition of a group)**.** Let G be a set. We say that G is a **group with law of composition** $*$ if the following axioms hold:

(G1) the assignment

$$(g, h) \mapsto g * h \in G, \qquad \textbf{(closure of } * \textbf{)}$$

defines a function $G \times G \to G$. We call $g * h$ the **product of** g **and** h;

(G2) there exists $e_G \in G$ such that for every $g \in G$ we have

$$g * e_G = g = e_G * g. \qquad \textbf{(existence of identity)}$$

We call e_G an **identity of** G.

(G3) for every $g \in G$ there exists some $h \in G$ such that

$$h * g = e_G = g * h. \qquad \textbf{(existence of inverse)}$$

We call such an h an **inverse of** g.

(G4) for any $g, h, k \in G$ we have

$$(g * h) * k = g * (h * k). \qquad \textbf{(associativity)}$$

We will often denote a group $(G, *)$ to emphasise the law of composition $*$, or simply G when $*$ is understood.

A group is called

- **commutative** or **abelian** if for every $g, h \in G$ we have $g * h = h * g$;
- **finite** if G is a finite set. We will also say that G has **finite order**, or, if $|G| = n$, that G **has order** n;
- **infinite** if G is an infinite set. We will also say that G has **infinite order**.

The axioms G1-4 have some immediate consequences:

Lemma 3.1.2. *Let* $(G, *)$ *be a group.*

a) Suppose that e_G and f_G satisfy G2 in Definition 3.1.1. Then, $e_G = f_G$, so that **the identity element of G is unique**.

b) Let $g \in G$ and suppose that $h, h' \in G$ both satisfy G3 in Definition 3.1.1. Then, $h = h'$, so that **an inverse of g is unique**.

Proof:

a) Suppose that e_G and f_G both satisfy G2. Then, we have

$$e_G \overset{G2}{=} e_G * f_G \overset{G2}{=} f_G,$$

where the first equality comes from G2 applied to f_G, and the second equality comes from G2 applied to e_G.

b) let $g \in G$ and suppose that h, h' both satisfy G3. Then,

$$h \overset{G2}{=} e_G * h \overset{G3}{=} (h' * g) * h \overset{G4}{=} h' * (g * h) \overset{G3}{=} h' * e_G \overset{G2}{=} h'.$$

□

Remark 3.1.3. 1. Axiom G2 in Definition 3.1.1 ensures that the set G appearing in a group $(G, *)$ must be nonempty.

2. As a consequence of Lemma 3.1.2 we are allowed to say the identity element of G - which we will denote e_G, or simply e if the group G is understood - and, for any $g \in G$, the inverse of g - which we will denote g^{-1}. An element $g \in G$ with $g \neq e_G$ will be called **nontrivial**, and we will sometimes refer to e_G as the **trivial element** (of G).

3. Axiom G1 is simply stating that to any pair of elements $g, h \in G$ there is a unique element $g * h \in G$. Note that it is not a consequence of the Axioms of a group that $g * h$ must necessarily equal $h * g$.

4. Since writing the '$*$' can become quite cumbersome we will often write simply gh to denote $g * h$.

5. As a consequence of G4 we can write an iterated product

$$g_1 * (g_2 * (\cdots * (g_{k-1} * g_k) \cdots) \in G$$

as an expression

$$g_1 * \cdots * g_k \in G, \quad \text{or} \quad g_1 \cdots g_k \in G.$$

G4 is essentially stating that it does not matter in which order we evaluate products in an iterated product.

6. For any $g \in G$, we will write g^i for the i-fold iterated product

$$g^i \overset{def}{=} g * \cdots * g \in G \quad (i \text{ times})$$

We will define $g^0 \overset{def}{=} e_G$, for any $g \in G$, and denote $g^{-i} \overset{def}{=} (g^i)^{-1}$.

Definition 3.1.4 (Subgroup)**.** Let $(G, *)$ be a group. A subset $H \subset G$ is called a **subgroup of** G if the following axioms are satisfied:

(SG1) $e_G \in H$;

(SG2) for any $h, h' \in H$ we have $h * h' \in H$;

(SG3) if $h \in H$ then $h^{-1} \in H$.

In fact, we can collect SG1-SG3 into the single axiom

(SG) for every $h, k \in H$, $h * k^{-1} \in H$.

If $H \subset G$ is a subgroup such that $H \neq G$ then we will say that H is a **proper subgroup**. The subgroup $\{e_G\} \subset G$ is called **the trivial subgroup**.

It is not too difficult to find examples of subgroups:

Definition 3.1.5. Let $(G, *)$ be a group , $g \in G$. We define the **subgroup generated by** g to be

$$\langle g \rangle \overset{def}{=} \{\dots, g^{-2}, g^{-1}, e_G, g, g^2, g^3, \dots\}.$$

As the name suggests, $\langle g \rangle$ is a (in fact, abelian) subgroup of G.

Lemma 3.1.6. *Let $(G, *)$ be a group, $g \in G$ nontrivial (ie, $g \neq e_G$). Then, exactly one of the following must hold:*

a) $g^i \neq g^j$ for any $i \neq j$ and $\langle g \rangle$ has infinite order;

b) there exists some $k > 1$ such that $|\langle g \rangle| = k$ and

$$\langle g \rangle = \{e_G, g, \dots, g^{k-1}\},$$

In particular, $g^{-i} = g^{k-i}$, for any $0 < i < k$.

Proof:

a) The condition is simply stating that all elements appearing in the definition of $\langle g \rangle$ are distinct. As there are infinitely many of them then the result follows.

b) Suppose that there exists two elements g^i and g^j such that $i < j$ and $g^i = g^j$. Hence,

$$e_G = g^{-i} * g^i = g^{-i} * g^j = g^{j-i},$$

and $j - i > 0$. Let $k > 1$ be the smallest integer such that $g^k = e_G$.[1]

Let $m \in \mathbb{Z}$. Then, we can find $q, r \in \mathbb{Z}$ with $0 \leq r < k$ and such that $m = qk + r$ (Theorem 2.1.2). Thus,

$$g^m = g^{kq+r} = g^{kq} * g^r = (g^k)^q * g^r = (e_G)^q * g^r = g^r.$$

By the minimality of k we must have that $g^r \neq e_G$, for each $0 < r < k$. Thus, have shown that

$$\langle g \rangle = \{e_G, g, \dots, g^{k-1}\},$$

and each of the group elements appearing are distinct, so that $|\langle g \rangle| = k$.

Now, observe that $g^i * g^{k-i} = e_G = g^{k-i} * g^i$ so that $g^{k-i} = g^{-i}$, by Lemma 3.1.2.

□

Corollary 3.1.7. *Let $(G, *)$ be a finite group, $g \in G$ a nontrivial element. Then, there is some $1 < k \leq |G|$ such that $g^k = e_G$.*

Proof: If there does not exist such $k > 1$ then $\langle g \rangle \subset G$ is infinite implying that G is infinite, which is absurd. □

Definition 3.1.8 (Order of an element)**.** Let $(G, *)$ be a group, $g \in G$ a nontrivial element.

- g is said to have **infinite order** if $\langle g \rangle \subset G$ is a subgroup of infinite order. In particular, we have $g^i \neq g^j$ for any $i \neq j$, by Lemma 3.1.6.

[1] Why does such an integer exist? It must be larger than 1 since g is nontrivial.

- g is said to have **order** k if $|\langle g\rangle| = k$. In particular, $g^k = e_G$ and k is the smallest positive integer for which this holds. We define e_G to have order 1.

We write $o(g) = k$ (resp. $o(g) = \infty$) if g has order k (resp. infinite order).

Example 3.1.9. 1. All of the examples introduced in Lecture 1, with their associated laws of composition, are examples of groups.

2. Let $n > 1$ be an integer. Then, $(\mathbb{Z}/n\mathbb{Z}, *)$, where
$$\bar{i} * \bar{j} = \overline{i+j},$$
defines a group with identity $e_G \overset{def}{=} \bar{0}$. If $\bar{i} \in G$ then its inverse is $\overline{-i}$. We will always write the law of composition for this group additively: $\bar{i} + \bar{j} \overset{def}{=} \overline{i+j}$. In particular, we write $-\bar{i} \overset{def}{=} \overline{-i}$.

   We should check that the law of composition given is well-defined: this means that if $\bar{i} = \bar{x}$ and $\bar{j} = \bar{y}$, then we must ensure that $\overline{i+j} = \overline{x+y}$. Otherwise, the assignment that we have given for $+$ does not define a function so that $(\mathbb{Z}/n\mathbb{Z}, +)$ does not satisfy G1. Now, if $\bar{i} = \bar{x}$ then $i - x \in n\mathbb{Z} = \{nr \mid r \in \mathbb{Z}\}$, so there is some $r \in \mathbb{Z}$ such that $i = x + nr$. Similarly, there is some $s \in \mathbb{Z}$ such that $j = y + ns$. Then,
$$\overline{i+j} = \overline{x + nr + y + ns} = \overline{x + y + n(r+s)} = \overline{x+y},$$
and the definition given is well-defined.

   If k is a divisor of n then $H = \{\overline{ak} \mid a \in \mathbb{Z}\}$ is a subgroup: if $\overline{ak}, \overline{bk} \in H$ then
$$\overline{ak} + (-\overline{bk}) = \overline{ak} + \overline{-bk} = \overline{ak - bk} = \overline{(a-b)k} \in H.$$

   The element $\bar{1} \in \mathbb{Z}/n\mathbb{Z}$ has order n.

3. Define **the symmetric group on** n **letters** S_n to be
$$S_n \overset{def}{=} \mathrm{Perm}(\{1, \dots, n\}) = \{f : \{1, \dots, n\} \to \{1, \dots, n\} \mid f \text{ is a bijective function}\},$$
with law of compositiong given by 'composition of functions'. The identity element is $e_{S_n} = \mathrm{id}_n$, where $\mathrm{id}_n(x) = x$, for every x. For any $f \in S_n$, the inverse f^{-1} is the inverse function. In general, for any set S we define
$$\mathrm{Perm}(S) = \{f : S \to S \mid f \text{ is a bijective function}\};$$
it is a group with law of composition given by composition of functions.

   The subset
$$H = \{f \in S_n \mid f(n) = n\}$$
is a subgroup. Indeed, if $f, g \in H$ then $(f \circ g^{-1})(1) = f(g^{-1}(1)) = f(1) = 1$, so that $fg^{-1} \in H$.

   If $n = 5$ the element $f \in S_5$ such that $f(1) = 1, f(2) = 3, f(3) = 4, f(4) = 2, f(5) = 5$ has order 3: indeed, that $f^3(1) = 1, f^3(5) = 5$, is straightforward and, for example,
$$f^3(2) = f(f(f(2))) = f(f(3)) = f(4) = 2,$$
and similarly it can be shown that $f^3(3) = 3, f^3(4) = 4$.

4. Let $n > 2$ be an integer. Then, the **dihedral group of order $2n$, denoted D_{2n},** is the group of symmetries of the regular n-gon. We can write the elements of this group as

$$D_{2n} = \{e, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\},$$

where r is the '*rotate by* $2\pi/n$ *counterclockwise*' transformation of the plane, and s is a reflection of the plane preserving the n-gon. We have

$$r^i * r^j = r^{i+j},\ sr = r^{-1}s,\ r^n = e,\ s^2 = e.$$

We say that $r, s \in D_{2n}$ are **generators** of D_{2n} subject to the above **relations**.

5. In general, we might present a group G via a **generators and relations presentation** as follows:

$$G = \langle x_1, \dots, x_n \mid R \rangle,$$

where $x_1, \dots, x_n$ are **generators of G subject to the relations** R. This means that each element $g \in G$ may be written as

$$g = x_{i_1}^{\pm} \cdots x_{i_p}^{\pm},\ i_1, \dots, i_p \in \{1, \dots, n\},$$

and such that we can use the relations R to transform one expression for g into another. An expression $x_{i_1} \cdots x_{i_p}$ as above is called a **word**.

For example, we have

$$D_{2n} = \langle r, s \mid s^2 = e,\ r^n = e,\ s * r = r^{-1} * s \rangle :$$

the word

$$r * r * r * s * s * s * r^{-1} * s * r,$$

can be reduced to r^5 using the given relations, since $s * s = e$ and $s * r^{-1} * s = r$.

6. Let $\mathrm{GL}_n(\mathbb{R})$ be the set of invertible $n \times n$ matrices with entries in $\mathbb{R}$, referred to as the $n \times n$ general linear group. This is a group with law of composition being matrix multiplication; the identity is the $n \times n$ identity matrix I_n. Similarly, we obtain groups $\mathrm{GL}_n(\mathbb{C})$, $\mathrm{GL}_n(\mathbb{Z})$, $\mathrm{GL}_n(\mathbb{Q})$, $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ etc. The element

$$g = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \mathrm{GL}_n(\mathbb{R}),$$

has order 4.

Let $B_n(\mathbb{R}) = \{B = [b_{ij}] \in \mathrm{GL}_n(\mathbb{R}) \mid b_{ij} = 0 \text{ when } i > j\}$, the set of all upper-triangular invertible matrices. This is a subgroup of $\mathrm{GL}_n(\mathbb{R})$. Similarly, we define

$$D_n(\mathbb{R}) \overset{def}{=} \{\text{invertible diagonal matrices}\} \subset \mathrm{GL}_n(\mathbb{R}),$$

$$U_n(\mathbb{R}) \overset{def}{=} \{A = [a_{ij}] \in B_n(\mathbb{R}) \mid a_{ii} = 1,\ \forall i\} \subset B_n(\mathbb{R});$$

they are all subgroups of $\mathrm{GL}_n(\mathbb{R})$.

7. The **quaternions** $(\mathcal{Q}_8, *)$, where

$$\mathcal{Q}_8 \overset{def}{=} \{\pm 1, \pm i. \pm j, \pm k\},$$

and

$$i * j = k,\ j * k = i,\ k * i = j,\ j * i = -k,\ k * j = -i,\ i * k = -j,$$
$$i^2 = j^2 = k^2 = -1,$$

with ± 1 scaling in the obvious way, defines a (nonabelian) group of order 8. The subset $H = \{\pm 1, \pm j\}$ is a subgroup.

8. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ are all (abelian) groups of infinite order. No element in any of these groups has finite order.

9. The set of nonzero complex numbers with law of composition coming from multiplication of numbers, $(\mathbb{C}^{\times},\cdot)$, is an abelian group. The set $\mu_n=\{z\in\mathbb{C}\mid z^n=1\}$ of n'th roots of unity is a (finite) subgroup.

4 Lecture 4 - Homomorphisms, isomorphisms.

Previous lecture - Next lecture

Keywords: group homomorphism, kernel, image. Isomorphism, automorphism.

Further Reading: Goodman 2.4, 2.5

In the previous lecture we introduced the main objects of study in group theory. In this lecture we will introduce the notion of a group homomorphism, which will allow us to observe how different groups can interact with each other. Moreover, we will introduce the fundamental notion of two groups G and H being isomorphic - this means that G and H *'are the same group but wearing different clothes'*.

4.1 Group homomorphisms, isomorphisms

Definition 4.1.1 (Group homomorphism)**.** Let $(G, *)$ and $(H, \bullet)$ be groups, $f : G \to H$ a function. We say that f is a **group homomorphism** if

(HOM) for any $g, h \in G$, we have $f(g * h) = f(g) \bullet f(h)$.

Given a group homomorphism $f : G \to H$ we define

- the **kernel of** f to be
$$\ker f = \{g \in G \mid f(g) = e_H \in H\} \subset G;$$

- the **image of** f to be
$$\text{im } f = \{h \in H \mid h = f(g) \text{ for some } g \in G\} \subset H.$$

Lemma 4.1.2. *Let $(G, *), (H, \bullet)$ be two groups, $f : G \to H$ a group homomorphism.*

a) $f(e_G) = e_H \in H$;

b) for every $g \in G$, $f(g^{-1}) = f(g)^{-1} \in H$;

c) $\ker f \subset G$ is a subgroup;

d) $\text{im } f \subset H$ is a subgroup;

e) f is injective if and only if $\ker f = \{e_G\}$.

Proof:

a) We have
$$f(e_G) = f(e_G * e_G) = f(e_G) \bullet f(e_G)$$
$$\implies e_H = f(e_G)^{-1} \bullet f(e_G) = f(e_G)^{-1} \bullet (f(e_G) \bullet f(e_G)) = \big(f(e_G)^{-1} \bullet f(e_G)\big) \bullet f(e_G)$$
$$\implies e_H = f(e_G).$$

b), c), d) Homework/worksheet problems.

