Algebra II

Lectures by A. Stasinski
Notes by Ben Napier

2020 Epiphany Term

Contents

Chapter 1

Groups

Lecture 1
On 14/1

Example (Familar examples of groups)**.**

(i) Every commutative ring is an abelian group under addition. Abelian means $xy = yx$ for all x, y in the group.

(ii) $\{A \in M_n(F) : \det A \neq 0\} = \mathrm{GL}_n(F)$ is a group for a field F.

Let's look at a formal definition.

Definition 1.1 (Group)**.** A group G is a set with a binary operation (that is, a function $G \times G \to G$)

$$(g, h) \mapsto g * h$$

such that

(i) (identity) there exists an identity element $1 \in G$ such that

$$g * 1 = 1 * g = g;$$

(ii) (associativity) for all $x, y, z \in G$

$$(x * y) * z = x * (y * z); \text{ and}$$

(iii) (inverse) for all $g \in G$ there exists $h \in G$ such that

$$g * h = 1 = h * g.$$

we typically denote $h = g^{-1}$.

Sometimes we write $(G, *)$ for a group; however, this is not very common. The operator being used is typically clear from context.

Example (More examples of groups)**.**

(i) $\mathbb{Z}/n$ under addition;

(ii) the group of units $(\mathbb{Z}/n)^\times$ under multiplication;

(iii) for any ring R, $R^\times$ is a group (but may be non-abelian).

▸

1.1 Groups and symmetry

A **symmetry** is a function $f : X \to X$ where X is some object. Often f is taken to be an isometry, then it is called **rigid**. There exists an identity Id which does not change X. We can compose two symmetries

$$f \circ g : X \xrightarrow{g} X \xrightarrow{f} X$$

and every symmetry is invertible.

Chapter 2

Dihedral groups

A **dihedral group** is the group of symmetries of a regular polygon, which includes *rotations* and *reflections*. Lecture 2 On 16/1

We have the dihedral group D_3, or the symmetry group of the regular triangle, defined as

$$D_3 = \{1, r, r^2, s, rs, r^2 s\}.$$

To relate this to transformations on a triangle: r is a rotation of $\frac{2\pi}{3}$ and s is a reflection (in any of the lines of symmetry).

Remark. (i) D_3 is a non-abelian group.

(ii) You may object that not *all* symmetries are in the group; for example, the product $r^2(r^2 s)$. However,

$$r^2(r^2 s) = r^3 rs = 1rs = rs \in D_3.$$

(iii) To describe D_3 completely, we need only r and s and three fundamental relations from which everything else follows:

$$D_3 = \langle r, s : r^3 = 1, s^2 = 1, srs = r^2 \rangle.$$

△

We can do a similar analysis for a square, and the group of symmetries here are called D_4. Similarly, for a regular n-gon ($n \geq 3$) we get the dihedral group D_n. We define this as

$$D_n = \langle r, s : r^n = 1, s^2 = 1, srs = r^{-1} \rangle.$$

You can see the main difference here is that we have n rotations. This algebraic definition of D_n makes sense for $n \in \{1, 2\}$; however, D_n clearly is not the symmetry group of an n-gon.

Lecture 3 On 21/1

Lemma 2.1. *In D_n, any*

$$r^{a_1}s^{b_1}r^{a_2}s^{b_2}\dots r^{a_m}s^{b_m}$$

can be written as $r^a s^b$ for $0 \le a \le n-1$ and $0 \le b \le 1$.

Proof. We use induction on the length m. We consider $m = 1$, the base case, then we have

$$r^n = 1, \qquad s^2 = 1$$

so it is true. Now suppose the lemma is true for some $m \ge 1$. We want to prove it is true $m+1$. Consider an expression of length $m+1$

$$x = r^{a_1}s^{b_1}\dots r^{a_m}s^{b_m}r^{a_{m+1}}b^{b_{m+1}}.$$

Using $s^2 = 1$, we can reduce to the cases $b_i = 0$ or $b_i = 1$ for all $i = 1, 2, \dots, m+1$. Cases:

(i) if $b_{m+1} = 0$, we can write (using $srs = r^{-1} \implies sr^is = r^{-i}$) $x = r^{a_1}s^{b_1}\dots r^{a_m+a_{m+1}}$ if $b_m = 0$ or $x = r^{a_1}s^{b_1}\dots r^{a_m+a_{m+1}}$ if $b_m = 1$; and

(ii) if $b_{m+1} = 1$, we can write $x = r^{a_1}s^{b_1}\dots r^{a_m+a_{m+1}}s$ if $b_m = 0$ and $x = r^{a_1}s^{b_1}\dots r^{a_m-a_{m+1}}$ if $b_m = 1$.

All of these expressions have length m, so by induction x can be written in the required form. $\square$

Chapter 3

Generators and cyclic groups

Definition 3.1. A set S of elements of a group G is said to be a set of generators if any element in G can be written as a product of elements in S (possibly together with inverses). We then write $G = \langle S \rangle$.

Example.

$$D_n = \langle r, s \rangle.$$

▸

Definition 3.2 (Cyclic)**.** A group which can be generator by a single element is called **cyclic**.

Example.

(i) $\mathbb{Z}/n = \langle \overline{1} \rangle$.

(ii) $\mathbb{Z} = \langle 1 \rangle$.

▸

3.1 Orders of groups of elements

The word *order* can mean different properties depending on whether you are referring to a *group* or an *element*.

Definition 3.3 (Order)**.** The **order** of a finite group G is the number of elements, written $|G|$ or $\#G$.

Definition 3.4 (Order of an element)**.** The **order** of an element g of a group G, written $\operatorname{ord}(g)$, is the smallest integer $n \geq 1$ such that $g^n = 1$. If no such n exists, $\operatorname{ord}(g) = \infty$.

Remark. If G is finite, then any element $g \in G$ has finite order as if $\{1, g, g^2, \ldots\}$ were all distinct then G would be infinite; therefore, $g^i = g^j$ for some $0 \leq i \leq j$, and hence $g^{j-i} = 1$. Note $\operatorname{ord}(g) = 1 \iff g = 1$. △

We can look at the order of an element $g \in G$ as the order of the cyclic group that it generates:

$$\langle g \rangle = \{1, g, g^2, \ldots\}.$$

Example. (i) In $\mathbb{Z}/6$, $\overline{1}$ and $\overline{5}$ both have order 6.

(ii) In D_n, r has order n and s has order 2.

(iii) The order of D_n is $2n$.

