IB Groups, Rings and Modules

Martin von Hodenberg (mjv43@cam.ac.uk)

February 2, 2022

These are my notes for the IB course 'Groups, Rings and Modules', which was lectured in Lent 2022 at Cambridge by Dr R.Zhou. These notes are written in LaTeX for my own revision purposes. Any suggestions or feedback is welcome.

Contents

0 Introduction **2**

1 Groups **2**

1.1 Recall of IA Groups 2
1.2 Simple groups 6
1.3 Group actions 7
1.4 Alternating groups 10
1.5 p-groups and p-subgroups 12
1.6 The Sylow theorems 13
1.7 Matrix groups 15

§0 Introduction

This course will contain several sections:

1. Groups; this will be a continuation from IA, focusing on simple groups, p-groups, and p-subgroups. The main result in this part of the course will be the Sylow theorems.
2. Rings; these are sets where you can add, subtract and multiply (e.g $\mathbb{Z}$ or $\mathbb{C}[X]$). We will study rings of integers such as $\mathbb{Z}[i], \mathbb{Z}[\sqrt{2}]$. These also generalise to polynomial rings. We will also study fields, which are rings where you can divide (e.g $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ or $\mathbb{Z}/p\mathbb{Z}$ for p prime).
3. Modules; these are an analogue of vector spaces where the scalars belong to a ring instead of a field. We will classify modules over certain "nice" rings. This allows us to prove Jordan Normal Form, and classify finite abelian groups.

§1 Groups

The first subsection will just recap the results seen in IA Groups; it can be skipped by anyone with a sufficient knowledge of the course.

§1.1 Recall of IA Groups

Definition (Group)

A group is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$ is a binary operation satisfying:

1. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associativity)
2. $\exists e \in G$ such that $e \cdot g = g \cdot e = g$ for all $g \in G$ (identity)
3. $\forall g \in G$, $\exists g^{-1} \in G$ such that $g \cdot g^{-1} = g^{-1} \cdot g = e$ (inverses)

Remarks.

- In practice, one often needs to check closure in order to check that $\cdot$ is well-defined.
- If using additive (respectively multiplicative) relations, we will often write 0 (or 1) for the identity.
- We write $|G|$ for the number of elements in G.

Definition (Subgroup)

A subset $H \subseteq G$ is a subgroup (written $H \leq G$) if H is closed under $\cdot$ and $(H, \cdot)$ is a group.

Remark. A non-empty subset H of G is a subgroup if $a, b \in H \implies a \cdot b^{-1} \in H$ (see IA Groups for the proof).

Example (Examples of groups)

Groups we have already seen include:

- Additive groups $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +)$.
- Cyclic and dihedral groups C_n and D_{2n}.
- Abelian groups: those groups G such that $a \cdot b = b \cdot a$ for all $a, b \in G$.
- Symmetric and alternating groups S_n = group of all permutations of $\{1, \ldots, n\}$ and $A_n \leq S_n$, the group of all even permutations.
- Quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ where i, j, k are quaternions.
- General and special linear groups $GL_n(\mathbb{R}) = n \times n$ matrices on $\mathbb{R}$ with $\det \neq 0$, where the group operation is matrix multiplication. This contains the subgroup $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$, which is the subgroup of matrices with $\det = 1$.

Definition (Direct product)

The direct product of groups G and H is the set $G \times H$ with operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Theorem 1.1.1 (Lagrange's theorem)

Let $H \leq G$. Then the left cosets of H in G are the sets $gH = \{gh : h \in H\}$ for $g \in G$. These partition G, and each has the same cardinality as H. From this we can deduce Lagrange's theorem:

If G is a finite group and $H \leq G$, then $|G| = |H|[G : H]$ where $[G : H]$ is the number of left cosets of H in G (the index of H in G).

Remark. Can also carry this out with right cosets. A corollary of Lagrange's theorem is thus that the number of left cosets = number of right cosets.

Definition (Order of an element)

Let $g \in G$. If $\exists n \geq 1$ such that $g^n = 1$, then the least such n is the order of g in G. If no such n exists, g has infinite order.

Remark. If g has order d, then

- $g^n = 1 \implies d | n$.
- $\{1, g, \ldots, g^{d-1}\} \leq G$ and so if G is finite, then $d || G|$ (Lagrange).

Definition (Normal subgroup)

A subgroup $H \leq G$ is normal if $g^{-1} H g = H$ for all $g \in G$. We write $H \trianglelefteq G$.

