MA30237 - Group Theory

Contents

1 Groups, subgroups and homomorphisms

1.1 Definitions (Monoids and groups)**.** A *monoid* is a set M equipped with an element $e \in M$ and binary operation $M \times M \to M$; $(a, b) \mapsto a * b$ such that the following axioms hold:

(Identity)	for all $a \in M$,	$e * a = a$ and $a * e = a$;
(Associativity)	for all $a, b, c \in M$,	$(a * b) * c = a * (b * c)$.

A monoid G is called a *group* if in addition:

(Inverses)	for all $a \in G$,	there exists $b \in G$ such that $a * b = e = b * a$.

A group or monoid M is said to be *abelian* or *commutative* if:

(Commutativity)	for all $a, b \in M$,	$a * b = b * a$.

1.2 Remarks. (i) If $f \in M$ satisfies the Identity Axiom (as well as e), then $f = f * e = e$. Hence the identity e is uniquely determined [Alg1A].

(ii) Likewise, $b \in M$ with $a * b = e = b * a$ is uniquely determined by $a \in M$ [Alg1A]. If such a b exists, a is called *invertible* with *inverse* b. Then b is invertible with inverse a.

A group G is thus a monoid in which every element is invertible.

(iii) If a_1 and a_2 have inverses b_1 and b_2 respectively, then $a_1 * a_2$ has inverse $b_2 * b_1$:

$$(a_1 * a_2) * (b_2 * b_1) = a_1 * (a_2 * b_2) * b_1 = a_1 * e * b_1 = a_1 * b_1 = e$$

and similarly $(b_2 * b_1) * (a_1 * a_2) = e$.

1.3 Definitions (Submonoids and subgroups)**.** A *submonoid* of a group or monoid M is a subset $H \subseteq M$ such that

$$e \in H \quad \text{and} \quad \text{for all } a, b \in H,\ a * b \in H.$$

Then H is a monoid with identity e and operation $H \times H \to H$; $(a, b) \mapsto a * b$ — the Identity and Associativity axioms hold in H because they hold in M.

We say H is a *subgroup* of M, written $H \leqslant M$, if H is also a group with these operations. When M is a group G, this means that for all $a \in H$ the inverse of a in G belongs to H.

1.4 Remark. By Remarks 1.2 it follows that in any monoid M, the set $M^\times$ of all invertible elements of M is a subgroup of M, i.e., $G = M^\times$ is a group with the induced operations.

1.5 Examples (Monoids and groups)**.** (i) Any ring R is an abelian group under addition with identity $e = 0$. Examples: the integers $\mathbb{Z}$, the set $\mathbb{Z}_n$ of integers modulo n, and the fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. The set $\mathbb{N} \subseteq \mathbb{Z}$ of natural numbers (with $0 \in \mathbb{N}$) is a submonoid of $\mathbb{Z}$, but not a subgroup.

(ii) Any ring R is also a monoid under multiplication, with identity $e = 1$, and this monoid is abelian if the ring is commutative.

The set $R^\times$ of all invertible elements in R (the *units* of R) is called the *multiplicative* (*sub*)*group* or the *group of units* of R. Examples: $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Z}_n^\times$ consists of the congruence classes $[m]_n$ with m coprime to n [Alg1A], while the multiplicative group of a field $\mathbb{F}$ is $\mathbb{F}^\times = \mathbb{F} \smallsetminus \{0\}$, i.e., it contains all of the nonzero elements of $\mathbb{F}$.

(iii) For any set X, the set X^X of all maps $X \to X$ is a monoid with $e = \mathrm{id}\colon X \to X$, the identity map, and composition $(f, g) \mapsto f \circ g$ as the binary operation. Then $\mathrm{Sym}(X) := (X^X)^\times$ is the group of all invertible maps $X \to X$ (equivalently, bijections) and is called the *symmetric group* on X. When X is finite, elements of $\mathrm{Sym}(X)$ are called *permutations* and when $X = \{1, 2, \dots n\}$, $\mathrm{Sym}(X)$ is often denoted Sym_n or S_n.

(iv) Let V be a finite dimensional vector space over a field $\mathbb{F}$. Then the set $\mathrm{End}(V)$ of linear maps $V \to V$ is a monoid under composition (and indeed also a ring, using addition of linear maps [Alg2A, Alg2B]). Its group of invertible elements is a subgroup of $\mathrm{Sym}(V)$, denoted $\mathrm{GL}(V)$, and called the *general linear group of V over $\mathbb{F}$*.

The ring $M_n(\mathbb{F})$ of $n \times n$ matrices over a field $\mathbb{F}$ is a monoid under matrix multiplication, with multiplicative group $\mathrm{GL}_n(\mathbb{F})$, the *general linear group* of $n \times n$ invertible matrices.

1.6 Notation. The above examples use a wide range of notations. Herein, *multiplicative notation* will primarily be used: the binary operation will be written ab, with identity element 1, and a^{-1} will denote the inverse of a; then for $n \in \mathbb{Z}$, a^n denotes the n-fold product $aa \cdots a$ if $n > 0$, $(a^{-1})^{-n}$ if $n < 0$, and 1 if $n = 0$, so that $a^n a^m = a^{n+m}$ for all $n, m \in \mathbb{Z}$ [Alg1A].

For abelian groups, *additive notation* is common: the binary operation is written $a + b$, with identity element 0 and $-a$ as the inverse of a; then a^n is written na, so that $na + ma = (n+m)a$.

1.7 Examples (Subgroups)**.** Any group (or monoid) G is a subgroup (or submonoid) of itself, and has a trivial subgroup $\{1\}$. Other subgroups H are called *proper* ($H < G$) and *nontrivial* ($\{1\} < H$). Here are some more interesting examples.

(i) Evidently $\mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R} \leqslant \mathbb{C}$ (as groups under addition). The subset $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ is also subgroup of $\mathbb{Z}$: $0 = n0 \in n\mathbb{Z}$, $nk_1 + nk_2 = n(k_1 + k_2) \in n\mathbb{Z}$, and $-nk = n(-k) \in n\mathbb{Z}$.

(ii) Similarly $\mathbb{Z}^\times \leqslant \mathbb{Q}^\times \leqslant \mathbb{R}^\times \leqslant \mathbb{C}^\times$ (under multiplication) The subset $\mu_n = \{a \in \mathbb{C}^\times : a^n = 1\}$ is also subgroup of $\mathbb{C}^\times$ called the *group of nth roots of unity*: $1^n = 1$ so $1 \in \mu_n$, and if $a, b \in \mu_n$ then $(ab)^n = a^n b^n = 1$ and $(a^{-1})^n = (a^n)^{-1} = 1$, so $ab \in \mu_n$ and $a^{-1} \in \mu_n$.

(iii) Recall that any permutation $\sigma \in S_n$ is either *even* or *odd*, i.e., σ is a product of an even number of transpositions or of an odd number (respectively), but not both. The set $A_n := \{\sigma \in S_n : \sigma \text{ is even}\}$ (aka Alt_n) is a subgroup of S_n called the *alternating group*.

(iv) The set of $n \times n$ matrices A over $\mathbb{F}$ with $\det(A) = 1$ is a subgroup of $\mathrm{GL}_n(\mathbb{F})$ called the *special linear group* $\mathrm{SL}_n(\mathbb{F})$.

1.8 Definitions (Homomorphisms and isomorphisms)**.** A map $\phi\colon G \to H$ between groups or monoids is a *homomorphism* if $\phi(1) = 1$ and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$. The *kernel* of a homomorphism ϕ is $\ker \phi := \{a \in G : \phi(a) = 1\}$. If ϕ has an inverse homomorphism $\phi^{-1}\colon H \to G$, then it is called an *isomorphism*, and G is said to be *isomorphic* to H, written $G \cong H$. An *automorphism* of G is an isomorphism $\phi\colon G \to G$ and the set of all automorphisms of G is denoted $\mathrm{Aut}(G)$.

1.9 Remarks. (i) If $\phi\colon G \to H$ satisfies $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$ and H is a group, then $\phi(1) = 1$ is automatic. If $a \in G$ is invertible, so is $\phi(a)$, with $\phi(a)^{-1} = \phi(a^{-1})$.

(ii) By definition $\mathrm{id}\colon G \to G$ is an isomorphism and the inverse of an isomorphism is an isomorphism. Also if $\phi\colon G \to H$ and $\psi\colon H \to K$ are homomorphisms then their composition $\psi \circ \phi\colon G \to K$ is a homomorphism [Alg1A]. This has two important consequences.

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

- Isomorphism is reflexive ($G \cong G$), symmetric (if $G \cong H$ then $H \cong G$) and transitive (if $G \cong H$ and $H \cong K$ then $G \cong K$). There is no structural difference between isomorphic groups: an isomorphism $\phi\colon G \to H$ simply renames the elements of G so that if $a, b, c \in G$ with $ab = c$ then $\phi(a), \phi(b), \phi(c) \in H$ with $\phi(a)\phi(b) = \phi(c)$.

(iii) For any group G and any set X, homomorphisms $\phi\colon G \to \mathrm{Sym}(X)$ are called *actions* of G on X (or *permutation representations* if X is finite); we will study them in detail.

(iv) For any group G, homomorphisms $\phi\colon G \to H$ with $H = \mathrm{GL}(V)$ or $\mathrm{GL}_n(\mathbb{F})$, where $\mathbb{F}$ is a field and V is a vector space over $\mathbb{F}$, are called (*linear*) *representations* of G; they form the topic of MA40054 Representation Theory of Finite Groups.

1.10 Lemma. Let $\phi\colon G \to H$ be a homomorphism between groups G and H.

If $A \leqslant G$ then $\phi(A) := \{\phi(a) : a \in A\} \leqslant H$

If $B \leqslant H$ then $\phi^{-1}(B) = \{a \in G : \phi(a) \in B\} \leqslant G$.

In particular, $\ker\phi = \phi^{-1}(\{1\}) \leqslant G$ and $\mathrm{im}\,\phi = \phi(G) \leqslant H$.

Furthermore ϕ is an isomorphism if and only if $\ker\phi = \{1\}$ and $\mathrm{im}\,\phi = H$.