□

Example 4.1.3. 1. Let $G = \mathbb{Z}/4\mathbb{Z}$ and $H = D_8 = \{e_H, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Define
$$f : G \to H \ ; \ \bar{i} \mapsto r^i.$$

Then, f is well-defined: if $\bar{i} = \bar{j}$ then the definition does not depend on the choice of representative. Indeed, in this case we have $i = j + 4k$, for some $k \in \mathbb{Z}$, so that
$$f(\bar{i}) = r^i = r^{j+4k} = r^j r^{4k} = r^j (r^4)^k = r^j = f(\bar{j}),$$

since $r^4 = e_H$. Moreover,

$$f(\bar{i} + \bar{j}) = f(\overline{i+j}) = r^{i+j} = r^i r^j = f(\bar{i})f(\bar{j}).$$

Also, $\ker f = \{e_G\}$ so that f is injective: if $\bar{i} \in \ker f$, with $i \in \{0, 1, 2, 3\}$, then

$$r^i = f(\bar{i}) = e_H \implies i = 0.$$

Hence, $\bar{i} = \bar{0}$ and $\ker f = \{\bar{0}\}$. f can't be surjective as $|D_8| = 8 > 4 = |\mathbb{Z}/4\mathbb{Z}|$.

2. Let $G = \mathbb{Z}/8\mathbb{Z}$, $H = \mathbb{Z}/2\mathbb{Z}$. Define

$$f : G \to H \ ; \ \bar{i} \mapsto \bar{i},$$

where the input is considered as a residue class modulo 8, and the output is a residue class modulo 2. This is well-defined and a homomorphism: if $\bar{i}, \bar{j} \in \mathbb{Z}/8\mathbb{Z}$ then

$$f(\bar{i} + \bar{j}) = f(\overline{i+j}) = \overline{i+j} = \bar{i} + \bar{j} = f(\bar{i}) + f(\bar{j}).$$

If $\bar{i} \in \ker f$ then we have $f(\bar{i}) = \bar{0}$, so that $i \in \bar{0} \in \mathbb{Z}/2\mathbb{Z}$. Hence, $i = 2k$, for some k. Therefore,

$$\ker f = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}.$$

f is surjective since $f(\bar{0}) = \bar{0}$ and $f(\bar{3}) = \bar{1}$ (also $f(\bar{1}) = f(\bar{5}) = f(\bar{7}) = \bar{1}$).

3. The assignment

$$f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \ ; \ \bar{i} \mapsto \bar{i},$$

is **not well-defined!**: note that $\bar{1} = \bar{3}$ but

$$f(\bar{1}) = \bar{1} \in \mathbb{Z}/4\mathbb{Z}, \ f(\bar{3}) = \bar{3} \in \mathbb{Z}/4\mathbb{Z},$$

and $\bar{1} \neq \bar{3}$ in $\mathbb{Z}/4\mathbb{Z}$. Hence, the given assignment defining f is **not a function**! However, the assignment

$$g : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \ ; \ \bar{i} \mapsto \overline{2i},$$

is well-defined, and an injective homomorphism of groups.

Definition 4.1.4. Let $f : G \to H$ be a group homomorphism of the groups $(G*), (H, \bullet)$. We say that f **is an isomorphism** if f is a bijective function.[1] If $(H, \bullet) = (G, *)$ then we call an isomorphism an **automorphism of** G.

If there exists an isomorphism $f : (G, *) \to (H, \bullet)$ then we say that G and H are **isomorphic as groups**, or simply **isomorphic**. We will write $G \cong H$, whenever G is isomorphic to H.

Example 4.1.5. 1. Let

$$\begin{aligned} G = D_6 &= \{\text{symmetries of triangle with vertices } (1, 0), (-1/2, \sqrt{3}/2), (-1/2, -\sqrt{3}/2)\} \\ &= \{e_G, r, r^2, s, sr, sr^2\}, \end{aligned}$$

where r is 'rotate by $2\pi/3$ counter-clockwise', s is 'reflect in x-axis', and define

$$\begin{aligned} H &= \{A = [a_{ij}] \in Mat_3(\mathbb{Z}) \mid a_{ij} \in \{0, 1\} \text{ and there is exactly one 1 in each row and each column}\} \\ &= \left\{ \begin{bmatrix} 1 & & \\ & 1 & \\ & & 1 \end{bmatrix}, \begin{bmatrix} & 1 & \\ 1 & & \\ & & 1 \end{bmatrix}, \begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix}, \begin{bmatrix} & 1 & \\ & & 1 \\ 1 & & \end{bmatrix}, \begin{bmatrix} & & 1 \\ & 1 & \\ 1 & & \end{bmatrix}, \begin{bmatrix} & & 1 \\ 1 & & \\ & 1 & \end{bmatrix} \right\} \\ &= \{e_H, x_1, x_2, x_3, x_4, x_5\} \quad (x_i \text{ corresponding to the } (i+1)\text{'th matrix above}) \end{aligned}$$

[1] According to Wikipedia, *isomorphism* comes from the Greek words *isos*, meaning 'equal', and *morphe*, meaning 'shape'.

Define

$$f : G \to H ;$$

$$\begin{array}{ccc} e_G & \mapsto & e_H \\ s & \mapsto & x_1 \\ sr & \mapsto & x_2 \\ r & \mapsto & x_5 \\ r^2 & \mapsto & x_3 \\ sr^2 & \mapsto & x_4 \end{array}$$

Then, f is a bijection - it is injective and $|G| = |H|$ - and it is a homomorphism, as can be checked directly (although somewhat tedious). Hence, G is isomorphic to H.

2. Consider the function

$$f : (\mathbb{Z}, +) \to U_2(\mathbb{Z}) = \left\{ \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \mid x \in \mathbb{Z} \right\} \subset \mathrm{GL}_2(\mathbb{Z}) \; ; \; x \mapsto \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix},$$

where $U_2(\mathbb{Z})$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z})$. This is an isomorphism of groups: indeed, if $x, y \in \mathbb{Z}$ then

$$f(x+y) = \begin{bmatrix} 1 & x+y \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & y \\ 0 & 1 \end{bmatrix} = f(x)f(y),$$

so that f is a group homomorphism. Moreover, let $x \in \ker f$. Then,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = f(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \implies x = 0,$$

so that $\ker f = \{0\}$, and f is injective (Lemma 4.1.2). Showing that f is surjective is straightforward.

3. If $|G| \neq |H|$ then G and H are not isomorphic.

4. Let $G = \mathbb{Z}/4\mathbb{Z}$ and $H = \left\{ A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in Mat_2(\mathbb{Z}) \mid a, b \in \{1, -1\} \right\} \subset \mathrm{GL}_2(\mathbb{Z})$. Then, G is not isomorphic to H: if $G \cong H$ then there would exist an isomorphism of groups $f : G \to H$. Moreover, $A = f(\overline{1}) \in H$ would satisfy $A^2 = I_2 = e_H$, by definition of H (every element $B \in H$ satisfies $B^2 = e_H$). Thus,

$$f(\overline{2}) = f(\overline{1} + \overline{1}) = f(\overline{1})f(\overline{1}) = A^2 = I_2 = e_H,$$

so that $\overline{2} \in \ker f$. Therefore, it is not possible for f to be injective, which contradicts that f is an isomorphism.

This example highlights the following fundamental fact

there exist groups having the same order that are not isomorphic

Remark 4.1.6. If G and H are isomorphic then they are, essentially, the same group. As we have assumed f to be a group homomorphism then it preserves the law of composition in both G and H (this is what HOM ensures).

It is a fundamental problem in group theory, if not the fundamental problem, to determine (essentially) all possible finite groups. This means that we would like to give a list of all possible *isomorphism classes* of groups: if G is any finite group, then there should be exactly one group K in our list such that G is isomorphic to K. The analagous problem in (finite dimensional) theory of vector spaces is pretty easy - you determine the answer in Math 54: if V is a vector space such that $\dim V = n$ then $V \cong F^n$, where

F is the scalar field. Thus, every finite dimensional vector space (over F) is isomorphic to one of the following

$$\{0\}, F, F^2, F^3, \dots, F^n, \dots \quad \text{(cf. Example 4 above)}$$

In group theory the problem is **significantly harder** - a list of the ‘building blocks’ of all finite groups (the so-called **simple groups**) was given in the 70-80s. The proof that this list is correct spans some 15000 pages spread over approxiamtely 500 journal articles and the most important information has been recorded in a book, referred to as ‘The Atlas’.

Later in this course we shall see how we can (in theory and in practice) determine a list of the isomorphism classes of **all finite abelian groups**. However, discussing the non-abelian case in this course is far beyond the author’s capabilities.

5 Lecture 5 - Cosets and Lagrange's Theorem.

Previous lecture - Next lecture

Keywords: Cosets. Index of a subgroup. Lagrange's Theorem.

In today's lecture we will prove one of the most fundamental results in group theory - **Lagrange's Theorem**. This result states that there are strong conditions on the existence of subgroups of a finite group.

5.1 Cosets

Let G be a group and $H \subset G$ be a subgroup. To this data we can define an equivalence relation $\sim_H$, or simply $\sim$, on G, and hence a partition of G corresponding to $\sim_H$ which we will call the **left H-partition**, as follows:

$$g \sim_H g' \quad \Leftrightarrow \quad g^{-1}g' \in H.$$

Let's check ER2 and ER3:

(ER2): suppose that $g \sim_H g'$ and $g^{-1}g' = h \in H$. Then, $(g')^{-1}g = h^{-1} \in H$, since H is a subgroup, so that $g' \sim_H g$.
(ER3): suppose that $g \sim_H g'$ and $g' \sim_H g''$. Thus, we have $g^{-1}g' \in H$ and $(g')^{-1}g'' \in H$. Then, $g^{-1}g'' = \left(g^{-1}g'(g')^{-1}g''\right) = \left(g^{-1}g'\right)\left((g')^{-1}g''\right) \in H$, since H is a subgroup. Hence, $g \sim_H g''$.

Definition 5.1.1. The equivalence classes of the equivalence relation corresponding to the left H-partition are called **left cosets of H (in G)**. We denote the set of equivalence classes G/H and call it **the set of left cosets of H in G**. The number of left cosets of H in G is **the index of H in G, denoteed** $[G : H]$, it may be infinite.

Lemma 5.1.2. *Let $[g] \in G/H$. Then,*

$$[g] = \{gh \mid h \in H\} \overset{def}{=} gH.$$

Proof: Let $h \in H$. Then, since $g^{-1}(gh) = h \in H$ we have that $g \sim_H gh$ so that $gh \in [g]$. Conversely, suppose that $k \in [g]$. Then, there is $h \in H$ such that $g^{-1}k = h$, so that $k = gh \in gH$. □

Corollary 5.1.3. *Let $[g] \in G/H$ be a left coset of H in G. Then, there is a bijection*

$$[g] \xleftrightarrow{1:1} H.$$

In particular, if H is finite then all left cosets of H in G have the same (finite) size, equal to $|H|$.

Proof: By Lemma 5.1.2 we have that $[g] = gH$. Consider the function

$$F : H \to gH \ ; \ h \mapsto gh.$$

Then, F is injective - if $F(h) = F(h')$ then $gh = gh'$ so that $h = h'$; and surjective - if $gh \in gH$ then $F(h) = gh$. Hence, F is a bijection. □

Example 5.1.4. Let $H = \{\pm 1, \pm i\} \subset \mathcal{Q}$, the group of quaternions. Then, there are exactly two left cosets of H in G

$$eH = \{\pm 1, \pm i\}, \ jH = \{\pm j, \pm k\}.$$

We always have H is a coset (it is the equivalence class of any $h \in H$), and for $g \notin H$, say $g = j$, you can check that

$$jH = \{jh \mid h \in H\} = \{\pm j, \pm ji\} = \{\pm j, \pm k\}.$$

Note that jH is **not a subgroup of** G!

In general

$$\boxed{gH \textbf{ is a subgroup if and only if } gH = eH \textbf{ if and only if } g \in H}$$

Remark. For the remainder of the course we will suppress the '$*$' when considering the law of composition in a group. As such, we will simply say 'Let G be a group', where the law of composition is implicitly understood to have been defined as part of the definition of G.[1]

5.2 Lagrange's Theorem

Theorem 5.2.1 (Lagrange's Theorem)**.** *Let G be a finite group, $H \subset G$ a subgroup. Then, the number of left cosets of H in G is $|G|/|H|$. That is,*

$$|G/H| = |G|/|H|.$$

Hence,

$$\boxed{\textbf{the order of } H \textbf{ divides the order of } G\textbf{.}}$$

Proof: Since G is finite then $H \subset G$ is finite and, by Corollary 5.1.3, every left coset of H in G has the same size, equal to $k = |H|$. Since a left coset of H in G is an equivalence class of the equivalence relation $\sim_H$ we know that there is a partition of G into equivalence classes. If there are r such equivalence classes (ie r left cosets of H), each of which has the same size k, then

$$|G| = \overset{r \text{ times}}{k + \cdots + k} = rk \quad \Longrightarrow \quad |G/H| = r = |G|/|H|.$$

□

Corollary 5.2.2. *Let G be a finite group, $g \in G$. Then, $o(g)$ divides $|G|$.*

Proof: Recall that $o(g) = |\langle g \rangle|$, and $\langle g \rangle \subset G$ is a subgroup of G. The result follows from Lagrange's Theorem. □

Hence,

$$\boxed{\textbf{the order of an element } g\textbf{, } o(g)\textbf{, divides the order of } G\textbf{.}}$$

Example 5.2.3.

1. Suppose that $H \subset D_8$ is a subgroup. Then, $|H|$ must be even. Indeed, Lagrange's Theorem implies that $|H|$ divides $|D_8| = 8$, we must have $|H| = 1, 2, 4, 8$. Note that Lagrange's Theorem **does not** imply that there must exist a subgroup of each of these orders. We will come back to this problem when we discuss Sylow's Theorems.

2. Let $f : \mathbb{Z}/5\mathbb{Z} \to S_4$ be a group homomorphism. Then, f must be the trivial homomorphism. Indeed, since $\ker f \subset \mathbb{Z}/5\mathbb{Z}$ is a subgroup then $|\ker f| = 1, 5$; if $|\ker f| = 1$ then f is injective. Hence, there must exist an element of S_5 of order 5, but 5 does not divide $|S_4| = 24$.

Remark 5.2.4. Why have we repeatedly used the adjective 'left'? There is an analagous notion of a **right coset of** H **in** G: define an equivalence relation on G by

$$g \sim^H g' \quad \Leftrightarrow \quad g'g^{-1} \in H.$$

It can be shown that this defines an equivalence relation on G and the equivalence classes are of the form

$$[g] = \{hg \mid h \in H\} \overset{def}{=} Hg.$$

[1] Why do we make an issue of this? It could be possible to define two *different* laws of composition on a set G so that we obtain two *different* groups $(G, *)$ and $(G, \bullet)$ with the same underlying set.

The resulting partition of G is called the **right H-partition of** G, and we denote the set of equivalence classes $H \setminus G$. There are analagous results to those obtained above for right cosets of H in G - in particular, there is an analogue of Lagrange's Theorem - **the number of right cosets of H in G equals** $|G|/|H|$ - so that, for a finite group G and a subgroup $H \subset G$

the number of <u>right</u> cosets equals the number of <u>left</u> cosets.

6 Lecture 6 - Groups of Prime Order. Cyclic groups.

Previous lecture - Next lecture

Keywords: Cyclic groups. Generator. Groups of prime power are cyclic.

This lecture discusses the simplest type of group: a *cyclic group*. These are groups in which every element can be expressed as a power of one particular element, the generator. We'll see that the "models" for these cyclic groups are the integers and the integers mod n, and that computations in these groups amount to "arithmetic upstairs", i.e. just keeping track of the exponents.

6.1 Groups of prime order

Let G be a group of prime order, so that $|G| = p$ is a prime. Let $g \in G$ be nontrivial. Thus, the subgroup $H = \langle g \rangle$ is a nontrivial subgroup of order $o(g)$ so that $H = G$, by Corollary 5.2.2. Hence, we have

$$G = \{e_G, g, g^2, \dots, g^{p-1}\}.$$

Moreover, $g^p = e_G$, for any nontrivial $g \in G$.

If G' is another group of order p then, for any nontrivial $h \in G'$, we find that

$$G' = \{e_{G'}, h, h^2, \dots, h^{p-1}\}.$$

It can then be shown that G and G' are isomorphic as groups.[1] In particular, any group G of prime order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Hence, any group of prime order p is a **cyclic group** (to be defined in the next section) - a group generated by a single element.

6.2 Cyclic groups

Lagrange's Theorem is a simple consequence of the existence of a particular equivalence relation that can be defined on any finite group G, given a subgroup H, and has allowed us to classify[2] all finite groups of prime order. Combining Lagrange's Theorem with the basic arithmetic properties of $\mathbb{Z}$ from Lecture 2 allows us to to understand the structure of a larger class of groups - the **cyclic groups**.

Definition 6.2.1 (Cyclic group)**.** A group G is **cyclic** if there exists $x \in G$ such that

$$G = \langle x \rangle = \{\dots, x^{-1}, e_G, x, x^2, \dots\}.$$

We call such an x a **generator of** G, and say that G is **generated by** x.

Remark 6.2.2. Let G be a cyclic group with generator $x \in G$. Then, x^{-1} is also a generator of G. In general, there are many generators of a cyclic group.