Proposition 1.1.2

If $H \trianglelefteq G$ then the set G/H of left cosets of H in G is a group (called the quotient group) with operation

$$g_1H \cdot g_2H = g_1g_2H.$$

Proof. Check $\cdot$ is well-defined:

Suppose $g_1H = g_1'H$ and $g_2H = g_2'H$ for some $g_1, g_1', g_2, g_2' \in G$. Then $g_1' = g_1h_1$ and $g_2' = g_2h_2$ for some $h_1, h_2 \in H$. Therefore

$$\begin{aligned} g_1'g_2' &= g_1h_1g_2h_2 \\ &= g_1g_2 \underbrace{({g_2}^{-1}h_1g_2)}_{\in H} \underbrace{h_2}_{\in H} \end{aligned}$$

Therefore $g_1'g_2'H = g_1g_2H$. Associativity is inherited from G, the identity is $H = eH$, and the inverse of gH is $g^{-1}H$. □

Definition (Homomorphism)

If G, H are groups, then a function $\phi : G \to H$ is a group homomorphism if $\phi(g_1g_2) = \phi(g_1g_2) = \phi(g_1)\phi(g_2)$. It has kernel

$$\ker\phi = \{g \in G : \ \phi(g) = e\} \leq G.$$

and image

$$\operatorname{Im}\phi = \{\phi(g) : \ g \in G\} \leq H.$$

Remark. If $a \in \ker\phi$ and $g \in G$, then

$$\begin{aligned} \phi(g^{-1}ag) &= \phi(g^{-1})\phi(a)\phi(g) \\ &= \phi(g^{-1})\phi(g) \\ &= \phi(g^{-1}g) = \phi(e) = e. \end{aligned}$$

So $g^{-1}ag \in \ker\phi$ and hence $\ker\phi$ is a normal subgroup of G.

Definition (Isomorphism)

An isomorphism of groups is a group homomorphism that is also a bijection. We say G and H are isomorphic and write $G \cong H$ if there exists an isomorphism $\phi : G \to H$. (Note it follows from the definition that ϕ^{-1} is also a group homomorphism)

Theorem 1.1.3 (First Isomorphism Theorem)

Let $\phi : G \to H$ be a group homomorphism. Then $\ker\phi \trianglelefteq G$ and

$$G/\ker\phi \cong \operatorname{Im}\phi.$$

Proof. Let $K = \ker\phi$. We have already checked K is normal. Now we define $\Phi : G/K \to \operatorname{Im}\phi$ by

$$gK \to \phi(g)..$$

To show Φ is well defined and injective:

$$\begin{aligned} g_1K = g_2K &\iff {g_2}^{-1}g_1 \in K \\ &\iff \phi({g_2}^{-1}g_1) = e \\ &\iff \phi(g_1) = \phi(g_2). \end{aligned}$$

To show Φ is a group hom.:

$$\begin{aligned} \Phi(g_1Kg_2K) &= \Phi(g_1g_2K) \\ &= \phi(g_1g_2) = \phi(g_1)\phi(g_2) \\ &= \Phi(g_1K)\Phi(g_2K) \end{aligned}$$

Showing Φ is surjective:

Let $x \in \operatorname{Im}\phi$, say $x = \phi(g)$ for some $g \in G$. Then $x = \phi(gR)$. □

Example

Let $\phi : \mathbb{C} \to \mathbb{C}^x = \{x \in C : x \neq 0\}$ given by $z \mapsto e^z$.

Since $e^{z+w} = e^z e^w$, this is a group homomorphism from $(\mathbb{C}, +) \to (\mathbb{C}^x, \times)$. We have that

$$\begin{aligned} \ker\phi &= \{z \in \mathbb{C} : \ e^x = 1\} = 2\pi i\mathbb{Z} \\ \operatorname{Im}\phi &= \mathbb{C}^x \text{ by existence of log} \end{aligned}$$

Hence $\mathbb{C}/2\pi i\mathbb{Z} \cong \mathbb{C}^x$.

Theorem 1.1.4 (Second Isomorphism Theorem)

Let $H \leq G$, and $K \trianglelefteq G$. Then $HK = \{hk : h \in H, k \in K\} \leq G$ and $H \cap K \trianglelefteq H$. Moreover,

$$HK/K \cong H/(H \cap K).$$

Proof. Let $h_1k_1, h_2k_2 \in HK$ (so $h_1h_2 \in H,\ k_1k_2 \in K$). Now

$$h_1k_1(h_2k_2)^{-1} = \underbrace{h_1{h_2}^{-1}}_{\in H}\underbrace{(h_2k_1{k_2}^{-1}{h_2}^{-1})}_{\in K} \in HK.$$