▶

Chapter 4

Symmetric group

Lecture 4
On 23/1

Definition 4.1 (Permutation)**.** A **permutation** of a set $S = \{1, 2, \ldots, n\}$ is a bijection $\sigma : S \to S$, often written

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Definition 4.2 (Cycle)**.** A k-cycle is a permutation σ such that

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_3, \quad \ldots, \quad \sigma(a_k) = a_1$$

and $\sigma(a) = a$ for all $a \neq \{a_1, \ldots, a_k\}$. We use the shorthand

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_k \\ a_2 & a_3 & \ldots & a_1 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \ldots & a_k \end{pmatrix}.$$

Example.

(i) A 3-cycle:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 6 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 5 & 6 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 2 & 5 \end{pmatrix}.$$

(ii) A 2-cycle:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (1\ 3);$$

we call 2-cycles **transpositions**.

Definition 4.3 (Disjoint cycle)**.** Two cycles are **disjoint** if there members do not intersect.

Example. (1 2 3) and (4 5) are disjoint but (1 2 3) and (2 4) are not. ▸

Proposition 4.4. *For any $n \in \mathbb{N}$, the set of permutations*

$$\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$$

is a group under composition, called the symmetric group S_n.

Proof. Let σ and τ be two bijections. Then $\sigma \circ \tau$ is also a bijection. Composition of functions is always associative. The identity bijection is $\mathrm{Id} : a \to a$. Finally, every bijection σ has an inverse σ^{-1} such that $\sigma \circ \sigma^{-1} = 1$. □

Remark. $\mathrm{ord}(S_n) = n!$. This is because we have n choices for the position of the first value, then $n - 1$ for the next, and so on. △

Example. $\sigma = (1\ 2\ 3) \in S_4$, and $\tau = (2\ 4) \in S_4$. Then

$$\sigma \circ \tau = (2\ 4\ 3\ 1).$$

▸

Example. Consider S_{10} with

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 3 & 2 & 1 & 4 & 8 & 9 & 7 & 6 & 10 \end{pmatrix}.$$

Then we have

$$\sigma = (1\ 5\ 4) \circ (2\ 3) \circ (6\ 8\ 7\ 9) \circ (10).$$

▸

Example. Let $\sigma = (1\ 2)$ and $\tau = (1\ 3)$ in S_3. Then

$$(1\ 2)(1\ 3) = (1\ 3\ 2).$$

▸

Proposition 4.5.

(i) Disjoint cycles commute with each other.

(ii) Every permutation is a product of disjoint cycles, and this is unique up to the order of the cycles and the different ways we can write the cycle.

Lecture 5 On 28/1

Example. Write (1 2 5)(4 6 8 9) as a product of transpositions. ▸

Solution.

$$\begin{aligned}\begin{pmatrix}1 & 2 & 5\end{pmatrix}\begin{pmatrix}4 & 6 & 8 & 9\end{pmatrix} &= \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 5\end{pmatrix}\begin{pmatrix}4 & 6 & 8 & 9\end{pmatrix}\\ &= \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 5\end{pmatrix}\begin{pmatrix}4 & 6\end{pmatrix}\begin{pmatrix}6 & 8 & 9\end{pmatrix}\\ &= \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 5\end{pmatrix}\begin{pmatrix}4 & 6\end{pmatrix}\begin{pmatrix}6 & 8\end{pmatrix}\begin{pmatrix}8 & 9\end{pmatrix}.\end{aligned}$$

□

Proposition 4.6. *Every permutation is a product of transpositions (but not uniquely).*

Proof. We know that every permutation is a product of disjoint cycles, so it suffices to show that any cycle is a product of cycles. Now

$$\begin{pmatrix}a_1 & a_2 & \dots & a_k\end{pmatrix} = \begin{pmatrix}a_1 & a_2\end{pmatrix}\begin{pmatrix}a_2 & a_3\end{pmatrix}\dots\begin{pmatrix}a_{k-1} & a_k\end{pmatrix}.$$

□

Example. Write $\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}2 & 3 & 4\end{pmatrix}$ as a product of transpositions in two different ways. ▸

Solution.

$$\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}2 & 3 & 4\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}$$
$$\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}2 & 3 & 4\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}.$$

□

Note that the number of products in both factorisation are even, this is not a coincidence.

4.1 Computations with permutations

Example. Let $\sigma = \begin{pmatrix}2 & 4 & 1\end{pmatrix} \in S_5$. Then $\sigma(1) = 2$, $\sigma(2) = 4$, and $\sigma(4) = 1$. So if we take $\sigma \circ \sigma = \sigma^2$ we get the permutation: $1 \mapsto 4$, $2 \mapsto 1$, and $4 \mapsto 2$. Thus $\sigma^2 = \begin{pmatrix}1 & 4 & 2\end{pmatrix}$. Considering σ^3 we have $1 \mapsto 1$, $2 \mapsto 2$, and $4 \mapsto 4$. Thus $\sigma^3 = 1$ so $\operatorname{ord}\sigma = 3$. More generally, a k-cycle ($k \in \mathbb{N}$) has order k. ▸

Lemma 4.7. *Let $\sigma = \sigma_1 \dots \sigma_m$ be a product of disjoint cycles of length k_u. Then*

$$\operatorname{ord}(\sigma) = \operatorname{lcm}(k_1, \dots, k_m).$$

Proof. Let $L = \operatorname{lcm}(k_1, \dots, k_m)$. We know that $\operatorname{ord}(\sigma_i) = k_i$ (see earlier example). So

$$\sigma^L = \sigma_1^L = \dots = \sigma_m^L = 1$$

and since disjoint cycles commute, $\text{ord}(\sigma) \leq L$. Suppose $\sigma_i^N = 1$ for some $N \in \mathbb{N}$. Then we can express $N = k_i q + r$ for some $q, r \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ where $r < k_i$. So $\sigma_i^N = \sigma_i^r = 1$ but k_i is the smallest non-zero number with this property so $r = 0$. Therefore $k_i \mid N$. Now let $\sigma = \text{ord}(\sigma)$.. Since disjoint cycles commute

$$1 = \sigma^N = \sigma_1^N \dots \sigma_m^N = 1$$

and $\sigma_1^N, \dots, \sigma_m^N$ are still disjoint so $\sigma_i^N = 1$ for $1 \leq i \leq n$. Thus $k_i \mid N$ and $L \mid N$. Therefore

$$L \leq N = \text{ord}(\sigma) \leq L \implies N = L.$$

□

Example (Inverses)**.** If $\sigma = \begin{pmatrix} 2 & 4 & 1 \end{pmatrix}$ then $\sigma^{-1} = \begin{pmatrix} 2 & 4 & 1 \end{pmatrix}$. In general, the inverse of a cycle is the cycle read backwards. That is,

$$\begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}^{-1} = \begin{pmatrix} a_k & a_{k-1} & \dots & a_1 \end{pmatrix}^{-1}.$$

