Groups, Rings and Modules

University of Cambridge Part IB Mathematical Tripos

Yue Wu

Yusuf Hamied Department of Chemistry
Lensfield Road,
Cambridge, CB2 1EW

yw628@cam.ac.uk

Contents

1 Groups

1.1 Basic Concept

Definition 1.1. A *group* is a triple $(G, \cdot, e)$ of a set G, a function $\cdot : G \times G \to G$ and an element $e \in G$ such that

(G1) Associativity. $\forall a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

(G2) Identity. $\forall a \in G$, $a \cdot e = e \cdot a = a$.

(G3) Inverse. For each $a \in G$, $\exists a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Definition 1.2. If $(G, \cdot, e)$ is a group and $H \subseteq G$ is a subset, then H is a *subgroup* of G, denoted $H \leq G$ if

(i) If $a, b \in H$, then $a \cdot b \in H$.

(ii) $e \in H$.

(iii) $(H, \cdot, e)$ is a group.

Lemma 1.3. $\varnothing \neq H \subseteq G$ is a subgroup $\iff \forall h_1, h_2 \in H$, $h_1 \cdot h_2^{-1} \in H$.

Examples.

(i) Additive groups. $(\mathbb{Z}, +, 0), (\mathbb{Q}, +, 0), (\mathbb{R}, +, 0), (\mathbb{C}, +, 0)$…

(ii) Groups of symmetry.

- S_n symmetry groups = bijections of $\{1, 2, \ldots, n\}$ to itself.
- D_{2n} dihedral group = symmetry of the regular n-gon.
- $\mathrm{GL}_n(\mathbb{R})$ general linear group = symmetry of the vector space $\mathbb{R}^n$.

(iii) Subgroups of these.

- Alternating groups $A_n \leq S_n$, the even permutations.
- Cyclic groups $C_n \leq D_{2n}$, rotational symmetry of n-gon.
- Special linear groups $\mathrm{SL}_n(\mathbb{R}^n) \leq \mathrm{GL}_n(\mathbb{R})$, $\{A \in \mathrm{GL}_n(\mathbb{R}) \mid \det A = 1\}$.

(iv) Abelian groups G such that $a \cdot b = b \cdot a$ $\forall a, b \in G$, e.g. $C_2 \times C_2 \cong K_4$.

(v) Quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$.

Definition 1.4. For a subgroup, the *left coset*

$$gH \coloneqq \{x \in G \mid x = g \cdot h \text{ for some } h \in H\}.$$

The collection of all left cosets of H, written $G : H$, gives a partition of G. All H-cosets is a bijection with H (also with each other).

Theorem 1.5 (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 H-cosets in G, known as the *index* of H in G.

Definition 1.6. The *order* of $g \in G$ is the least $n \in \mathbb{N} \cup \{\infty\}$ such that $g^n = e$. Write $\text{ord}(g)$ for the number.

If $g^m = e$, then $\text{ord}(g) \mid m$.

Lemma 1.7. Let G be a finite group. $\text{ord}(g) \mid |G| \ \forall g \in G$.

Proof. If $n = \text{ord}(g)$, then $H = \{e, g, g^2, \ldots, g^{n-1}\}$. Claim that H is a subgroup of G. If $g^i, g^j \in H$, then $g^i \cdot (g^j)^{-1} = g^{i-j}$, write $i - j = p \cdot n + r$, with $0 \leq r \leq n$.

$$g^{i-j} = g^{pn+r} = (g^n)^p \cdot g^r = g^r \in H \,,$$

so H is indeed of subgroup. By Lagrange's theorem, $n = |H|$ divides G. □

1.2 Normal Subgroups, Quotient, Homomorphism and Isomorphism

If $gH = g'H$, then $g^{-1}g' \in H$ and the converse hold. Let G/H be the set of the left H-cosets in G, try to defnne

$$(g_1H) \cdot (g_2H) = g_1g_2H \,.$$

This is well-defnned only if the result is consistent for different choices of coset representatives. If $g_2H = g_2hH$ is another coset representative, then

$$(g_1H) \cdot (g_2hH) = g_1g_2hH = g_1g_2H \,.$$

If $g_1H = g_1hH$, then

$$(g_1hH) \cdot (g_2H) = g_1hg_2H \,,$$

which is equal to g_1g_2H if and only if

$$(g_1g_2)^{-1}g_1hg_2 = g_2^{-1}hg_2 \in H \,.$$

Hence this defnnition is legal if and only if $g^{-1}hg \in H$ for all $g \in G$, $h \in H$.

Definition 1.8. A subgroup $H \leq G$ is *normal*, denoted $H \lhd G$, if

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

$\forall h \in H, g \in G$.

Proposition 1.9. If $H \lhd G$, then the set G/H of left H-cosets form a group under the operation $(g_1H) \cdot (g_2H) = g_1g_2H$, with $e_{G/H} = eH$. This is the *quotient group* of G by H.

Proof. The discussions show that this well-defnnes a binary operation on G/H. All the axioms follow from the fact that they hold in G. □

Definition 1.10. If $(G, \cdot_G, e_G)$ and $(H, \cdot_H, e_H)$ are groups, then a function $\phi : G \to H$ is a *homomorphism* if

(i) $\phi(g_1 \cdot_G g_2) = \phi(g_1) \cdot_H \phi(g_2)$

(ii) $\phi(e_G) = e_H$

The *kernel* of ϕ is $\ker(\phi) \coloneqq \{g \in G \mid \phi(g) = e_H\}$, and the *image* of ϕ is $\mathrm{im}(\phi) \coloneqq \{h \in H \mid h = \phi(g) \text{ for some } g \in G\}$.

Lemma 1.11. If $\phi : G \to H$ is a homomorphism, then $\phi(g^{-1}) = \phi(g)^{-1}$.

Proof.

$$\begin{aligned}\phi(g \cdot_G g^{-1}) &= \phi(e_G) = e_H \\ &= \phi(g) \cdot_H \phi(g)^{-1} .\end{aligned}$$

By the uniqueness of inverse, we must have $\phi(g^{-1}) = \phi(g)^{-1}$. □

Lemma 1.12. For a homomorphism $\phi : G \to H$, the kernel $\ker(\phi)$ is a normal subgroup of G, and the image $\mathrm{im}(\phi)$ is a subgroup of H.