Thus $HK \leq G$ (by our previous remark). Let $\phi : H \to G/K$ be given by $h \to hK$. This is the composite of $H \to G$ and the quotient map $G \to G/K$; hence ϕ is a group homomorphism. Thus

$$\begin{aligned} \ker\phi &= \{h \in H : hK = K\} = H \cap K \trianglelefteq H \\ \operatorname{Im}\phi &= \{hK : \ h \in H\} = HK/K \end{aligned}$$

Now by the First Isomorphism Theorem

$$HK/K \cong H/(H \cap K).$$

□

Remark (1.2)**.** Suppose $K \trianglelefteq G$. There is a bijection

$$\{\text{subgroups of } G/K\} \leftrightarrow \{\text{subgroups of } G \text{ containing } K\},$$

where $X \mapsto \{g \in G : gK \in X\}$ and $H/K \leftarrow H$. This further restricts to a bijection

$$\{\text{normal subgroups of } G/K\} \leftrightarrow \{\text{normal subgroups of } G \text{ containing } K\},$$

Theorem 1.1.5 (Third Isomorphism Theorem)
Let $K \leq H \leq G$ be normal subgroups of G. Then

$$\frac{G/K}{H/K} \cong G/H.$$

Proof. Let $\phi : G/K \to G/K$ be defined by $gK \mapsto gH$. If $g_1K = g_2K$, then ${g_2}^{-1}g_1 \in K \leq H \implies g_1H = g_2H$. Thus ϕ is well-defined.

Thus ϕ is a surjective homomorphim with kernel H/K. Now just apply the First Isomorphism Theorem. □

§1.2 Simple groups

If $K \trianglelefteq G$, then studying the groups K and G/K gives some information about G. However, this approach is not always available. This is the case when a group is simple.

Definition (Simple group)
A group G is simple if $\{e\}$ and G are its only normal subgroups.

Remark. It is convention to not consider the trivial group a simple group.

Lemma 1.2.1
Let G be an abelian group. G is simple iff $G \cong C_p$ for some prime p.

Proof. $\impliedby$**:** Let $H \leq C_p$. Lagrange's theorem says that $|H| \,||C_p| = p$. Since p is prime, $|H| = 1$ or p. So H is the trivial group or C_p.

$\implies$**:** Let $g \in G$ where $g \neq e$. Consider the subgroup generated by g:

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

This is normal in G since G is abelian. Since G is simple, $\langle g \rangle = G$. If G is infinite, $G \cong (\mathbb{Z}, +)$ and $2\mathbb{Z} \leq \mathbb{Z}$ which gives a contradiction.

Otherwise, we now know $G \cong C_n$ for some n. Let g be a generator. If $m|n$ then $g^{n/m}$ generates a subgroup of order m and so G simple $\implies$ the only factors of n are 1 and n. Therefore n is prime. □

Lemma 1.2.2

If G is a finite group, then G has a composition series

$$e = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m = G,$$

with each quotient G_i/G_{i-1} simple.

Proof. We induct on $|G|$. If $|G| = 1$ it's obvious. If $|G| > 1$, let G_{m-1} be a normal subgroup of largest possible order that isn't G itself. Remark 1.2 implies G/G_{m-1} is simple. Then apply the induction hypothesis to G_{m-1}. □

§1.3 Group actions

Definition (Permutation group)

For X any set, let $\mathrm{Sym}(X)$ be the group of all bijections $X \to X$ under composition. This clearly forms a group with $e = \mathrm{Id}_X$.

A group G is a permutation group of degree n if $G \leq \mathrm{Sym}(X)$ with $|X| = n$.

Example (Examples of permutation group)

- $S_n = \mathrm{Sym}(\{1, 2, \ldots, n\})$ is a permutation group of degree n, as is $A_n \leq S_n$.
- $D_{2n} =$ (symmetries of a regular n-gon) is a subgroup of $\mathrm{Sym}(\{\text{vertices of n-gon}\})$.

Definition (Group action)

An actio of a group G on a set X is a function $* : G \times X \to X$ satisfying

(i) $e * x = x$ for all $x \in X$

(ii) $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G$, $x \in X$.

Proposition 1.3.1

An action of a group G on a set X is equivalent to specifying a group homomorphism $\phi : G \to \mathrm{Sym}(X)$.

Proof. For each $g \in G$, let $\phi_g : X \to X$ send $x \mapsto g * x$.

We have $\phi_{g_1 g_2}(x) = (g_1 g_2) * x = g_1 * (g_2 * x) = \phi_{g_1} \circ \phi_{g_2}(x)$. (†)

In particular, $\phi_g \circ \phi_{g^{-1}} = \phi_{g^{-1}} \circ \phi_g = \phi_e = \mathrm{Id}_X$. Thus $\phi_g \in \mathrm{Sym}(X)$. Then the map $\phi : G \to \mathrm{Sym}(X)$ given by $g \mapsto \phi_g$ is a group homomorphism by (†).