For a product $\sigma = \sigma_1 \dots \sigma_m$ then

$$\sigma^{-1} = \sigma_m^{-1} \dots \sigma_1^{-1}.$$

▸

Lemma 4.8. *Let $\sigma = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix} \in S_n$ be a cycle and $\lambda \in S_n$. Then*

$$\lambda \sigma \lambda^{-1} = \begin{pmatrix} \lambda(a_1) & \lambda(a_2) & \dots & \lambda(a_k) \end{pmatrix}.$$

Proof.

$$\lambda\sigma\lambda^{-1}(\lambda(a_1)) = \lambda\sigma(a_1) = \lambda(a_2)$$
$$\vdots$$
$$\lambda\sigma\lambda^{-1}(\lambda(a_k)) = \lambda\sigma(a_k) = \lambda(a_1).$$

□

Lecture 6
On 30/1

Example. S_3 is generated by (1 2) and (2 3). We see:

$$\begin{aligned} (1\ 2)^2 &= 1 \\ (1\ 2)(2\ 3) &= (1\ 2\ 3) \\ (1\ 2\ 3)^2 &= (1\ 3\ 2) \\ (1\ 3\ 2)(1\ 2) &= (1\ 3) \end{aligned}$$

and as $\text{ord}(S_3) = 3! = 6$, we have all the elements. ▸

Chapter 5

Subgroups, cosets, and Lagrange

Definition 5.1 (Subgroup)**.** Let G be a group. $H \subset G$ is a **subgroup** of G if

(i) $1 \in H$ where 1 is the identity of G;

(ii) for all $h_1, h_2 \in H$, $h_1 h_2 \in H$; and

(iii) for any $h \in H$, $h^{-1} \in H$.

We refer to a subgroup $H \subset G$ as **proper** if $H \neq G$.

Example (Examples of subgroups)**.**

(i) $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}\} \subset \mathbb{Z}/6$;

(ii) $\langle r \rangle = \{1, r, r^2, \ldots, r^n\} \subset D_n$; and

(iii) $\langle 2 \rangle = 2\mathbb{Z} \subset \mathbb{Z}$.

▸

Remark. It is interesting to note that, in the examples above, the order of the subgroup always divides the order of the group it is contained within. This is not a coincidence, and we will show that this always holds. △

5.1 Cosets

Definition 5.2 (Coset)**.** Let G be a group, $H \subset G$ be a subgroup, and $g \in G$. Then

$$gH = \{gh : h \in H\}$$

is called the **left coset** of H with respect to g. Similarly,

$$Hg = \{hg : h \in H\}$$

is called the **right coset** of H with respect to g.

Remark. If G is abelian, $gH = Hg$. △

Example. Let $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$. We will write our cosets additively here, so $g + H$ (instead of gH). Now

$$\begin{aligned} 0 + H &= H \\ 1 + H &= \{1 + 2n : n \in \mathbb{Z}\} \\ 2 + H &= H \\ &\vdots \end{aligned}$$

so we see that there is only two distinct cosets: $2\mathbb{Z}$ and $1 + 2\mathbb{Z}$. ▸

Example. Take $G = D_3$ and $H = \langle s \rangle = \{1, s\}$. The left cosets are

$$1H = H, \qquad rH, \qquad r^2H$$

as $rsH = rH$ and $r^2sH = r^2H$ (from the fact that $s \in H$). We know that rH and r^2H are distinct as otherwise there would exist $h, h' \in H$ such that $rh = r^2h'$, but then $h(h')^{-1} = r$ which is a contradiction as $r \notin H$. ▸

Remark. The last example provides the neat fact that if $xH = yH$ then

$$y^{-1}x \in H.$$

The converse is also true; therefore

$$xH = yH \iff y^{-1}x \in H.$$

△

Lemma 5.3. *Let G be a group and $H \subset G$ be a subgroup. Then*

$$G = \bigcup_{g \in G} gH$$

and for any two cosets gH and $g'H$ either $gH = g'H$ or $gH \cap g'H = \varnothing$.

Proof. For all $g \in G$, $g \in gH$; hence,

$$G = \bigcup_{g \in G} gH.$$

Now let gH and $g'H$ be two distinct cosets and consider $x \in gH \cap g'H$. Then

$$x = gh = g'h'$$

where $g, g' \in G$ and $h, h' \in H$. Then

$$xH = ghH = gH = g'h'H = g'H$$

but gH and $g'H$ are distinct; contradiction. Therefore, no such x can exist and so $gH \cap g'H = \varnothing$. □

Theorem 5.4 (Lagrange)**.** *Let G be a finite group and $H \subset G$ be a subgroup. Then*

$$|G| = m \cdot |H|$$

where m is the number of left cosets of H in G.

Proof. Let $g_1H, g_2H, \ldots, g_mH$ be the distinct left cosets of H in G where $g_i \in G$. Then

$$G = \bigcup_{i=1}^{m} g_iH$$

and we know that each $g \in G$ lies in exactly one of these cosets. Thus

$$|G| = \sum_{i=1}^{m} |g_iH|.$$

We define the function

$$f : g_iH \to H, \qquad f(g_ih) = h.$$

f is clearly surjective and $f(g_ih) = f(g_ih') \implies h = h' \implies g_ih = g_ih'$ so f is injective; therefore, f is a bijection. Therefore $|g_iH| = |H|$ and so

$$|G| = \sum_{i=1}^{m} |g_iH| = m \cdot |H|.$$

□

Definition 5.5 (Index)**.** Let G be a group and $H \subset G$ be a subgroup. Then we define the **index** of H in G as $\frac{|G|}{|H|}$ and it represents the number of cosets of H in G.

Example. Find all subgroups of S_3. ▸ Lecture 7 On 4/2

Solution. We have $|S_3| = 6$; hence, if $H \subset S_3$ is a subgroup then $|H| \in \{1, 2, 3, 6\}$.

$|H| = 1$ This must be the trivial subgroup: $\{1\} \subset S_3$.

$|H| = 2$ We must have $H = \{1, x\}$ where $x \in S_3$ has order 2. Thus x must have a representation as a product of disjoint transpositions; however, as we are in S_3 we cannot have a product of more than 1 transpositions. Hence

$$x \in \{(1\ 2), (1\ 3), (2\ 3)\}.$$

$|H| = 3$ We must have $H = \{1, x, x^2\}$ where $x \in S_3$ has order 3. Here the only two distinct x are $(1\ 2\ 3)$ and $(1\ 3\ 2)$, but $(1\ 2\ 3)^2 = (1\ 3\ 2)$ so we have one subgroup.

$|H| = 3$ $H = S_3$.