Example 6.2.3. a) e_G is a generator of a cyclic group G if and only if G is the trivial group.

b) Let $G = \mathbb{Z}$. Then, G is cyclic and generated by 1. The set of all generators of G is $\{\pm 1\}$.

c) Let $n \in \mathbb{Z}_{>1}$ and $G = \mathbb{Z}/n\mathbb{Z}$. Then, G is cyclic and generated by 1. The set of generators of G is

$$\{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \mid x \in \{1, \dots, n-1\},\ \gcd(x, n) = 1\}.$$

d) Let $G = \mu_6 = \{z \in \mathbb{C} \mid z^6 = 1\}$, considered as a subgroup of $(\mathbb{C}^\times, \cdot)$, the law of composition being multiplication of complex numbers - μ_6 is the group of sixth roots of unity. Then, μ_6 is cyclic with generator $w = \frac{1}{2}(1 + \sqrt{-3})$.[3]

[1] What is the isomorphism between G and G'?

[2] This means that we have understood essentially all finite groups of prime order - they are isomorphic to $\mathbb{Z}/p\mathbb{Z}$, so that they have the same structure as $\mathbb{Z}/p\mathbb{Z}$.

[3] This is a particular example of a more general result: any finite subgroup of $(\mathbb{C}^\times, \cdot)$ is cyclic.

e) The dihedral group D_8 is not a cyclic group as there does not exit any element of order 8. In general, D_{2n} is not cyclic.

f) S_n is cyclic if and only if $n = 2$.

g) $(\mathbb{Q}, +)$ is not cyclic.

In fact, the examples above describe **all possible cyclic groups**:

Theorem 6.2.4 (Structure Theorem of cyclic groups)**.** *Let G be a cyclic group generated by $x \in G$. Then,*

a) if G is infinite then G is isomorphic to $\mathbb{Z}$;

b) if G has order n then G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Let $H \subset G$ be a nontrivial subgroup. Then,

a) (G infinite) H is isomorphic to $\mathbb{Z}$ and generated by x^i, where $i = \min\{r \in \mathbb{Z}_{>0} \mid x^r \in H\}$.

b) (G of finite order n) Suppose $|H| = k$ so that $n = km$, by Lagrange's Theorem. Then, H is cyclic and generated by x^m. Hence, H is isomorphic to $\mathbb{Z}/k\mathbb{Z}$.

Proof:

a) Suppose that G is infinite and $G = \langle x \rangle$. Then, by the definition of a cyclic group we have

$$G = \{\dots, x^{-1}, e_G, x, x^2, \dots, \}.$$

Define

$$f : \mathbb{Z} \to G \; ; \; r \mapsto x^r.$$

Then, f is a group homomorphism. Moreover, f is injective - if $f(r) = e_G$ then $x^r = e_G = x^0$ so that $r = 0$, by Lemma 3.1.6 - and f is surjective, as x is a generator of G. Hence, f is an isomorphism and G is isomorphic to $\mathbb{Z}$.

If $H \subset G$ is a nontrivial subgroup and $i = \min\{r \in \mathbb{Z}_{>0} \mid x^r \in H\}$ then we claim that x^i generates H: we need only show that any nontrivial $h \in H$ is of the form $h = x^{ia}$, for some $a \in Z$. So, let $h \in H$ be nontrivial. Then, we must have $h = x^r$, for some $r \in \mathbb{Z}$. By the division algorithm we can find $q, b \in \mathbb{Z}$ with $0 \leq b < i$ such that $r = qi + b$. Hence, we see that

$$x^b = x^{r-qi} = x^r(x^i)^{-q} \in H.$$

Since $0 \leq b < i$ and i is the minimal positive integer such that $x^i \in H$, we must have that $b = 0$ so that $r = qi$. Hence, $h = (x^i)^q$ and

$$H = \langle x^i \rangle = \{\dots, x^{-i}, e_G, x^i, x^{2i}, \dots, \}.$$

b) If G is finite of order n and cyclic, then

$$G = \langle x \rangle = \{e_G, x, \dots, x^{n-1}\},$$

and $x^n = e_G$ by Lemma 3.1.6. Define

$$f : \mathbb{Z}/n\mathbb{Z} \to G \; ; \; \overline{r} \mapsto x^r.$$

This function is well-defined: if $\overline{r} = \overline{s}$, so that $r - s \in n\mathbb{Z}$, then

$$f(\overline{r}) = x^r = x^{s+nk} = x^s(x^n)^k = x^s(e_G)^k = x^s = f(\overline{s}).$$

Moreover, f is an isomorphism of groups. In a similar way as proved in a), it can be shown that any nontrivial subgroup H is of the stated form.

□

Example 6.2.5. Let $n = 10 = 2.5$. Then, the subgroups of $\mathbb{Z}/10\mathbb{Z}$ are

$$\{\overline{0}\}, \; \{\overline{0}, \overline{5}\} \cong \mathbb{Z}/2\mathbb{Z}, \; \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\} \cong \mathbb{Z}/5\mathbb{Z}, \; \mathbb{Z}/10\mathbb{Z}.$$

7 Lecture 7 - Group actions. Orbits, stabilisers.

Previous lecture - Next lecture

Keywords: Group action. Orbit, stabiliser. Transitive action. Fixed Point.

We now come to the most important concept in group theory, that of a **group action**. It is through group actions that we can realise a group as a mathematical object that captures the notion of symmetry - if a group G acts on a set S then the (abstract) group G captures some of the symmetry of S. Moreover, every important topic that we will discuss in this course can be reformulated in the language of group actions.

7.1 Group actions

Definition 7.1.1 ((Left) Group action)**.** Let G be a group, S an arbitrary (nonempty) set. A **(left) group action of** G **on** S is a function

$$a : G \times S \to S \; ; \; (g, x) \mapsto a(g, x) \overset{def}{=} g \cdot x,$$

satisfying the following properties

(ACT1) $e \cdot x = x$, for every $x \in S$;

(ACT2) $g \cdot (h \cdot x) = (gh) \cdot x$, for every $g, h \in G$, $x \in S$.

When there exists a (left) group action of G on S (via the function a), we will say that G **acts on** S **(via** a**)**.

The relationship between group actions and 'symmetry' are a consequence of the following result[1]:

Lemma 7.1.2. *Let $a : G \times S \to S$ be a group action of G on S. Then, we can define a group homomorphism*

$$\tilde{a} : G \to \mathrm{Perm}(S) \; ; \; g \mapsto \tilde{a}(g) \overset{def}{=} \begin{bmatrix} a_g : S \to S \\ x \mapsto g \cdot x \end{bmatrix}.$$

where Perm(S) *is the group of bijections on S. Conversely, given a group homomorphism $G \to$* Perm(S) *we can define a group action of G on S. Thus,*

$$\boxed{\textbf{a group action of } G \textbf{ on } S \textbf{ is } \underline{\textbf{the same as}} \textbf{ a group homomorphism } \tilde{a} : G \to \mathrm{Perm}(S)}$$

Proof: Suppose that a defines a group action of G on S. Define the function

$$\tilde{a} : G \to \mathrm{Perm}(S) \; ; \; g \mapsto \tilde{a}(g) \overset{def}{=} \begin{bmatrix} a_g : S \to S \\ x \mapsto g \cdot x \end{bmatrix}$$

as above. This definition says that to $g \in G$ we are associating the bijection (of S) $a_g \in \mathrm{Perm}(S)$, where $a_g(x) = g \cdot x$. This function is well-defined: namely, a_g is a bijective function on S. Indeed, ACT1 implies that $a_e = \mathrm{id}_S$ is the identity function on S and, for any $x \in S$

$$g \cdot (g^{-1} \cdot x) \overset{ACT2}{=} e \cdot x \overset{ACT2}{=} g^{-1} \cdot (g \cdot x).$$

Hence, for any $x \in S$

$$(a_g \circ a_{g^{-1}})(x) = a_g(a_{g^{-1}}(x)) = g \cdot (g^{-1} \cdot x) = e \cdot x = a_e(x)$$

$$\implies a_g \circ a_{g^{-1}} = \mathrm{id}_S,$$

and similarly $a_{g^{-1}} \circ a_g = \mathrm{id}_S$. Thus, a_g is bijective with inverse $(a_g)^{-1} = a_{g^{-1}}$.

[1] Recal that, for any set S we define Perm(S) to be the set of all bijective functions $f : S \to S$.

We need to check that $\tilde{a}$ is a group homomorphism: let $g, h \in G$. Then, we want to show an equality of functions $\tilde{a}(gh) = \tilde{a}(g) \circ \tilde{a}(h)$ or, using slightly different notation, $a_{gh} = a_g \circ a_h$. Now, for $x \in S$ we have

$$a_{gh}(x) = (gh) \cdot x \overset{ACT2}{=} g \cdot (h \cdot x) = a_g(h \cdot x) = a_g(a_h(x)) = (a_g \circ a_h)(x).$$

Hence, $a_{gh} = a_g \circ a_h$ and $\tilde{a}$ is a group homomorphism.

The converse result will be a homework problem. □

Example 7.1.3. 1. Let $G = \mathbb{Z}/2\mathbb{Z} = \{1, -1\}$, $S = \mathbb{R}$. Define

$$a : G \times S \to S \; ; \; (g, x) \mapsto g \cdot x \overset{def}{=} \begin{cases} x, \text{ if } g = 1, \\ -x, \text{ if } g = -1. \end{cases}$$

This defines an action of G on S.

2. Let $G = \mathbb{Z}/2\mathbb{Z} = \{1, -1\}$, $S = \mathbb{R}$. Define

$$a : G \times S \to S \; ; \; (g, x) \mapsto g \cdot x \overset{def}{=} \begin{cases} x, \text{ if } g = 1, \, x \neq 0, \\ x^{-1}, \text{ if } g = -1, \, x \neq 0, \\ 0, \text{ if } x = 0. \end{cases}$$

This defines an action of G on S.

Thus, it is possible for a group to act on a set via different actions.

3. Let $G = \mathbb{Z}, S = \mathbb{R}$. Define

$$a : G \times S \to S \; ; \; (n, x) \mapsto n \cdot x \overset{def}{=} x + n;$$

since

$$m \cdot (n \cdot x) = (n \cdot x) + m = (x + n) + m = x + (n + m) = (n + m) \cdot x,$$

this is a group action.

4. Let $G = \mathrm{GL}_2(\mathbb{Z})$, $S = \mathrm{Mat}_2(\mathbb{Z})$. Define

$$a : G \times S \to S \; ; \; (g, x) \mapsto gxg^{-1}.$$

This defines an action of G on S.

5. Let $G = SO(2) \overset{def}{=} \left\{ \begin{bmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{bmatrix} \mid t \in \mathbb{R} \right\} \subset \mathrm{GL}_2(\mathbb{R})$, $S = \mathbb{R}^2$. Define

$$a : G \times S \to S \; ; \; (g, v) \mapsto g \cdot v \overset{def}{=} gv.$$

This defines an action of G on S.

6. Let $G = \mathbb{Z}$, $S = \mathbb{Z}$. Define

$$a : G \times S \to S \; ; \; (n, x) \mapsto n \cdot x \overset{def}{=} nx.$$

This does not define a group action of G on S as ACT1 does not hold: $0 \cdot 1 = 0 \neq 1$. ACT2 is also not satisfied.

7. Let $G = \mathrm{GL}_2(\mathbb{Z})$, $S = \mathrm{Mat}_2(\mathbb{Z})$. Define

$$a : G \times S \to S \ ; \ (g, x) \mapsto g \cdot x \overset{def}{=} xg.$$

ACT1 is satisfied - $I_2 \cdot x = xI_2 = x$ - but ACT2 is not satisfied: let $g = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $h = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, $x = I_2$. Then,

$$g \cdot (h \cdot x) = (h \cdot x)g = (I_2 h)g = hg,$$
$$(gh) \cdot x = I_2(gh) = gh,$$

but $gh = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = hg$.

7.2 Orbits, stabilisers

A group action of G on S allows (a 'shadow' of) G to be realised as symmetries of the set S. Associated to a group action are the fundamental concepts of **orbit** and **stabiliser**.

Definition 7.2.1. Suppose that G acts on S and let $x \in S$.

a) the **orbit through** x is the subset (of S)

$$G \cdot x = \{g \cdot x \mid g \in G\} \subset S.$$

We will also denote the orbit through x by $\mathcal{O}_x$.

b) the **stabiliser of** x **(in** G**)** is the subset

$$\mathrm{Stab}_G(x) = \{g \in G \mid g \cdot x = x\}.$$

c) If $\mathcal{O}_x = S$ then the action is said to be **transitive**.

d) If $\mathrm{Stab}_G(x) = G$ then x is a **fixed point of the action**.

Lemma 7.2.2. *Let G act on S, $x \in S$. The stabiliser of x in G, $\mathrm{Stab}_G(x)$, is a subgroup of G.*

Proof: Let $g, h \in \mathrm{Stab}_G(x)$ -it suffices to show that SUB holds. Now,

$$x = e \cdot x = h^{-1} \cdot (h \cdot x) = h^{-1} \cdot x,$$

since $h \cdot x = x$, and

$$(gh^{-1}) \cdot x \overset{ACT2}{=} g \cdot (h^{-1} \cdot x) = g \cdot x = x.$$

Hence, $gh^{-1} \in \mathrm{Stab}_G(x)$. □

Remark 7.2.3. Lemma 7.2.2 can be used to prove that a given subset $H \subset G$ is a subgroup without having to check the subgroup axiom SUB directly: if we can realise $H = \mathrm{Stab}_G(x)$ for some group action of G, then H must be a subgroup.

Example 7.2.4. Recall Example 7.1.3:

1.
$$\mathcal{O}_0 = \{0\}, \ \mathrm{Stab}_G(0) = \mathbb{Z}/2\mathbb{Z},$$
$$\mathcal{O}_2 = \{2, -2\}, \ \mathrm{Stab}_G(2) = \{1\} \subset \mathbb{Z}/2\mathbb{Z}.$$

2.

$$\mathcal{O}_1 = \{1\},\ \mathrm{Stab}_G(1) = \mathbb{Z}/2\mathbb{Z},$$
$$\mathcal{O}_0 = \{0\},\ \mathrm{Stab}_G(0) = \mathbb{Z}/2\mathbb{Z},$$
$$\mathcal{O}_2 = \left\{2, \frac{1}{2}\right\},\ \mathrm{Stab}_G(2) = \{1\}.$$

3.

$$\mathcal{O}_0 = \mathbb{Z},\ \mathrm{Stab}_G(0) = \{0\},$$
$$\mathcal{O}_1 = \mathbb{Z},\ \mathrm{Stab}_G(1) = \{0\},$$
$$\mathcal{O}_{\frac{1}{2}} = \left\{\dots, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \dots,\right\},\ \mathrm{Stab}_G\left(\frac{1}{2}\right) = \{0\}.$$

4.

$$\mathcal{O}_0 = \{0\},\ \mathrm{Stab}_G(0) = \mathrm{GL}_2(\mathbb{Z}),$$
$$\text{Let } A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \text{ then } \mathcal{O}_A = \{B \in \mathrm{Mat}_2(\mathbb{Z}) \mid B^2 = 0,\ B \neq 0\},$$
$$\mathrm{Stab}_G(A) = \left\{\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \mid a, b \in \mathbb{Z}\right\}.$$

5.

$$\mathcal{O}_0 = \{0\},\ \mathrm{Stab}_G(0) = SO(2),$$
$$\mathcal{O}_{e_1} = \{v \in \mathbb{R}^2 \mid ||v|| = 1\},\ \mathrm{Stab}_G(e_1) = \{I_2\}.$$

8 Lecture 8 - More on group actions. Conjugacy. Centralizers. Normalizers. Normal subgroups.

Previous lecture - Next lecture

Keywords: Orbit Partition. Conjugation. Centralizer. Center. Normalizer. Normal Subgroup.

This lecture goes further into the notion of a group action, in particular exploring more "theoretical" group actions, in which a group acts on itself or on the set of its subgroups. These abstract applications provide useful tools for studying the structure of a group.

8.1 Orbit Partition, Groups acting on themselves

Theorem 8.1.1 (Orbit partition)**.** *Let G act on S (via a). Then, we can define an equivalence relation on S such that the equivalence classes are precisely the orbits of the action as follows: if $x, y \in S$ then define*

$$x \sim_a y \ \Leftrightarrow\ y = g \cdot x, \text{ for some } g \in G.$$

Hence, S is partitioned into the orbits of the action of G on S.