Proof. See [Alg1A]. □

1.11 Examples (Homomorphisms)**.** (i) For any $n \in \mathbb{Z}$ the map $\pi_n\colon \mathbb{Z} \to \mathbb{Z}_n$; $m \mapsto [m]_n$ is a surjective homomorphism with $\ker\pi_n = n\mathbb{Z}$: note $\pi(0) = [0]_n$ is the additive identity in $\mathbb{Z}_n$ and $[m_1 + m_2]_n = [m_1]_n + [m_2]_n$. Note that $[m]_n = m[1]_n$.

More generally, for any group G and any $a \in G$, the map $p_a\colon \mathbb{Z} \to G$; $m \mapsto a^m$ is a homomorphism with image $\langle a\rangle := \{a^m : m \in \mathbb{Z}\}$ called the *cyclic subgroup of G generated by a*. If $G = \langle a\rangle$, G is called a *cyclic group*. The kernel of p_a is $n\mathbb{Z}$, where either

- p_a is injective, $n = 0$ ($0\mathbb{Z} = \{0\}$), and a has *infinite order* $o(a) = \infty$, or
- n is the smallest $n \in \mathbb{N}$ such that $a^n = 1$ and is called the *order* $o(a) = n$ of a, in which case $\langle a\rangle = \{a^0 = 1, a^1 = a, a^2, \ldots a^{n-1}\}$ is finite with $|\langle a\rangle| = o(a)$.

(ii) Since $\exp(0) = 1$ and $\exp(x+y) = \exp(x)\exp(y)$, $\exp\colon \mathbb{R} \to \mathbb{R}^\times$ is a homomorphism from the additive group $\mathbb{R}$ to the multiplicative group $\mathbb{R}^\times$.

(iii) The alternating group A_n is the kernel of the *sign homomorphism* $\varepsilon\colon S_n \to \mu_2 = \mathbb{Z}^\times = \{\pm 1\}$ given by $\varepsilon(\sigma) = 1$ if σ is even, and $\varepsilon(\sigma) = -1$ if σ is odd.

(iv) Since $\det(I_n) = 1$ and $\det(AB) = \det(A)\det(B)$, $\det\colon \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F}^\times$ is a homomorphism with kernel the special linear group $\mathrm{SL}_n(\mathbb{F})$.

2 Groups act!

2.1 Definition (Actions)**.** A (*left*) *action* of a group or monoid G on a set X is a map

$$G \times X \to X;\ (a, x) \mapsto a \cdot x$$

such that:

(Identity)	for all $x \in X$,	$1 \cdot x = x$;
(Composition)	for all $a, b \in G$ and $x \in X$,	$(ab) \cdot x = a \cdot (b \cdot x)$.

Then G *acts* on X and X is a (*left*) *G-set*.

2.2 Remarks. Given an action of G on X, any $a \in G$ defines a map $\phi_a\colon X \to X$ by $\phi_a(x) = a \cdot x$. Hence there is a map $\phi\colon G \to X^X$ with $\phi(a) = \phi_a$. In terms of ϕ, the Identity Axiom says $\phi(1) = \mathrm{id}$ and the Composition Axiom says $\phi(ab) = \phi(a) \circ \phi(b)$, i.e., $\phi\colon G \to X^X$ is a homomorphism, sometimes called the *action homomorphism* of the G-set X.

By Remark 1.9(i), if $a \in G$ is invertible, then $\phi_a\colon X \to X$ is invertible with inverse $\phi_{a^{-1}}$. In particular, if G is a group then an action $(a, x) \to a \cdot x$ on G of X is the same thing as a homomorphism $\phi\colon G \to \mathrm{Sym}(X)$: for any such ϕ, $a \cdot x := \phi(a)(x)$ defines an action of G and X. However, the notation $a \cdot x$ is easier to work with than $\phi(a)(x)$!

2.3 Examples (Actions)**.** (i) If G acts on X with action homomorphism ϕ, then so does any $H \leqslant G$, with action homomorphism $\phi|_H$. Hence for any $a \in G$, $\langle a \rangle$ acts on X.

For example, for any set X, $\mathrm{Sym}(X)$ acts tautologically on X by $\sigma \cdot x = \sigma(x)$, hence so does any $G \leqslant \mathrm{Sym}(X)$ (with action homomorphism the inclusion of G into $\mathrm{Sym}(X)$).

(ii) Let $G = D_{2n}$ be the *dihedral group* of symmetries of a regular n-gon $P \subseteq \mathbb{R}^2$ with vertices $x_1, \ldots x_n$. Then G acts on $\{x_1, \ldots x_n\}$ by $a \cdot x_j = a(x_j)$, hence on $\{1, \ldots n\}$: if $a(x_j) = x_k$, then $a \cdot j = k$. For example, D_8 is the group of symmetries of the square with vertices $x_1 = (1, 0)$, $x_2 = (0, 1)$, $x_3 = (-1, 0)$, $x_4 = (0, -1)$, and hence D_8 acts on $\{x_1, x_2, x_3, x_4\}$ and $\{1, 2, 3, 4\}$. It also acts (e.g.) on the set of diagonals $\{\{x_1, x_3\}, \{x_2, x_4\}\}$.

(iii) Let $X = \{\Delta_{13,24}, \Delta_{12,34}, \Delta_{14,23}\}$ where $\Delta_{13,24} = \{\{1, 3\}, \{2, 4\}\}$, $\Delta_{12,34} = \{\{1, 2\}, \{3, 4\}\}$, and $\Delta_{14,23} = \{\{1, 4\}, \{2, 3\}\}$ are the 3 partitions of the 4 element set $\{1, 2, 3, 4\}$ into two 2 element subsets. Then S_4 acts on X by $\sigma \cdot \{\{i, j\}, \{k, \ell\}\} = \{\{\sigma(i), \sigma(j)\}, \{\sigma(k), \sigma(\ell)\}\}$.

(iv) If a group G acts on X, then for any set Y, G acts 'pointwise' on the set X^Y of all maps $f\colon Y \to X$ by $(a \cdot f)(y) = a \cdot (f(y))$. In particular, it acts on the set $X^\ell := X^{\{1,\ldots\ell\}}$ of all ℓ-tuples in X by $a \cdot (x_1, \ldots x_\ell) = (a \cdot x_1, \ldots a \cdot x_\ell)$.

(v) Let V be an n-dimensional vector space. Then $\mathrm{GL}(V)$ acts on V by linear transformations: $g \cdot v = g(v)$ for $g \in \mathrm{GL}(V)$, $v \in V$. By (iv) it follows that $\mathrm{GL}(V)$ also acts on V^n. Since an invertible linear transformation g of V sends a basis $(v_1, \ldots v_n)$ to a basis $(g(v_1), \ldots g(v_n))$, $\mathrm{GL}(V)$ acts on the set of bases for V.

2.4 Example (Left action)**.** Any group (or monoid) G acts on $X = G$ by left multiplication $a \cdot x := ax$ $\forall\, a, x \in G$: $1 \cdot x = 1x = x$ and $(ab) \cdot x = (ab)x = a(bx) = a \cdot (b \cdot x)$. The action homomorphism $\lambda\colon a \mapsto \lambda_a$ (with $\lambda_a(x) = ax$) has $\ker \lambda = \{1\}$ (if $\lambda_a = \mathrm{id}$ then $1 = \lambda_a(1) = a1 = a$). If G is a group, Lemma 1.10 implies $\lambda\colon G \to \mathrm{Sym}(G)$ is injective and hence [Alg1A]:

> **Cayley's Theorem** (Jordan 1870)**.** Any group G is isomorphic to a subgroup of $\mathrm{Sym}(G)$.

Similarly any group G acts on $X = G$ by right multiplication, with action homomorphism $\rho\colon G \to \mathrm{Sym}(G)$; $a \mapsto \rho_a$ given by $\rho_a(x) := xa^{-1}$.

2.5 Definition. For any group G and any $a, x \in G$ the *conjugate* of x by a is ${}^a x := axa^{-1}$.

2.6 Proposition. Any group G acts on $X = G$ by *conjugation*: $a \cdot x = {}^a x$ for all $a, x \in G$, and the action homomorphism $a \mapsto \kappa_a$, with $\kappa_a(x) = {}^a x$, is a homomorphism $\kappa\colon G \to \mathrm{Aut}(G)$, i.e., for all $a \in G$, κ_a is an automorphism of G.

Proof. This is an action because ${}^1 x = 1x1^{-1} = x$ and

$$ {}^{ab}x = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = {}^a({}^b x). $$

Now note that $\kappa_a(1) = {}^a1 = a1a^{-1} = aa^{-1} = 1$ and

$$\kappa_a(xy) = axya^{-1} = axa^{-1}\,aya^{-1} = \kappa_a(x)\kappa_a(y).$$

Since κ_a is invertible (with $\kappa_a^{-1} = \kappa_{a^{-1}}$), it is an automorphism of G. □

2.7 Example (Similar matrices)**.** More generally, if G is a subgroup of a monoid M, then G acts on M by conjugation. Let $G = \mathrm{GL}_n(\mathbb{F})$ and $M = M_n(\mathbb{F})$. Then then there is an action of invertible matrices $P \in \mathrm{GL}_n(\mathbb{F})$ on matrices $A \in M_n(\mathbb{F})$ by $P \cdot A = PAP^{-1}$.

This is useful! Any $A \in M_n(\mathbb{F})$ acts on $v \in \mathbb{F}^n$ by $A \cdot v = Av$. Suppose $v_1, \ldots v_n$ is a basis of eigenvectors of A and define $P \in \mathrm{GL}_n(\mathbb{F})$ by $Pe_i = v_i$ (where $e_1, \ldots e_n$ is the standard basis). Then $D := P^{-1} \cdot A = P^{-1}AP$ is diagonal, i.e., $A = P \cdot D$.

3 Orbits and stabilizers

3.1 Definitions (Orbits and stabilizers)**.** If a group G acts on a set X, then the *G-orbit* of $x \in X$ is

$$\mathrm{orb}_G(x) = G \cdot x := \{a \cdot x : a \in G\}$$

and the *stabilizer* in G of $x \in X$ is

$$\mathrm{Stab}_G(x) = G_x := \{a \in G : a \cdot x = x\}.$$

The action is called *transitive* if $\mathrm{orb}_G(x) = X$ for all $x \in X$, and *free* if $\mathrm{Stab}_G(x) = \{1\}$ for all $x \in X$; if it is both free and transitive, it is said to be *regular* (or *simply transitive*). Observe that $\bigcap_{x\in X} \mathrm{Stab}_G(x)$ is the kernel of the action homomorphism. If this is $\{1\}$, G is isomorphic to a subgroup of $\mathrm{Sym}(X)$ and the action is called *faithful*. (In particular any free action is faithful.)