Proof. Let $g, h \in \ker(\phi)$, then

$$\phi(g \cdot h^{-1}) = \phi(g) * \phi(g)^{-1} = e_H * e_H^{-1} = e_H ,$$

so $gh^{-1} \in \ker(\phi)$. Also $\phi(e_G) = e_H$ so it is a subgroup. Let $x \in G$, we have

$$\begin{aligned}\phi(x^{-1}gx) &= \phi(x^{-1}) * \phi(g) * \phi(x) = \phi(x^{-1}) * \phi(x) \\ &= \phi(x^{-1}x) = \phi(e_G) = e_H ,\end{aligned}$$

so $x^{-1}gx \in \ker(\phi)$ and hence $\ker \phi$ is normal.

Let $\phi(g), \phi(h) \in \mathrm{im}(\phi)$, then

$$\phi(g) * \phi(h) = \phi(gh^{-1}) \in \mathrm{im}(\phi) .$$

Furthermore, $e_H = \phi(e_G) \in \mathrm{im}(\phi)$, so $\mathrm{im}(\phi)$ is non-empty, and is a subgroup of H. □

Definition 1.13. An *isomorphism* is a homomorphism which is also a bijection.

If a function $\phi : G \to H$ is an isomorphism, then the inverse function $\phi^{-1} : H \to G$ is too.

Definition 1.14. Two groups are *isomorphic* is there is an isomorphism between them. We write $G \cong H$.

We often consider isomorphic groups to be "the same", and do not distinguish between them. We should be aware that we are careless when doing this.

Is is helpful to be able to break groups apart into smaller pieces. The following three isomorphism theorems allow us to do this in various ways. The first relates the kernel and image of an isomorphism.

Theorem 1.15. Let $\phi : G \to H$ be a homomorphism, then

$$G/\ker(\phi) \cong \mathrm{im}(\phi) .$$

Proof. Let

$$\begin{aligned} f : G/\ker(\phi) &\longrightarrow \operatorname{im}(\phi) \\ g\ker(\phi) &\longmapsto \phi(g)\,. \end{aligned}$$

First let us prove f is well-defnned since it uses a coset representative. If $g\ker(\phi) = g'\ker(\phi)$, then $g^{-1}g' \in \ker(\phi)$ and so $\phi(g^{-1}g') = e_H$. Thus

$$e_H = \phi(g^{-1}g') = \phi(g^{-1}) * \phi(g')\,,$$

and so multiplying by $\phi(g)$ gives $\phi(g) = \phi(g')$, so the function is well-defnned.

f is a homomorphism since

$$\begin{aligned} f(g\ker(\phi)\cdot g'\ker(\phi)) &= f(gg'\ker\phi) \\ &= \phi(gg') \\ &= \phi(g) * \phi(g') \\ &= f(g\ker(\phi)) * f(g'\ker(\phi))\,. \end{aligned}$$

Let $h \in \operatorname{im}(\phi)$, then $h = \phi(g)$ for some g, so $h = f(g\ker\phi)$ is in the image of f. Therefore, f is surjective. Suppose that $f(g\ker(\phi)) = f(g'\ker(\phi))$, then $\phi(g) = \phi(g')$, so $\phi(g^{-1}g) = e_H$. Hence, $g^{-1}g' \in \ker(\phi)$ and $g\ker(\phi) = g'\ker(\phi)$, so f is injective. Therefore, f is an isomorphism. □

Example. Consider the function $\phi : \mathbb{C} \to \mathbb{C}\backslash\{0\}$ by $z \mapsto e^z$. As $e^{z+w} = e^z \cdot e^w$, ϕ defnnes a homomorphism

$$\phi : (\mathbb{C}, +, 0) \to (\mathbb{C}\backslash\{0\}, \times, 1)\,.$$

The existence of log shows that ϕ is surjective, and so $\operatorname{im}(\phi) = \mathbb{C}\backslash\{0\}$. The kernel is given by

$$\ker\phi = \{z \in \mathbb{C} \mid e^z = 1\} = 2\pi i\mathbb{Z}\,.$$

The conclusion is that

$$(\mathbb{C}/(2\pi i\mathbb{Z}), +, 0) \cong (\mathbb{C}\backslash\{0\}, \times, 1)\,.$$

Theorem 1.16 (Second isomorphism theorem). Let $H \leq G$ and $K \lhd G$. Then $HK \coloneqq \{h \cdot k \mid h \in H, k \in K\}$ is a subgroup of G, and $H \cap K$ is a normal subgroup of G. Moreover,

$$\frac{HK}{K} \cong \frac{H}{H \cap K}\,.$$

Proof. Let $hk, h'k' \in HK$, then

$$h'k'(hk)^{-1} = h'k'k^{-1}h^{-1} = (h'h^{-1})(hk'k^{-1}h^{-1})\,.$$

The first term is in H, and the second term is $k'k^{-1} \in K$ conjugated by h, which is also in K. Therefore, $h'k'(hk)^{-1}$ lies in HK, and HK also contains e_G, so it is a subgroup.