Proof: ER1: since $x = e \cdot x$ then $x \sim_a x$,

ER2: If $x \sim_a y$, so that $y = g \cdot x$, for some $g \in G$. Then,

$$x = e \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y \implies y \sim_a x.$$

ER3: Suppose that $x \sim_a y$ and $y \sim_a z$, so that $y = g \cdot x$, $z = h \cdot y$, for some $g, h \in G$. Then,

$$z = h \cdot y = h \cdot (g \cdot x) = (hg) \cdot x \implies x \sim_a z.$$

For any $x \in S$

$$\mathcal{O}_x = \{g \cdot x \mid g \in G\} = \{y \in S \mid y = g \cdot x, \text{ for some } g \in G\} = \{y \in S \mid x \sim y\} = [x].$$

□

Corollary 8.1.2. *Let G act on S. Then, distinct orbits in S are disjoint; equivalently, if $\mathcal{O}_x \cap \mathcal{O}_y \neq \varnothing$ then $\mathcal{O}_x = \mathcal{O}_y$.*

Corollary 8.1.3 (Orbit decomposition formula)**.** *Let G act on the* **finite** *set S. If $\mathcal{O}_1, \dots, \mathcal{O}_k$ are the distinct orbits in S then*

$$|S| = |\mathcal{O}_1| + \dots + |\mathcal{O}_k|.$$

The following examples of groups acting on themselves are fundamental and will reappear frequently:

Example 8.1.4 (Fundamental group actions)**.** Let G be a group. Then, G acts on the following sets S in the prescribed manner:

1. Let $S = G$ and define
$$a : G \times S \to S \ ;\ (g, h) \mapsto g \cdot h \overset{def}{=} gh.$$
This action is called **permutation action of G on itself**.

2. Let $S = G$ and define
$$a : G \times S \to S \ ;\ (g, h) \mapsto g \cdot h \overset{def}{=} ghg^{-1}.$$
This action is called the **conjugation action of G on itself**.

3. Let $S = \mathrm{Sub}(G) = \{H \subset G \mid H \text{ is a subgroup of } G\}$, the set of all subgroups of G. Define

$$a : G \times S \to S \; ; \; (g, H) \mapsto g \cdot H \overset{def}{=} gHg^{-1},$$

where

$$gHg^{-1} \overset{def}{=} \{ghg^{-1} \mid h \in H\}.$$

4. Let $S = P(G) = \{A \subset G\}$, the set of all subsets of G. Define

$$a : G \times S \to S \; ; \; (g, A) \mapsto g \cdot A \overset{def}{=} gA,$$

where

$$gA \overset{def}{=} \{ga \mid a \in A\}.$$

Remark 8.1.5. If G is finite then, for a subgroup $H \subset G$ and subset $A \subset G$,

$$|gHg^{-1}| = |H|, \text{ and } |gA| = |A|,$$

for any $g \in G$.

8.2 Conjugacy Classes. Centralisers. normalisers

Let's take a closer look at some of the fundamental group actions introduced above.

Definition 8.2.1 (Centralizer of $g \in G$)**.** Let $g \in G$, where G is a group. Consider Example 2 in Example 8.1.4 (the conjugation action of G on itself). The **centralizer of** g **(in** G**)** is

$$\mathrm{Cent}_G(g) \overset{def}{=} \mathrm{Stab}_G(g),$$

for this action. Thus,

$$\mathrm{Cent}_G(g) = \{h \in G \mid h \cdot g = g\} = \{h \in G \mid hgh^{-1} = g\}.$$

We define **the center of** G**, denoted** $Z(G)$, to be

$$Z(G) \overset{def}{=} \bigcap_{g \in G} \mathrm{Cent}_G(g).$$

Hence, $Z(G)$ is the set of all elements in G that commute with every element in G.

The previous definition used the stabilizer under the group action of conjugacy in Example 2 of 8.1.4. Using the orbits of this action, we define the following:

Definition 8.2.2 (Conjugacy class)**.** Let $g \in G$. The equivalence class of g with respect to the equivalence relation coming from the conjugation action of G on itself is called **the conjugacy class of** g **in** G, denoted by $C(g)$; thus

$$C(g) = \{g' \in G \mid g' = hgh^{-1} \text{ for some } h \in H\}.$$

We will sometimes simply refer to **a conjugacy class in** G, the reference to some $g \in G$ being implicit.

Definition 8.2.3 (Normalizer of $H \subset G$)**.** Let $H \in \mathrm{Sub}(G)$ be a subgroup of a group G. Consider Example 3 in Example 8.1.4. The **normalizer of** H **(in** G**)** is

$$\mathrm{Norm}_G(H) \overset{def}{=} \mathrm{Stab}_G(H),$$

for this action. Thus,

$$\mathrm{Norm}_G(H) = \{g \in G \mid g \cdot H = H\} = \{g \in G \mid gHg^{-1} = H\}.$$

Since stabilisers of group actions are subgroups (Lemma 7.2.2) then **the centralizer of $g \in G$ is a subgroup of G** and **the normalizer of $H \subset G$ is a subgroup of G**. The conjugacy class of an element is not, in general, a subgroup.

Definition 8.2.4 (Normal subgroup)**.** Let $H \subset G$ be a subgroup. If $G = \mathrm{Norm}_G(H)$, so that H is a fixed point for the action in Example 3 of Example 8.1.4, then we say that H is a **normal subgroup in** G. In other words, H is normal if $gHg^{-1} = H$ for all $g \in G$, or in still other words, if $gH = Hg$ for all $g \in G$.

Example 8.2.5.

1. Assume that G is abelian. Then, for any $g \in G$, $\mathrm{Cent}_G(g) = G$. Moreover, the converse is true: suppose that, for any $g \in G$, $G = \mathrm{Cent}_G(g)$, the G is abelian.
2. Let $G = D_8 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Then, $\mathrm{Cent}_G(r^2) = G$, while G is not abelian. Also, $\mathrm{Cent}_G(s) = \{e, s, r^2, sr^2\}$ as can be seen by inspection.
3. Let $G = S_3 = \{e, s, t, st, ts, sts\}$, where
$$s(1) = 2, s(2) = 1, s(3) = 3, t(1) = 1, t(2) = 3, t(3) = 2.$$
Then, $\mathrm{Cent}_G(s) = \{e, s\}$: indeed, since $\mathrm{Cent}_G(s) \subset G$ is a subgroup, we must have its order divides the order of G, equal to 6. Hence, $|\mathrm{Cent}_G(s)| = 2, 3, 6$. We have seen that the only subgroup of order 3 in G is $H = \{e, st, ts\}$ so that, since $s \notin H$, then $H \neq \mathrm{Cent}_G(s)$. So, we must have $|\mathrm{Cent}_G(s)| = 2, 6$ and, as $st \neq ts$ - for example, $st(1) = s(1) = 2$ while $ts(1) = t(2) = 3$ - then $t \notin \mathrm{Cent}_G(s)$ and $|\mathrm{Cent}_G(s)| \leq 5$. Hence, $|\mathrm{Cent}_G(s)| = 2$ and the claim follows.
4. Assume that G is abelian. Then, every subgroup of G is normal in G.
5. Let $H \in \mathrm{Sub}(G)$, $h \in H$. Then, $h \in \mathrm{Norm}_G(H)$. Hence, $H \subset \mathrm{Norm}_G(H)$, for any subgroup H in G.
6. Let $G = D_8$ and $H = \{e, s\} \subset G$. Then, $\mathrm{Norm}_G(H) = \{e, s, r^2, sr^2\}$: indeed, we have
$$r^2Hr^{-2} = r^2Hr^2 = \{r^2hr^2 \mid h \in H\} = \{e, r^2sr^2\} = \{e, s\} = H$$
$$sr^2H(sr^2)^{-1} = sr^2Hr^2s = s(r^2Hr^2)s = sHs = H,$$
7. For any group G, $C(e_G) = \{e_G\}$. Hence, **if G is a nontrivial group then there always exists at least two conjugacy classes**.
8. Let G be an abelian group. Then, for any $g \in G$
$$C(g) = \{g\}.$$
In fact, G is abelian if and only if $C(g) = \{g\}$, for any $g \in G$.
9. Let $G = D_8$. Then, you can verify (by direct computation) that
$$C(e) = \{e\},\ C(r) = \{r, r^3\},\ C(r^2) = \{r^2\},\ C(s) = \{s, sr^2\},\ C(sr) = \{sr, sr^3\}.$$
In fact, this was problem 3 on the pseudoquiz, but without the terminology "conjugacy class".
10. Let $G = \mathrm{GL}_2(\mathbb{C})$. Then,
$$C\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) = \{A \in \mathrm{GL}_2(\mathbb{C}) \mid (A - I_2)^2 = 0,\ A \neq I_2\}.$$
This is a consequence of the theory of the Jordan form of a linear operator on $\mathbb{C}^2$; we will see how to prove this in a homework/worksheet problem.

If G is finite then the existence of the conjugacy equivalence relation described above imposes a condition relating the order of G to the number/size of conjugacy classes:

Theorem 8.2.6 (Class equation)**.** *Let G be a finite group. Suppose that there exists k conjugacy classes and $e_G, g_2, \dots, g_k$ are distinct class representatives of the conjugacy classes of G. Then,*

$$|G| = 1 + \sum_{i=2}^{k} |C(g_i)|.$$

Proof: Homework/worksheet. □

9 Lecture 9 - Symmetric groups. Orbit-Stabilizer Theorem. p-groups. Fixed point congruence for p-groups.

Previous lecture - Next lecture

Keywords: S_n, generators and conjugacy in S_n. Orbit-Stabilizer Theorem.

9.1 Symmetric groups, cycle decompositions

Note: See also the "S_n factsheet" on the website for a summary of this information, without proofs.

Let $[n] = \{1, \dots, n\}$. Then, the symmetric group S_n acts on $[n]$ in the following (obvious) way (recall that elements of S_n are functions on $[n]$):

$$S_n \times [n] \to [n] \ ; \ (\omega, i) \mapsto \omega(i).$$

In this way we obtain a **permutation of** $[n]$. Let $\omega \in S_n$ and consider the subgroup $H(\omega) = \langle \omega \rangle \subset S_n$; it is an abelian subgroup of order $o(\omega)$. We now restrict the action defined above to this subgroup

$$H(\omega) \times [n] \to [n] \ ; \ (\omega^r, i) \mapsto \overbrace{(\omega \circ \cdots \circ \omega)}^{r \text{ times}} (i).$$

This action defines a partition of $[n]$ into the orbits of this action and, given $i \in [n]$, we denote the orbit of i

$$(i_1 \cdots i_k) \overset{def}{=} \mathcal{O}_i = \{i_1, \dots, i_k\},$$

where $i_1 = \min\{j \in \mathcal{O}_i\}$, and

$$i_2 = \omega(i_1), \ i_3 = \omega(i_2) = \omega^2(i_1), \dots, i_k = \omega(i_{k-2}) = \omega^{k-1}(i_1), \ i_1 = \omega(i_k) = \omega^k(i_1).$$

and call $(i_1 \cdots i_k)$ a k-**cycle**, or simply a **cycle**. Note that we are saying that $i = \omega^r(i_1)$, for some r, and $\omega^k \in \mathrm{Stab}_H(i_1)$. In fact, k is the smallest positive integer such that $\omega^k \in \mathrm{Stab}_H(i_1)$.

Conversely, given a cycle $(i_1 \cdots i_k)$, we obtain a unique element $\omega \in S_n$ corresponding to that cycle. We will also refer to this element of S_n as a k-**cycle**.

Two cycles $(i_1 \cdots i_r)$ and $(j_1 \cdots j_s)$ are said to be **disjoint** if

$$\{i_1, \dots, i_r\} \cap \{j_1, \dots, j_s\} = \varnothing.$$

Hence, to any $\omega \in S_n$ we can consider the above partition of $[n]$ into orbits, and label the orbits by (disjoint) cycles. Thus, we can denote an element $\omega \in S_n$ as

$$\omega \leftrightarrow (i_1 \cdots i_r)(j_1 \cdots j_s) \cdots (k_1 \cdots k_t),$$

where $i_2 = \omega(i_1), i_3 = \omega(i_2), \dots, j_2 = \omega(j_1), j_3 = \omega(j_2), \dots$ etc. and

$$\{i_1, \dots, i_r\} \cap \{j_1, \dots, j_s\} = \varnothing,$$

because cycles <u>are</u> orbits. This presentation of an element of $\omega \in S_n$ is called the **cycle decomposition of** ω.

The cycle decomposition implies

$$\boxed{\textbf{the } r\textbf{-cycles, } r = 1, \dots, n\textbf{, generate the symmetric group } S_n}$$

However, the relations satisfied by these generators are not so straightforward to determine.

Example 9.1.1. Consider the element $\omega \in S_5$, which sends $1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 2, 5 \mapsto 5$
The partition of $\{1, 2, 3, 4, 5\}$ is

$$\{1, 2, 3, 4, 5\} = \{1\} \cup \{2, 3, 4\} \cup \{5\}$$

as you can check that $o(\omega) = 3$ and $\omega(1) = 1, \omega(5) = 5$ and

$$\omega(2) = 3,\ \omega^2(2) = \omega(\omega(2)) = \omega(3) = 4,\ \omega^3(2) = 2,$$

so the orbit of 2 under the action of $H(\omega)$ is $\{2, 3, 4\}$. Hence, the cycle decomposition of ω is $(1)(234)(5)$. In words, the function $\omega \in S_5$ sends

1 to 1, so we have the 1-cycle (1) appearing,

2 to 3, 3 to 4, 4 to 2, so we have the 3-cycle (234) appearing,

5 to 5, so we have the 1-cycle (5) appearing.

Remark 9.1.2. When a cycle contains exactly one integer we will not include it in the cycle decomposition; so in the above example we have

$$\omega = (234) \in S_5.$$

This requires **keeping track of the symmetric group we are working with** - for example, the element $(2457)(16) \in S_9$ is missing the 1-cycles $(3), (9), (8)$. However, if we did not state that $(2457)(16)$ is an element of S_9 then there would be ambiguity in our notation.

Introducing the cycle notation for elements of S_n allows us to give a nice description of conjugacy classes in S_n.

Definition 9.1.3 (Partitions of integers)**.** A sequence of integers $n_1 \geq ... \geq n_k \geq 1$ such that $n_1 + ... + n_k = n$ is called **a partition of** n.[1]

We will denote a partition $n_1 \geq ... \geq n_k$ either as a sequence $\nu : (n_1, n_2, ..., n_k)$ or by the expression $\nu : 1^{r_1}2^{r_2}\cdots$, where r_i is the number of times i appears in the partition; partitions will be denoted by Greek alphabet letters such as λ, μ, ν, π etc.

We define **the length of** $\nu : (n_1, ..., n_k)$ to be $|\nu| = n_1 + ... + n_k$.

For example, the partition

$$\nu :\ 4 + 4 + 3 + 2 + 2 + 2 + 1 + 1 = 19,$$

will be expressed either as the sequence $\nu : (4, 4, 3, 2, 2, 2, 1, 1)$ or as the expression $\nu : 1^2 2^3 3 4^2$; the length of ν is $|\nu| = 19$.

To any element $\omega \in S_n$ we associate a partition as follows: let $1 \leq k_1 \leq ... \leq k_r$ be the lengths of the cycles appearing in the cycle decomposition of ω. Then, we define the **cycle type of** ω to be the partition of n

$$\pi_\omega \overset{def}{=} (k_r, ..., k_1).$$

Theorem 9.1.4 (Classification of conjugacy classes in S_n)**.** *Let $\omega, \sigma \in S_n$. Then,*

$$C(\omega) = C(\sigma) \ \Leftrightarrow\ \pi_\omega = \pi_\sigma.$$

Proof: Let $\sigma \in S_n$ have cycle type $(k_1, ..., k_r)$. Denote $e_i = k_1 + ... k_i$; note that $e_r = n$. We will show that σ is conjugate to the element

$$\delta \overset{def}{=} (12\cdots e_1)(e_1 + 1 \cdots e_2)\cdots(e_{r-1} + 1 \cdots n).$$

[1] There's potential for confusion of notation here as we have two definitions: *partitions of a set* and *partitions of an integer*. However, the context in which we use the word should make it clear to which of these definitions we are referring.

We will make use of the following identity

$$\tau(i_1 \cdots i_s)\tau^{-1} = (\tau(i_1) \cdots \tau(i_s));$$

this can be verified by showing that both sides are equal functions on $\{1, \dots, n\}$.

We are going to define a $\tau \in S_n$ such that

$$\tau\delta\tau^{-1} = \sigma.$$

Suppose that the k_1-cycle of σ is $(i_1 \cdots i_{k_1})$; let

$$\tau(1) = i_1,\ \tau(2) = i_2,\ \dots\ , \tau(e_1) = i_{k_1}.$$

Suppose that the k_2-cycle of σ is $(j_1 \cdots j_{k_2})$; let

$$\tau(e_1 + 1) = j_1,\ \tau(e_1 + 2) = j_2,\ \dots\ , \tau(e_2) = j_{k_2}.$$

Proceeding in this manner we obtain a well-defined element $\tau \in S_n$ - τ is surjective since every number between 1 and n appears once in the cycle notation of σ. Hence, it is bijective. □

Example 9.1.5. Consider the elements $\omega = (12)(34), \sigma = (13)(24) \in S_4$. Then, by Theorem 9.1.4, we have that (12)(34) and (13)(24) are conjugate. You can check that

$$(23)\sigma(23) = \omega.$$

9.2 Cayley's Theorem

This section is optional reading and will not be tested

If a group G acts on a set S then we obtain a group homomorphism

$$G \to \mathrm{Perm}(S),$$

so that im G is a subgroup of permutations of S. It is in this way that we consider that G captures some of the symmetry of S. Loosely speaking, a 'symmetry of S' should be an 'operation' that we can apply to S that can be 'undone' and leaves S 'unchanged'; this is precisely a 'bijection/permutation of S'.