3.2 Orbit Partition Theorem. Let G be a group and X be a G-set. Then $\{\mathrm{orb}_G(x) : x \in X\}$ is a partition of X, i.e., $\bigcup_{x\in X} \mathrm{orb}_G(x) = X$ and for all $x, y \in X$ either $\mathrm{orb}_G(x) = \mathrm{orb}_G(y)$ or $\mathrm{orb}_G(x) \cap \mathrm{orb}_G(y) = \varnothing$.

Proof. Define a relation $\sim$ on X by $x \sim y$ iff $y \in \mathrm{orb}_G(x)$. Clearly $x = 1 \cdot x \in \mathrm{orb}_G(x)$, so $\sim$ is reflexive. If $y = a \cdot x \in \mathrm{orb}_G(x)$ then $x = a^{-1} \cdot y \in \mathrm{orb}_G(y)$ so $\sim$ is symmetric. Now if $z = a \cdot y$ and $y = b \cdot x$ then $z = a \cdot (b \cdot x) = (ab) \cdot x$ so $\sim$ is transitive and thus an equivalence relation. By definition, the orbits are the equivalence classes, so they partition X. □

3.3 Proposition. Let G be a group acting on X. Then for all $x \in X$, $\mathrm{Stab}_G(x) \leqslant G$.

Proof. Clearly $1 \in \mathrm{Stab}_G(x)$, and if $a, b \in \mathrm{Stab}_G(x)$ then $(ab) \cdot x = a \cdot (b \cdot x) = a \cdot x = x$ so $ab \in \mathrm{Stab}_G(x)$. Finally if $\phi\colon a \mapsto \phi_a$ denotes the action homomorphism and ϕ_a fixes x, then so does $\phi_{a^{-1}} = \phi_a^{-1}$. □

3.4 Remark. A good way to show that a subset H of G is a subgroup is to exhibit it as a stabilizer of something.

3.5 Examples (Orbits and stabilizers)**.** Let us revisit Examples 2.3.

(i) If G acts on X and $H \leqslant G$, then $\mathrm{orb}_H(x) \subseteq \mathrm{orb}_G(x)$ for any $x \in X$. If $a \in G$, then the *a-orbit* of $x \in X$ is $\mathrm{orb}_a(x) := \mathrm{orb}_{\langle a\rangle}(x) = \{\phi_a^k(x) : k \in \mathbb{Z}\}$ where $\phi_a(x) = a \cdot x$.

In particular, for $\sigma \in S_n$ and $j \in \{1, \dots n\}$, then $\mathrm{orb}_\sigma(j) = \{\sigma^k(j) : k \in \mathbb{Z}\}$ is called a *cycle* of σ with length $\ell = |\mathrm{orb}_\sigma(j)|$ (or an ℓ-*cycle* for short). By Theorem 3.2, the action of $\langle\sigma\rangle$ partitions $\{1, \dots n\}$ into a disjoint union $X_1, X_2, \dots X_m$ of cycles of σ with lengths $\ell_1 \geqslant \ell_2 \geqslant \cdots \geqslant \ell_m$ (wlog). Then σ has a *cycle type* $(\ell_1, \dots \ell_m)$.

For example if $\sigma \in S_8$ is defined by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 4 & 2 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\ 3\ 4\ 2\ 5)(6\ 7)(8)$$

then σ has cycle type $(5, 2, 1)$

(ii) The action of D_{2n} on the vertices $\{x_1, \dots x_n\}$ of a regular n-gon is transitive and the stabilizer of x_k is $\{1, s_k\}$ where s_k is the unique reflection fixing x_k. Hence the action is faithful and D_{2n} is isomorphic to a subgroup of S_n.

(iii) The action of S_4 on $X = \{\Delta_{13,24}, \Delta_{12,34}, \Delta_{14,23}\}$ is transitive, with image $\mathrm{Sym}(X)$ and kernel the *Klein four group* $V_4 := \{\mathrm{id}, (1\ 3)(2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$. The stabilizer of $\Delta_{13,24} = \{\{1, 3\}, \{2, 4\}\}$ is (isomorphic to) the dihedral group D_8.

(iv) If G acts on X and the action of G on $\{(x_1, \dots x_\ell) \in X^\ell : x_i \neq x_j \text{ for } i \neq j\}$ is transitive, the action of G on X is said to be ℓ-*transitive*. Observe that the action of S_n on $\{1, \dots n\}$ is ℓ-transitive for all $\ell \leqslant n$.

(v) Let V be an n-dimensional vector space. Then the action of $\mathrm{GL}(V)$ on bases of V is regular: if $(v_1, \dots v_n)$ is a basis for V, then for any $(v'_1, \dots v'_n) \in V^n$ there is a unique linear map g with $g(v_j) = v'_j$ for all j, and if $(v'_1, \dots v'_n)$ is also a basis then g is invertible.

We now turn to the important example of the action of a group G on itself by conjugation (Definition 2.5), where the equivalence relation defining the orbits is *conjugacy*.

3.6 Definitions (Conjugacy)**.** $x, y \in G$ are *conjugate* if $y = {}^a x := axa^{-1}$ for some $a \in G$, and the orbit of $x \in G$ under the conjugation action is the *conjugacy class* ${}^G x := \{{}^a x : a \in G\}$ of x. By the Orbit Partition Theorem 3.2, G is a disjoint union of conjugacy classes. The image of of the action homomorphism $\kappa\colon G \to \mathrm{Aut}(G)$ is the subgroup of *inner automorphisms* of G and its kernel is

$$Z(G) := \{a \in G : \forall\, x \in G,\ axa^{-1} = x\} = \{a \in G : \forall\, x \in G,\ ax = xa\},$$

called the *centre* of G. The stabilizer of $x \in G$ under conjugation is its *centralizer*

$$C_G(x) := \{a \in G : axa^{-1} = x\} = \{a \in G : ax = xa\},$$

which is thus a subgroup of G, and $C_G(x) = G$ if and only if $x \in Z(G)$.

3.7 Example (Conjugate permutations)**.** Let $\sigma \in \mathrm{Sym}(X)$ with $\sigma(x) = y$. Then for any $\gamma \in \mathrm{Sym}(X)$, $({}^\gamma\sigma)(\gamma(x)) = (\gamma \circ \sigma \circ \gamma^{-1})(\gamma(x)) = \gamma(y)$. For example if $\sigma = (1\ 3\ 4\ 2\ 5)(6\ 7)(8) \in S_8$ then

$${}^\gamma\sigma = (\gamma(1)\ \gamma(3)\ \gamma(4)\ \gamma(2)\ \gamma(5))\,(\gamma(6)\ \gamma(7))\,(\gamma(8)).$$

In general, if $\sigma \in S_n$ has cycle type $(\ell_1, \dots \ell_m)$, the conjugacy class ${}^{S_n}\sigma$ consists of all permutations of that type. For example if $\sigma = (1\ 2)(3\ 4)$, ${}^{S_4}\sigma = \{(1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$.

3.8 Example. Cayley's Theorem (Example 2.4) shows that the action $\lambda\colon G \to \mathrm{Sym}(G)$ of a group G on itself by left multiplication is faithful. More is true: if $a \in \mathrm{Stab}_G(x)$ for some $x \in X = G$, then $ax = a \cdot x = x$ and so $a = axx^{-1} = xx^{-1} = 1$; hence the action is free. Now given $x, y \in G$, let $a = yx^{-1}$; then $a \cdot x = (yx^{-1})x = y$ so the action is transitive, hence regular.

Now suppose $H \leqslant G$. Then $\lambda|_H\colon H \to \mathrm{Sym}(G)$ defines a free action of H on G with $\mathrm{orb}_H(x) = Hx := \{hx : h \in H\}$, a *right coset* of H in G. Hence by the Orbit Partition Theorem 3.2, the right cosets of H form a partition of G. Now for any $x \in G$, the map $H \to Hx$; $h \mapsto hx$ is a bijection, so the right cosets all have the same cardinality as H. If G is finite, $|G|$ (the number of elements in G) is called the *order* of G and we have [Alg1A]:

> **Lagrange's Theorem** (Jordan 1861)**.** Let G be a finite group with a subgroup H. Then the order of H divides the order of G.

In particular, if $H = \langle a \rangle$ for some $a \in G$, have that $o(a)$ divides $|G|$.

Using instead right multiplication $\rho|_H\colon H \to \mathrm{Sym}(G)$ gives the partition of G into *left cosets* $xH := \{xh : h \in H\}$. However, since H is a subgroup, $H^{-1} := \{h^{-1} : h \in H\} = H$ and so $(xH)^{-1} := \{g^{-1} : g \in xH\} = Hx^{-1}$. Hence inversion defines a bijection between the sets of left and right cosets of H in G, and their cardinality is called the *index* $[G : H]$ of H in G.

Lagrange's Theorem then states that if G is a finite group, $[G : H] = |G|/|H|$.

3.9 Definition. For $H \leqslant G$, the set $G/H := \{xH : x \in G\}$ of left cosets of H in G is called the *left coset space* of H in G. (Similarly the set of right cosets is sometimes denoted $H\backslash G$.)

3.10 Proposition. For any $H \leqslant G$, the left coset space G/H is a transitive G-set with the action $a \cdot (xH) := (ax)H$. Furthermore $\mathrm{Stab}_G(xH) = xHx^{-1} := \{xhx^{-1} : h \in H\}$.

Proof. Clearly $(1x)H = xH$ and $((ab)x)H = (a(bx))H = a \cdot (bx)H$, so this is an action, and $(yx^{-1})xH = yH$ so it is transitive. Now

$$\mathrm{Stab}_G(xH) = \{a \in G : axH = xH\} = \{a \in G : x^{-1}ax \in H\} = xHx^{-1}. \qquad \square$$

3.11 Remark. In particular, for the identity coset $1H = H$, $\mathrm{Stab}_G(H) = H$. The kernel of the action is thus the subgroup $\mathrm{Core}_G(H) := \bigcap_{x \in G} xHx^{-1}$ of H, called the *core* of H in G.