Conversely, let $\phi : G \to \mathrm{Sym}(X)$ be a group homomorphism. Define $* : G \times X \to X$ given by $(g, x) \mapsto \phi(g)(x)$. Then

(i) $e * x = \phi(e)(x) = \mathrm{Id}_X(x) = x$.

(ii) $(g_1g_2) * x = \phi(g_1g_2)(x) = \phi(g_1)(\phi(g_2)(x)) = g_1 * (g_2 * x)$.

□

Definition

We say $\phi : G \to \mathrm{Sym}(X)$ is a permutation representation of G.

Definition (Orbit and stabiliser)

Let G act on a set X.

(i) The orbit of $x \in X$ is $\mathrm{orb}_G(x) = \{g * x : \ g \in G\} \subset X$

(ii) The stabiliser of $x \in X$ is

$$G_x = \{g \in G : \ g * x = x\} \leq G.$$

Recall the Orbit-Stabiliser Theorem from IA Groups: There is a bijection $\mathrm{orb}_G(x) \leftrightarrow$ the set of left cosets of G_x in G. In particular if G is finite, then

$$|G| = |\mathrm{orb}_G(x)||G_x|.$$

Example (Example of Orbit-Stabiliser)

Let G be the group of all symmetries of a cube, acting on the set of veretices X. We can reach any vertex from any other one, so $|\mathrm{orb}_G(x)| = 8$. Some basic geometry gives $|G_x| = 6$. Therefore $|G| = 48$.

Remark.

- $\ker \phi = \bigcap_{x \in X} G_x$ is called the kernel of the group action.
- The orbits partition X. We say the action is transitive if there is only one orbit.
- $G_{g*x} = gG_xg^{-1}$, so if $x, y \in X$ belong to the same orbit, then their stabilisers are conjugate.

Later on a lot of the proofs will involve picking a nice group action. So let's look at some examples of group actions.

(i) Let G act on itself by left multiplication, i.e $g * x = gx$. The kernel of this action is

$$\{g \in G : gx = x \quad \forall x \in G\} = e.$$

Thus G is injective into $\mathrm{Sym}(G)$. This proves Cayley's theorem:

Theorem 1.3.2 (Cayley's theorem)

Any finite group G is isomorphic to a subgroup of the symmetric group S_n for some n. (Take $n = |G|$.)

Proof. As above in (i). □

(ii) Let $H \leq G$; then G acts on G/H by left multiplication, i.e $g * xH = gxH$. This action is transitive (since $(x_2 {x_1}^{-1})x_1 H = x_2 H$) with

$$\begin{aligned} G_{xH} &= \{g \in G : gxH = xH\} \\ &= \left\{g \in G : x^{-1}gx \in H\right\} \\ &= xHx^{-1} \end{aligned}$$

Thus $\ker(\phi) = \bigcap_{x \in G} xHx^{-1}$. This is the largest normal subgroup of G that is contained in H.

Theorem 1.3.3

Let G be a non-abelian simple group, and $H \leq G$ a subgroup of index $n > 1$. Then $n \geq (5$ and G is isomorphic to a subgroup of A_n.

Proof. Let G act on $X = G/H$ by left multiplication, and let $\phi : G \to \mathrm{Sym}(X)$ be the associated permutation representation. As G is simple, $\ker(\phi) = e$ or G. If $\ker(\phi) = G$, then $\mathrm{Im}(\phi) = e$. This is a contradiction since G acts transitively on X and $|X| > 1$. Thus $\ker(\phi) = e$ and $G \cong \mathrm{Im}(\phi) \leq S_n$. Since $G \leq S_n$ and $A_n \trianglelefteq S_n$, the second isomorphism theorem gives $G \cap A_n \trianglelefteq G$ and $G/(G \cap A_n) \cong GA_n/A_n \leq S_n/A_n \cong C_2$. Since G is simple, $G \cap A_n = e$ (this is impossible as $G \leq C_2$ but G isn't abelian) or G. Thus $G \leq A_n$. Finally, if $n \leq 4$, then A_n has no non-abelian simple subgroups. □

(iii) Let G act on itself by conjugation, i.e $g * x = gxg^{-1}$. We define the conjugacy class of $x \in G$ to be

$$\mathrm{ccl}_G(x) = \mathrm{orb}_G(x) = \left\{gxg^{-1} \in G : \quad g \in G\right\}.$$

We also define the centraliser of x by

$$C_G(x) = G_x = \{g \in G : \quad gx = xg\} \leq G.$$

We define the centre of G by

$$Z(G) = \mathrm{Ker}(\phi) = \{g \in G : \quad gx = xg \ \forall x \in G\}.$$

Note that the $\phi(g) : G \to G$ given by $h \mapsto ghg^{-1}$ satisfies

$$\phi(g)(h_1 h_2) = gh_1 h_2 g^{-1} = gh_1 g^{-1} gh_2 g^{-1} = \phi(g)(h_1)\phi(g)(h_2).$$

Thus $\phi(g)$ is a group homomorphism, and also a bijection i.e $\phi(g)$ is an isomorphism.