A group G is an abstract collection of symmetries, and whenever G acts on a set S then we obtain a 'realisation' of these symmetries as permutations of S. However, it may be the case that distinct elements of G are realised as the same permutation of S. Is there a way that we can realise any group G concretely as the symmetries of some actual set, so that G can be considered as a group of permutations? The answer is yes, and may be quite surprising:

Theorem 9.2.1 (Cayley's Theorem)**.** *Let G be a group. Then, there is an injective homomorphism*

$$L : G \to \mathrm{Perm}(G)\ ;\ g \mapsto L_g \in \mathrm{Perm}(G),$$

where L_g is the left multiplication *function,*

$$L_g : G \to G\ ;\ h \mapsto L_g(h) = gh.$$

Proof: We need to check the following:

- L is well-defined, namely L_g is a bijective function, for every $g \in G$: indeed, we have $L_g \circ L_{g^{-1}} = \mathrm{id}_G = L_{g^{-1}} \circ L_g$, so that $L_g^{-1} = L_{g^{-1}}$.
- L is a homomorphism: this follows from noticing that L is the homomorphism of groups associated to the action of G on G

$$G \times G \to G\ ;\ (g, h) \mapsto gh,$$

  defined in Fundamental Example 8.1.4.

- L is injective: suppose that L_g is the identity function (so that $g \in \ker L$). Then,

$$e = L_g(e) = ge = g \implies \ker L = \{e\}.$$

□

Why does Cayley's Theorem enable us to realise G as permutations of some set? Since the map L is injective then we have that G is isomorphic[2] to im $G \subset \text{Perm}(G)$ so that

G can be realised as a (sub)group of permutations of the set G.

9.3 Orbit-Stabiliser Theorem

Theorem 9.3.1 (Orbit-Stabiliser Theorem). *Let G be a finite group acting on the set S, $x \in S$. Then,*

$$|\mathcal{O}_x| = |G|/|Stab_G(x)|.$$

In particular,

the size of an orbit divides the order of G.

Proof: Denote $H = \text{Stab}_G(x)$. Then, using Lagrange's Theorem, it suffices to show that there is a bijection

$$\mathcal{O}_x \to G/H.$$

Define

$$f : \mathcal{O}_x \to G/H \; ; \; y = g \cdot x \mapsto gH.$$

We need to check that f is well-defined: namely, suppose that we have $y = g \cdot x$ and $y = g' \cdot x$. Then, we need to ensure that

$$g'H = f(y) = gH,$$

so that f is a function. As $g \cdot x = g' \cdot x$ then $x = g^{-1} \cdot (g' \cdot x) = (g^{-1}g') \cdot x$, then $g^{-1}g' \in \text{Stab}_G(x) = H$ and $gH = g'H$.

f **is injective**: suppose that $y = g \cdot x, y' = g' \cdot x$ and $f(y) = f(y')$. Then,

$$gH = g'H \implies g^{-1}g' \in H \implies x = g^{-1}g' \cdot x \implies y = g \cdot x = g' \cdot x = y'.$$

f **is surjective**: let $gH \in G/H$. If $y = g \cdot x \in \mathcal{O}_x$ then $f(y) = gH$. □

Corollary 9.3.2. *Let G be a finite group. The size of a conjugacy class in G divides the order of G.*

Proof: Consider the action of G on itself by conjugation. Then, an orbit of this action is a conjugacy class in G, and the result follows from the Orbit-Stabiliser Theorem. □

Example 9.3.3. 1. The group $\mathbb{Z}/9\mathbb{Z}$ acts on the set $\mathbb{Z}/3\mathbb{Z}$ by

$$\bar{i} \cdot \bar{a} \overset{def}{=} \overline{a + 2i}, \quad \bar{i} \in \mathbb{Z}/9\mathbb{Z}, \bar{a} \in \mathbb{Z}/3\mathbb{Z}.$$

If $\bar{i} \in \text{Stab}_{\mathbb{Z}/9\mathbb{Z}}(\bar{a})$ then $\overline{a + 2i} = \bar{a}$, so that $(a + 2i) - a = 2i$ is divisible by 3, which means that i is divisible by 3 (because 3 is prime). Conversely, if i is divisible by 3 then $\bar{i} \in \text{Stab}_{\mathbb{Z}/9\mathbb{Z}}(\bar{a})$; thus, $\text{Stab}_{\mathbb{Z}/9\mathbb{Z}}(\bar{a}) = \{\bar{0}, \bar{3}, \bar{6}\}$. Hence, the Orbit-Stabiliser Theorem implies that

$$|\mathcal{O}_{\bar{1}}| = 9/3 = 3 \implies \mathcal{O}_{\bar{1}} = \mathbb{Z}/3\mathbb{Z}.$$

[2] The isomorphism being defined by L!

2. Let S_5 act on itself by conjugation. Theorem 9.1.4 tells us that two elements $\sigma, \tau \in S_n$ are conjugate precisely when they have the same cycle type; the Orbit-Stabiliser theorem now allows us to determine how many elements there are of a given cycle type. For example, there are 20 elements in S_5 with cycle type $(3, 2)$. Indeed, the element $(123)(45) \in S_5$ has the following stabiliser

$$\mathrm{Stab}_{S_5}((123)(45)) = \{\sigma \in S_5 \mid (\sigma(1)\sigma(2)\sigma(3))(\sigma(4)\sigma(5)) = (123)(45)\}.$$

This is because

$$\sigma \cdot (123)(45) \cdot \sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3))\,(\sigma(4)\sigma(5))\,.$$

Now, $(123) = (\sigma(1)\sigma(2)\sigma(3))$ if and only if $\sigma(i+1) = \sigma(i) + 1 \mod 3$, for $i \in \{1, 2, 3\}$. This means that $\sigma(\{1, 2, 3\}) = \{1, 2, 3\}$ and σ, when restricted to $\{1, 2, 3\}$, is completely determined by what $\sigma(1)$ is equal to; thus, there are three such choices. Similarly, σ, when restricted to $\{4, 5\}$, is completely determined by what $\sigma(4)$ is equal to, and there are two such choices. Hence, there are $2.3 = 6$ such functions and $|\mathrm{Stab}_{S_5}((123)(45))| = 2.3 = 6$. Now, $|S_5| = 5! = 120$, so that the number of conjugates of $(123)(45)$ is 120/6=20.

Furthermore, this calculation shows that there are 20 elements in S_5 of order 6 - the elements of cycle type $(3, 2)$ are precisely the elements in S_5 of order 6.

9.4 Application: p-groups

In this section we will see that the Orbit-Stabiliser Theorem implies some restrictions on how certain groups can act on sets.

Definition 9.4.1 (p-group)**.** A finite group G is a p-**group** if the order of G is p^r, for some prime p and $r > 0$.

Example 9.4.2. 1. Let p be a prime. Then, $G = \mathbb{Z}/p^r\mathbb{Z}$ is a p-group whenever $r > 0$.

2. Consider the vector space $\mathbb{F}_p^r$. Then, $(\mathbb{F}_p^r, +)$ is a p-group.

3. The group of unit quaternions $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ is a 2-group.

These examples show that a p-group need not be cyclic nor abelian, in contrast to a group whose order is a prime p (the case $r = 1$).

The Orbit-Stabiliser Theorem has some useful consequences whenever a p-group acts on a finite set S.

Theorem 9.4.3 (Fixed point congruence for p-groups)**.** *Let G be a p-group acting on the finite set S. Suppose there are k fixed points of this action. Then,*

$$k \equiv |S| \mod p.$$

Proof: If $x \in S$ is a fixed point then the orbit through x admits a straightforward description: $\mathcal{O}_x = \{x\}$. The Orbit-Stabiliser Theorem implies that the size of any orbit must divide $|G| = p^r$. Hence, if an orbit contains more than one element then it must have size divisible by p. Thus, if $\mathcal{O}_1, \ldots, \mathcal{O}_s$ are the distinct orbits in S, then there are exactly k orbits consisting of one element. Assume that $|\mathcal{O}_1| = \ldots = |\mathcal{O}_k| = 1$. Then, by the Orbit Decomposition Formula,

$$|S| = |\mathcal{O}_1| + \ldots + |O_s| = k + |\mathcal{O}_{k+1}| + \ldots + |\mathcal{O}_s| \equiv k \mod p.$$

□

Corollary 9.4.4. *Let G be a p-group. Suppose that G acts on S and $|S| \not\equiv 0 \mod p$. Then, there exists a fixed point of this action.*

Proof: If there is not a fixed point of this action then Theorem 9.4.3 implies that

$$|S| \equiv 0 \mod p.$$

This contradicts the assumption on $|S|$ in the statement of the result. □

Here is an example of how we can use these 'fixed-point results':

Theorem 9.4.5. *Let G be a p-group. Then, there exists nontrivial $g \in G$ such that $g^p = e$.*

Proof: Assume $|G| = p^r$. Define

$$S = \{(g_0, \dots, g_{p-1}) \mid g_0, \dots, g_{p-1} \in G,\ g_0 \cdots g_{p-1} = e\}.$$

Suppose $(g_0, \dots, g_{p-1}) \in S$. If $g_0, \dots, g_{p-2} \in G$ are arbitrary then $g_{p-1} = (g_0 \cdots g_{p-2})^{-1}$. Hence, $|S| = (p^r)^{p-1} = p^{r(p-1)}$.

Now, if $(g_0, \dots, g_{p-1}) \in S$ then so is $(g_1, \dots, g_{p-1}, g_0)$: $g_0^{-1} = g_1 \cdots g_{p-1}$ and we always have

$$g_0 g_0^{-1} = g_0^{-1} g_0 = e.$$

Hence, we can define an action of $H = \mathbb{Z}/p\mathbb{Z}$ on S as follows: for $\bar{i} \in \mathbb{Z}/p\mathbb{Z}$

$$\bar{i} \cdot (g_0, \dots, g_{p-1}) \overset{def}{=} (g_{\overline{0+i}}, \dots, g_{\overline{p-1+i}})$$

where the subscript $\overline{x}$ denotes $x \mod p$ (by some abuse of notation). For example,

$$\overline{2} \cdot (g_0, \dots, g_{p-1}) = (g_2, g_3, \dots, g_{p-1}, g_0, g_1).$$

So the action of H is by cyclically shifting the entries of an element of S.

Since $(e, \dots, e)$ is a fixed point, Theorem 9.4.3 implies that the number of fixed points is a positive multiple of p. Any fixed point is of the form $(g, \dots, g)$, for some $g \in G$, and since $(g, \dots, g) \in S$ then $g^p = e$. □

10 Lecture 10 - Sylow's Theorems.

Previous lecture - Next lecture

Keywords: Sylow *p*-subgroup. Sylow's Theorems.

Lagrange's Theorem gives a necessary condition on the order of a subgroup H of a finite group G - the order of H divides the order of G. This gives a tight restriction on the potential subgroups of any finite group G.

Is this a sufficient condition? That is: if k divides the order of G then is there a subgroup of G of order k? A glance at some small groups (of order less than 10) would support this claim. However, **this statement is false**: for example, there is no subgroup of T_+, the group of rotational symmetries of the tetrahedron (which has order 12), of order 6.

This lecture is concerned with a sufficient condition for a subgroup of a finite group to exist:

> **if p is a prime such that p^r divides the order of G, with r maximal, then there exists a subgroup of G of order p^r.**

Moreover, we will obtain strong conditions relating all possible such subgroups.

10.1 Sylow's Theorems

Define

$$\mathrm{Syl}_p \overset{def}{=} \{H \subset G \mid H \in \mathrm{Sub}(G), |H| = p^r\}.$$

A subgroup $H \in \mathrm{Syl}_p$ will be called a **Sylow p-subgroup of G**.

Most of this lecture is concerned with the proof of the following result:

Theorem 10.1.1 (Sylow)**.** *Let G be a finite group of order n. Suppose that $n = p^r m$, where p is a prime, $m \neq 1$, and p does not divide m. Then,*

($SYL1$) *There exists a Sylow p-subgroup of G.*

($SYL2$) *All Sylow p-subgroups are conjugate and any p-subgroup of G is contained in a Sylow p-subgroup.*

($SYL3$) *If k_p is the number of Sylow p-subgroups then $k_p \equiv 1 \mod p$.*

Then,

- SYL1 is equivalent to showing that $\mathrm{Syl}_p \neq \varnothing$;
- if we let G act on Syl_p by conjugation - $g \cdot H = gHg^{-1}$ - then SYL_2 is equivalent to showing that there is exactly one orbit of this action;
- SYL3 is equivalent to showing that $|\mathrm{Syl}_p| \equiv 1 \mod p$.

To establish SYL1, SYL2, SYL3 we consider G acting on several sets, illustrating the far-reaching consequences of group actions.

Proof: Let G be a finite group of order n, with $n = p^r m$, $m \neq 1$ and $\gcd(p, m) = 1$. In particular, n **is not a prime power** (otherwise the result is trivial!).

SYL1: let $X = \{A \in P(G) \mid |A| = p^r\}$. Then, $|X| = \binom{n}{p^r}$ and $|X| \not\equiv 0 \mod p$.[1]

We define an action of G on X as follows,

$$G \times X \to X \ ; \ (g, A) \mapsto g \cdot A \overset{def}{=} gA.$$

[1] This is a homework/worksheet problem.

There must exist an orbit $\mathcal{O}$ such that $|\mathcal{O}| \not\equiv 0 \mod p$, by the condition on $|X|$ given above; moreover, since $|\mathcal{O}|$ divides n, by the Orbit-Stabiliser Theorem, then $|\mathcal{O}|$ divides m. Suppose that $\mathcal{O} = \mathcal{O}_A$ for some $A \subset G$, and denote $S = \mathrm{Stab}_G(A)$; the Orbit-Stabiliser Theorem implies that $|S|$ is divisible by p^r, by the restriction on $|\mathcal{O}|$ just stated, in particular $|S| \geq p^r$. Fix $a \in A$. For $g \in S$ we have $ga \in A$, so that $g \in Aa^{-1}$. Since g is arbitrary then $S \subset Aa^{-1}$ and $|S| \leq |Aa^{-1}| = p^r$. Hence, $|S| = p^r$ and $S \in \mathrm{Syl}_p$.

SYL2: Let $S \in \mathrm{Syl}_p$, H a p-subgroup of G. Consider $Y = G/S$ and let H act on Y via

$$H \times Y \to Y \ ; \ (h, gS) \mapsto h \cdot gS \overset{def}{=} hgS.$$

As $|Y| = m$ and $\gcd(p, m) = 1$, the Orbit Decomposition Formula implies that some orbit $\mathcal{O}$ must satisfy $|\mathcal{O}| \not\equiv 0 \mod p$ - else, every orbit has size divisible by p so that $|Y|$ is divisible by p - and the Orbit-Stabiliser Theorem then gives $|\mathcal{O}|$ divides $|H|$, a power of p. Hence, $|\mathcal{O}| = 1$ so that some coset gS must satisfy $hgS = gS$, for every $h \in H$. Hence, $g^{-1}hgS = S$, for every $h \in H$, and $g^{-1}hg \in S$, for every $h \in H$. Thus, $g^{-1}Hg \subset S$ and, $H \subset gSg^{-1}$. If $H \in Syl_p$ then $H = gSg^{-1}$ because $|H| = |S| = |gSg^{-1}|$, showing that any other Sylow p-subgroup H is conjugate to S.

SYL3: Let $S \in \mathrm{Syl}_p$. Then, S acts on Syl_p by conjugation:

$$S \times \mathrm{Syl}_p \to \mathrm{Syl}_p \ ; \ (g, H) \mapsto g \cdot H \overset{def}{=} gHg^{-1}.$$

If $S' \in \mathrm{Syl}_p$ is such that $g \cdot S' = S'$, for every $g \in S$, then

$$gS'g^{-1} = S', \text{ for every } g \in S, \text{ implying that } SS' = S'S.$$

Thus, $K = SS'$ is a subgroup of G and S, S' are normal subgroups of K. In addition, S' is a Sylow p-subgroup of K, hence conjugate to S by SYL2. So, there is $k \in K$ with

$$S = kS'k^{-1} = S',$$

the last equality a consequenc of S' being normal in K. Hence, we have seen that the only fixed point in Syl_p (under the action of S) is S. As S is a p-group then

$$\text{no. of fixed points of action } \equiv |\mathrm{Syl}_p| \mod p,$$

by Theorem 9.4.3, and $|\mathrm{Syl}_p| \equiv 1 \mod p$.