Hence we get the following subgroup structure for S_3.

$$\begin{tikzcd}
 & & S_3 \arrow[dll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\langle(1\ 2)\rangle & \langle(1\ 3)\rangle & & \langle(2\ 3)\rangle & \langle(1\ 2\ 3)\rangle \\
 & & \{1\} \arrow[ull, dash] \arrow[ul, dash] \arrow[ur, dash] \arrow[urr, dash] & &
\end{tikzcd}$$

□

5.2 An application to number theory

An application of Lagrange's theorem (and some ring theory) is the *Fermat-Euler* theorem. We must define $\varphi(n)$ first, however.

Definition 5.6 (Euler's totient function)**. Euler's totient function** $\varphi(n) : \mathbb{N} \to \mathbb{N}$ is the number of positive integers up to n that are coprime to n.

Theorem 5.7 (Fermat-Euler)**.** *Let $a, n \in \mathbb{N}$ be coprime, then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. We have

$$a^{\varphi(n)} \equiv 1 \pmod{n} \iff a^{\varphi(n)} - 1 \in n\mathbb{Z} \iff \overline{a^{\varphi(n)}} = \overline{1} \qquad \text{in } (\mathbb{Z}/n)^\times.$$

From last term we have

$$\left|(\mathbb{Z}/n)^\times\right| = \varphi(n)$$

By Lagrange's theorem we have that $|\overline{a}|$ divides $\varphi(n)$. Thus $\text{ord}(\overline{a})m = \varphi(n)$ for some $m \in \mathbb{Z}$. Therefore

$$\overline{a}^{\varphi(n)} = ((\overline{a})^{\text{ord}(\overline{a})})^m = (\overline{1})^m = \overline{1}.$$

□

Chapter 6

Homomorphisms and isomorphisms

This content will be very familiar from the definitions for rings.

Definition 6.1 (Homomorphism)**.** Let G and H be groups. A **homomorphism** $\varphi : G \to H$ is a function such that

$$\varphi(xy) = \varphi(x)\varphi(y)$$

for all $x, y \in G$.

If a homomorphism $\varphi : G \to H$ is bijective, it is an **isomorphism**. We denote $G \cong H$.

Remark. A point on notation: in the definition for a homomorphism we are using the binary operation in G for xy and the binary operation in H for $\varphi(x)\varphi(y)$. These are not necessarily the same. △

Example. Any group of order 2 is isomorphic to $\mathbb{Z}/2$. To show that, we consider the group $\{e, x\}$ where e is the identity and $x \neq e$. If we define the function $e \mapsto \overline{0}$ and $x \mapsto \overline{1}$ we see that it is indeed an isomorphism, so $\{e, x\} \cong \mathbb{Z}/2$. ▸

Example. Similarly to the last example, any group of order 3 is isomorphic to $\mathbb{Z}/3$. To see this, take the group $\{e, x, y\}$ with e identity. It is clear to see that $xy = e$ as if $xy = x$ then $y = 1$ and if $xy = y$ then $x = 1$. Furthermore, we have that $x^2 = y$ as if $x^2 = 1$ then $x^2y = y$, but $x^2y = x(xy) = x = y$; a contradiction. Similarly $y^2 = x$. We define the map $\varphi : \{e, x, y\} \to \mathbb{Z}/3$ by

$$e \mapsto \overline{0}, \qquad x \mapsto \overline{1}, \qquad y \mapsto \overline{2}.$$

It is trivial to see that this is an isomorphism. ▸

Example. We can relate D_n to $\mathbb{Z}/n$ by defining the homomorphism

$$\varphi : D_n \to \mathbb{Z}/2, \qquad \varphi(r^i s^j) = \overline{j} \pmod 2.$$

To confirm this, we just need to check that

$$\varphi(xy) = \varphi(x) + \varphi(y)$$

for all $x, y \in D_n$ (don't be confused by the notation, we use the additive notation for $\mathbb{Z}/2$ but the multiplicative notation for D_n as usual):

$$\varphi(r^a s^b \cdot r^c s^d) = \varphi(r^a s^b r^c (s^b s^b) s^d) = \varphi(r^{a-c} s^{b+d}) = \overline{b+d}$$
$$\varphi(r^a s^b)\varphi(r^c s^d) = \overline{b} + \overline{d} = \overline{b+d}.$$

▸

Example. Prove that the map

$$\varphi : \mathbb{Z}/6 \to S_3, \qquad \varphi(\overline{a}) = (1\ 2\ 3)^a$$

is a homomorphism. ▸

Solution. First, we must show that φ is well-defined. That is, if $\overline{a} = \overline{b}$ then $\varphi(\overline{a}) = \varphi(\overline{b})$. If $\overline{a} = \overline{b}$ then $a - b = 6m$ for some $m \in \mathbb{Z}$. So

$$\phi(\overline{a}) = (1\ 2\ 3)^{\overline{a}} = (1\ 2\ 3)^{b+6m} = (1\ 2\ 3)^b((1\ 2\ 3)^3)^{2m} = (1\ 2\ 3)^b = \varphi(\overline{b})$$

as a 3-cycle has order 3. So we have shown that φ is well-defined, now we must show that it is a homomorphism:

$$\varphi(\overline{a} + \overline{b}) = (1\ 2\ 3)^{a+b} = (1\ 2\ 3)^a(1\ 2\ 3)^b = \varphi(\overline{a})\varphi(\overline{b}).$$

□

We define the **kernel** and **image** of a homomorphism identically to how we did last term in ring theory.

Lecture 8 On 6/2

Just as for rings, we see that a homomorphism φ is injective if and only if $\ker\varphi = \{1\}$ (the proof for this is the same again).

6.1 Normal subgroups, quotients, and the FIT

Recall that *ideals* are special kinds of subsets of a ring R such that the quotient R/I is again a ring. Moreover, we have seen that ideals are exactly the kernels of ring homomorphisms.

Analogously, we will define certain subgroups called *normal* such that we can form quotient groups. Moreover, the normal subgroups will be exactly the kernels of group homomorphisms.

Definition 6.2 (Normal)**.** The subgroup $H \subset G$ is said to be **normal** (in G) if for every $g \in G$ and $h \in H$ we have

$$g^{-1}hg \in H.$$

Example. The following examples are easy to show.

(i) If G is abelian, any subgroup H is normal.

(ii) The subgroup $\langle r \rangle$ of D_n is normal.

▶

Definition 6.3 (Quotient group)**.** Let N be a normal subgroup of a group G. The **quotient group** G/N is the group

$$G/N = \{gN : g \in G\}$$

with the operation $(gN)(g'N) = gg'N$. The identity in G/N is $1 \cdot N = N$ and $(gN)^{-1} = g^{-1}N$.

Just ling for rings modulo ideals, we have a canonical surjective homomorphism

$$G \to G/N, \qquad g \mapsto gN$$

whose kernel is exactly N. Just like ideals are kernels, we thus deduce that normal subgroups are kernels.