Define

$$\begin{aligned} \phi : H &\longrightarrow G/K \\ h &\longmapsto hK\,. \end{aligned}$$

This is a homomorphism. The image of ϕ is the set of K-cosets which may be represented by an element of H, i.e.

$$\mathrm{im}(\phi) = \frac{HK}{K}\,.$$

The kernel of ϕ is

$$\ker(\phi) = \{h \in H \mid hK = eK\} = \{h \in H \mid h \in K\} = H \cap K\,.$$

As $H \cap K$ is the kernel of a homomorphism, it is normal in H. By the first isomorphism theorem,

$$\frac{H}{H \cap K} \cong \frac{HK}{K}\,.$$

Note that if $K \lhd G$, then there is a bijection between subgroups of G/K subgroups of G containing K, given by

$$\begin{aligned}\{\text{subgroups of } G/K\} &\longleftrightarrow \{\text{subgroups of } G \text{ which contains } K\}\\ X \leq \frac{G}{K} &\longmapsto \{g \in G \mid gK \in X\}\\ \frac{L}{K} \leq \frac{G}{K} &\longmapsfrom K \lhd L \leq G\,.\end{aligned}$$

This specialises to a bijection between normal subgroups as well.

$$\{\text{normal subgroups of } G/K\} \longleftrightarrow \{\text{normal subgroups of } G \text{ which contains } K\}\,.$$

Theorem 1.17 (Third isomorphism theorem). Let $K \leq L \leq G$ be normal subgroups of G, then

$$\frac{G/K}{L/K} \cong \frac{G}{L}\,.$$

Proof. Let

$$\begin{aligned}\phi : G/K &\longrightarrow G/L\\ gK &\longmapsto gL\,.\end{aligned}$$

If $gK = g'K$, then $g^{-1}g' \in K \in L$ so $gL = gL'$, so well-defnned. It is a homomorphism, and onto.

$$\begin{aligned}\ker(\phi) = \{gK \in G/K \mid gL = eL\} &= L/K\,,\\ \Updownarrow&\\ g \in L&\end{aligned}$$

so done by 1^{st} isomorphism theorem. □

Definition 1.18. A non-trivial group G is *simple* if its only normal subgroups are $\{e\}$ or G.

Lemma 1.19. An abelian group is simple $\iff$ it is C_p for some prime number p.

Proof.

($\Leftarrow$) If $H \leq C_p$, then $|H| \mid |C_p| = p$ by Lagrange's theorem, so $|H| = 1$ or p, so $H = \{e\}$ or C_p.

($\Rightarrow$) Let G be a simple abelian group. All subgroups of G are normal since

$$g^{-1}hg = g^{-1}gh = h \ \forall h \in H \lhd G\,.$$

Let $e \neq g \in G$, and $H = \{\dots, e, g, g^2, \dots\}$ is a normal subgroup. As $g \neq e$, $H \neq \{e\}$ so $H = G$ as G is simple, so G is cyclic. Then $G \cong (\mathbb{Z}, +, 0)$ or $G \cong C_n$. But $2\mathbb{Z} \lhd \mathbb{Z}$, so $\mathbb{Z}$ is not simple. It $n \mid m$, then $g^{n/m}$ generates a subgroup of C_n of order m, and it is normal. Therefore for C_n to be simple, only 1 and n can divide n. □

Theorem 1.20. It G is a finite group, then there are subgroups

$$G = H_1 > H_2 > \cdots > H_s = \{e\}\,.$$

Proof. If G is simple, let $H_2 = \{e\}$ and done.

If not, let $H_2 \lhd G$ be a proper normal subgroup of the largest order among all proper normal subgroups. Then claim G/H_2 is simple: if not, it has a proper $K \lhd G/H_2$. However, by the correspondence between normal subgroups of G/H_2 and normal subgroups of G containing H_2, $K \cong L/H_2$ for some $L \lhd G$ such that $H_2 \lhd L$. We find a proper normal subgroup of G with order strictly large than H_2, so contradiction.

So we found an $H_2 \lhd G$ with G/H_2 simple. Repeat this process to get the required sequence of normal subgroups. This process eventually stops as $|G|$ is finite. □

1.3 Actions and Permutations

Recall *permutation groups*

$$\begin{aligned} S_n &\coloneqq \text{symmetry group on } \{1, 2, \dots, n\} \\ &\equiv \text{group of bijections from } \{1, 2, \dots, n\} \text{ to itself.} \end{aligned}$$

Can defnne the *sign* function on S_n

$$\begin{aligned} \text{sign} : S_n &\longrightarrow (\{\pm 1\}, \times, +1) \\ \sigma &\longmapsto \begin{cases} +1 & \sigma = \text{even } \# \text{ permutations} \\ -1 & \sigma = \text{odd } \# \text{ permutations.} \end{cases} \end{aligned}$$

It is a homomorphism, so S_n has a normal subgroup

$$A_n \coloneqq \ker(\text{sign}) \lhd S_n$$

called the *alternating group*, and it has an index 2. More generally, for a set X, have the *symmetry group*

$$\text{Sym}(X) \coloneqq \{\sigma : X \to X \mid \sigma \text{ is a bijection}\}\,.$$

Definition 1.21. A group is a *permutation group* on X if it is a subgroup of $\mathrm{Sym}(X)$. Say it is a permutation group of *degree* n if $|X| = n$.

Examples.

(i) $S_n = \mathrm{Sym}(\{1, 2, \ldots, n\})$ is a permutation group of degree n.

(ii) $D_{2n} = \mathrm{Sym}(\text{vertices of a regular } n\text{-gon})$.

Definition 1.22. An *action* of a group G on a set X is a function

$$- * - : G \times X \to X$$

such that

(i) $\forall x \in X, g_i \in G,\ g_1 * (g_2 * x) = (g_1 g_2) * x$

(ii) $\forall x \in X,\ e * x = x$.

Lemma 1.23. An action G on X is the same as a homomorphism $\phi : G \to \mathrm{Sym}(X)$.

Proof. Let $- * - : G \times X \to X$ be a function. Define $\phi(g) = g * - : X \to X$ be a function. Note

$$\begin{aligned} \phi(g^{-1}) \circ \phi(g)(x) &= g^{-1} * (g * x) \\ &= (g^{-1} g) * x \\ &= x \end{aligned}$$

$\forall x$, so $\phi(g^{-1})$ is inverse to $\phi(g)$, so $\phi(g)$ is a bijection. This defnnes a function $\phi : G \to \mathrm{Sym}(X)$. Note

$$(\phi(h) \circ \phi(g))(x) = \phi(hg)(x)\ \forall x \in X, h, g \in G\,,$$

so ϕ is a homomorphism.

Conversely, let $\phi : G \to \mathrm{Sym}(X)$ be a homomorphism. Let $g * x = \phi(g)(x)$, then

$$\begin{aligned} g * (h * x) &= \phi(g)(\phi(h)(x)) \\ &= (\phi(g) \circ \phi(h))(x) \\ &= \phi(gh)(x) \\ &= (gh) * x\,, \end{aligned}$$

so it defnnes a group action. □

Definition 1.24. A permutation representation of a group G is a homomorphism $G \to \mathrm{Sym}(X)$.