3.12 Definition (Morphisms of G-sets)**.** For any group G, a map $\Phi\colon X \to Y$ between G-sets is called a *G-set morphism* if for all $g \in G$, $x \in X$, $\Phi(g \cdot x) = g \cdot \Phi(x)$. If Φ has an inverse (which is automatically a G-set morphism: write $x = \Phi^{-1}(y)$ and apply Φ^{-1} to $\Phi(g \cdot x) = g \cdot \Phi(x)$) then it is called a *$G$-set isomorphism*; X and Y are then called *isomorphic* G-sets, written $X \cong_G Y$. A *G-set automorphism* of X is an isomorphism $\Phi\colon X \to X$ and the set these is denoted $\mathrm{Aut}_G(X)$.

3.13 Remark. If G acts on X and $x \in X$, then $\mathrm{orb}_G(x) \subseteq X$ is a G-set, by restricting the action, and the inclusion $\mathrm{orb}_G(x) \to X$ is a G-set morphism. Together with Proposition 3.10, this sets the scene for an amazingly useful theorem (see Alg1A for a partial version).

3.14 Orbit–Stabilizer Theorem. Let G be a group acting on a set X and for $x \in X$, let $G_x = \mathrm{Stab}_G(x)$ be its stabilizer. Then $a \cdot x \mapsto aG_x$ (for $a \in G$) defines a G-set isomorphism

$$\Psi\colon \mathrm{orb}_G(x) \to G/G_x.$$

[**Aside on functions**. A function $f\colon X \to Y$ can be viewed as a special kind of relation $R \subseteq X \times Y$ often called the *graph* of f: $(x, y) \in R$ if $y = f(x)$. To yield a function $f\colon X \to Y$,

R must be *everywhere defined* (every $x \in X$ is related to some $y \in Y$) and *uniquely defined* (if x is related to y_1 and y_2 then $y_1 = y_2$). Compare these with surjectivity and injectivity.]

Proof. Clearly Ψ is everywhere defined and surjective. To show it is uniquely defined and injective, observe that

$$a \cdot x = b \cdot x \Leftrightarrow (b^{-1}a) \cdot x = x \Leftrightarrow b^{-1}a \in G_x \Leftrightarrow aG_x = bG_x.$$

Hence Ψ is a bijection. To show it is a G-set isomorphism, observe that

$$\Psi(g \cdot (a \cdot x)) = \Psi((ga) \cdot x) = (ga)G_x = g \cdot (aG_x) = g \cdot \Psi(a \cdot x). \qquad \square$$

3.15 Corollary. If a group G acts on X and $\mathrm{orb}_G(x)$ is finite then $G_x = \mathrm{Stab}_G(x)$ has finite index $[G : G_x] = |\,\mathrm{orb}_G(x)|$. If also G is finite, $|G| = |G_x|\,|\,\mathrm{orb}_G(x)|$.

3.16 Remark. The Orbit Partition Theorem 3.2 and the Orbit–Stabilizer Theorem 3.14 together imply that any G-set is, up to G-set isomorphism, a disjoint union of left coset spaces.

3.17 Examples. (i) Take $G = \langle\sigma\rangle \leqslant S_8$, with $\sigma = (1\ 3\ 4\ 2\ 5)(6\ 7)(8)$ acting on $X = \{1, \dots 8\}$ and $x = 1$. (Note $\sigma^5 = (6\ 7)$ and so $o(\sigma) = 10$.) Then the G-set isomorphism is

$$1 = \sigma^5(1) \mapsto \mathrm{Stab}_G(1) = \{\mathrm{id}, \sigma^5\}, \quad 3 = \sigma(1) = \sigma^6(1) \mapsto \sigma\,\mathrm{Stab}_G(1) = \{\sigma, \sigma^6\}$$
$$4 \mapsto \{\sigma^2, \sigma^7\}, \quad 2 \mapsto \{\sigma^3, \sigma^8\}, \quad 5 \mapsto \{\sigma^4, \sigma^9\}$$

(ii) $G = D_8$ acts transitively on the set $\{x_1, x_2, x_3, x_4\}$ of vertices of a square with $\mathrm{Stab}_G(x_1) = \{\mathrm{id}, s_1\}$. The other left cosets are $\{r, rs_1 = s_v\}$, $\{r^2, r^2s_1 = s_2\}$ and $\{r^3, r^3s_1 = s_h\}$.

(iii) $G = S_4$ acts transitively on $\{\Delta_{12,34}, \Delta_{13,24}, \Delta_{14,23}\}$. Then

$$\mathrm{Stab}_G(\Delta_{13,24}) = \{\mathrm{id}, (1\ 3), (2\ 4), (1\ 3)(2\ 4), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\},$$

which is (isomorphic to) D_8 and has index $24/8 = 3$.

3.18 Remark. It is often useful to distinguish the subset $X^G := \{x \in X : a \cdot x = x \text{ for all } a \in G\}$ of fixed points of the G-action, i.e., $x \in X^G$ iff $\mathrm{Stab}_G(x) = G$ iff $|\,\mathrm{orb}_G(x)| = 1$.

3.19 Corollary. Suppose G is a group acting on a finite set X with fixed point set X^G. Let $X_1, \dots X_m$ be the (disjoint) orbits of G in X with $|X_i| \geqslant 2$, and let H_i be the stabilizer of a point in X_i for each $i \in \{1, \dots m\}$. Then each H_i has finite index $[G : H_i]$ in G and

$$|X| = |X^G| + \sum_{i=1}^{m} [G : H_i].$$

Corollary 3.19 has an important application to the conjugation action for finite G. Here $X^G = \{x \in G : axa^{-1} = x \text{ for all } a \in G\} = Z(G)$, the centre of G.

3.20 Theorem (The Class Equation)**.** For a finite group G,

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(a_i)]$$

where the sum is taken over the m conjugacy classes in G with more than one element and a_i is an element of each such class.

3.21 Example. To compute the Class Equation for a group G, note that $o({}^a b) = o(b)$ so elements in the same conjugacy class have the same order. In S_n, σ and τ are conjugate if and only if they have the same cycle type. A permutation is even if the number of even length cycles is even, and permutations of the same cycle type are conjugate in A_n unless their cycle lengths are distinct odd integers (exercises). Thus for $G = A_5$, the conjugacy classes ${}^G\sigma$ are given in the table

σ	$o(\sigma)$	$\lvert{}^G\sigma\rvert$	$\lvert C_G(\sigma)\rvert$
id	1	1	60
(1 2)(3 4)(5)	2	15	4
(1 2 3)(4)(5)	3	20	3
(1 2 3 4 5)	5	12	5
(1 2 3 5 4)	5	12	5

where only the 5-cycles split into two conjugacy classes. The Class Equation of A_5 is thus $60 = 1 + 15 + 20 + 12 + 12$.

4 Conjugacy, normality and simplicity

4.1 Definitions (Conjugate and normal subgroups)**.** The conjugation action $\kappa\colon G \to \mathrm{Aut}(G)$ gives rise to an action of G on the set of all subsets of G by $a \cdot H = {}^a H := \{aha^{-1} : h \in H\}$ which is called the *conjugate* of H by a also denoted aHa^{-1}: check ${}^1H = H$ and for all $a, b \in G$, ${}^a({}^b H) = {}^{ab}H$.

If $H \leqslant G$, then ${}^a H \leqslant G$ because conjugation by a is an automorphism of G: $1 = {}^a 1 \in {}^a H$ and for $g, h \in H$, ${}^a g\, {}^a h = {}^a(gh) \in {}^a H$ and $({}^a h)^{-1} = {}^a(h^{-1}) \in {}^a H$. The orbit of H is its *conjugacy class* ${}^G H := \{{}^a H : a \in G\}$ of H in G. A subgroup $H \leqslant G$ which is fixed by the action, i.e., ${}^a H = H$ for all $a \in G$ is called *normal subgroup* of G, written $H \trianglelefteq G$. In general, the stabilizer of H is its *normalizer*

$$N_G(H) = \{a \in G : {}^a H = H\}.$$

Thus $H \trianglelefteq N_G(H) \leqslant G$. The Orbit–Stabilizer Theorem 3.14 in this case is a G-set isomorphism between ${}^G H$ and $G/N_G(H)$.

4.2 Remarks. (i) To show $H \trianglelefteq G$, it suffices to show $H \leqslant G$ and ${}^a H \subseteq H$ for all $a \in G$ (because $a^{-1} \in G$, so ${}^{a^{-1}} H \subseteq H$, which implies $H \subseteq {}^a H$).

(ii) If $H \trianglelefteq G$ and $a \in H$, then ${}^G a \subseteq H$. Hence any normal subgroup of G is a union of conjugacy classes of G.

(iii) For any group G, $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$.

(iv) $H \trianglelefteq G$ if and only if $Ha = aH$ for all $a \in G$, i.e., the left and right cosets of H coincide.

(v) For any homomorphism $\phi\colon G \to \tilde{G}$, $\ker\phi \trianglelefteq G$ [Check!].

In particular, suppose $H \leqslant G$ and the left coset space G/H can be made into a group in such a way that $\phi\colon G \to G/H; a \mapsto aH$ is a homomorphism. Then $\phi(1) = 1H$, so the identity element of G/H must be the identity coset, and the group operation must be $aH\, bH = \phi(a)\phi(b) = \phi(ab) = (ab)H$. Hence $\ker\phi = \{a \in G : aH = 1H\} = H$ and so $H \trianglelefteq G$. This has a converse.

4.3 Proposition. Suppose $N \trianglelefteq G$. Then G/N is a group with identity element $1N$ and group operation $aN\, bN = (ab)N$, and $\phi\colon G \to G/N; a \mapsto aN$ is a homomorphism.