Definition (Automorphism)

$\mathrm{Aut}(G) = \{$ group isomorphisms $\zeta : G \to G\}$. Then $\mathrm{Aut}(G) \leq \mathrm{Sym}(G)$ and $\phi : G \to \mathrm{Sym}(G)$ has image in $\mathrm{Aut}(G)$.

(iv) Let X be the set of all subgroups of G. Then G acts on X by conjugation, i.e $g * H = gHg^{-1}$. The stabiliser of H is

$$\left\{g \in G : \quad gHg^{-1} = H\right\} = N_G(H).$$

This is also called the normaliser of H in G, and is the largest subgroup of G containing H as a normal subgroup. In particular,

$$H \trianglelefteq G \iff N_G(H) = G.$$

§1.4 Alternating groups

From IA Groups, we know that elements in S_n are conjugate iff they have the same cycle type. For example, in S_5, we have the following:

Cycle type	Number of elements	Sign
id	1	+1
$(**)$	10	-1
$(**)(**)$	15	+1
$(***)$	20	+1
$(**)(***)$	20	-1
$(****)$	30	-1
$(*****)$	24	+1
Total:	$120=5!=\lvert S_5\rvert$	

Let $g \in A_n$. Then $C_{A_n}(g) = C_{S_n}(g) \cap A_n$. We effectively have two cases:

- If there exists an odd permutation commuting with g, then $|C_{A_n}(g)| = \frac{1}{2}|C_{S_n}(g)|$ and by Orbit-Stabiliser, $|\operatorname{ccl}_{A_n}(g)| = |\operatorname{ccl}_{S_n}(g)|$.
- Otherwise, $|C_{A_n}(g)| = |C_{S_n}(g)|$ and by Orbit-Stabiliser, $|\operatorname{ccl}_{A_n}(g)| = \frac{1}{2}|\operatorname{ccl}_{S_n}(g)|$.

Example (Conjugacy classes of A_5)

If we take $n = 5$, then first consider the element $(12)(34)$, which commutes with (12). Also, (123) commutes with (45).

But if we take $g = (12345)$, then $h \in C_{S_5}(g)$ means

$$\begin{aligned}(12345) &= h(12345)h^{-1} \\ &= (h(1)h(2)h(3)h(4)h(5)) \implies h \in \langle g\rangle \leq A_5.\end{aligned}$$

In this case, the conjugacy class does split.

Thus A_5 has conjugacy classes of sizes 1,15,20,12,12.

Proposition 1.4.1

A_5 is simple.

Proof. If $H \trianglelefteq A_5$, then H is a union of conjugacy classes. Therefore

$$|H| = 1 + 15a + 20b + 12c \quad \text{for some } a, b \in \{0, 1\} \text{ and } c \in \{0, 1, 2\}.$$

Since $H|60$, this implies $H = 1$ or 60, i.e A_5 is simple. □

Now we move on to a more general statement about A_n being simple. Before we can do that, we will need some lemmas for the proof.

Lemma 1.4.2

A_n is generated by 3-cycles.

Proof. Each $\sigma \in A_n$ is a product of an even number of transpositions. Thus it suffices to write the product of any two transpositions as a product of 3-cycles. For a, b, c, d distinct, we can have

$$\begin{cases} (ab)(bc) = (abc) \\ (ab)(cd) = (acb)(acd). \end{cases}$$

□

Lemma 1.4.3

If $n \geq 5$, then all 3-cycles in A_n are conjugate.

Proof. We claim that every 3-cycle is conjugate to (123). Indeed, if (abc) is a 3-cycle, then $(abc) = \sigma(abc)\sigma^{-1}$ for some $\sigma \in S_n$. If $\sigma \notin A_n$, then replace σ by $\sigma(45)$ (using the fact that $n \geq 5$). □

Theorem 1.4.4

A_n is simple for all $n \geq 5$.

Proof. Let $e \neq N \trianglelefteq A_n$. Suffices to show that N contains a 3-cycle, since by 1.4.2 and 1.4.3 we then have $N = A_n$.

Take $e \neq \sigma \in N$ and write σ in its disjoint cycle decomposition. Consider the cases:

1. σ contains a cycle of length $r \geq 4$. WLOG $\sigma = (123\dots r)\tau$, where τ is some product of cycles that fixes $1, 2, \dots, r$.