Lemma 6.4. *Let $\varphi : G \to H$ be a homomorphism of groups. Then* $\ker \varphi$ *is normal in G. Conversely, if N is a normal subgroup of G, then N is the kernel of a homomorphism.*

Proof. For the first statement, let $x \in \ker \varphi$ and $g \in G$. Then

$$\varphi(gxg^{-1}) = \varphi(g)\varphi(g)^{-1} = 1$$

so $gxg^{-1} \in \ker \varphi$ and so φ is normal. The second statement comes directly from what we have noted about $G \to G/n$. □

Lemma 6.5. *Let G be a finite group and N be a normal subgroup. Then*

$$|G/N| = \frac{|G|}{|N|}.$$

Proof. By Lagrane's theorem, we have that $\frac{|G|}{|N|}$ is the number of left cosets of N. By the definition of G/N, its order is the number of cosets of N. □

Theorem 6.6 (FIT for groups)**.** *Let $\varphi : G \to H$ be a group homomorphism. Then*
$$G/\ker\varphi \cong \operatorname{im}\varphi.$$

Proof. The proof is very similar to that of rings, so we omit most of it. We note that the isomorphism is given by the map $g\ker\varphi \to \varphi(g)$. ☐

Example. Let φ be a homomorphism defined by
$$\varphi : D_n \to \mathbb{Z}/2, \qquad \varphi(r^i s^j) = \overline{j} \pmod 2.$$
This map is clearly surjective and has kernel $\langle r\rangle$. Thus, $\langle r\rangle$ is normal in D_n (which we already knew). Moreover, FIT imlpies that
$$D_n/\langle r\rangle \cong \mathbb{Z}/2.$$
▸

Example. Let
$$\varphi : \mathbb{Z}/6 \to S_3, \qquad \varphi(\overline{a}) = (1\ 2\ 3)^a$$
be a homomorphism. We see that
$$\operatorname{im}\varphi = \langle(1\ 2\ 3)\rangle, \qquad \ker\varphi = \{\overline{0}, \overline{3}\}$$
so
$$(\mathbb{Z}/6)/\{\overline{0}, \overline{3}\} \cong \langle(1\ 2\ 3)\rangle.$$
▸

Chapter 7

Relating and identifying finite groups

Lecture 9
On 11/2

Recall that we have seen that any group of order 2 must be isomorphic to $\mathbb{Z}/2$, and similarly any group of order 3 must be isomorphic to $\mathbb{Z}/3$.

Lemma 7.1.

(i) Let G be a cyclic group of order n. Then $G \cong \mathbb{Z}/n$.

(ii) Let G be a group of prime order p. Then G is cyclic, so that $G \cong \mathbb{Z}/p$.

Proof.

(i) Let G be cyclic of order n, and let g be a generator. It is easy to check that $g^i \mapsto \bar{i} \in \mathbb{Z}/n$ defines an isomorphism.

(ii) Let G be a group of prime order p. Then the subgroup $\langle g \rangle \subset G$ for any $g \neq 1$ must be of order p by Lagrange's theorem and thus $\langle g \rangle = G$, so G is cyclic. By the previous part, $G \cong \mathbb{Z}/p$.

□

Among the finite groups, we have seen the cyclic groups $\mathbb{Z}/n$, the dihedral groups D_n, and the symmetric groups S_n. Note that there is some overlap between these, for example $\mathbb{Z}/1 \cong S_1$, $D_1 \cong \mathbb{Z}/2$, and $D_3 \cong S_3$.

7.1 Direct products

Definition 7.2 (Direct product)**.** Let G, H be groups. Their **direct product** is

$$G \times H = \{(g, h) \in G \times H\}$$

where the binary operation is defined componentwise, in terms of the operations in G and H.

Example. Suppose that G is a group of order 4. If G is cyclic, then $G \cong \mathbb{Z}/4$. If G is not cyclic, then every element has order 1 or 2 (because then no element has order 4). Since only 1 has order 1, we have

$$G = \{1, a, b, c\},$$

where a, b, c are distinct and have order 2. Since none of a, b, c are the identity, we must have $ab \in \{1, c\}$. If $ab = 1$ then $a^2 b = a$ and so $b = a$; a contradiction. Thus $ab = c$. Similarly, $ba = c$. So $ab = ba$. By symmetry $ac = ca$ and $bc = cb$; thus G is abelian. We can show (by constructing an isomorphism) that $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. This group is often called the *Klein 4-group*. Since D_2 has order 4 and is not cyclic, we have proved that $D_2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. ▸

Isomorphisms preserve the order of elements. Therefore, one can easily prove that groups are not isomorphic by showing that one has an element of a certain order, while another does not.

Example. Is $\mathbb{Z}/3 \times S_3$ isomorphic to D_9? ▸

Solution. $|\mathbb{Z}/3 \times S_3| = 3 \cdot 6 = 18 = |D_9|$, so maybe. Every element of D_9 must have an order that divdes 9 or 2; on the other hand, in $\mathbb{Z}/3 \times S_3$ we have the element

$$(\bar{1}, (1\ 2))$$

that has order 6. Hence, $\mathbb{Z}/3 \times S_3 \not\cong D_9$. □

7.2 $D_3 \cong S_3$

In this section, we will provide two ways of proving this. One is a more direct hands-on approach while the other is more *structural.* The first method helps us to understand how to define a homomorphism using generators, while the second method helps to understand the *structural/ geometrical* connecting between dihedral groups and symmetric groups.

Method 1 We know

$$D_3 = \{1, r, r^2, s, rs, r^2 s\}$$

and

$$S_3 = \{1, (1\ 2), (2\ 3), (1\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Any homomorphism $\varphi : D_3 \to S_3$ is completely determined by the values $\varphi(r)$ and $\varphi(s)$ since all other values of D_3 are products of rs and ss, and φ is multiplicative. If φ is an isomorphism, it must preserve the order of elements. So

Table 7.1: A list of all the groups (up to isomorphisms) of order at most 8.

Order	Group
1	$\mathbb{Z}/1$
2	$\mathbb{Z}/2$
3	$\mathbb{Z}/3$
4	$\mathbb{Z}/4$, $D_2 \cong \mathbb{Z}/2 \times \mathbb{Z}/2$
5	$\mathbb{Z}/5$
6	$\mathbb{Z}/6$, $S_3 \cong D_3$
7	$\mathbb{Z}/7$
8	$\mathbb{Z}/8$, $\mathbb{Z}/2 \times \mathbb{Z}/4$, D_4, Q_8

$\varphi(r)$ must have order 3 and $\varphi(s)$ must have order 2. So we define $\varphi : D_3 \to S_3$ such that

$$\varphi(r) = (1\ 2\ 3), \qquad \varphi(s) = (1\ 2).$$

If φ is a homomorphism, it follows that $\varphi(1) = 1$ and

$$\begin{aligned} \varphi(r^2) &= \varphi(r)^2 = (1\ 3\ 2) \\ \varphi(r^2 s) &= \varphi(r)^2 \varphi(s) = (1\ 3\ 2)(1\ 2) = (2\ 3) \\ \varphi(rs) &= \varphi(r)\varphi(s) = (1\ 2\ 3)(1\ 2) = (1\ 3). \end{aligned}$$

What remains to check is that φ is *well-defined*. We have the relation $srs = r^2$, so in order for φ to be a function we must have $\varphi(srs) = \varphi(r^2)$. But

$$\varphi(srs) = (1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2),$$

so this is true. We see that from its values that it is bijective, and hence is an isomorphism.