The lemma above has shown that a permutation representation is the same as a group action. The good thing about thinking of group actions as homomorphisms is that we can use all we know about homomorphisms on them.

Definition 1.25. For an action of G on X, we write

$$\begin{aligned} G^X &\coloneqq \mathrm{im}(\phi : G \to \mathrm{Sym}(X)) \\ G_X &\coloneqq \ker(\phi : G \to \mathrm{Sym}(X))\,. \end{aligned}$$

Proposition 1.26. $G^X \cong G/G_X$.

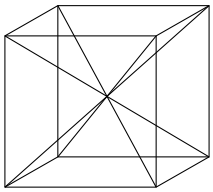
Proof. 1st isomorphism theorem. □

Examples.

(i)

$$\begin{aligned} G &= \text{symmetries of the cube} \\ X &= \{\text{diagonals of the cube}\} \\ G^X &= \mathrm{Sym}(X) \cong S_4 \\ G_X &= \{\text{id, sending each vertex to its opposite}\}. \end{aligned}$$

Have $\left|G^X\right| = 4! = 24$ and $|G_X| = 2$, so $|G| = 48$.



(ii) The group G acts on itself via $g*g' = g\cdot g'$. This corresponds to a $\phi : G \to \mathrm{Sym}(G)$.

$$G_X = \{g \in G \mid g * g' = g' \ \forall g' \in G\} = \{e\},$$

so $G = G/\{e\} \cong C^X \leq \mathrm{Sym}(G)$. This gives the Cayley's theorem. Every group is (isomorphic to) a subgroup of a symmetric group.

(iii) For $H \subseteq G$. Let $X = G/H$ set of left H-cosets. G acts on $X = G/H$ via $g * g'H = (gg')H$. This is well defnned so we get $\phi : G \to \mathrm{Sym}(X)$.

Now consider $G_X = \ker(\phi)$. If $g \in G_X$, then for every $g_1 \in G$, we have $g * g_1H = g_1H$. This means $g_1^{-1}gg_1 \in H$. In other words, we have $g \in g_1Hg_1^{-1}$. This has to hold for all $g_1 \in G$, so

$$G_X \subseteq \bigcap_{g_1 \in G} g_1Hg_1^{-1}.$$

This argument is completely inversible: if $g \in \bigcap_{g_1\in G} g_1Hg_1^{-1}$, then for each $g_1 \in G$, we know that $g_1^{-1}gg_1 \in H$ and hence $gg_1H = g_1H$. So $g * g_1H = g_1H$ and hence $g \in G_X$. Thus we have

$$\ker(\phi) = G_X = \bigcap_{g_1 \in G} g_1Hg_1^{-1}.$$

Since this is a kernel, it is a normal subgroup of G, and is contained in H. Starting with an arbitrary subgroup H, this allows us to generate a normal subgroup. (If we think about the construction, we see that this is the largest normal subgroup of G that is contained in H.)

Theorem 1.27. Let G be a finite group, $H \leq G$ be a subgroup of index n. Then there is a $K \lhd G$ with $K \leq H$ such that $|G/K| \mid n!$ and $n \mid |G/K|$.

Proof. We apply the previous example. Act by G on G/H, set $K = G_X \lhd G$. Then $G/G_X \cong G^X \leq \mathrm{Sym}(G/H) \cong S_n$, so by Lagrange's theorem, $|G/K| \mid |S_n| = n!$. We also have $K \leq H$, so $|G/K| \leq |G : H| = n$. □

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

Proof. Act by G on the set G/H gives a homomorphism $\phi : G \to \mathrm{Sym}(G/H)$. Then $G_X \lhd G$ is normal, so as G is simple, $G_X = \{e\}$ or $G_X = G$. As $g * (eH) \neq eH$ for $g \notin H$, which exists since the subgroup H is proper, the kernel of this action is not G, so $G_X = \{e\}$. Therefore, ϕ is injective, so $G = G/G_X \cong G^X \leq \mathrm{Sym}(G/H) \cong S_n$.

Now $A_n \lhd S_n$, so $G \cap A_n \lhd G$, so as G is simple, $G \cap A_n = \{e\}$ or $G \cap A_n = G$. If $G \cap A_n = \{e\}$, then

$$G = \frac{G}{G \cap A_n} \cong \frac{G \cdot A_n}{A_n} \leq \frac{S_n}{A_n} \cong C_2$$

by the second isomorphism theorem. Hence, $|G| \leq 2$. This is a contradiction as G is non-abelian. Therefore, we have

$$G \cap A_n = G \implies G \leq A_n \,.$$

A_1, A_2, A_3, A_4 have no non-abelian simple subgroups. □

Definition 1.28. Let G act on X. The *orbit* of $x \in X$ is

$$G \cdot x \coloneqq \{x' \in X \mid x' = g * x \text{ for some } g \in G\} \,.$$

The *stabiliser* of $x \in X$ is

$$G_x \coloneqq \{g \in G \mid g * x = x\} \,.$$

Lemma 1.29. G_x is a subgroup of G.

Proof. $e(x) = x$ by defnnition. For $g, h \in G_x$, $gh^{-1}(x) = g(h^{-1} * (x)) = g(x) = x$. □

Lemma 1.30. The orbits of an action partition X.

Proof. $\forall x \in X$, $x \in G \cdot x$ as $e * x = x$. So every x is in some orbit.

Then suppose $z \in G \cdot x$ and $z \in G \cdot y$, we have to show that $G \cdot x = G \cdot y$. We know that $z = g_1 * x = g_2 * y$ for some $g_1, g_2 \in G$, so $y = (g_2^{-1} g_1) * x$. For any $w = g_3(y) \in G \cdot y$, we have $w = (g_3 g_2^{-1} g_1) * x$, so w is also in $G \cdot x$. Thus $G \cdot y \subseteq G \cdot x$ and similarly $G \cdot x \subset G \cdot y$, so $G \cdot x = G \cdot y$. □

Let $g \in G$, $x \in X$. Each $g \in G$ gives us a member $g * x \in G \cdot x$, and conversely, every object in $G \cdot x$ arises this way. However, different elements in G can give us the same orbit. In particular, if $g \in G_x$, then hg and h give us the same object in $G \cdot x$. So we have a correspondence between things in $G \cdot x$ and members of G, up to G_x.