   Let $\delta = (123)$. Then consider the element

   $$\underbrace{\sigma^{-1}}_{\in N}\underbrace{\delta^{-1}\sigma\delta}_{\in N} = (r\dots 21)(132)(12\dots r)(123) = (23r) \in N.$$

   Note τ gets cancelled as it fixes 1 to r. Therefore N contains a 3-cycle.

2. σ contains two 3-cycles. WLOG $\sigma = (123)(456)\tau$. Let $b = (124)$. Then

   $$\sigma^{-1}\delta^{-1}\sigma\delta = (132)(465)(142)(123)(456)(124) = (12436) \in N.$$

   Then we are back to Case 1, so N contains a 3-cycle..

3. σ contains two 2-cycles. WLOG $\sigma = (12)(34)\tau$. Let $\delta = (123)$ and consider

   $$\sigma^{-1}\delta^{-1}\sigma\delta = (12)(34)(132)(12)(34)(123) = (14)(23) = \pi \in N.$$

   Let $\varepsilon = (235)$. Then

   $$\pi^{-1}\varepsilon^{-1}\pi\varepsilon = (14)(23)(253)(14)(23)(235) = (253).$$

   Thus N contains a 3-cycle.

To conclude the proof, we consider the remaining cases:

1. Cycle type $(* *) \implies \sigma \notin A_n$.
2. Cycle type $(***) \implies \sigma$ is a 3-cycle.
3. Cycle type $(**)(***) \implies \sigma \notin A_n$.

This concludes the proof. □

§1.5 p-groups and p-subgroups

Definition (p-group)

Let p be a prime. A finite group G is a p-group if $|G| = p^n$, $n \geq 1$.

Theorem 1.5.1

If G is a p-group, then $Z(G) \neq 1$.

Proof. For $g \in G$, we have $|\operatorname{ccl}_G(g)||C_G(g)| = |G| = p^n$. So each conjugacy class must have size that is a power of p. Since G is a dijoint union of conjugacy classes,

$$\begin{aligned} |G| \equiv (\text{number of conjugacy classes of size } 1) \mod p \\ \implies 0 \equiv |Z(G)| \mod p \\ \implies Z(G) \neq 1. \end{aligned}$$

We have used the fact that the conjugacy classes of size 1 are precisely the elements of $Z(G)$:

$$g \in Z(G) \iff x^{-1}gx = g \ \forall x \in G \iff \operatorname{ccl}_G(g) = \{g\}.$$

□

Corollary 1.5.2

The only simple p-group is C_p.

Proof. Let G be a simple p-group. Since $Z(G) \trianglelefteq G$, we have $Z(G) = 1$ or G. By 1.5.1, we must have $Z(G) = G$. Therefore G is abelian. Conclude by Lemma 1.2.1. □

Corollary 1.5.3

Let G be a p-group of order p^n. Then G has a subgroup of order p^r for $0 \leq r \leq n$.

Proof. By Lemma 1.2.2, G has a composition series

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{m-1} \trianglelefteq G_m = G.$$

with each G_i/G_{i-1} simple. Since G is a p-group, all of the G_i/G_{i-1} must be p-groups. Therefore have by Proposition 1.5.2 that $G_i/G_{p-1} \cong C_p$.

Thus $|G_i| = p^i$ for all $0 \leq i \leq m$ and $m = n$. □

Lemma 1.5.4

For G a group, if $G/Z(G)$ is cyclic, then G is abelian (so in fact $G/Z(G) = 1$).

Proof. Let $gZ(G)$ be a generator for $G/Z(G)$. Then each coset is of the form $g^r Z(G)$ for some $r \in \mathbb{Z}$. Thus

$$G = \{g^r z : \ r \in \mathbb{Z}, z \in Z(G)\}.$$

We now check that elements in this group always commute:

$$\begin{aligned} g^{r_1} z_1 g^{r_2} z_2 &= g^{r_1+r_2} z_1 z_2 \quad \text{since } z \in Z(G) \\ &= g^{r_1+r_2} z_2 z_1 \\ &= g^{r_2} z_2 g^{r_1} z_1. \end{aligned}$$

Therefore G is abelian. □

Corollary 1.5.5

If $|G| = p^2$ then G is abelian.

Proof. We know that $|Z(G)| \in \{1, p, p^2\}$. We can't have 1 by 1.5.1. If we have p, then $|G/Z(G)| = p$ and therefore is cyclic. Now applying 1.5.4 we have that G is abelian. If we have p^2 then $Z(G) = G$ so G is abelian. □

§1.6 The Sylow theorems

Theorem 1.6.1 (Sylow theorems)

Let G be a finite group of order $p^a m$ where p is a prime with $p \nmid m$. Then

(i) The set $\mathrm{Syl}_p(G) = \{P \leq G : \ |P| = p^a\}$ of Sylow p-subgroups is non-empty.