Second method D_3 acts on a triangle which was labelled by its vertices $(1, 2, 3)$. Applying an element of D_3 to the triangle, we obtain a new triangle whose vertices have been permuted. Hence we obtain a function $\varphi : D_3 \to S_3$ which sends any symmetry in D_3 to the corresponding permutation in S_3. This map is well defined by construction, because given a n element in D_3 we have uniquely associated a permutation. The map is also a homomorphism by construction because composing two symmetries corresponds to composing the two corresponding permutations. The kernel of φ is $\{1\}$ because if a symmetry gives rise to the identity permutation, it means it is the identity symmetry. Thus φ is injective. Since $|D_6| = 6 = |S_3|$, any injection must be a bijection. Therefore, φ is an isomorphism.

7.3 List of groups of small order

Lecture 10 On 13/2

Table 7.1 shows a list of groups of small orders. We know from a previous lemma that the groups for $2, 3, 5, 7$ are exhaustive. Furthermore, we know that $\mathbb{Z}/4$ is exhaustive from a previous example.

Chapter 8

The alternating groups

Lecture 11
On 18/2

This chapter will introduce a family of normal subgrounds of the symmetric groups, called the *alternating groups*.

Let $x_1, \ldots, x_n$ be indeterminates and consider the polynomial

$$F(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i).$$

For example, for $n = 3$ we have

$$F(x_1, x_2, x_3) = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2).$$

Given $\sigma \in S_n$, we define F^σ by appling σ to the indices:

$$F^\sigma(x_1, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_{\sigma(j)} - x_{\sigma(i)}).$$

For example, if $\sigma = (2\ 3)$ then

$$F^\sigma(x_1, x_2, x_3) = (x_3 - x_1)(x_2 - x_1)(x_2 - x_3) = -F(x_1, x_2, x_3).$$

We always have

$$F^\sigma(x_1, \ldots, x_n) = (-1)^s F(x_1, \ldots, x_n)$$

for some integer s, and we call $(-1)^s$ the **sign** of σ and write $\operatorname{sgn}(\sigma) = (-1)^s$. We thus have a function $\operatorname{sgn} : S_n \to \{\pm 1\}$. The result of applying some σ_1 and then σ_2 to F is just the result of applying $\sigma_2\sigma_1$ to F. That is,

$$\begin{aligned}
(F^{\sigma_1}(x_1, \ldots, x_2))^{\sigma_2} &= (\operatorname{sgn}(\sigma_1) F(x_1, \ldots, x_n))^{\sigma_2} \\
&= \operatorname{sgn}(\sigma_1) \operatorname{sgn}(\sigma_2) F(x_1, \ldots, x_n) \\
&= F^{\sigma_2\sigma_1}(x_1, \ldots, x_n).
\end{aligned}$$

Hence $\operatorname{sgn}(\sigma_2\sigma_1) = \operatorname{sgn}(\sigma_2)\operatorname{sgn}(\sigma_1)$ and thus sgn is a group homomorphism.

Theorem 8.1. *For a given permutation $\sigma \in S_n$, the number of factors in any factorisation of σ into transpositions is even if* $\operatorname{sgn}(\sigma) = 1$ *and odd if* $\operatorname{sgn}(\sigma) = -1$.

Proof.

Claim We claim that for any transposition $\tau \in S_n$ we have

$$F^\tau(x_1, \dots, x_n) = -F(x_1, \dots, x_n),$$

and thus if σ is the product of s transpositions then

$$F^\sigma(x_1, \dots, x_n) = (-1)^s F(x_1, \dots x_n).$$

Proof of claim Let $\tau = (a\ b)$ such that $a > b$. Then

$$\begin{aligned}
F^\tau(x_1, \dots, x_n) &= \prod_{1 \le i < j \le n} \left(x_{\tau(j)} - x_{\tau(i)}\right) \\
&= \prod_{j \in \{2, \dots, n\}} \prod_{i \in \{1, \dots, j-1\}} \left(x_{\tau(j)} - x_{\tau(i)}\right) \\
&= \left(x_{\tau(2)} - x_{\tau(1)}\right) \dots \left(x_{\tau(a)} - x_{\tau(b)}\right) \dots \left(x_{\tau(n)} - x_{\tau(n-1)}\right) \\
&= \left(x_{\tau(2)} - x_{\tau(1)}\right) \dots (-1)\left(x_a - x_b\right) \dots \left(x_{\tau(n)} - x_{\tau(n-1)}\right) \\
&= -F(x_1, \dots, x_n).
\end{aligned}$$

This proves the claim. So if $\sigma \in S_n$ is factorised into transpositions, then

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ has an even number of factors} \\ -1 & \text{otherwise.} \end{cases}$$

$\square$

If $\operatorname{sgn}(\sigma) = 1$ for $\sigma \in S_n$ then we say that σ is an **even** permutation. If $\operatorname{sgn}(\sigma) = -1$ then we say that it is an **odd** permutation.

Example. (i) $(1\ 2\ 5) = (1\ 2)(2\ 5)$ is even.

(ii) $(4\ 8\ 9\ 6) = (4\ 8)(8\ 9)(9\ 6)$ is odd.

(iii) For *any* k-cycle $\sigma \in S_n$, we have

$$\operatorname{sgn}(\sigma) = (-1)^{k-1}$$

as every permutation is a product of transpositions.

▸

We can now define the *alternating groups*.

Definition 8.2. The **alternating group** A_n is the subgroup of S_n consisting of even permutations.

Remark. In other words, A_n is the kernel of sgn. △

Example. Recall the subgroups of S_3, we have

$$A_3 = \langle (1\ 2\ 3) \rangle = \{1, (1\ 2\ 3), (1\ 3\ 2)\}.$$

We know that A_4 has 12 elements, so A_4 is the subgroup consisting of 1, all 3-cycles, and all products of 2-cycles. ▶

Lecture 12
On 27/2

Example. How many 3-cycles are there in S_{10}? ▶

Solution. Consider the cycle $(a\ b\ c) \in S_{10}$. We have 10 choices for a, 9 choices for b, and 8 choices for c. The number of 3-cycles is

$$\frac{10 \cdot 9 \cdot 8}{3}$$

as we can shift each 3-cycle along twice, so we divide by 3 to get rid of duplicates. □

Chapter 9

Linear groups

Omitted due to strikes.