Theorem 1.31 (Orbit-stabiliser theorem). Let G act on x. Then for any $x \in X$, there is a bijection

$$\begin{aligned} \phi : G \cdot x &\longleftrightarrow G : G_x \\ g * x &\mapsto\!\!\!\!\leftarrow g G_x \,, \end{aligned}$$

and in particular, if G is finite, then $|G \cdot x| = |G : G_x|$.

Proof. ϕ is well-defnned since if $g \cdot G_x = h \cdot G_x$, then $h = gk$ for some $k \in G_x$, so $h * x = g * (k * x) = g * x$.

This map is injective because if $gG_x = hG_x$, then $G_x = g^{-1}hG_x$ so $g^{-1}h \in G_x$, then $g^{-1}h * x = x \implies g * x = h * x$, and this map is clearly surjective. The rest follows from Lagrange's theorem. □

1.4 Conjugacy Classes, Centralisers, Normalisers

Can defnne an action of G on the set G via

$$g * h = ghg^{-1} .$$

The function $\phi(g) : G \to G$ satisfies

$$\begin{aligned} \phi(g)(ab) &= gabg^{-1} = (gag^{-1})(gbg^{-1}) \\ &= \phi(a)\phi(b) , \end{aligned}$$

so $\phi(g)$ is a homomorphism. It is also a bijection, with inverse $\phi(g^{-1})$. We can take the collection of all isomorphisms of G, and form a new group out of it.

Definition 1.32. The *automorphism group* of a group G is

$$\mathrm{Aut}(G) \coloneqq \{f \in \mathrm{Sym}(G) \mid f \text{ is a group isomorphism}\} .$$

This is a group under composition, with the identity map as the identity element.

It is a subgroup of $\mathrm{Sym}(G)$.

Definition 1.33. The *conjugacy class* of $g \in G$ is

$$\mathrm{Cl}_G(g) \coloneqq G \cdot g = \{h \in G \mid h = xgx^{-1} \ \forall x \in G\} .$$

The *centralisers* of $g \in G$ is

$$C_G(g) \coloneqq G_g = \{x \in G \mid xgx^{-1} = g\} ,$$

i.e. the set of all $x \in G$ which commute with g.

The *centre* of G is

$$Z(G) \coloneqq \ker(\phi) = \{x \in G \mid xgx^{-1} = g \ \forall g \in G\} = \bigcap_{g \in G} C_G(g) ,$$

i.e. the set of all $x \in G$ which commute with all $g \in G$.

Proposition 1.34.

$$|\mathrm{Cl}_G(x)| = |G : C_G(x)| = \frac{|G|}{|C_G(x)|} .$$

Proof. Orbit-stabiliser. □

Definition 1.35. The *normaliser* of $H \leq G$ is

$$N_G(H) \coloneqq \{g \in G \mid gHg^{-1} = H\},$$

i.e. the largest subgroup of G inside which H is normal.

Theorem 1.36. A_n is simple for all $n \geq 5$.

Proof.

- **Claim 1.** A_n is generated by 3-cycles.

  Proof. Every element of A_n is a product of evenly-many transpositions, so need to show that the product of two transpositions can be written in terms of 3-cycles.

  Let a, b, c, d be distinct.

  - $(a\ b)(a\ b) = e$.
  - $(a\ b)(b\ c) = (a\ b\ c)$
  - $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$. □

- **Claim 2.** If $H \lhd A_n$ contains a 3-cycle, then it is A_n.

  Proof. We will show that if H contains a 3-cycle, it contains every 3-cycle, then done since A_n is generated by 3-cycles. Suppose $(a\ b\ c) \in H$ and want to show that $(1\ 2\ 3) \in H$. Since they have the same cycle shape, there is some $\sigma \in S_n$ such that $(a\ b\ c) = \sigma^{-1}(1\ 2\ 3)\sigma$.

  If σ is even, then $\sigma \in A_n$, so since $H \lhd A_n$, we have $(1\ 2\ 3) \in H$ and done. If σ is odd, take $\overline{\sigma} = \sigma(4\ 5) \in A_n$ (here comes the condition $n \geq 5$), then $\sigma^{-1}(1\ 2\ 3)\sigma = \overline{\sigma}^{-1}(1\ 2\ 3)\overline{\sigma} = (a\ b\ c)$ so done. □

Let $H \lhd A_n$. We want to show that H contains a 3-cycle, so it is A_n itself. We split into different cases.

(i) **Claim 3.** If H contains a σ which can be written as

$$\sigma = (1\ 2\ 3\ \mathit{dots}\ r) \cdot \tau$$

for $r \geq 4$ and τ arbitrary, then H contains a 3-cycle.

Proof. Let $\delta = (1\ 2\ 3)$ and consider

$$\underbrace{\underbrace{\sigma^{-1}}_{\in H} \cdot \underbrace{\delta^{-1} \cdot \sigma \cdot \delta}_{\in H}}_{\in H} = (r\ \ldots\ 2\ 1)(1\ 3\ 2)(1\ 2\ \ldots\ r)(1\ 2\ 3)$$

$$= (2\ 3\ r),$$

where we used the assumption that $(1\ 2\ \ldots\ r)\tau$ are disjoint so τ commute with $(1\ 2\ \ldots\ r)$ and δ. □

(ii) **Claim 4.** If H contains a $\sigma = (1\ 2\ 3)(4\ 5\ 6) \cdot \tau$ disjoint, then it contains a 3-cycle.

Proof. Let $\delta = (1\ 2\ 4)$. Then

$$\begin{aligned}\sigma^{-1}\delta^{-1}\sigma\delta &= (1\ 3\ 2)(4\ 6\ 5)(1\ 4\ 2)(1\ 3\ 2)(4\ 5\ 6)(1\ 2\ 4) \\ &= (1\ 2\ 4\ 3\ 6) \in H\,.\end{aligned}$$

This is a 5-cycle, so the previous case applies. □

(iii) **Claim 5.** If H contains a $\sigma = (1\ 2\ 3) \cdot \tau$ disjoint, then it contains a 3-cycle.