(ii) All elements of $\mathrm{Syl}_p(G)$ are conjugate.

(iii) We define $n_p = |\mathrm{Syl}_p(G)|$ satisfies $n_p \equiv 1 \mod p$ and $n_p \mid |G|$ (and so $n_p | m$)

Proof. (i) Let Ω be the set of all **subsets** of G of order p^a. We know that

$$|\Omega| = \binom{p^a m}{p^a} = \left(\frac{p^a m}{p^a}\right)\left(\frac{p^a m - 1}{p^a - 1}\right) \cdots \left(\frac{p^a m - p^a + 1}{1}\right).$$

For $0 \leq k \leq p^a$, the number $p^a m - k$ and $p^a - k$ are divisible by the same power of p.

Therefore $|\Omega|$ is coprime to p. (†)

Let G act on Ω by left-multiplication, i.e for $g \in G$ and $x \in \Omega$ we have

$$g * X = \{gx : \ x \in X\} \in \Omega.$$

For any $X \in \Omega$ we have

$$|G_x| \, |\operatorname{orb}_G(X)| = |G| = p^a m.$$

By (†), there exists X such that $|\operatorname{orb}_G(X)|$ is coprime to p. This is because the orbits give a partition of Ω, and so they can't all divide p. Thus

$$p^a | \, |G_x \tag{1}$$

On the other hand, if $g \in G$ and $x \in X$, then $g \in (gx^{-1}) * X$ and hence

$$\begin{aligned} G = \bigcup_{g \in G} g * X &= \bigcup_{y \in \operatorname{orb}_G(X)} Y \\ \implies |G| &\leq |\operatorname{orb}_G| \cdot |X| \quad \text{since } |Y| = |X| \\ \implies |G_x| &= \frac{|G|}{|\operatorname{orb}_G(X)| = |X| = p^a}. \end{aligned} \tag{2}$$

By 1 and 2, $|G_X| = p^a$, i.e $G_x \in \operatorname{Syl}_p(G)$.

(ii) We prove a stronger result. We claim that if $P \in \operatorname{Syl}_p(G)$ and $Q \leq G$ is a p-subgroup, then $Q \leq gP^{-1}g^{-1}$ for some $g \in G$.

The proof is as follows: let Q act on the set of left cosets (not a group!) G/P by left multiplication, i.e $q * gP = qgP$. By Orbit-Stabiliser, each orbit has size $|Q|$, so either 1 or a multiple of p. Since $|G/P| = m$ by definition, and m is coprime to p, there must exist some orbit of size 1, i.e

$$\begin{aligned} &\exists g \in G : \quad qgP = gP \quad \forall q \in Q \\ \implies &g^{-1}qg \in P \quad \forall q \in Q \\ \implies &Q \leq gPg^{-1}. \end{aligned}$$

So we are done.

(iii) Let G act on $\operatorname{Syl}_p(G)$ by conjugation. Sylow (ii) tells us this action is transitive. Thus orbit-stabiliser implies

$$n_p = |\operatorname{Syl}_p(G)| \mid |G|.$$

Now to show that $n_p \equiv 1 \mod p$, let $P \in \operatorname{Syl}_p(G)$ act on $\operatorname{Syl}_p(G)$ by conjugation. The orbits have size dividing $|P| = p^a$, so either 1 or a multiple of p. To show $n_p \equiv 1 \mod p$, it suffices to show that $\{P\}$ is the unique orbit of size 1.

If $\{Q\}$ is another orbit of size 1, then P normalises Q, i.e $P \leq N_G(Q)$. Now P, Q are both Sylow p-subgroups of $N_G(Q)$ since $|N_G(Q)| \leq p^a$. Thus by (ii), P and Q are conjugate in $N_G(Q)$ - but $Q \trianglelefteq N_G(Q)$, thus $P = Q$. This completes the proof.

□

Now let's look at an application of these theorems.

Corollary 1.6.2

If $n_p = 1$, then the unique Sylow p-subgroup is normal.

Proof. Let $g \in G$ and $P \in \mathrm{Syl}_p(G)$. Then $gPg^{-1} \in \mathrm{Syl}_p(G)$, and so $gPg^{-1} = P$. Thus $P \trianglelefteq G$. □

This is very useful to show groups of certain orders can't be simple.

Example

Let $|G| = 1000 = 2^3 \cdot 5^3$. Then $n_5 = 1 \mod 5$ and $n_5 | 8$ so $n_5 = 1$. Thus the unique Sylow 5-subgroup is normal and hence G is not simple.