Chapter 10

Group actions

Example. The group S_n acts on the set $X = \{1, 2, \ldots, n\}$; that is, if $x \in X$, then an element $\sigma \in S_n$ sends x to $\sigma(x)$. ▶

Example. D_3 acts on a regular triangle which we can encode as a set of ordered triples

$$\{(1, 2, 3), (1, 3, 2), \ldots\}$$

where 1, 2, and 3 denote the vertices of the triangle. This set is then all the different positions that the triangle can take. For example, we saw that $r \in D_3$ acts on $(1, 2, 3)$ by sending it to $(3, 2, 1)$. ▶

Remark. One important notion of group actions is that if we first act by an element $h \in G$ and then by an element $g \in G$, that is the same as acting by the element $gh \in G$. △

Definition 10.1 (Group action)**.** Let G be a group and X a set. An **action** of G on X is a function

$$G \times X \to X, \qquad (g, x) \mapsto g * x$$

such that for all $g, h \in G$ and $x \in X$:

(i) $g * (h * x) = (gh) * x$; and

(ii) $1 * x = x$.

We usually write $g * x$ simply as gx.

Remark. We can think of a group actions as *multiplying elements of the group onto points of a space.* △

Example. $\mathbb{Z}$ can act on $\mathbb{R}$ by translation. That is, for $n \in \mathbb{Z}$ and $x \in \mathbb{R}$ we can define

$$n * x = n + x.$$

We have

(i)
$$m * (n * x) = m + (n + x) = (m + n) + x = (m * n) * x; \text{ and}$$

(ii)
$$0 * x = 0 + x = x.$$

▶

Example. $\mathbb{Z}$ can also act on $\mathbb{R}$ in another way:

$$n * x = (-1)^n x.$$

We check that this is indeed an action:

(i)
$$m*(n*x) = m*(-1)^n x = (-1)^m(-1)^n * x = (-1)^{m+n} x = (m+n)*x; \text{ and}$$

(ii)
$$0 * x = (-1)^0 x = x.$$

▶

10.1 Orbits and stabilisers

Definition 10.2. Let G be a group acting on a set X. For any $x \in X$, we define the **orbit of** x as

$$\mathrm{Orb}(x) = \{gx : g \in G\},$$

and the **stabiliser of** x as

$$\mathrm{Stab}(x) = \{g \in G : gx = x\}.$$

Remark. $\mathrm{Stab}(x)$ is a subgroup of G, but in general there is no reason for $\mathrm{Orb}(x)$ to be a group (it should be thought of as a space). △

Lecture 13
On 17/3

Example. Recall how $\mathbb{Z}$ acts on $\mathbb{R}$ as a translation. Let $x \in \mathbb{R}$. Then

$$\mathrm{Orb}(x) = \{n + x : n \in \mathbb{Z}\} = \mathbb{Z} + x,$$
$$\mathrm{Stab}(x) = \{n \in \mathbb{Z} : n + x = x\} = \{0\}.$$

▶

Example. Recall the other way that showed that $\mathbb{Z}$ could act on $\mathbb{R}$ ($n * x = (-1)^n x$). Then for $x \in \mathbb{R}$

$$\mathrm{Orb}(x) = \{(-1)^n x : n \in \mathbb{Z}\} = \{\pm x\},$$
$$\mathrm{Stab}(x) = \{n \in \mathbb{Z} : (-1)^n x = x\} = \begin{cases} 2\mathbb{Z} & \text{if } x \neq 0, \\ \mathbb{Z} & \text{otherwise.} \end{cases}$$

▶

10.2 Cosets and conjugacy classes as orbits

Any group G acts on itself: for $g \in G$ we have $x \mapsto gx$ for $x \in G$. Here

$$\begin{aligned}\mathrm{Orb}(x) &= G,\\ \mathrm{Stab}(x) &= 1.\end{aligned}$$

Let $H \subset G$ be a subset of G and let it act on G as above. For $x \in G$ we have

$$\mathrm{Orb}(x) = \{hx : h \in H\} = Hx,$$

a right coset of H.

Consider the action $x \mapsto gxg^{-1}$ for $g, x \in G$ of G on itself (easy exercise to check that this is an action). We call this action **conjugation**. Under tis action, the orbit

$$\mathrm{Orb}(x) = \{gxg^{-1} : g \in G\}$$

is called a **conjugacy class** (of x). The stabiliser

$$\mathrm{Stab}(x) = \{g \in G : gxg^{-1} = x\}$$

is called the **centraliser** (of x), and is usually denoted $C_G(x)$.

Example. Find the conjugacy classes in D_5. ▸

Solution.

(i) $1 \in D_5$ is *always* fixed by any conjugations, hence $\mathrm{Orb}(1) = \{1\}$.

(ii) Now take $r \in D_5$, it is fixed by any power of r (that is, $r^i r r^{-i} = r$) and

$$(r^i s)r(r^i s)^{-1} = r^{-1} = r^4$$

so

$$\mathrm{Orb}(r) = \{r, r^4\}.$$

(iii) Now lets consider $r^2 \in D_5$. Again, conjugation by r^i on r^2 fixes r^2, but

$$(r^i s)r^2(r^i s)^{-1} = r^{-2} = r^3$$

so

$$\mathrm{Orb}(r^2) = \{r^2, r^3\}.$$

(iv) Now finally we will consider $s \in D_5$. We have

$$\begin{aligned}(r^i)s(r^{-i}) &= r^{2i}s,\\ (r^i s)s(r^i s)^{-1} &= r^{2i}s.\end{aligned}$$

Therefore,

$$\mathrm{Orb}(s) = \{s, r^2 s, r^4 s, rs, r^3 s\}$$

and we have exhausted all elements in D_5, hence our conjugacy classes are

$$\{1\}, \quad \{r, r^4\}, \quad \{r^2, r^3\}, \quad \{s, rs, r^2 s, r^3 s, r^4 s\}.$$

□

Chapter 11

The Orbit-Stabiliser theorem

Theorem 11.1. *Let G be a group acting on a set X, and let $x \in X$. Then there is a bijection*

$$\beta : \mathrm{Orb}(x) \to \{g\,\mathrm{Stab}(x) : g \in G\}, \qquad \beta(gx) = g\,\mathrm{Stab}(x).$$