Proof. The main task is to show that the group operation is well-defined. For any $x \in aN = Na$ and $y \in bN$, $xy = (xb)(b^{-1}y)$ with $xb \in N(ab) = (ab)N$ and $b^{-1}y \in N$. Hence $xy \in (ab)N$ i.e., $(xy)N = (ab)N$. The group axioms for G/N follow from those in G: $(1N)(aN) = (1a)N = aN = (a1)N = aN(1N)$, $aN(bNcN) = (abc)N = (aNbN)cN$ and $a^{-1}NaN = (a^{-1}a)N = 1N = (aa^{-1}N) = aNa^{-1}N$. Now $a \mapsto aN$ is a homomorphism $G \to G/N$ by construction. □

4.4 Definition. G/N is called the *quotient* or *factor group* of G by $N \trianglelefteq G$.

4.5 Remark. There is a bijection between normal subgroups of G and *congruences* on G, which are equivalence relations $\simeq$ on G such that $a_1 \simeq b_1$ and $a_2 \simeq b_2$ implies $a_1a_2 \simeq b_1b_2$. Indeed, for any congruence on G, $N := [1] \trianglelefteq G$, and conversely if $N \trianglelefteq G$, then $a \simeq b$ if $a^{-1}b \in N$ defines a congruence. Since this is the equivalence relation defining the left cosets of N, congruences provide another way to see that G/N is a group. [Tedious Exercise.]

4.6 Examples (Normal subgroups)**.** (i) If $H \leqslant G$ with index $[G : H] = 2$ (e.g. $A_n \leqslant S_n$) then its left cosets are H and $G \smallsetminus H$, which are also the right cosets, so $H \trianglelefteq G$ and G/H is the unique group up to isomorphism with 2 elements.

(ii) From Example 3.5(iii) we know $V_4 = \{\mathrm{id}, (1\ 3)(2\ 4), (1\ 2)(3\ 4), (1\ 4)(2\ 3)\}$ is the kernel of the action of S_4 on the three "bisections" of $\{1, 2, 3, 4\}$, hence a normal subgroup.

(iii) If $N \trianglelefteq S_n$ contains a permutation of cycle type $(\ell_1, \ell_2, \ldots, \ell_m)$ then by Remark 4.2(ii), it contains all permutations of that cycle type.

4.7 First Isomorphism Theorem. Let $\phi\colon G \to H$ be a homomorphism and let $N = \ker\phi$. Then $aN \mapsto \phi(a)$ (for $a \in G$) defines an isomorphism

$$\Phi\colon G/\ker\phi \to \operatorname{im}\phi.$$

Proof. Clearly Φ is everywhere defined and surjective. To show it is uniquely defined and injective, observe

$$aN = bN \quad\Leftrightarrow\quad a^{-1}b \in N \quad\Leftrightarrow\quad 1 = \phi(a^{-1}b) = \phi(a)^{-1}\phi(b) \quad\Leftrightarrow\quad \phi(a) = \phi(b).$$

Now

$$\Phi(aN\,bN) = \Phi((ab)N) = \phi(ab) = \phi(a)\phi(b) = \Phi(aN)\,\Phi(bN),$$

so Φ is a homomorphism, hence an isomorphism. □

4.8 Remark. G acts on H by $g \cdot h = \phi(g)h$ with $\mathrm{Stab}_G(1) = \ker\phi$ and so Φ is also an isomorphism of G-sets $G/\ker\phi \to \operatorname{im}\phi = \mathrm{orb}_G(1)$ by the Orbit–Stabilizer Theorem 3.14.

4.9 Examples (Quotients)**.** (i) For $n \in \mathbb{Z}^+$, $A_n = \ker(\varepsilon\colon S_n \to \mu_2) \trianglelefteq S_n$, and $S_n/A_n \cong \mu_2$.

(ii) V_4 is the kernel of a homomorphism $S_4 \to S_3$ and so $S_4/V_4 \cong S_3$.

(iii) If G is a group and $a \in G$ with $o(a) = n$, then $p_a\colon \mathbb{Z} \to G; m \mapsto a^m$ is a homomorphism with $\ker p_a = n\mathbb{Z}$ and $\operatorname{im} p_a = \langle a\rangle$. Hence $\langle a\rangle \cong \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

We now introduce an important notion.

4.10 Definition. A group G is *simple* if $G \neq \{1\}$ and the only normal subgroups of G are $\{1\}$ and G.

4.11 Remark. We shall see that simple groups are a bit like prime numbers. If $g \in \mathbb{N}$ is not prime and n divides g with $1 < n < g$, then g factorizes into smaller integers n and g/n.

Analogously, if a group G is not simple, with $N \trianglelefteq G$ and $1 < N < G$, then G "factorizes" into "simpler" groups N and G/N.

4.12 Examples (Simple groups)**.** (i) If G has prime order p, then the only subgroups of G are $\{1\}$ and G, so G is simple (and cyclic, since for all $a \neq 1$, $o(a) = p$ and $G = \langle a \rangle \cong \mathbb{Z}_p$).

(ii) S_n is not simple for $n \geqslant 3$ since $A_n \trianglelefteq S_n$; A_3 is cyclic of prime order, hence simple, but A_4 is not simple, since $V_4 \trianglelefteq A_4$.

(iii) A_5 is a simple group. To see this, suppose $N \trianglelefteq A_5$. Then N is a union of conjugacy classes of A_5 including the identity. By the Class Equation of A_5 ($|A_5| = 60 = 1{+}20{+}15{+}12{+}12$), $|N| = 1 + 20a + 15b + 12c$ where $a, b \in \{0, 1\}$ and $c \in \{0, 1, 2\}$. However, by Lagrange's Theorem, $|N|$ is a divisor d of $60 = 2^2 \cdot 3 \cdot 5$. The only such d with $12 < d < 60$ are $d = 15, 20, 30$ and these do not have the required form, so $N = \{1\}$ or $N = A_5$.

5 Cyclic groups and p-groups

5.1 Proposition. Let $G = \langle a \rangle$ be a finite cyclic group of order $n = dm$. Then $\langle a^m \rangle \leqslant G$ is the unique subgroup of G order d.

Proof. Clearly $\langle a^m \rangle$ is such a subgroup, so it suffices to show that if $H \leqslant G$ has order d then $H \subseteq \langle a^m \rangle$. If a^k in H, then $a^{kd} = 1$ by Lagrange's Theorem, so $n = md$ divides kd and hence $k = rm$ for some $r \in \mathbb{N}$. Now $a^k = (a^m)^r \in \langle a^m \rangle$. □

5.2 Definition. The *direct product* of groups $G_1, G_2, \ldots G_\ell$ is the group $G_1 \times G_2 \times \cdots \times G_\ell$ with identity $(1, 1, \ldots 1)$ and group operation $(a_1, a_2, \ldots a_\ell)(b_1, b_2, \ldots b_\ell) = (a_1 b_1, a_2 b_2, \ldots a_\ell b_\ell)$. (Check the axioms, noting that $(a_1, a_2, \ldots a_\ell)$ has inverse $(a_1^{-1}, a_2^{-1}, \ldots a_\ell^{-1})$.)

5.3 Example. If G_i is finite of order $|G_i| = n_i$ for $i \in \{1, \ldots \ell\}$, then $|G_1 \times \cdots \times G_\ell| = n_1 \cdots n_\ell$, and if also each $G_i = \langle a_i \rangle$ is cyclic, then $(a_1, \ldots a_\ell)$ has order $\operatorname{lcm}(n_1, \ldots n_\ell)$ in $G_1 \times \cdots \times G_\ell$. In particular if the n_i are coprime, $G_1 \times \cdots \times G_\ell = \langle (a_1, \ldots a_\ell) \rangle$ is also cyclic: this is the Chinese Remainder Theorem [Alg1A]. Hence if $n_i = p_i^{s_i}$ for $s_i \in \mathbb{N}$ and p_i prime, and $G = \langle a \rangle$ is cyclic of order $n = p_1^{s_1} \cdots p_\ell^{s_\ell}$ then $(a_1, \ldots a_\ell)^m \mapsto a^m \colon G_1 \times \cdots \times G_\ell \to G$ is an isomorphism. Thus any cyclic group is isomorphic to a product of cyclic groups with prime power orders. Groups of prime power order play a key role in finite group theory.

5.4 Definition. Let p be a prime. A *finite p-group* is a group of order p^s for some $s \in \mathbb{N}$.

5.5 p-Group Action Theorem. Suppose a finite p-group G acts on a finite set X with fixed point set $X^G \subseteq X$. Then $|X^G| \equiv |X| \pmod p$. In particular, if $|X| \equiv 0 \pmod p$ and X^G is nonempty, then X^G has at least p elements.

Proof. This is immediate from Corollary 3.19 and the fact that if $H = \operatorname{Stab}_G(x)$ for $x \notin X^G$ then $H \neq G$ and so $[G : H]$ is divisible by p. □

5.6 Corollary (p-Group Centre Theorem)**.** For a nontrivial finite p-group G, $Z(G) \neq \{1\}$.

Indeed G acts on $X = G$ by conjugation, with $1 \in Z(G) = X^G$ and $|Z(G)| \equiv |X| \equiv 0 \pmod p$.

5.7 Remark. This is not true for all finite groups: for example, $Z(S_3) = \{1\}$.

5.8 Lemma. Let P, H be subgroups of a group G. Then P acts on $X = G/H$ by $a \cdot (xH) = (ax)H$ for $a \in P$ and $x \in G$, with fixed point set

$$X^P = \{xH \in X : P \leqslant {}^xH\}.$$

Proof. The action is just the restriction to P of the action of G on the left coset space G/H. Now for any $a \in P$ and $x \in G$, $a \cdot (xH) = xH$ if and only if $x^{-1}axH = H$, i.e., $x^{-1}ax \in H$, i.e., $a \in {}^xH$. Thus X^P is as stated. □

Note that $P \leqslant {}^xH$ if and only if ${}^yP \leqslant H$ with $y = x^{-1}$. Hence when P is a p-group, the p-Group Action Theorem 5.5 gives the following way to count conjugates of P in H.

5.9 Corollary (p-Group Conjugacy)**.** Let G be a finite group, p a prime, and let $P, H \leqslant G$ with P a p-group. Then

$$|\{xH \in G/H : P \leqslant {}^xH\}| = |\{y^{-1}H \in G/H : {}^yP \leqslant H\}| \equiv [G : H] \pmod{p}.$$

In particular if p does not divide the index $[G : H]$ of H, P is conjugate to a subgroup of H.

5.10 Corollary (p-Group Normalizer Theorem)**.** Let G be finite p-group and $P < G$ a proper subgroup. Then $P < N_G(P)$.

Indeed, by Corollary 5.9 with $H = P$, $|N_G(P)/P| = |\{xP \in G/P : P = {}^xP\}| \equiv [G : P] \bmod p$.