Example

Let $|G| = 132 = 2^2 \cdot 3 \cdot 11$. We have that $n_{11} = 1 \mod 11$ and $n_{11} | 12$. So $n_{11} = 1$ or 12. Suppose G is simple. Then $n_{11} \neq 1$ (otherwise the Sylow 11-subgroup is normal). Hence $n_{11} = 12$.

Now $n_3 \equiv 1 \mod 3$ and $n_3 | 44$. Thus $n_3 \in \{1, 4, 22\}$. But the case $n_3 = 1$ can't occur as before. Now suppose $n_3 = 4$. Then letting G act on $\mathrm{Syl}_3(G)$ by conjugation gives a group homomorphism $\phi : G \to S_4$. But then $\operatorname{Ker}\phi \trianglelefteq G \implies \operatorname{Ker}\phi = 1$ or G. But $\operatorname{Ker}\phi = 1$ would mean that G injects into S_4, which is a contradiction as $|G| = 132 > 24 = |S_4|$, and $\operatorname{Ker}\phi = G$ would be a contradiction to Sylow (ii).

Thus $n_3 = 22$ and $n_{11} = 12$. Thus G has $22 \cdot (3-1) = 44$ elements of order 3 and $120 = 12 \cdot (11-1)$ elements of order 11. But $44 + 120 > 132 = |G|$ which is a contradiction. Hence G is not simple.

§1.7 Matrix groups

Matrix groups provide a wealth of examples of finite groups, and are crucial in the classification of finite simple groups. First we will recap a few groups we've seen before in IA Groups.

For a field F, let $GL_n(F)$ be the set of $n \times n$ invertible matrices over F.

This contains the subgroup $SL_n = \operatorname{Ker}(GL_n(F) \xrightarrow{\det} F^\times)$. Here $F^\times = F \setminus \{0\}$.

Let $Z \trianglelefteq GL_n(F)$ be the normal subgroup of scalar multiples of I. This is in fact the centre of $GL_n(F)$, but we won't prove this in the course since the proof is pretty involved.

Definition

We define the projective general linear group by

$$PGL_n(F) = GL_n(F)/Z,$$

and the projective special linear group by

$$PGL_n(F) = \frac{SL_n(F)}{Z \cap SL_n(F)} \cong \frac{Z \cdot SL_n(F)}{Z} \leq PGL_n(F) \quad \text{by 2nd isom. theorem.}$$

Example

Consider $G = GL_n(\mathbb{Z}/p\mathbb{Z})$. A list of n vectors in $(\mathbb{Z}/p\mathbb{Z})^n$ are the columns of some $A \in G$ iff they are linearly independent. Thus

$$\begin{aligned}|G| &= \underbrace{(p^n-1)}_{\text{1st col.}}\underbrace{(p^n-p)}_{\text{2nd col.}}\underbrace{(p^n-p^2)}_{\text{3rd col.}}\dots\underbrace{(p^n-p^{n-1})}_{\text{last col.}} \\ &= p^{1+2+\dots+n-1}(p^{n-1}-1)(p^n-1)\dots(p-1) \\ &= p^{n(n-1)/2}\prod_{i=1}^{n}(p^i-1).\end{aligned}$$

So the Sylow p-subgroups have size $p^{n(n-1)/2}$. Let

$$U = \left\{ \begin{pmatrix} 1 & & & \\ & 1 & M & \\ & & & \ddots \\ & & & 1 \end{pmatrix} \right\} \leq G$$

be the set of upper triangular matrices with 1's on the diagonal. Then $U \in \mathrm{Syl}_p(G)$, since it has $n(n-1)/2$ entries and each can take p values.

Just as $PGL_2(\mathbb{C})$ acts on $\mathbb{C} \cup \{\infty\}$ via Möbius transformations, $PGL_2(\mathbb{Z}/p\mathbb{Z})$ acts on $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$ via

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \frac{az+b}{cz+d}.$$

Since scalar matrices act trivially, we obtain an action of $PGL_2(\mathbb{Z}/p\mathbb{Z})$.

Lemma 1.7.1

The permutation representation $PGL_2(\mathbb{Z}/p\mathbb{Z}) \to S_{p+1}$ is injective (in fact an isomorphism if $p = 2$ or 3).

Proof. Suppose $\frac{az+b}{cz+d} = z$ for all $z \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$.

- Setting $z = 0$ gives $b = 0$.
- Setting $z = \infty$ gives $c = 0$.
- Setting $z = 1$ gives $a = d$.

So $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a scalar matrix, hence it is trivial in $PGL_2(\mathbb{Z}/p\mathbb{Z})$. □