Proof. If τ is a product of 2-cycles, then

$$\sigma^2 = (1\ 2\ 3)^2 = (1\ 3\ 2)$$

is a three cycle. If τ is anything longer, then it falls into one of the previous cases. □

(iv) **Claim 6.** If H contains $\sigma = (1\ 2)(3\ 4)\tau$ disjoint, then it contains a 3-cycle.

Proof. If τ is a product of 2-cycles, let $\delta = (1\ 2\ 3)$ then

$$\begin{aligned}u &= \delta^{-1}\delta^{-1}\sigma\delta \\ &= (1\ 2)(3\ 4)(1\ 3\ 2)(1\ 2)(3\ 4)(1\ 2\ 3) \\ &= (1\ 4)(2\ 3) \in H\,.\end{aligned}$$

Then let

$$v = (1\ 5\ 2)u(1\ 2\ 5) = (1\ 3)(4\ 5) \in H\,,$$

where we used $n \geq 5$ again. Consider

$$uv = (1\ 4)(2\ 3)(1\ 3)(4\ 5) = (1\ 2\ 3\ 4\ 5) \in H\,.$$

This is the first case so done.

If τ is longer, it fits in one of the previous cases. □

Combining these results, we are done. □

1.5 Finite p-groups.

We seems never talk about things like the sum of orders to two subgroups. From this point of view, the simplest groups are those of prime orders, but they are all cyclic. The next simplest groups are those whose order is a power of prime.

Definition 1.37. A finite group is a p-group if $|G| = p^n$ for some prime number p and $n \geq 1$.

Theorem 1.38. If G is a finite p-group, then its centre $Z(G) = \{x \in G \mid xg = gx\ \forall g \in G\}$ is non-trivial.

Proof. Let G act on itself by conjugation. Each orbit of this action (which are precisely the conjugacy classes) has size dividing $|G| = p^n$, so is either a singleton, or has size divisible by p.

Since the conjugacy classes partition G, the sum of the sizes of the conjugacy classes is $|G|$. In particular,

$$|G| = \#\{\text{conjugacy classes of size } 1\} + \sum \text{orders of all other conjugacy classes}\,.$$

By the above discussion, the second term is divisible by p, as is $|p|^n$. Therefore, the number of conjugacy classes of size 1 is divisible by p. $\{e\}$ is a conjugacy class of size 1, so $\#\{\text{conjugacy classes of size } 1\} \geq p \geq 2$. There must be a conjugacy class $\{x\} \neq \{e\}$.

Then, $g^{-1}xg = x\ \forall g \in G$, i.e. $x \in Z(G)$, so $Z(G)$ is non-trivial. □

Corollary. Let G be a p-group of order p^n, $n \geq 2$. G is not simple.

Proof. $Z(G) \lhd G$. □

This allows us to prove interesting things about p-groups by induction on their orders, by considering the smaller p-group $G/Z(G)$. One way to do this is via the following lemma.

Lemma 1.39. For any group G, if $G/Z(G)$ is cyclic, then G is abelian.

In other words, if $G/Z(G)$ is cyclic, then it is trivial, since the centre of an abelian group is the abelian group itself.

Proof. Let the coset $gZ(G)$ be a generator of the cyclic group $G/Z(G)$, so every coset of $Z(G)$ is of the form $g^rZ(G)$. It follows that every element $x \in G$ must be in the form g^rz for some $z \in Z(G)$, $r \in \mathbb{Z}$.

To show that G is abelian, let $x' = g^{r'}z'$ another element in G with some $z' \in Z(G)$ and $r' \in \mathbb{Z}$. As $z, z' \in Z(G)$, they commute with every element in G, so

$$xx' = g^rzg^{r'}z' = g^{r'}g^rz'z = g^{r'}z'g^rz = x'x\,,$$

and hence G is abelian. □

This lemma is particularly useful when applied to p-groups.

Corollary. If p is prime and $|G| = p^2$, then G is abelian.

Proof. Since $Z(G) \leq G$, its order must be 1, p or p^2. $Z(G)$ is non-trivial, so $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$, it is the whole group so G is trivially abelian. Otherwise, $|G/Z(G)| = p^2/p = p$ must be cyclic, so it must be cyclic, then G is again abelian. □

Theorem 1.40. Let G be a group of order p^a, where p is prime. Then G has a subgroup of order p^n for any $0 \leq b \leq a$.

Remark. This means that G has a subgroup of every possible order. This is not true for general groups, e.g. A_5 has an order of 60, but it has no subgroup of order 30 (as a subgroup of index 2 has to be normal, but A_5 is simple).

Proof. We induct on a. If $a = 1$, then $\{e\}$ and G are subgroups of order p^0 and p^1 so done.

Suppose $a > 1$ and we want to construct a subgroup of order p^n. If $b = 0$ then trivial. Otherwise, $Z(G)$ is non-trivial, so let $x \in Z(G)$, $x \neq e$. Since $\text{ord}(x) \mid |G|$, it order is a power of p. If it has a order p^c, then $x^{p^{c-1}}$ has order p. By renaming, suppose that x has order p, we have generated a subgroup $\langle x \rangle$ of order p. Since $x \in Z(G)$, $\langle x \rangle$ commutes with every $g \in G$, so $\langle x \rangle \lhd G$. Therefore, $G/\langle x \rangle$ is a group of order p^{a-1}.

Since this is a strictly smaller group, we may suppose by induction that $G/\langle x \rangle$ has a subgroup of any possible order. In particular, it has a subgroup L if order p^{b-1}. By the subgroup correspondence, there is some $K \leq G$ such that $\langle x \rangle \lhd K$ and $L = K/\langle x \rangle$. Then K has an order p^b. □

1.6 Finite Abelian Groups

Theorem 1.41 (Classification of finite abelian groups). Let G be a finite abelian group. Then there exists some $d_1, \ldots, d_r$ such that

$$G \cong C_{d_1} \times C_{d_2} \times \ldots C_{d_r}\,.$$

Moreover, we can choose the d_1 such that $d_{i+1} \mid d_i$ for each i, in which case this expression is unique.