□

Corollary 10.1.2. *The number of Sylow p-subgroups is equal to the index of $N_G(S)$, where $S \in \mathrm{Syl}_p$.*

Proof: G acts on Syl_p by conjugation and SYL2 implies that there is only one orbit $\mathcal{O}$ of this action; hence, $\mathrm{Syl}_p = \mathcal{O}$. If $S \in \mathrm{Syl}_p$ then $\mathrm{Stab}_G(S) = N_G(S)$ and the Orbit-Stabiliser Theorem gives

$$|\mathrm{Syl}_p| = |\mathcal{O}| = |G|/|N_G(S)| = [G : N_G(S)].$$

□

Corollary 10.1.3. *Let $|G| = p^r m$, with $\gcd(p, m) = 1$. If k_p is the number of Sylow p-subgroups in G, then k_p divides m.*[2]

Proof: Worksheet problem. □

10.2 An application: groups of order pq

Let G be a group of order $n = pq$, where p and q are distinct primes and $p > q$. Then, Sylow's Theorems imply that there exist subgroups H, K of G of order p, q respectively. As H and K have prime orders then they are cyclic.

[2] Updated 7/7/2014.

Consider the subgroup H of order p - we will see that H is normal. Recall that H is normal if and only if $gHg^{-1} = H$, for every $g \in G$, and that this is equivalent to $\mathrm{Norm}_G(H) = G$.

$\mathrm{Norm}_G(H)$ is a subgroup of G so that its order divides G - hence, $|\mathrm{Norm}_G(H)|$ equals either $1, p, q$ or pq. Moreover, $H \subset \mathrm{Norm}_G(H)$ so that p divides $\mathrm{Norm}_G(H)$ - hence, $|\mathrm{Norm}_G(H)|$ is equal to p or pq. If $|\mathrm{Norm}_G(H)| = p$ then $|\mathrm{Syl}_p| = q$, by Corollary 10.1.2, and SYL3 implies that

$$q = |\mathrm{Syl}_p| \equiv 1 \mod p.$$

As $q < p$ then $q \equiv 1 \mod p$ if and only if $q = 1$. Hence, it is not possible that $q \equiv 1 \mod p$ so that $|\mathrm{Norm}_G(H)| \neq p$, implying that $|\mathrm{Norm}_G(H)| = pq$. Thus, $\mathrm{Norm}_G(H) = G$ and H is normal.

We have just shown

every group of order pq has a proper, nontrivial normal subgroup

11 Lecture 11 - Product and Quotient groups.

Previous lecture - Next lecture

Keywords: Product Group. Quotient group. Canonical homomorphism.

In this lecture we introduce two ways to construct a new group from given groups. The product construction takes any two groups and builds a new one which is larger than either. The quotient construction takes one group, and a normal subgroup within it, and builds a new group which is smaller than the original.

11.1 Direct products

Let G be a group. We have seen how to construct a new group - the quotient group G/N - from G given a normal subgroup N of G. In general, it is not so straightforward to identify the group G/N; that is, it might be difficult to determine if the group G/N is a group that we are familiar with (for example, a symmetric group. a dihedral group, a cyclic group etc.).

Consider the following question: **given a group G and a group H, is there a group M such that G is a normal subgroup of M and M/G is isomorphic to H?** We will see that the answer is **yes** and is actually quite simple to establish.

Definition 11.1.1. Let G, H be two groups. The **direct product of G and H** is the group $(G \times H, *)$, where

$$G \times H = \{(g, h) \mid g \in G, h \in H\}, \quad \textit{(the set of ordered pairs)}$$

$$(g, h) * (g', h') \overset{def}{=} (gg', hh').$$

In particular, the law of composition in $G \times H$ is '**component-wise composition**'.

The identity element in $G \times H$ is $e_{G \times H} = (e_G, e_H)$, and $(g, h)^{-1} = (g^{-1}, h^{-1})$.

Example 11.1.2.

1. Let $G = \mathbb{Z}/3\mathbb{Z}$, $H = \mathbb{Z}/4\mathbb{Z}$. Then,

$$G \times H = \{(\bar{i}, \bar{j}) \mid \bar{i} \in \mathbb{Z}/3\mathbb{Z}, \bar{j} \in \mathbb{Z}/4\mathbb{Z}\}.$$

   We have $|G \times H| = 12$, and $e_{G \times H} = (\bar{0}, \bar{0})$. Also,

$$(\bar{2}, \bar{2}) * (\bar{1}, \bar{2}) = (\bar{2} + \bar{1}, \bar{2} + \bar{2}) = (\bar{0}, \bar{0}),$$

   so that the inverse of $(\bar{2}, \bar{2})$ in $G \times H$ is $(\bar{1}, \bar{2})$.

   Notice that the order of $x = (\bar{1}, \bar{1})$ is 12, so that $G \times H$ is a cyclic group isomorphic to $\mathbb{Z}/12\mathbb{Z}$.[1]

2. If $G = \mathbb{Z}/4\mathbb{Z}$, $H = \mathbb{Z}/2\mathbb{Z}$ then $G \times H$ has order 8. However, $G \times H$ is abelian but not cyclic - hence, not isomorphic to $\mathbb{Z}/8\mathbb{Z}$.

11.2 Quotient groups

Let G be a group and $N \subset G$ a **normal** subgroup - it is extremely important that N is normal in what follows. Consider the set of (left) cosets of N in G, denoted G/N. Then, an element of the set G/N is a (left) coset of N in G. In fact, since N is normal in G, we have that $gNg^{-1} = N$, for every $g \in G$. This condition is equivalent to the equality of sets $gN = Ng$, for every every $g \in G$; hence,

if N is normal, $g \in G$, then the left coset of N containing g is also a right coset of N containing g

[1] In general, if $\gcd(m, n) = 1$ then $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is cyclic of order mn.

In what follows we will investigate some of the consequences of this fact.

Definition 11.2.1. Let G be a group, $N \subset G$ a normal subgroup. Define the **quotient group of** G **by** N to be $(G/N, *)$, where we define

$$* : G/N \times G/N \to G/N \; ; \; (gN, hN) \mapsto gN * hN \overset{def}{=} ghN.$$

The definition of $*$ above has some potential ambiguity: if $gN = g'N$ and $hN = h'N$ (so that the cosets of g and g' are equal, and the cosets of h and h' are equal), then we need to ensure that $ghN = g'h'N$, otherwise $*$ is not a function. However, we need not worry: suppose that $gN = g'N$ and $hN = h'N$. Thus, there exists $n, m \in N$ such that

$$gn = g', \; hm = h'.$$

Moreover, since N is normal, then $nh \in Nh = hN$, and there is $p \in N$ such that $nh = hp$. Thus,

$$g'h' = gnhm = gh(pm) \in ghN,$$

and $g'h'N = ghN$.[2]

Of course, we need to justify the phrase 'quotient group':

Theorem 11.2.2. *Let G be a group, N a normal subgroup. Then, $(G/N, *)$, where $*$ is defined above, is a group.*

Proof: We need to show that $(G/N, *)$ satisfies G1, G2, G3, G4 of Definition 3.1.1.

G1: this is precisely what we have established above.

G2: define $e_{G/N} \overset{def}{=} e_G N$. Then, for any $g \in G$ we have

$$e_{G/N} * gN = e_G N * gN = e_G gN = gN = g e_G N = gN * e_G N = gN * e_{G/N}.$$

G3: homework/worksheet.

G4: homework/worksheet.

□

Remark 11.2.3. In general, it is not so straightforward to determine what the quotient group G/N is for given G and N. However, we can determine some information about G/N:

- if G is finite then Lagrange's Theorem gives the order of G/N - we have $|G/N| = |G|/|N|$;
- if G is abelian then G/N is abelian;
- if G is cyclic then G/N is cyclic.

Beware, **the converse of these statements are false in general**.

Example 11.2.4. 1. Let $G = D_8 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$. Then, $N = \{e, r, r^2, r^3\}$ is a normal subgroup of G and G/N is isomorphic to $\mathbb{Z}/2\mathbb{Z}$: indeed, we have $|G/N| = |G|/|N| = 2$, so that G/N is a group of prime order and so must be isomorphic to a cyclic group (THEOREM ???) of order 2.

Note that G/N is cyclic (and abelian) while G is not cyclic (and not abelian).

[2] Recall that left cosets are equivalence classes of a particular equivalence relation, and equivalence classes are either disjoint or equal.

2. Let $G = Q = \{\pm 1, \pm i, \pm j, \pm k\}$, the group of unit quaternions with identity element $e = 1$. Then, $N = \{1, -1\}$ is a normal subgroup of G and the quotient group G/N has order 4. Every group of order 4 is isomorphic to either $\mathbb{Z}/4\mathbb{Z}$ or the subgroup

$$K_4 = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \{1, -1\} \right\} \subset \mathrm{Mat}_2(\mathbb{Z}).$$

Note that K_4 is not isomorphic to $\mathbb{Z}/4\mathbb{Z}$: indeed, K_4 does not possess an element of order 4.

We will see that G/N is isomorphic to K_4 by showing that there is no element of order 4 in G/N. Note that

$$G/N = \{eN, iN, jN, kN\},$$

because $iN = \{\pm i\}, jN = \{\pm j\}, kN = \{\pm k\}$, and, for example,

$$(iN)^2 = iN * iN = i^2 N = (-1)N = eN.$$

Similarly, $(jN)^2 = (kN)^2 = eN$. Hence, each of the nontrivial elements in G/N has order 2 and the claim follows. In fact, the isomorphism from G/N is

$$f : K_4 \to G/N \; ; \begin{array}{ccc} [1\ 1] & \mapsto & eN \\ [1\ -1] & \mapsto & iN \\ [-1\ 1] & \mapsto & jN' \\ [-1\ -1] & \mapsto & kN \end{array}$$

where $[a\ b]$ denotes the matrix $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$. f is a bijection by construction and it is not too hard to check that f is a homomorphism: for example,

$$f([1\ -1] * [-1\ 1]) = f([-1\ -1]) = kN,$$

$$f([1\ -1]) * f([-1\ 1]) = iN * jN = ijN = kN,$$

so that

$$f([1\ -1] * [-1\ 1]) = f([1\ -1]) * f([-1\ 1]).$$

3. Let G be a group, $H \subset G$ **any** subgroup. Then, H is a normal subgroup of $\mathrm{Norm}_G(H)$ always (but not necessarily a normal subgroup of G). Hence, we can consider the quotient group $\mathrm{Norm}_G(H)/H$.

For example, if $G = \mathrm{GL}_3(\mathbb{Z})$ and $D_3 \subset G$ is the subgroup of diagonal (invertible) matrices, then it can be shown that $\mathrm{Norm}_G(D_3)/D_3$ is isomorphic to S_3. In general, if $G = \mathrm{GL}_n(\mathbb{Z})$ and $D_n \subset G$ is the subgroup of diagonal matrices, then $\mathrm{Norm}_G(D_n)/D_n$ is isomorphic to S_n.

12 Lecture 12 - The canonical homomorphism and First Isomorphism Theorem.

Previous lecture - Next lecture

Keywords: Quotient group. Canonical Homomorphism

12.1 The canonical homomorphism

If G is a group and $N \subset G$ is a normal subgroup, we have seen how we can obtain a new group, the quotient group G/N. Recall from the section on Equivalence Relations that to any equivalence relation R defined on a set A we can consider **the natural mapping associated to** R

$$\pi : A \to A/\sim \ ; \ a \mapsto [a].$$

Since G/N is the set of equivalence classes of a certain equivalence relation defined on G - arising from the left N-partition - we have the natural mapping

$$\pi : G \to G/N \ ; \ g \mapsto gN.$$

In the given situation we will denote the above natural mapping by π_N, so that

$$\pi_N : G \to G/N \ ; \ g \mapsto gN,$$

and call it **the canonical homomorphism (associated to** N**)** or simply **the quotient homomorphism of** G/N.

Lemma 12.1.1. *Let G be a group, N a normal subgroup. Then,*

a) *π_N is a group homomorphism.*

b) $\ker \pi_N = N$.

c) $\operatorname{im} \pi_N = G/N$.

Proof:

a) let $g, h \in G$. Then,
$$\pi_N(gh) = ghN = gN * hN = \pi_N(g) * \pi_N(h).$$
Thus, π_N is a group homomorphism.[1]

b) Let $n \in N$. Then, $\pi_N(n) = nN = N = eN = e_{G/N}$, so that $n \in \ker \pi_N$. Hence, $N \subset \ker \pi_N$. We will now show that $\ker \pi_N \subset N$: if $g \in \ker \pi_N$ then $\pi_N(g) = e_{G/N}$. Thus, $gN = eN$ implying that $g \in N$.

c) This is straightforward.

□

In fact, the quotient homomorphism is 'the only' surjective homomorphism with domain G and kernel N: this is (essentially) what the First Isomorphism Theorem states. First, we need the following

Lemma 12.1.2. *Let $f : G \to H$ be a group homomorphism. Then, $\ker f \subset G$ is a normal subgroup.*

Proof: Homework/worksheet. □

Thus, since every normal subgroup is the kernel of some homomorphism (the quotient homomorphism), we obtain the following slogan

> **the normal subgroups of G <u>are precisely</u> those subgroups that are kernels**

[1] In fact, the definition of the law of composition on the quotient group is defined so that the natural mapping associated to the equivalence relation definiing G/N is a group homomorphism.

12.2 First Isomorphism Theorem

In this section we prove an extremely useful result about quotient groups. Starting with a homomorphism $f\colon G \to H$, it may not be the case that f is either surjective or injective. The theorem and its proof explain how to "modify" f to produce a new, but closely related map which is an isomorphism. The basic idea is to replace the codomain H with $\text{im } f$, forcing surjectivity, and to replace the domain G by the quotient $G/\ker f$, which turns out to force injectivity. The theorem is useful in many contexts, in particular when trying to understand the structure of a given quotient group.

Theorem 12.2.1 (First Isomorphism Theorem)**.** *Let $f : G \to H$ be a group homomorphism. Then, if we denote $K = \ker f$, the* **induced homomorphism**

$$\overline{f} : G/K \to \text{im } f \ ; \ gK \mapsto f(g),$$

is an isomorphism. In particular, if G is finite then $|\text{im } f| = |G|/|\ker f|$.

Proof: There are several things we must establish:

- the map $\overline{f}$ is well-defined, so that its definition does not depend on the choice of representative we have chosen for a coset in G/K. So, if $gK = g'K$ we need to show that $\overline{f}(gK) = \overline{f}(g'K)$ (otherwise $\overline{f}$ is not a function!). Now, $gK = g'K$ implies that there is $k \in K$ such that $g = g'k$. Then,
$$\overline{f}(gK) = f(g) = f(g'k) = f(g')f(k) = f(g')e_H = f(g') = \overline{f}(g'K).$$
- $\overline{f}$ is a homomorphism: let $gK, hK \in G/K$. Then,
$$\overline{f}(gK * hK) = \overline{f}(ghK) = f(gh) = f(g)f(h) = \overline{f}(gK)\overline{f}(hK).$$
- $\overline{f}$ is injective: if $hK \in \ker \overline{f}$ then
$$\overline{f}(hK) = e_H \implies f(h) = e_H \implies h \in K = \ker f \implies hK = eK.$$

  Hence, $\ker \overline{f} = \{e_{G/K}\}$ and $\overline{f}$ is injective.
- $\overline{f}$ is surjective: let $h \in \text{im } f$. Then, there is some $g \in G$ such that $f(g) = h$. Hence, we have $\overline{f}(gK) = f(g) = h$.

□

Remark 12.2.2. The First Isomorphism Theorem (Theorem 12.2.1) is the group-theoretic analogue of the Rank Theorem from linear algebra (in a sense that can be made precise). When G is finite, this result implies that there is a strong restriction on the existence of nontrivial homomorphisms with domain G.

Example 12.2.3.

1. Let $f : G \to H$ be a group a homomorphism, with $|G| = 15, |H| = 28$. Then, f must be the trivial homomorphism
$$f : G \to H \ ; \ g \mapsto e_H.$$

   Indeed, since $\text{im } f \subset H$ is a subgroup then $|\text{im } f|$ must divide 28. Theorem 12.2.1 implies that $|\text{im } f|$ must also be a divisor of $|G| = 15$. However, $\gcd(15, 28) = 1$ so that $|\text{im } f| = 1$ and $\text{im } f = \{e_H\}$ is the trivial subgroup of H.

2. Suppose that $f : D_{10} \to \mathbb{Z}/5\mathbb{Z}$ is a surjective homomorphism of groups. Thus, $\text{im } f = \mathbb{Z}/5\mathbb{Z}$ so that $D_{10}/\ker f \cong \mathbb{Z}/5\mathbb{Z}$, by Theorem 12.2.1. We must have that $|\ker f| = |D_{10}|/|\text{im } f| = 10/5 = 2$, so that $\ker f = \{e, s\}$, for some $s \in D_{10}$ of order 2. The only elements of order 2 are precisely the reflections of the pentagon. Now, we can write $D_{10} = \{e, r, \dots, r^4, s, sr, \dots, sr^4\}$, where r is '*rotate by* $2\pi/5$ *counterclockwise*'. Thus, we must have
$$f(srs) = f(r^{-1}) \implies f(s) + f(r) + f(s) = -f(r) \implies f(r) + f(r) = \overline{0} \in \mathbb{Z}/5\mathbb{Z}.$$

   Since there are no elements of order two in $\mathbb{Z}/5\mathbb{Z}$ this last equality is impossible, so that our assumption of the existence of a surjective homomorphism $f : D_{10} \to \mathbb{Z}/5\mathbb{Z}$ is false. Hence, there are no surjective homomorphisms $D_{10} \to \mathbb{Z}/5\mathbb{Z}$.