5.11 Cauchy's Order p Theorem (1845)**.** Let G be a finite group with order divisible by a prime p. Then G has an element of order p.

Proof (McKay 1959). Let $X = \{(a_1, a_2, \dots a_p) \in G^p := G \times G \times \cdots \times G : a_1a_2 \cdots a_p = 1\}$, so $|X| = |G|^{p-1}$ is divisible by p (observe $a_p = (a_1a_2 \cdots a_{p-1})^{-1}$). Setting $\sigma = (1\ 2\ \cdots\ p)$, $\langle\sigma\rangle \leqslant S_p$ acts on X by $\sigma^k \cdot (a_1, a_2, \dots a_p) = (a_{\sigma^k(1)}, a_{\sigma^k(2)}, \dots a_{\sigma^k(p)})$: we check that $a_{\sigma(1)}a_{\sigma(2)} \cdots a_{\sigma(p)} = a_2a_3 \cdots a_pa_1 = a_1^{-1}(a_1a_2 \cdots a_p)a_1 = a_1^{-1}1a_1 = 1$, and the action axioms are immediate. But $(1, \dots 1) \in X^{\langle\sigma\rangle}$ and so the p-Group Action Theorem 5.5 (for the p-group $\langle\sigma\rangle$) implies the existence of another fixed point. This must have the form $(a, \dots a)$ for $1 \neq a \in G$, and so $a^p = 1$ and $o(a) = p$. □

6 Sylow theory

6.1 Example (Converse to Lagrange fails)**.** Lagrange's Theorem 3.8 implies that if a finite group G has a subgroup of order m then m divides $|G|$. The converse does not hold in general. For example A_4 has order 12, but if $H \leqslant A_4$ has order 6, then for any $\sigma \in A_4$, σ either preserves or swaps the two left cosets of H, so $\sigma^2 H = H$, i.e., $\sigma^2 \in H$. Since any 3-cycle is a square, all eight 3-cycles belong to H, which is impossible. Hence A_4 has no subgroup of order 6.

6.2 Definition. Let G be a finite group and p a prime. A *Sylow p-subgroup* is a finite p-group $P \leqslant G$ whose index $[G : P]$ is not divisible by p. We let $\mathrm{Syl}_p(G)$ denote the set of Sylow p-subgroups of G and $n_p(G) = |\mathrm{Syl}_p(G)|$ the number of Sylow p-subgroups of G.

6.3 Theorem (Sylow 1872)**.** Let G be a finite group, p a prime, and $r \in \mathbb{N}$.

(i) If p^r divides $|G|$ then G has a subgroup of order p^r; in particular $\mathrm{Syl}_p(G)$ is nonempty.

(ii) All $P \in \mathrm{Syl}_p(G)$ are conjugate, hence isomorphic, and $\mathrm{Syl}_p(N_G(P)) = \{P\}$.

(iii) $n_p(G) = [G : N_G(P)]$ divides $[G : P]$ and has the form $1 + pk$ for some $k \in \mathbb{N}$; furthermore $n_p(G) = 1$ if and only if G has a normal Sylow p-subgroup.

Proof. (i) We induct on r, starting from the fact that G has a subgroup of order $p^0 = 1$. Suppose $P \leqslant G$ is a subgroup of G of order p^r.

We apply Corollary 5.9 with $H = P$: as in Corollary 5.10, we obtain $[N_G(P) : P] \equiv [G : P] \pmod{p}$. Now $P \trianglelefteq N_G(P)$ so $N_G(P)/P$ is a group with quotient homomorphism $\phi\colon N_G(P) \to N_G(P)/P$ (sending $x \in N_G(P)$ to xP). If p^{r+1} divides G, say $|G| = p^{r+1}m$, then $[G : P] = |G|/|P| = p^{r+1}m/p^r = pm$ is divisible by p, hence so is $[N_G(P) : P]$. Therefore $N_G(P)/P$ has a subgroup K of order p by Cauchy's Order p Theorem 5.11.

Now $\phi^{-1}(K)$ is a subgroup of G which is a disjoint union of p left cosets of P, hence has order $pp^r = p^{r+1}$.

(ii) Suppose $P, Q \in \mathrm{Syl}_p(G)$ and apply Corollary 5.9 with $H = Q$. Since $[G : Q]$ is not divisible by p, P is conjugate to a subgroup ${}^yP \leqslant Q$, but this must be an equality because $|{}^yP| = |P| = |Q|$; now $g \mapsto {}^yg$ is an isomorphism $P \to Q$.

If $Q \in \mathrm{Syl}_p(N_G(P))$ then $Q = {}^aP$ for some $a \in N_G(P)$, but ${}^aP = P$ for any such a, so $Q = P$.

(iii) The number of conjugates of P is $[G : N_G(P)]$ by the Orbit–Stabilizer Theorem 3.14 applied to the conjugation action on subgroups, so (ii) implies $n_p(G) = [G : N_G(P)]$, which divides $[G : P]$ because $P \leqslant N_G(P)$.

We now apply Corollary 5.9 with $H = N_G(P)$. Then $\{y^{-1}N_G(P) \in X : {}^yP \leqslant N_G(P)\} = \{N_G(P)\}$, since if ${}^yP \leqslant N_G(P)$ then ${}^yP = P$ by (ii), so $y \in N_G(P)$. Hence $n_p(G) = [G : N_G(P)]$ is congruent to 1 modulo p.

Finally $n_p(G) = 1$ iff $N_G(P) = G$ iff $P \trianglelefteq G$. □

6.4 Remarks. Parts (i), (ii) and (iii) of this Theorem (typically in the form "Sylow p-subgroups exist", "Sylow p-subgroups are conjugate" and "$n_p(G)$ divides $|G|$ and is congruent to 1 mod p") are traditionally called Sylow's First, Second and Third Theorems. However, Sylow originally combined these results into two theorems, not three.

When there is no ambiguity, we often write n_p or $n(p)$ for $n_p(G)$.

6.5 Examples (Groups which cannot be simple)**.** By the p-Group Centre Theorem 5.6, a group of order p^s (with p prime) is simple if and only if it is abelian, hence cyclic of prime order (i.e., $s = 1$). The Sylow Theorems (in particular Theorem 6.3(iii)) show that many other groups cannot be simple.

(i) Let G be a group of order mp^r where p is prime, $1 < m < p$ and $r \geqslant 1$. By the Sylow Theorems $n_p = |\mathrm{Syl}_p(G)|$ satisfies

$$n_p = 1 + pk \text{ and } n_p \text{ divides } |G|/p^r = m$$

Since $p > m$, $n_p = 1$ and the unique Sylow p-subgroup is normal, so G is not simple.

(ii) Let G be a group of order p^2q where p and q are distinct primes. If $p > q$ then (i) implies that $n_p = 1$ and we have a normal Sylow p-subgroup. Otherwise $p < q$ and $n_q = 1 + qk$ divides $|G|/q = p^2$ so $n_q = 1$ or p^2. If $n_q = 1$ we have a normal Sylow q-subgroup. On the other hand, distinct Sylow q-subgroups Q_1, Q_2 have $Q_1 \cap Q_2 = \{1\}$, since they are cyclic of prime order, so if $n_q = p^2$, the Sylow q-subgroups account for $p^2(q-1)$ elements of order q in G. This only leaves p^2 elements of order $\neq q$. But the Sylow p-subgroups have order p^2, so $n_p = 1$. Hence G is not simple in this case either.

6.6 Theorem (Poincaré)**.** If G is a simple group and $\{1\} < H < G$ has finite index $[G : H] = n$, then G is isomorphic to a subgroup of A_n, hence is finite with $|G|$ dividing $|A_n| = \frac{1}{2}n!$.

Proof. Let $\phi\colon G \to \mathrm{Sym}(G/H) \cong S_n$ be the action homomorphism of the action of G on the left cosets of H. Then $\ker\phi \leqslant H < G$, so $\ker\phi = \{1\}$ since G is simple. Hence $G \cong \mathrm{im}\,\phi \cong G' \leqslant S_n$. If $\varepsilon|_{G'}\colon G' \to \mu_2$ has $\ker\varepsilon|_{G'} = \{1\}$, then $|G| = |G'| \leqslant 2$, which is impossible (since $\{1\} < H < G$). So $\ker\varepsilon|_{G'} = G'$ since G' is simple, i.e., $G' \leqslant A_n$ and $|G| = |G'|$ divides $|A_n|$ by Lagrange's Theorem. □

6.7 Example. Let G be a simple group of order $36 = 2^2\,3^2$. Then by the Sylow Theorems G has a Sylow 3-subgroup, which has order 9, hence index 4. By Poincaré, it follows that $36 = |G|$ divides $4!/2 = 12$. This is absurd, so there cannot be a simple group of order 36.

7 Finitely generated abelian groups

7.1 Remark. In this section, all groups are abelian, and we use additive notation: the identity is 0, the group operation is $+$, and the inverse of a is $-a$. The product $G_1 \times \cdots \times G_\ell$ of abelian groups $G_1, \ldots G_\ell$ may also be denoted $G_1 \oplus \cdots \oplus G_\ell$ and called their *direct sum.*

7.2 Definition. For subgroups $H_1, H_2 \ldots H_\ell$ of an abelian group G, $H_1 + \cdots + H_\ell := \{a_1 + \cdots + a_\ell : a_j \in H_j\}$ and we say the sum is *direct* if $\forall\, a_j \in H_j$ $(j \in \{1, \ldots \ell\})$, $a_1 + \cdots + a_\ell = 0$ implies $a_j = 0$ for all j.

7.3 Proposition. Let G be abelian and suppose that $G = H_1 + \cdots + H_\ell$ is a direct sum of subgroups $H_1, \ldots H_\ell$. Then $\phi\colon H_1 \oplus \cdots \oplus H_\ell \to G; (a_1, \ldots a_\ell) \to a_1 + \cdots + a_\ell$ is an isomorphism.

Proof. Clearly $\phi((a_1, \ldots a_\ell) + (b_1, \ldots b_\ell)) = \phi((a_1 + b_1, \ldots a_\ell + b_\ell)) = a_1 + b_1 + \cdots + a_\ell + b_\ell = a_1 + \cdots + a_\ell + b_1 + \cdots + b_\ell = \phi((a_1, \ldots a_\ell)) + \phi((b_1, \ldots b_\ell))$, since G is abelian, so ϕ is a homomorphism. Now ϕ is surjective with kernel $\{(0, \ldots 0)\}$ by definition of a direct sum, hence an isomorphism. □

7.4 Fundamental Theorem of Finite Abelian Groups. Let G be a finite abelian group. Then G is a direct sum of cyclic subgroups of prime power order. Furthermore the number of cyclic summands of order p^r (p prime, $r \in \mathbb{Z}^+$) is uniquely determined by G.