In particular, if G is finite then

$$|\mathrm{Orb}(x)| = \frac{|G|}{|\mathrm{Stab}(x)|}.$$

Example. Recall the conjugacy classes of D_5. We saw that

$$\mathrm{Orb}(r) = \{r, r^4\}.$$

Now

$$\begin{aligned} \mathrm{Stab}(r) &= \{r^i s^j \in D_5 : (r^i s^j) r (r^i s^j)^{-1} = r\} \\ &= \langle r \rangle \cup \{r^i s \in D_5 : r^i s r s r^{-i} = r^{-1} = r\} \\ &= \langle r \rangle \end{aligned}$$

so $|\mathrm{Orb}(r)| = 2$ and $|\mathrm{Stab}(x)| = 5$, which agrees wth the Orbit-Stabiliser theorem. Moreover, $\mathrm{Orb}(s)$ has five elements, so $\mathrm{Stab}(x)$ must have 2 elements. Indeed

$$\begin{aligned} \mathrm{Stab}(s) &= \{r^i : r^i s r^{-i} = s\} \cup \{r^i s : r^i s s (r^i s)^{-1} = s\} \\ &= \{r^i : r^{2i} = 1\} \cup \{r^i s : r^{2i} = 1\} \\ &= \{1, s\}. \end{aligned}$$

▸

11.1 Cauchy's theorem

Theorem 11.2 (Cauchy). *Let G be a finite group and p be a prime such that p divides the order of G. Then G has a cyclic subgroup of order p (equivalently, G has an element of order p).*

Example. D_{20} has a subgroup of order 5 as $|D_{20}| = 40 = 8 \cdot 5$. ▸

Chapter 12

Finite abelian cnd cyclic groups

Lecture 14
On 19/3

Theorem 12.1. *Let G be a finite abelian group. Then G is isomorphic to*

$$\mathbb{Z}/a_1 \times \mathbb{Z}/a_2 \times \ldots \times \mathbb{Z}/a_t$$

for some t, $a_i \in \mathbb{N}$, $a_1 \geq 2$ such that

$$a_1 \mid a_2 \mid \ldots \mid a_t.$$

Moreover, the integers a_i are uniquely determined by G.

Proof. Omitted. □

Theorem 12.2 (CRT)**.** *Suppose that $m, n \in \mathbb{N}$ are coprime. Then*

$$\mathbb{Z}/mn \cong \mathbb{Z}/m \times \mathbb{Z}/n.$$

Proof. Omitted. □

Example. (i) $\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$.

(ii) $\mathbb{Z}/4 \ncong \mathbb{Z}/2 \times \mathbb{Z}/4$.

(iii) Let $G = \mathbb{Z}/12$. We know that

$$\mathbb{Z}/12 \cong \mathbb{Z}/a_1 \times \ldots \times \mathbb{Z}/a_t$$

for some $t \in \mathbb{N}$ and $a_i \in \mathbb{Z}$. Moreover, we have

$$\mathbb{Z}/12 \cong \mathbb{Z}/4 \times \mathbb{Z}/3,$$

but $4 \not| 3$ and $3 \not| 4$ so 3 and 4 cannot take our values of a_i stated above. We see that $\mathbb{Z}/12 \cong \mathbb{Z}/a_1$ where $a_i = 12$, and is unique. Hence there are no other decompositions of $\mathbb{Z}/12$. For example, if $a_1 = 2$ and $a_2 = 6$ then we know

$$\mathbb{Z}/12 \ncong \mathbb{Z}/2 \times \mathbb{Z}/6.$$

▸

Example. Find (up to isomorphisms) all the abelian groups of order 16. ▸

Solution. By the first theorem presented in the chapter, we need to find the groups of the form

$$\mathbb{Z}/2^{a_1} \times \mathbb{Z}/2^{a_2} \times \ldots \times \mathbb{Z}/2^{a_n}$$

with $a_1 \geq 1$ such that $a_1 + \ldots + a_n = 4$. We have five possibilities:

(i) $1 + 1 + 1 + 1 = 4$;

(ii) $1 + 1 + 2 = 4$;

(iii) $1 + 3 = 4$;

(iv) $2 + 2 = 4$; and

(v) $4 = 4$.

Hence are possible abelian groups are

(i) $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$;

(ii) $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/4$;

(iii) $\mathbb{Z}/2 \times \mathbb{Z}/8$;

(iv) $\mathbb{Z}/4 \times \mathbb{Z}/4$; and

(v) $\mathbb{Z}/16$.

□

12.1 Cyclic groups

Theorem 12.3. *Let G be a finite cyclic group, $x \in G$, and $a \in \mathbb{Z}$ with $a \neq 0$. Then the following hold.*

(i) If $n = \mathrm{ord}(x)$, then $\mathrm{ord}(x^a) = \frac{n}{\gcd(n,a)}$.

(ii) $\langle x \rangle = \langle x^a \rangle$ if and only if $\gcd(n, a) = 1$. Thus the number of generators of $\langle x \rangle$ is $\varphi(n)$ (Euler's totient function).

Proof. Omitted. □

Example. We have $\mathbb{Z}/20 = \langle \overline{1} \rangle$ and an element $\overline{a} = a \cdot \overline{1}$ generates the whole group if and only if

$$\mathrm{ord}(\overline{a}) = \frac{20}{\gcd(20, a)} = 20 \qquad \Longleftrightarrow \qquad \gcd(20, a) = 1.$$

Thus $\mathbb{Z}/20$ has $\varphi(20) = \varphi(4)\varphi(5) = 2 \cdot 4 = 8$ generators, namely

$$\overline{1}, \overline{3}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{17}, \overline{19}.$$

▸

Theorem 12.4. *Let $H = \langle x \rangle$ be a fintie cyclic group of order n. Then every subgroup of H is cyclc and for each $a \in \mathbb{N}$ dividing n there is a unique subgroup of order a, namely $\langle x^{n/a} \rangle$.*

Example. Find all the subgroups of $\mathbb{Z}/12$. ▸

Solution. We know that every subgroup is cyclic and that for any positive divisor d of 12, there is a unique subgroup of order d generated by $\overline{12/d}$. The possible divisors are

$$1, 2, 3, 4, 6, 12.$$

We thus have the corresponding six subgroups:

$$\begin{aligned}
\langle \overline{12} \rangle &= \{\overline{0}\} \\
\langle \overline{12/2} \rangle &= \{\overline{0}, \overline{6}\} \\
\langle \overline{12/3} \rangle &= \{\overline{4}, \overline{8}, \overline{0}\} \\
\langle \overline{12/4} \rangle &= \{\overline{3}, \overline{6}, \overline{9}, \overline{0}\} \\
\langle \overline{12/6} \rangle &= \{\overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{0}\} \\
\langle \overline{12/12} \rangle &= \{\overline{1}\} = \mathbb{Z}/12.
\end{aligned}$$

□