13 Lecture 13 - Finite abelian groups.

Previous lecture - Next lecture

Keywords: Structure theorem of finite abelian groups.

This lecture and the next are optional reading. They discuss how to completely characterize finite abelian groups. This lecture shows how to decompose a finite abelian group into a product of p-groups; the next shows how to further decompose the p-group factors.

We begin with a result that shows how to recover G and H as quotients of the product $G \times H$:

Theorem 13.0.1. *Let G, H be groups. Then,*

$$G \times \{e_H\} = \{(g, e_H) \mid g \in G\} \subset G \times H,$$

is a normal subgroup in $G \times H$ isomorphic to G. Moreover, the quotient group $G \times H/G \times \{e_H\}$ is isomorphic to H.

Proof: Let $K = G \times \{e_H\}$. Then, K is a subgroup: if $(g, e_H), (g', e_H) \in K$ then $(g, e_H) * (g', e_H)^{-1} = (g(g')^{-1}, e_H) \in K$. Furthermore, if $(g, e_H) \in K$ and $(z, h) \in G \times H$ then

$$(z, h) * (g, e_H) * (z, h)^{-1} = (zgz^{-1}, zz^{-1}) = (zgz^{-1}, e_H) \in K \implies (z, h)K(z, h)^{-1} = K,$$

so that K is normal in $G \times H$. The function

$$\alpha : G \to K \ ; \ g \mapsto (g, e_H),$$

provides an isomorphism from G to K.

Now, define

$$\beta : H \to (G \times H)/K \ ; \ h \mapsto (e_G, h)K.$$

Then,

- β is a homomorphism: let $h, h' \in H$ then

$$\beta(hh') = (e_G, hh')K = ((e_G, h) * (e_G, h'))\, K = (e_G, h)K(e_G, h')K = \beta(h)\beta(h').$$

- β is injective: let $h \in \ker \beta$. Then,

$$\beta(h) = (e_G, e_H)K \implies (e_G, h)K = (e_G, e_H)K \implies (e_G, h) \in K \implies h = e_H.$$

- β is surjective: let $(g, h)K \in (G \times H)/K$. Then, $(g, h) = (e_G, h) * (g, e_H) \in (e_G, h)K$, and $(g, h)K = (e_G, h)K$. Then, $\beta(h) = (g, h)K$.

□

13.1 Structure Theorem of finite abelian groups

In this section we will prove the following

Theorem 13.1.1 (Structure Theorem of finite abelian groups)**.** *Let A be an abelian group with $|A| = p_1^{n_1} \cdots p_r^{n_r}$, where $p_1, \dots, p_r$ are distinct primes and $n_1, \dots, n_r \geq 1$. Then, A is isomorphic to a product*

$$U_1 \times U_2 \times \cdots \times U_r,$$

where U_i is a p_i-group and $|U_i| = p_i^{n_i}$.

Lemma 13.1.2. *Let G be a finite abelian group, $H \subset G$ a Sylow p-subgroup, for some prime p dividing $|G|$. Consider the subset*

$$K = \{g \in G \mid p \text{ does not divide } o(g)\}.$$

Then, K is a subgroup of G isomorphic to the quotient group G/H.

Proof: Since $o(e_G) = 1$, we see that $e_G \in K$ so that K is nonempty. Let $g, h \in K$ and denote $r = o(g), s = o(h) = o(h^{-1})$. Then, p does not divide r nor s so that p does not divide rs. Since

$$(gh^{-1})^{rs} = g^{rs}h^{-rs} = (g^r)^s(h^{-s})^r = e_G,$$

the order of gh^{-1} divides rs. Hence, p does not divide $o(gh^{-1})$ and $gh^{-1} \in K$, showing that K is a subgroup of G.

Consider the following map

$$\alpha : K \to G/H \ ; \ k \mapsto kH.$$

As $\alpha = \pi_H \circ i_K$ is the composition of two group homomorphisms, α is a group homomorphism; we will see that α is an isomorphism.

- α *is injective*: let $k \in \ker \alpha \subset K$. Then, $\alpha(k) = kH = e_{G/H} = eH$, implying that $k \in H$. As H is a p-group then every element has order equal to a power of p. However, p does not divide $o(k)$ so that the only possibility is $k = e \in K$ (as $o(k) = 1$).

- α *is surjective*: let $gH \in G/H$. Suppose that $|G| = p^a m$, with $\gcd(p, m) = 1$. Then, we can find integers $u, v \in \mathbb{Z}$ such that $p^a u + mv = 1$. Hence,

  $$g = g^1 = g^{p^a u} g^{mv}.$$

  Note that $e = (g^{p^a m})^u = (g^{p^a u})^m$, so that the order of $g^{p^a u}$ divides m; hence, $g^{p^a u} \in K$, because $\gcd(p, m) = 1$.

  Claim: $g^{mv} \in H$: notice that $(g^{mv})^{p^a} = e$ so that g^{mv} has order a power of p. Thus, the subgroup $\langle g^{mv} \rangle \subset G$ is a p-subgroup. Sylow's Theorem implies that a conjugate of $\langle g^{mv} \rangle$ is a subgroup of H, say $x\langle g^{mv} \rangle x^{-1} \subset H$. Since G is abelian then $xAx^{-1} = A$, for any subset $A \subset G$; in particular, $\langle g^{mv} \rangle = x\langle g^{mv} \rangle x^{-1} \subset H$ and $g^{mv} \in H$.

  Now, $g = g^{p^a u} g^{mv} \in g^{p^a u} H \implies gH = g^{p^a u} H$, with $g^{p^a u} \in K$, so that $\alpha(g^{p^a u}) = gH$ and α is surjective.

□

Lemma 13.1.3. *Let G be a finite abelian group, $H \subset G$ a Sylow p-subgroup for some prime p dividing $|G|$. Then, G is isomorphic to the direct product $H \times G/H$.*

Proof: Let G be a finite abelian group, $H \subset G$ a Sylow p-subgroup, and let K be the subgroup defined in Lemma 13.1.2.

Consider the function

$$\beta : H \times K \to G \ ; \ (h, k) \mapsto hk.$$

We will show that β is an isomorphism.

- β is a group homomorphism: homework/worksheet problem.

- β is injective: let $(h, k) \in \ker \beta$ then $\beta(hk) = hk = e_G$ so that $k = h^{-1}$. Since $o(h)$ is a power of p, and $o(k)$ is not divisible by k, the only possibility is that $o(h) = o(k) = 1$, so that $h = k = e_G$. Hence, $\ker \beta = \{(e_G, e_G)\}$.

- β is surjective: homework problem.

We combine this isomorphism with the one from Lemma 13.1.2 to obtain the desired isomorphism between G and $H \times G/H$. □

We are now in a position to prove Theorem 13.1.1.

Proof:[of Structure Theorem] Let A be abelian. If A is a p-group, for some prime p, (this is the case $r = 1$), then there is nothing to prove. We are going to proceed by induction on r: assume that the result is true for $r < k$, we will show it holds true for $r = k$.

So, let $r = k$ and consider the prime p_k. Sylow's Theorem (Theorem 10.1.1) implies the existence of a Sylow p_k-subgroup $U_k \subset A$ such that $|U_k| = p_k^{n_k}$, and U_k is normal as A is abelian. Hence, we can consider the (finite abelian) quotient group A/U_k. Since $|A/U_k| = |A|/|U_k| = p_1^{n_1} \cdots p_{k-1}^{n_{k-1}}$, the induction hypothesis implies that A/U_k is isomorphic to

$$U_1 \times \cdots \times U_{k-1},$$

with each U_i a p_i-group of order $p_i^{n_i}$. Lemma 13.1.3 implies that

$$A \cong (A/U_k) \times U_k \cong U_1 \times \cdots \times U_{k-1} \times U_k.$$

□

14 Lecture 14 - Finite abelian p-groups. The Hall polynomial.

Previous lecture - Next lecture

Keywords: Structure theorem of abelian p-groups. Type of an abelian p-group. Labelled Young diagrams, Hall polynomial.

The material from here on is optional reading and was not covered on the exam.

14.1 Structure Theorem of finite abelian p-groups

Recall that a p-group is a group G whose order is a power of a prime p.

Theorem 14.1.1. *Let A be a finite abelian group, $|A| = p^r$ for some prime p. Then, there exists unique integers $r_1 \geq r_2 \geq ... \geq r_k \geq 1$ such that A is isomorphic to*

$$(\mathbb{Z}/p^{r_1}\mathbb{Z}) \times (\mathbb{Z}/p^{r_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{r_k}\mathbb{Z}) .$$

Proof: We will not discuss the proof of this result - a supplementary note of the the proof will be posted online for those that are interested. The proof and its contents will not be examinable. □

Suppose that A is a finite abelian p-group, $B \subset A$ a subgroup. Then, Lagrange's Theorem implies that B is a finite abelian p-group; moreover, as $B \subset A$ is normal then we can consider the quotient group B/A and, again by Lagrange's Theorem, we have that B/A is a finite abelian group. Hence, we can find sequences of integers

$$s_1 \geq ... \geq s_l \geq 1, \quad \text{and} \quad t_1 \geq ... \geq t_m \geq 1,$$

such that

$$B \cong (\mathbb{Z}/p^{s_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{s_l}\mathbb{Z}) , \quad \text{and} \quad A/B \cong \left(\mathbb{Z}/p^{t_1}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p^{t_m}\mathbb{Z}\right) .$$

Definition 14.1.2. Let A be a finite abelian p-group. Then, since A is isomorphic to

$$(\mathbb{Z}/p^{r_1}\mathbb{Z}) \times (\mathbb{Z}/p^{r_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{r_k}\mathbb{Z}) .,$$

with $r_1 \geq r_2 \geq ... \geq r_k \geq 1$, we can associate a partition $\pi_A : (r_1, ... , r_k)$ to A - we call π_A **the type of** A.

14.2 Combinatorics of finite abelian p-groups of type (a, b)

For the remainder of this lecture we will only consider finite abelian p-groups A whose type is of the form $\pi_A : (a, b)$ - these are those finite abelian p-groups that are isomorphic to

$$(\mathbb{Z}/p^a\mathbb{Z}) \times (\mathbb{Z}/p^b\mathbb{Z}), \quad a \geq b \geq 1.$$

Let A be a finite abelian p-group (of type (a, b)), $B \subset A$ a subgroup. We are going to investigate the following

Questions: What are the allowed types of B? How many subgroups of A exist with a given type?

It suffices to consider the case $A = (\mathbb{Z}/p^a\mathbb{Z}) \times (\mathbb{Z}/p^b\mathbb{Z})$. Then, any element $g \in A$ can be written as an ordered pair

$$g = (\overline{x}, \overline{y}), \quad \overline{x} \in \mathbb{Z}/p^a\mathbb{Z},\ \overline{y} \in \mathbb{Z}/p^b\mathbb{Z}.$$

We will always assume that $0 \leq x \leq p^a - 1$ and $0 \leq y \leq p^b - 1$, so that we will simply write (x, y) instead of $(\overline{x}, \overline{y})$.

We are going to introduce a pictorial way of representing $g \in A$:

1. Write x and y in their 'base p' expansions
$$x = c_{a-1}p^{a-1} + c_{a-2}p^{a-2} + ... + c_1p + c_0,$$
$$y = d_{b-1}p^{b-1} + d_{b-2}p^{b-2} + ... + d_1p + d_0.$$
2. Define the **labelled Young diagram associated to g, denoted** $\mathrm{Yng}(g)$**,**
$$\begin{array}{|c|c|c|c|c|c|c|c|}\hline c_{a-1} & c_{a-2} & \cdots & \cdots & \cdots & \cdots & c_1 & c_0 \\ \hline d_{b-1} & d_{b-2} & \cdots & d_1 & d_0 & \multicolumn{3}{c}{} \\ \cline{1-5}\end{array}$$
If $c_i = 0$ (or $d_i = 0$) then we will leave the box empty. In particular,
$$\mathrm{Yng}(e_A) = \begin{array}{|c|c|c|c|c|c|c|c|}\hline & & \cdots & \cdots & \cdots & \cdots & & \\ \hline & & \cdots & & & \multicolumn{3}{c}{} \\ \cline{1-5}\end{array}$$
We will also refer to the unlabelled diagram $\mathrm{Yng}(e_A)$ as the **Young diagram of A (or π_A)**.

For example, the element $(3, 2) \in \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ would be represented as
$$\begin{array}{|c|c|c|}\hline & 1 & 1 \\ \hline 1 & & \multicolumn{1}{c}{} \\ \cline{1-2}\end{array}$$
since $a = 3$, $b = 2$ and
$$3 = 0.4 + 1.2 + 1.1, \quad 2 = 1.2 + 0.1.$$
Consider the 'multiplication by p' homomorphism
$$m_p : A \to A \,;\ (x, y) \mapsto (px, py).$$
We see that, in our pictorial representation,
$$\begin{array}{|c|c|c|c|c|c|c|}\hline c_{a-1} & c_{a-2} & \cdots & \cdots & \cdots & c_1 & c_0 \\ \hline d_{b-1} & d_{b-2} & \cdots & d_1 & d_0 & \multicolumn{2}{c}{} \\ \cline{1-5}\end{array} \mapsto \begin{array}{|c|c|c|c|c|c|c|}\hline c_{a-2} & \cdots & \cdots & \cdots & c_1 & c_0 & \\ \hline d_{b-2} & \cdots & d_1 & d_0 & & \multicolumn{2}{c}{} \\ \cline{1-5}\end{array}$$
For example, since $2 \cdot (3, 2) = (6, 0) \in \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, and $6 = 1.4 + 1.2$, then
$$\begin{array}{|c|c|c|}\hline & 1 & 1 \\ \hline 1 & & \multicolumn{1}{c}{} \\ \cline{1-2}\end{array} \mapsto \begin{array}{|c|c|c|}\hline 1 & 1 & \\ \hline & & \multicolumn{1}{c}{} \\ \cline{1-2}\end{array}$$
In a similar way, the 'multiplication by p^i' homomorphism
$$m_{p^i} : A \to A \,;\ (x, y) \mapsto (p^i x, p^i y),$$
shifts all entries in the labelled Young diagram $\mathrm{Yng}(x, y)$ i entries to the left.

Theorem 14.2.1. *Let A be a finite abelian p-group of type $\lambda = (a, b)$, $B \subset A$ a subgroup of type $\mu = (r_1, r_2, \dots, r_k)$. Then, $k \leq 2$ and $r_1 \leq a$, $r_2 \leq b$.*

Proof: It is straightforward to see that $r_1 \leq a$: otherwise there is an element $x \in B$ such that $x^{p^{r_1}} = e_B$, while $x^n \neq e$ for any $n < p^{r_1}$, implying that there is an element in A of order strictly larger than p^a. Considering how m_{p^a} operates on labelled Young diagrams, we see that m_{p^a} is the zero homomorphism on A, so that no such x can exist.

If $r_2 > b$, then we have $b < r_2 \leq r_1 \leq a$.

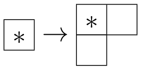
In A there are exactly $p^2 - 1$ elements of order p: every element $g \in A$ of order p is a nontrivial element in $\ker m_p$, and these are precisely those elements in A with $\mathrm{Yng}(g)$ having empty boxes in every column except the first, and there must be at least one box in the first column labelled. A quick count sees that there are $p^2 - 1$ possible ways to label the first column so that this holds. A similar argument shows that there exists $p^k - 1$ elements in B of order p. However, $B \subset A$ so that the maximum number of elements of order p is no larger than $p^2 - 1$. Hence, $p^k - 1 \leq p^2 - 1$ implying that $k \leq 2$. □

Remark 14.2.2. It is also possible to show the following: if A is a finite abelian p-group of type $\lambda = (a, b)$, $B \subset A$ a subgroup such that A/B has type $\mu = (s_1, \dots, s_l)$, then $l \leq 2$ and $s_1 \leq a$, $s_2 \leq b$.

If A is a finite abelian p-group of type $\lambda = (a, b)$, we have just seen that any subgroup B must have type ν such that the Young diagram of B 'sits inside' the Young diagram of A. Moreover, given any partition ν such that the corresponding Young diagram of ν sits inside the Young diagram of A, there is a subgroup $B \subset A$ of type ν.[1] **This gives an answer to the first question posed at the beginning of this lecture**. The remaining question - determining the number of subgroups of a given type - is more subtle.