We will prove this in chapter 3 as a special case of the classification of modules over certain rings.

Example. The abelian groups of order 8 are C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$.

Sometimes the decomposition given by this theorem is not the most useful form. To get a nicer decomposition, we can use the following lemma.

Lemma 1.42. If n and m are coprime, then $C_{mn} \cong C_m \times C_n$.

Remark. This is essentially the Chinese remainder theorem, and this formulation is how you should think of that theorem.

Proof. If suffice to find an element of order nm in $C_m \times C_n$, then since $C_m \times C_n$ has order mn, it must be cyclic and hence isomorphic to C_{mn}.

Let $g \in C_m$ have order m and $h \in C_n$ have order n, and consider the element $(g, h) \in C_m \times C_n$. Suppose the order of g, h is k, then $(g, h)^k = (e, e)$. Hence $(g^k, h^k) = (e, e)$. So $m \mid k$ and $n \mid k$. As m, n are coprime, this means that $mn \mid k$. As $k = \text{ord}(g, h)$ and $(g, h) \in C_m \times C_n$ is a group of order mn, we must have $k \mid mn$. So $k = mn$. □

Corollary. For any finite abelian group G, we have

$$G \cong C_{d_1} \times C_{d_2} \times \cdots \times C_{d_r}\,,$$

where each d_i is a prime power.

Proof. From the classification theorem, iteratively apply the previous lemma to break down each component up into prime powers. □

1.7 Sylow's Theorems

Definition 1.43. Let G be a finite group of order $p^a \cdot m$, with p prime and $p \nmid m$. A *Sylow p-subgroup* of G is a subgroup $P \leq G$ of order p^a.

Theorem 1.44 (Sylow's theorems). Let G be a finite group of order $p^a \cdot m$, with p prime and $p \nmid m$.

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

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

(iii) The number $n_p = \left|\mathrm{Syl}_p(G)\right|$ of Sylow p-subgroups satisfies $n_p \equiv 1 \pmod{p}$ and $n_p \mid |G|$, and hence $n_p \mid m$.

These are sometimes known as Sylow's first/second/third theorem respectively.

Proof.

(i) First show that $\mathrm{Syl}_p(G) \neq \varnothing$. Let Ω be the set of subsets of G with p^a elements. G acts on this via
$$g * \{x_1, x_2, \ldots, x_{p^a}\} = \{g \cdot x_1, g \cdot x_2, \ldots, g \cdot x_{p^a}\}.$$
Let $\Sigma \subseteq \Omega$ be an orbit of this action.
If $\{x_1, \ldots, x_{p^a}\} \in \Sigma$, then for any $g \in G$,
$$(g \cdot x_1^{-1}) * \{x_1, \ldots, x_{p^a}\} = \{g, \ldots\} \in \Sigma$$
contains g, so any element of the group lies in some element of Σ, so
$$|\Sigma| \geq \frac{|G|}{p^a} = m.$$
If $|\Sigma| = m$, then by orbit-stabiliser theorem, the stabiliser of any $\{x_1, \ldots, x_{p^a}\}$ has index m, so has order p^a, and thus is a Sylow p-subgroup.
We would then like to show not every orbit can have size $> m$. If $|\Sigma| > m$, then as $|\Sigma| \mid |G| = p^a m$ by orbit-stabiliser theorem, we must have $p \mid |\Sigma|$. Our strategy is to show $|\Omega| \not\equiv 0 \pmod{p}$, so since Ω is the disjoint union of all orbits, not every orbit can have size $> m$.
This is done by calculating
$$|\Omega| = \binom{p^a m}{p^a} = \prod_{j=0}^{p^a-1} \frac{p^a m - j}{p^a - j}.$$
As $j < p^a$, the largest power of p dividing $p^a m - j$ is the largest power of p dividing j. Similarly, the largest power of p dividing $pa - j$ is also the largest power of p dividing j. So we have the same power of p on top and bottom for each term in the product, so they cancel and the result is not divisible by p.

(ii) We will prove something stronger. Let p be a Sylow p-subgroup, and Q be a p-subgroup (with order $|Q| = p^b$ where $b \leq a$). We will show that Q may be conjugated into P, i.e. $g^{-1}Qg \leq P$ for some $g \in G$.

Let Q act on the set of left cosets G/P via $q * gP = (qg)P$. By orbit-stabiliser, the size of each orbit divides $|Q|$, so each orbit has size 1 or divisible by p. But $|G/P| = \frac{p^a \cdot m}{p^a} = m$ is coprime to p, so some orbit has size 1. Let gP has size 1, then

$$qgP = gP \ \forall q \in Q \iff g^{-1}qg \in P \iff g^{-1}Qg \leq P\,.$$

(iii) G acts on the set of $\mathrm{Syl}_p(G)$ by conjugation. By (ii), the action has a single orbit, The orbit-stabiliser theorem applied to the orbit shows that $n_p = \left|\mathrm{Syl}_p(G)\right|$ divides $|G|$. This is the second claim.

Let $P \in \mathrm{Syl}_p(G)$ and act on $\mathrm{Syl}_p(G)$ by conjugation. Note $\{P\}$ is an orbit of this action with size 1. We will show that the other orbits have sizes divisible by p. By orbit-stabiliser, all orbits have size either 1 or divisible by p. Need to show that there are no other orbit of size 1. Suppose $\{Q\}$ is such an orbit, i.e. $\forall p \in P$, $p^{-1}Qp = Q$, so

$$\begin{aligned} P &\leq N_G(Q) = \text{normaliser of } Q \text{ in G} \\ &= \{g \in G \mid g^{-1}Qg = Q\}\,. \end{aligned}$$

Now $N_G(Q)$ is itself a group, and we can look at its Sylow p-subgroups. We know that $Q \leq N_G(Q) \leq G$, so $p^a \mid |N_G(Q)| \mid p^a m$. Thus p^a is the biggest power of p that divides $|N_G(Q)|$, so Q is a Sylow p-subgroup of $N_G(Q)$.