7.5 Remarks. Together with Proposition 7.3, this theorem shows that any finite abelian group G is isomorphic to a direct sum

$$(*) \qquad \mathbb{Z}_{p_1^{r_1}} \oplus \mathbb{Z}_{p_2^{r_2}} \oplus \cdots \oplus \mathbb{Z}_{p_\ell^{r_\ell}},$$

for some $\ell \in \mathbb{N}$, $r_j \in \mathbb{Z}^+$ and primes p_j $(j \in \{1, \ldots \ell\})$. However, the ordering of the cyclic summands is not uniquely determined. To classify finite abelian groups up to isomorphism, we fix the ordering in (*) so that $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_\ell$ and if $p_i = p_{i+1}$ then $r_i \leqslant r_{i+1}$. For example if G is a direct sum of cyclic subgroups with orders $9, 2, 4, 3, 4$, then $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$.

Finding all abelian groups of a given order $n = p_1^{s_1} \cdots p_m^{s_m}$, where $p_1 < p_2 < \cdots < p_m$ are primes, reduces then to the problem of finding, for each $k \in \{1, \ldots m\}$, all partitions

$$1 \leqslant r_1 \leqslant r_2 \leqslant \ldots \leqslant r_j \quad (j \in \mathbb{Z}^+) \quad \text{with} \quad r_1 + \cdots + r_j = s_k$$

of s_k. Each such partition gives a possible factorization $p_k^{s_k} = p_k^{r_1} \cdots p_k^{r_j}$.

7.6 Example. To find (up to isomorphism) all abelian groups of order 72, observe that $72 = 2^3\,3^2$. The possible factorizations of 2^3 are (8), (2, 4), (2, 2, 2) whereas for 3^2, they are are (3^2), (3, 3). We then have that (up to isomorphism) the abelian groups of order 72 are

$$\begin{array}{lll} \mathbb{Z}_8 \oplus \mathbb{Z}_9, & \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \\ \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, & \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3, & \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3. \end{array}$$

7.7 Definition. For $\ell \in \mathbb{N}$, we say that $a_1, \dots a_\ell \in G$ *generate* an abelian group G, and call $a_1, \dots a_\ell$ *generators* of G, if $G = \langle a_1\rangle + \langle a_2\rangle + \cdots + \langle a_\ell\rangle$. Equivalently, letting $\mathcal{A} = (a_1, \dots a_\ell)$, the homomorphism $\phi_{\mathcal{A}} \colon \mathbb{Z}^\ell \to G; (m_1, \dots m_\ell) = m_1a_1 + \cdots + m_\ell a_\ell$ is surjective. We then say G is *finitely generated* with ℓ-*generator presentation* $\mathcal{A}$, calling any $R \in \ker \phi_{\mathcal{A}}$ a *relation* on $\mathcal{A}$.

7.8 Remarks. Note that a finite group $G = \{0, a_1, \dots a_N\}$ is generated by $\mathcal{A} = (a_1, \dots a_N)$, hence finitely generated! In general, G is generated by $\mathcal{A} = (a_1, \dots a_\ell)$ if and only if any $a \in G$ can be written $a = m_1a_1 + \cdots + m_\ell a_\ell$ for some $m_1, \dots m_\ell \in \mathbb{Z}$. This makes G look like a "vector space" over $\mathbb{Z}$ "spanned" by $a_1, \dots a_\ell$—except that $\mathbb{Z}$ is not a field!

Also $R = (m_1, \dots m_\ell) \in \ker \phi_{\mathcal{A}}$ if and only if $m_1a_1 + \cdots + m_\ell a_\ell = 0$, i.e., R defines a "linear dependence relation" on $a_1, \dots a_\ell$. However, for $m \in \mathbb{Z}$, $a \in G$, $ma = 0$ only implies that $o(a)$ divides m, so we replace "linear independence" by direct sum: the sum $G = \langle a_1\rangle + \langle a_2\rangle + \cdots + \langle a_\ell\rangle$ is direct if and only if $m_1a_1 + \cdots + m_\ell a_\ell = 0$ implies $m_ia_i = 0$ for all $i \in \{1, \dots \ell\}$.

7.9 Example. Suppose $G = \langle a_1\rangle + \langle a_2\rangle + \langle a_3\rangle + \langle a_4\rangle$,

$$\phi_{\mathcal{A}} \colon \mathbb{Z}^4 \to G; (m_1, m_2, m_3, m_4) \mapsto m_1a_1 + m_2a_2 + m_3a_3 + m_4a_4$$

and $\ker \phi_{\mathcal{A}} = \langle(4, 2, -4, 0)\rangle + \langle(1, 2, -1, 0)\rangle + \langle(2, 0, -1, 1)\rangle + \langle(2, -1, 0, -1)\rangle$. Thus the generators $a_1, a_2, a_3, a_4 \in G$ satisfy the relations

$$4a_1 + 2a_2 - 4a_3 = 0, \quad a_1 + 2a_2 - a_3 = 0, \quad 2a_1 - a_3 + a_4 = 0, \quad 2a_1 - a_2 - a_4 = 0,$$

and all other relations are consequences of these. By the 4th relation $a_4 = 2a_1 - a_2$, so $G = \langle a_1\rangle + \langle a_2\rangle + \langle a_3\rangle$, and substituting a_4 into the 3rd relation gives $4a_1 - a_2 - a_3 = 0$, so $a_3 = 4a_1 - a_2$ and $G = \langle a_1\rangle + \langle a_2\rangle$ with $-12a_1 + 6a_2 = 0$ and $-3a_1 + 3a_2 = 0$. We cannot divide by 3 here, but we can eliminate a_2 to get $6a_1 = 0$. If we set $\tilde{a}_2 = a_2 - a_1$, then $G = \langle a_1\rangle + \langle \tilde{a}_2\rangle$ with $6a_1 = 0$ and $3\tilde{a}_2 = 0$, i.e., $G \cong \mathbb{Z}_6 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

7.10 Lemma. Let G be an abelian group with an ℓ-generator presentation. Then G is a direct sum of a subgroup G' with an $(\ell - 1)$-generator presentation and a cyclic subgroup G''.

Proof. If G has an ℓ-generator presentation $\mathcal{A} = (a_1, \dots a_\ell)$ with $\ker \phi_{\mathcal{A}} = \{0\}$, then G is a direct sum of $G' = \langle a_1\rangle + \cdots + \langle a_{\ell-1}\rangle$ and $G'' = \langle a_\ell\rangle \cong \mathbb{Z}$.

Otherwise, define the *height* of an ℓ-generator presentation $\mathcal{A}$ of G to be the least norm $|m| \in \mathbb{Z}^+$ of any nonzero coefficient m that appears in some relation $R \in \ker \phi_{\mathcal{A}}$. Let $\mathcal{A} = (a_1, \dots a_\ell)$ be a presentation of least height $m \in \mathbb{Z}^+$, with the generators ordered so that $R := (m_1, \dots m_{\ell-1}, m) \in \ker \phi_{\mathcal{A}}$, i.e., $m_1a_1 + \cdots + m_{\ell-1}a_{\ell-1} + ma_\ell = 0$ in G.

For any other relation $R' \in \ker \phi_{\mathcal{A}}$, write the coefficient m' of a_ℓ as $m' = k'm + r$ with $0 \leqslant r < m$ and $k' \in \mathbb{Z}$. Then $R' - k'R \in \ker \phi_{\mathcal{A}}$ has coefficient $r < m$, so $r = 0$ by minimality of m.

For any other generator a_j, write the coefficient m_j of a_j in R as $m_j = k_jm + r$ with $0 \leqslant r < m$ and $k_j \in \mathbb{Z}$. Then $\mathcal{A}' = (a_1, a_2, \dots a_{\ell-1}, a_\ell + k_ja_j)$ has $(m_1, \dots m_{j-1}, r, m_{j+1}, \dots m_{\ell-1}, m) \in \ker \phi_{\mathcal{A}'}$, which has coefficient $r < m$, so $r = 0$ by minimality of m.

Thus $R = m(k_1, \dots k_{\ell-1}, 1)$ and all other relations have the form $R' = (m'_1, \dots m'_{\ell-1}, k'm)$, so we may remove a_ℓ from all other relations by subtracting a multiple of R. If we set $\tilde{a}_\ell := k_1a_1 + \cdots k_{\ell-1}a_{\ell-1} + a_\ell$, we thus obtain a presentation $\tilde{\mathcal{A}} = (a_1, \dots a_{\ell-1}, \tilde{a}_\ell)$ where $\ker \phi_{\tilde{\mathcal{A}}} = K' + \langle(0, \dots 0, m)\rangle$ and $K' \leqslant \mathbb{Z}^{\ell-1} \oplus \{0\}$. Thus $G = G' + \langle\tilde{a}_\ell\rangle = \phi_{\tilde{\mathcal{A}}}(\mathbb{Z}^{\ell-1} \oplus \{0\}) + \phi_{\tilde{\mathcal{A}}}(\{0\} \oplus \mathbb{Z})$ is a direct sum of $G' = \langle a_1\rangle + \cdots + \langle a_{\ell-1}\rangle$ and a cyclic subgroup $G'' = \langle\tilde{a}_\ell\rangle$ of order m. □

7.11 Proposition. Any finitely generated abelian group is a direct sum of cyclic groups with infinite and/or prime power orders.