14.3 The Hall polynomial

Consider the case $A = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so that $\pi_A = (2, 1)$, and the partition $\nu = (1)$. Then, the Young diagram of ν sits inside the Young diagram of π_A



so that there is a subgroup $B \subset A$ such that $B \cong \mathbb{Z}/2\mathbb{Z}$. Notice that the following subgroups are all isomorphic to $\mathbb{Z}/2\mathbb{Z}$

$$B_1 = \{(0,0),(0,1)\},\ B_2 = \{(0,0),(2,0)\},\ B_3 = \{(0,0),(2,1)\}.$$

In fact, this gives all such subgroups of A with type $\nu = (1)$, there are $3 = 2 + 1$ of them.

You can check that there are $4 = 3 + 1$ subgroups in $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ of type $\nu = (1)$, and $6 = 5 + 1$ subgroups in $\mathbb{Z}/25\mathbb{Z} \times 5\mathbb{Z}$ of type $\nu = (1)$. We will see that this type of behaviour is not coincidental; it is a consequence of the following *remarkable* Theorem due to Phillip Hall:

Theorem 14.3.1 (Hall polynomial - P. Hall)**.** *Let A be a finite abelian p-group of type λ (not necessarily of type (a, b)), μ, ν arbitrary partitions. Then, there exists a polynomial $g^{\lambda}_{\mu\nu}(t)$ with integer coefficients, called the* **Hall polynomial corresponding to** *λ, μ, ν, such that*

$$g^{\lambda}_{\mu\nu}(p) = \textit{no. of subgroups } B \subset A \textit{ of type } \nu, \textit{ such that } A/B \textit{ has type } \mu.$$

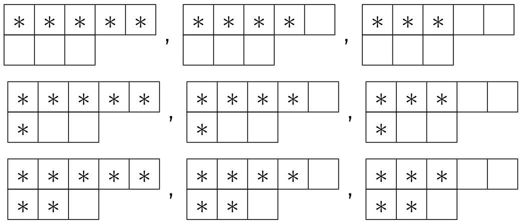
In particular, $g^{\lambda}_{\mu\nu}(t)$ is independent of p.

The proof of this result utilises requires techniques that are too sophisticated for a first class in algebra: it makes use of the pictorial description of elements of A and the **combinatorics of (skew) Young tableaux** and **Littlewood-Richardson combinatorics**, as well as facts on **discrete valuation rings**. However, we will content ourselves with a formula for $g^{\lambda}_{\mu\nu}(t)$ when $\nu = (r)$ - this enables the computation of the number of cyclic subgroups of A.

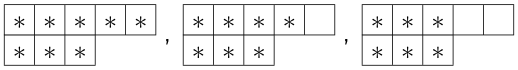
Suppose that A is a finite abelian p-group of type $\lambda = (a, b)$ (as before). Let μ be a partition whose Young diagram is a subdiagram of the Young diagram of λ, and such that the boxes leftover in the Young diagram of λ when we 'delete' the Young (sub)diagram of μ satisfy the following property: **each leftover box occupies a distinct column**.

If (λ, μ) is such a pair of partitions, and the number of leftover boxes equals r, then we say that (λ, μ) is r-**admissable**.

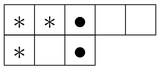
For example, if $\lambda = (5, 3)$ then the allowed μ are given below (the $*$'d subdiagrams):



[1] Homework/worksheet problem.



Also, we see that $\mu = (2,1)$ is not allowed:



there are two leftover boxes occupying the same column (the $\bullet$'d boxes).

Definition 14.3.2. Let (λ, μ) be r-admissable. Define

$$I(\lambda, \mu) = \{i \in \{1, \dots, a\} \mid \text{there is a leftover box in column } i, \text{ but no leftover box in column } i+1\}$$

For example, if $\lambda = (5,3), \mu = (4,2)$ then $I(\lambda, \mu) = \{3, 5\}$ (see above).

Theorem 14.3.3. *Let A be a finite abelian p-group of type $\lambda = (a, b)$, $\mu = (c, d)$ a partition such that (λ, μ) is r-admissable (for $r \leq a$). Then,*

$$g^{\lambda}_{\mu(r)} = \frac{t^{b-d}}{1-t^{-1}} \prod_{i \in I(\lambda,\mu)} (1 - t^{-m_i(\lambda)}).$$

Here, $m_i(\lambda)$ is the number of times i appears in the partition λ.

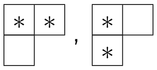
Corollary 14.3.4. *Let A be a finite abelian p-group of type $\lambda = (a, b)$. The number of cyclic subgroups of A of order p^r is equal to*

$$\sum_{\mu} g^{\lambda}_{\mu(r)}(p),$$

the sum being taken over all μ such that (λ, μ) is r-admissable.

Example 14.3.5.

1. Let A be a finite abelian p-group of type $\lambda = (2,1)$. Then, there are exactly two partitions μ for which (λ, μ) is 1-admissable - namely $\mu_1 = (2,0), \mu_2 = (1,1)$, as can be seen

   In this case $I(\lambda, \mu_1) = \{1\}$, $I(\lambda, \mu_2) = \{2\}$, so that

   $$g^{\lambda}_{\mu_1(r)}(t) = \frac{t}{1-t^{-1}}\left(1 - t^{-1}\right) = t,$$

   since $i = 1$ appears once in λ, and

   $$g^{\lambda}_{\mu_2(r)}(t) = \frac{1}{1-t^{-1}}\left(1 - t^{-1}\right) = 1,$$

   since $i = 2$ appears once in λ. Hence, the number of cyclic subgroups of A of order p is $p + 1$.

2. Let A be a finite abelian p-group of type (a, b) with $a > b$. Then, there is exactly one partition μ for which (λ, μ) is a-admissable: $\mu = (b, 0)$. In this case, $I(\lambda, \mu) = \{a\}$ so that

   $$g^{\lambda}_{(b)(a)}(t) = \frac{t^b}{1-t^{-1}}\left(1 - t^{-1}\right) = t^b.$$

   Hence, there are p^b cyclic subgroups of order p^a in $\mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}$.

15 Lecture 15 - Structure Theorem of finitely generated abelian groups.

Previous lecture

Keywords: Elementary divisors, invariant factors. Classification of finite abelian groups. Finitely generated abelian groups, free abelian groups. Torsion subgroup.

In this Lecture we will only be considering abelian groups and **will always write the law of composition additively**. We are going to provide a complete classification of abelian groups that can be generated by a finite number of elements - we will see that such groups can be written as a direct product of an infinite subgroup and a finite subgroup. The infinite subgroup will obey similar properties to a (finite dimensional) vector space; in particular, it admits a well defined **rank** (analogue of dimension for a vector space).

15.1 Classification of finite abelian groups

Let A be a finite abelian group. We have seen the following results for A:

Theorem (Theorem 13.1.1)**.** *If $|A| = p_1^{n_1} \cdots p_r^{n_r}$, with $p_1, \dots, p_r$ distinct primes, then*

$$A \cong U_1 \times \cdots \times U_r,$$

where U_i is a p_i-group, $|U_i| = p_i^{n_i}$. Moreover, U_i is the Sylow p_i-subgroup of A.

Theorem (Theorem 14.1.1)**.** *If U is a p-group, say $|U| = p^r$, then there exists unique integers $r_1 \geq \dots \geq r_k \geq 1$ such that $r = \sum_{i=1}^k r_i$ and*

$$U \cong (\mathbb{Z}/p^{r_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{r_k}\mathbb{Z}).$$

These results imply the following:

every finite abelian group is isomorphic to a product of cyclic groups.

Since the product of cyclic groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is isomorphic to the cyclic group $\mathbb{Z}/6\mathbb{Z}$ - $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is generated by $(\overline{1}, \overline{1})$, for example - we see that **a finite abelian group may be isomorphic to different products of cyclic groups**. In general, we have already seen that

Lemma 15.1.1. *Let $a_1, \dots, a_k$ be positive integers and, for $i = 1, \dots, k$, denote $b_i = a_1 \cdots a_{i-1} a_{i+1} \cdots a_k$. Assume that $\gcd(a_i, b_i) = 1$, for each $i = 1, \dots, k$. Then,*

$$(\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_k\mathbb{Z}) \cong \mathbb{Z}/a_1 \cdots a_k\mathbb{Z}.$$

Question: Is there a way to write a finite abelian group <u>uniquely</u> as a product of cyclic groups?

Suppose that A is a finite abelian group such that $|A| = p_1^{n_1} \cdots p_m^{n_m}$, and let $\pi_i = (r_{1,i}, \dots, r_{k_i,i})$ be the type of the Sylow p_i-subgroup U_i of A, so π_i is a partition of n_i. Hence, we have

$$U_i \cong (\mathbb{Z}/p_i^{r_{1,i}}\mathbb{Z}) \times \cdots (\mathbb{Z}/p_i^{r_{k_i,i}}\mathbb{Z}).$$

Definition 15.1.2. Define the **elementary divisors of** A to be the prime powers appearing above:

$$p_1^{r_{1,1}}, \dots, p_1^{r_{k_1,1}}, p_2^{r_{1,2}}, \dots, p_2^{r_{k_2,2}}, \dots, p_m^{r_{1,m}}, \dots, p_m^{r_{k_m,m}}.$$

Let $k = \max\{k_1, \dots, k_m\}$. Define the **invariant factors of** A to be the following integers: for $i = 1, \dots, k$,

$$c_i = p_1^{r_{i,1}} \cdots p_m^{r_{i,m}},$$

where, if $r_{i,j}$ is not defined we omit the prime p_j in the product (eg. if $i > k_j$).

Example 15.1.3. Suppose that

$$A = \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}.$$

The elementary divisors of A are $2^4, 2, 3^2, 3, 3, 5^2$. The invariant factors are

$$c_1 = 2^4.3^2.5^2 =, \; c_2 = 2.3, \; c_3 = 3.$$

Lemma 15.1.4. *Let A be a finite abelian group and $c_1, \dots, c_m$ its invariant factors. Then, c_{i+1} divides c_i.*

Proof: Homework/worksheet problem. □

Combining the above Theorems with Lemma 15.1.1 and Lemma 15.1.4 shows that the answer to the question posed is **yes**!

Theorem 15.1.5 (Classification of finite abelian groups)**.** *Let A be a finite abelian group, $|A| = n$. Then, there exists unique integers $c_1, \dots, c_k$ such that c_{i+1} divides c_i, and A is isomorphic to*

$$(\mathbb{Z}/c_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/c_k\mathbb{Z}).$$

Example 15.1.6. Theorem 15.1.5 allows us to determine **all** possible finite abelian groups of a given order. For example, we will determine all finite abelian groups of order $n = 2^5.11 = 352$:

1. Denote $p_1 = 2, p_2 = 11, \; n_1 = 5, n_2 = 1$ (the exponents of the primes appearing in the prime decomposition of n).
2. Determine all possible elementary divisors: this amounts to determining all partitions of n_1, n_2. We see that
$$5, 14, 23, 1^2 3, 12^2, 1^3 2, 1^5,$$
are all partitions of $n_1 = 5$, and there is exactly one partition of $n_2 = 1$.
3. For each list of partitions (λ_1, λ_2) of (n_1, n_2) we write down the corresponding elementary divisiors:
$$(5, 1): \; 2^5, 11,$$
$$(14, 1): \; 2^4, 2, 11,$$
$$(23, 1): \; 2^3, 2^2, 11,$$
$$(1^2 3, 1): \; 2^3, 2, 2, 11,$$
$$(12^2, 1): \; 2^2, 2^2, 2, 11,$$
$$(1^3 2, 1): \; 2^2, 2, 2, 2, 11,$$
$$(1^5, 11): \; 2, 2, 2, 2, 2, 11.$$
4. For each of the collection of elementary divisors listed determine the invariant factors:
$$(5, 1): \; c_1 = 2^5.11,$$
$$(14, 1): \; c_1 = 2^4.11, c_2 = 2,$$
$$(23, 1): \; c_1 = 2^3.11, c_2 = 2^2,$$
$$(1^2 3, 1): \; c_1 = 2^3.11, c_2 = 2, c_3 = 2,$$
$$(12^2, 1): \; c_1 = 2^2.11, c_2 = 2^2, c_3 = 2,$$
$$(1^3 2, 1): \; c_1 = 2^2.11, c_2 = 2, c_3 = 2, c_4 = 2,$$
$$(1^5, 11): \; c_1 = 2.11, c_2 = 2, c_3 = 2, c_4 = 2, c_5 = 2.$$

5. List the possible groups with the given invariant factors:

$$(5,1): \ \mathbb{Z}/(2^5.11)\mathbb{Z},$$
$$(14,1): \ \mathbb{Z}/(2^4.11)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$(23,1): \ \mathbb{Z}/(2^3.11)\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z},$$
$$(1^23,1): \ \mathbb{Z}/(2^3.11)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$(12^2,1): \ \mathbb{Z}/(2^2.11)\mathbb{Z} \times \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$(1^32,1): \ \mathbb{Z}/(2^2.11)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$(1^5,11): \ \mathbb{Z}/(2.11)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Every finite abelian group of order 352 **is isomorphic to precisely one of the groups listed**.

15.2 Finitely generated abelian groups

Definition 15.2.1. Let G be an abelian group. We say that G is **finitely generated** if there exists $\{g_1, \dots, g_n\} \subset G$ such that, for every $g \in G$, there exist integers $r_1, \dots, r_n$ with

$$g = r_1g_1 + \cdots + r_ng_n.$$

If such a set $\{g_1, \dots, g_n\}$ exists then we will call it a **spanning set of** G (in analogy with spanning sets in the theory of vector spaces).

We say that a finitely generated abelian group G is **free**(if there exists a spanning set $\{g_1, \dots, g_n\}$ of G such that, for every $g \in G$, there exists **unique** integers $r_1, \dots, r_n$ with

$$g = r_1g_1 + \cdots + r_ng_n.$$

In this case we will call such a spanning set $\{g_1, \dots, g_n\}$ a **basis of** G and define the **rank** of G to be n (the size of a basis).[1]

It is tempting to think of (finitely generated) free abelian groups as being 'the same as' vector spaces: this means that both objects possess similar properties. This is true in some respects (eg. Lemma **??**), but there is a major difference - **if** G **is a free group of rank** n **then** G **can contain a subgroup** H**,** $H \neq G$**, that is free and has rank** n**.** For example, the group $\mathbb{Z}$ is a free abelian group of rank 1, and the subgroup $2\mathbb{Z} = \{2x \mid x \in \mathbb{Z}\} \subset \mathbb{Z}$, is also a free group of rank 1.

Example 15.2.2. 1. Any finite abelian group A is finitely generated - a set of generators is given by A itself!

2. For any $n \geq 1$, the abelian group

$$\mathbb{Z}^n = \mathbb{Z} \overset{n \text{ times}}{\times \cdots \times} \mathbb{Z}$$

is finitely generated and free - a basis is given by $\{(1,0,\dots,0),(0,1,0\dots,0),\dots,(0,\dots,0,1)\}$.

3. Let A be a finite abelian group, $n \geq 1$. Then, $\mathbb{Z}^n \times A$ is finitely generated. In fact, if G and H are finitely generated then so is $G \times H$.

4. The abelian group $(\mathbb{Q}, +)$ is not finitely generated: if $\{x_1, \dots, x_n\} \subset \mathbb{Q}$ were a spanning set, with $x_i = a_i/b_i$, $\gcd(a_i, b_i) = 1$, then we have, for any integers $r_1, \dots, r_n$

$$r_1x_1 + \dots + r_nx_n = \frac{y}{b_1 \cdots b_n}, \text{ for some } y \in \mathbb{Z}.$$

In particular, if $c > |b_1 \cdots b_n|$ then it is not possible to write $\frac{1}{c}$ as a linear combination of $\{x_1, \dots, x_n\}$.

In fact, Example 3 above gives essentially all examples of finitely generated abelian groups, as we will see in the next section.

[1] This is a well-defined definition - if $\{g_1, \dots, g_n\}$ and $\{h_1, \dots, h_m\}$ are two bases of G then $n = m$. We will not see a proof of this fact in this course, however.

15.3 Structure theorem of finitely generated abelian groups

Definition 15.3.1. Let G be an abelian group. Define **the torsion subgroup of** G to be

$$G_{tor} = \{g \in G \mid g \text{ has finite order}\}.$$

This is a well-defined definition - namely, G_{tor} is a subgroup of G.

Lemma 15.3.2. *Let G be a finitely generated abelian group, G_{tor} the torsion subgroup of G. Then, G_{tor} is a finite abelian group.*

Lemma 15.3.3. *Let G be a finitely generated abelian group, G_{tor} the torsion subgroup of G. Then, G/G_{tor} is a (finitely generated) free abelian group.*

Theorem 15.3.4 (Structure Theorem of finitely generated abelian groups)**.** *Let G be a finitely generated abelian group. Then, there exists a finitely generated free abelian group F and a finite abelian group A such that G is isomorphic to $F \times A$. Moreover, A is isomorphic to G_{tor}.*

References

[1] Milne, J. S.; *Group Theory*, `http://www.jmilne.org/math/CourseNotes/GT.pdf`