By (ii), Q is conjugated to P inside $N_G(Q)$, but the only conjugate of Q in $N_G(Q)$ is Q tautologically, so $Q = P$.

So the original action has exactly 1 orbit of size 1, and the other have sizes divisible by p, so $n_p = \left|\mathrm{Syl}_p(G)\right| \equiv 1 \pmod 1$. □

Lemma 1.45. If there is a unique Sylow p-subgroup, i.e. $n_p = 1$, then it is normal in G.

Proof. Let P be the unique Sylow p-subgroup, and let $g \in G$. Then by Sylow's second theorem, $g^{-1}Pg$ is P itself, so P is normal. □

Corollary. Let G be a non-abelian simple group and prime number $p \mid |G|$. Then $|G| \mid \frac{(n_p)!}{2}$ and $n_p \geq 5$.

Proof. G acts on the set of Sylow p-subgroups $\mathrm{Syl}_g(p)$ by conjugation, giving the permutation representation

$$\phi : G \to \mathrm{Sym}(\mathrm{Syl}_p(G)) \cong S_{n_p}\,.$$

We know $\ker(\phi) \lhd G$, but G is simple, so $\ker\phi$ is either $\{e\}$ or G.

If $\ker(\phi) = G$, then all Sylow p-subgroups are normal. This contradicts with G being simple, so $\ker(\phi) = \{e\}$, and so G is isomorphic to a subgroup of S_{n_p}. Now consider

$$G \xrightarrow{\phi} S_{n_p} \xrightarrow{\text{sign}} \{\pm 1\}\,.$$

If this is injective, then the kernel is an index 2 normal subgroup of G, again contradicts with G being simple. Therefore we can only have $\ker \operatorname{sign} \circ \phi$ being the whole G, so $G \cong \operatorname{im}(\phi) \leq A_{n+p}$, and $|G| \mid \frac{(n_p)!}{2}$.

For the final statement, can check that $A_1, \ldots, A_4$ has no non-abelian simple subgroups. $\square$

Example. Let $|G| = 1000 = 2^3 \cdot 5^3$, then $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 8 = 2^3$. Then we can only have $n_5 = 1$, so G has a normal subgroup of order 5^3, and G is not simple.

Example. Let $|G| = 132 = 2^2 \cdot 3 \cdot 11$. Suppose G is simple. Have $n_1 1 \equiv 1 \pmod{11}$, $n_{11} \mid 2^2 \cdot 3 = 12$, so $n_{11} = 1$ or 12. As G is assumed simple, $n_{11} \neq 1$, so $n_{11} = 12$.

Similarly, $n_3 \equiv 1 \pmod 3$ and $n_3 \mid 2^2 \cdot 11 = 44$, so $n_3 = 1, 4$ or 22. G is simple so $n_3 \neq 1$. If $n_3 = 4$, then the corollary gives $|G| = 132 \mid \frac{4!}{2} = 12$, a contradiction so n_3 must be 22.

Every Sylow 11-subgroup is cyclic, so contains $11 - 1 = 10$ elements of order 11. These subgroups only intersect at $\{e\}$, so there are $11 \times 10 = 120$ elements of G of order 11.

Every Sylow 3-subgroup is cyclic, so contains 2 elements of order 3. They only intersect in $\{e\}$ so there are $22 \times 2 = 44$ elements of order 3.

We have found too many elements of G. This cannot happen, so a group of order 132 is never simple.

Example. $\mathrm{GL}_n(\mathbb{Z}/p) = \{\text{invertible } n \times n \text{ matrices with entries in } \mathbb{Z}/p\}$, p is a prime number. What is the order of this group? Giving a matrix $A \in \mathrm{GL}_n(\mathbb{Z}/p)$ is the same as giving n linearly independent vectors in the vector space $(\mathbb{Z}/p)^n$. We can pick the first vector to be anything except zero, so there are $p^n - 1$ ways of choosing the first vector.Next,we need to pick the second vector, which can be anything that is not in the span of the first vector, so there are $p_n - p$ways of choosing the second vector. Continuing in this way we have

$$(p^n - 1)(o^n - p)(p^n - p^2) \ldots (p^n - p^{n-1}) = p^{1+2+\cdots+(n-1)}(p^n - 1)(p^{n-1} - 1) \ldots (p - 1)\,.$$

So $p^{\binom{n}{2}}$ is the largest power of p dividing $|\mathrm{GL}_n(\mathbb{Z}/p)|$.

To give a Sylow p-subgroup of $\mathrm{GL}_n(\mathbb{Z}/p)$, we consider the subgroup of matrices of the following form

$$U \coloneqq \left\{ \begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z}/p) \right\}.$$

We have $|U| = p^{\binom{n}{2}}$, so it is a Sylow p-subgroup.

Example. $\mathrm{GL}_2(\mathbb{Z}/p)$ has order $p(p^2 - 1)(p - 1) = p(p - 1)^2(p + 1)$. Suppose $l \mid p - 1$ and $l^3 \nmid |\mathrm{GL}_2(\mathbb{Z}/p)|$. $l \neq p$ is a prime number, so there must be a subgroup of order

l^2. Note

$$(\mathbb{Z}/p)^\times = \{x \in \mathbb{Z}/p \,|\, \exists y \text{ such that } xy \equiv 1 \pmod{p}\} \cong C_{p-1}\,,$$

so as $l \mid p-1$, there is a subgroup $C_l \leq C_{p-1} \cong (\mathbb{Z}/p)^\times$. We immediately find a subgroup

$$C_l \times C_l \leq (\mathbb{Z}/p)^\times \times (\mathbb{Z}/p)^\times \leq \mathrm{GL}_2(\mathbb{Z}/p)\,,$$

where the second inclusion is the diagonal matrices, identifying

$$(a, b) \longleftrightarrow \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\,,$$

so this is a Sylow p-subgroup.

A non-examinable fact:

Theorem 1.46 (Feit-Thompson theorem). If G is a non-abelian finite group of odd order, then it is not simple.