Proof. We prove this for abelian groups G with an ℓ-generator presentation by induction on ℓ. Lemma 7.10 implies that G is the direct sum of subgroups G' and G'', where G' has an $(\ell-1)$-generator presentation and G'' is cyclic, hence a direct sum cyclic groups as stated. If $\ell = 1$, $G' = \{0\}$; otherwise we have by induction on ℓ that G' is a direct sum of cyclic groups as stated. Now a direct sum of direct sums is a direct sum: $a = a' + a'' = (a'_1 + \cdots + a'_m) + (a''_1 + \cdots a''_n) = a'_1 + \cdots + a'_m + a''_1 + \cdots a''_n$ and if $a'_1 + \cdots + a'_m + a''_1 + \cdots a''_n = 0$ then $a'_1 + \cdots + a'_m = 0$ and $a''_1 + \cdots a''_n = 0$, hence $a'_j = 0 = a''_k$ for all j, k. Thus G is a direct sum of cyclic groups as stated. □

7.12 Definition. Let G be any abelian group and let p be a prime. The subset

$$G_p = \{a \in G : o(a) \text{ is a power of } p\}$$

is called the *p-primary subgroup* of G.

7.13 Lemma. G_p is a subgroup of G.

Proof. As $o(0) = 1 = p^0$, $0 \in G_p$. Now let $a, b \in G_p$ with orders p^r, p^s. Then $p^{\max\{r,s\}}(a + b) = p^{\max\{r,s\}}a + p^{\max\{r,s\}}b = 0 + 0 = 0$, so $o(a + b)$ divides $p^{\max\{r,s\}}$ and is thus a power of p. Hence $a + b \in G_p$, and as $o(-a) = o(a) = p^r$ we have $-a \in G_p$. Hence $G_p \leqslant G$. □

7.14 Proposition. Let G be a finite abelian group where $|G| = p_1^{s_1} \cdots p_m^{s_m}$ for some positive integers $s_1, \dots s_m$. Then G is a direct sum of $G_{p_1}, G_{p_2}, \dots G_{p_m}$.

Proof. Suppose that $a_1 + \cdots + a_m = 0$ with $a_i \in G_{p_i}$ for $i \in \{1, \dots m\}$; then $o(a_i)$ is a power of p_i dividing $|G|$ by Lagrange's Theorem, so $p_i^{s_i}a_i = 0$. Hence if, for each $i \in \{1, \dots m\}$, we define $q_i = |G|/p_i^{s_i} = \prod_{j\neq i} p_j^{s_j}$ then $0 = q_i(a_1 + \cdots + a_m) = q_ia_i$, and hence $a_i = 0$, since q_i is coprime to $o(a_i)$.

Now $q_1, \dots q_m$ are also coprime, so there exist $k_1, \dots k_m \in \mathbb{Z}$ with $k_1q_1 + \cdots + k_mq_m = 1$. Thus for any $a \in G$,

$$a = (k_1q_1 + \cdots + k_mq_m)a = k_1q_1a + \cdots + k_mq_ma.$$

Since $p_i^{s_i}(k_iq_ia) = k_i|G|a = 0$, $k_iq_ia \in G_{p_i}$. Hence $G = G_{p_1} + \cdots + G_{p_m}$ and the sum is direct. □

Proof of Theorem 7.4. The existence part of Theorem 7.4 follows from Proposition 7.11. For the uniqueness, observe first that if $H \leqslant G$ has order p^r for a prime p, then $H \leqslant G_p$. Thus it suffices to show that if $G = G_p$ for some prime p, then for each $r \in \mathbb{Z}^+$, the number k_r of cyclic summands of order p^r in G is uniquely determined. We proceed by induction the highest power s with $k_s > 0$. If $s = 0$, $G = \{0\}$ and there is nothing to prove. Suppose now that $G = \langle a_1\rangle + \cdots + \langle a_k\rangle + G'$ is a direct sum where $o(a_i) = p^s$ and $o(a) \leqslant p^{s-1}$ for all $a \in G'$.

Let $\phi\colon G \to G; a \mapsto p^{s-1}a$; then $\ker\phi = \langle pa_1\rangle + \cdots + \langle pa_k\rangle + G'$, where the number k'_r of cyclic summands of order p^r is uniquely determined by induction, and $\operatorname{im}\phi = \langle p^{s-1}a_1\rangle + \cdots + \langle p^{s-1}a_k\rangle$, which is a sum of cyclic groups of order p and $k = |\operatorname{im}\phi|/p$ is uniquely determined by G. Then $k_s = k$, $k_{s-1} = k'_{s-1} - k$ and $k_r = k'_r$ for $r \leqslant s - 2$ and we are done. □

8 Composition series and solvable groups

8.1 Definitions (Subnormal series and solvable groups)**.** A *subnormal series* for a group G is a series

$$\{1\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_\ell = G$$

where $H_{i-1} \trianglelefteq H_i$, $i \in \{1, \dots \ell\}$, and the quotient groups H_i/H_{i-1} are called its *factors*. If the factors are simple, the series is called a *composition series* and the factors are called *composition factors*. We say that G is *solvable* if it has a subnormal series with abelian factors.

8.2 Examples (Subnormal series)**.** For any group G, $\{1\} \leqslant G$ is a subnormal series with factor $G/\{1\} \cong G$. Hence any abelian group G is solvable.

(i) Let $G = \langle a \rangle$ be cyclic of order 6. Then $\langle a^3 \rangle \leqslant G$ has order 2 and index 3 and

$$\{1\} \leqslant \langle a^3 \rangle \leqslant G$$

is a composition series with factors $\langle a^3 \rangle/\{1\} \cong \mathbb{Z}_2$ and $G/\langle a^3 \rangle \cong \mathbb{Z}_3$. Similarly

$$\{1\} \leqslant \langle a^2 \rangle \leqslant G$$

is a composition series with factors $\langle a^2 \rangle/\{1\} \cong \mathbb{Z}_3$ and $G/\langle a^2 \rangle \cong \mathbb{Z}_2$.

(ii) S_3 has a composition series $\{1\} < A_3 < S_3$ with factors $A_3/\{1\} \cong \mathbb{Z}_3$ and $S_3/A_3 \cong \mathbb{Z}_2$, so S_3 is solvable. Unlike the previous example, S_3 has no normal subgroup of order 2.

(iii) S_4 has subnormal series $1 < V_4 < A_4 < S_4$ with factors $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, $A_4/V_4 \cong \mathbb{Z}_3$ and $S_4/A_4 \cong \mathbb{Z}_2$. Notice that $A_4/V_4 \leqslant S_4/V_4$ is isomorphic to $A_3 \leqslant S_3$.

(iv) If $G = G_1 \times \cdots \times G_\ell$ is a direct product group then the map

$$\phi\colon G_1 \times \cdots \times G_\ell \to G_\ell; (a_1, \dots a_\ell) \mapsto a_\ell$$

is a surjective homomorphism with $\ker\phi = G_1 \times \cdots \times G_{\ell-1} \times \{1\} \cong G_1 \times \cdots \times G_{\ell-1}$ and $G/\ker\phi \cong G_\ell$ by the First Isomorphism Theorem 4.7. Iterating this process, we obtain a subnormal series of G with factors (isomorphic to) $G_1, \dots G_\ell$. In particular if $G_1, \dots G_\ell$ are simple groups, there is at least one group with these composition factors.

(v) Any finite p-group G (for a prime p) is solvable. Indeed this is immediate if $|G| = p$, while if $|G| = p^s$, we have seen in exercises that G has a normal subgroup N of order p^{s-1}, and G/N is cyclic, so the result follows by induction on s.

8.3 Definition. For $K \leqslant G$, $\mathcal{S}(G, K) := \{H : K \leqslant H \leqslant G\}$ and $\mathcal{S}(G) := \mathcal{S}(G, \{1\})$.

8.4 Subgroup Correspondence Theorem. Let $\phi\colon G \to H$ be a homomorphism. Then the map $\Psi\colon \mathcal{S}(\operatorname{im}\phi) \to \mathcal{S}(G, \ker\phi)$; $B \mapsto \phi^{-1}(B)$ is a well-defined bijection. Furthermore $N \trianglelefteq \operatorname{im}\phi$ if and only if $\Psi(N) \trianglelefteq G$.

Proof. If $B \leqslant H$ then $\ker\phi \leqslant \phi^{-1}(B) \leqslant G$ by Lemma 1.10, so Ψ is well-defined. Now for $B \leqslant \operatorname{im}\phi$, $\phi(\phi^{-1}(B)) = B$, while for any $A \leqslant G$, $\phi^{-1}(\phi(A)) = \{g \in G : \phi(g) \in \phi(A)\}$, but if $\phi(g) = \phi(a)$ for some $a \in A$, then $\phi(a^{-1}g) = 1$ so $a^{-1}g \in \ker\phi$. Hence if $\ker\phi \leqslant A$, $g \in A$ and $\phi^{-1}(\phi(A)) = A$. Thus Ψ is a bijection with inverse $A \mapsto \phi(A)$.

Finally for any $h = \phi(g) \in \operatorname{im}\phi$,

$$\phi(a) \in {}^hN = hNh^{-1} \quad \Leftrightarrow \quad \phi(g^{-1}ag) = \phi(g)^{-1}\phi(a)\phi(g) \in N \quad \Leftrightarrow \quad a \in {}^g\Psi(N)$$

so $N \trianglelefteq \operatorname{im}\phi$ iff $\Psi(N) \trianglelefteq G$. □

8.5 Third Isomorphism Theorem. Suppose that $N, K \trianglelefteq G$ and $N \leqslant K$. Then $K/N \trianglelefteq G/N$ and

$$(G/N)/(K/N) \cong G/K.$$

Proof. Since $aN = bN$ implies $a^{-1}b \in N \leqslant K$ and hence $aK = bK$, there is a well-defined map

$$\phi\colon G/N \to G/K;\ aN \mapsto aK.$$

Since

$$\phi(aN\, bN) = \phi(abN) = abK = aK\, bK = \phi(aN)\phi(bN),$$

ϕ is a homomorphism, and it is clearly surjective. The identity in G/K is the coset $1K = K$ and

$$\phi(aN) = K \quad \Leftrightarrow \quad aK = K \quad \Leftrightarrow \quad a \in K,$$

so $\ker\phi = \{aN : a \in K\} = K/N$. By the First Isomorphism Theorem 4.7, $K/N \trianglelefteq G/N$ and

$$(G/N)/(K/N) = (G/N)/\ker\phi \cong \operatorname{im}\phi = G/K. \qquad \square$$

8.6 Proposition. Any subnormal series $\{1\} = H_0 < H_1 < \cdots < H_\ell = G$ for a (nontrivial) finite group G can be refined to a composition series $\{1\} = K_0 < K_1 < \cdots < K_m = G$, i.e., for all $i \in \{0, \dots \ell\}$, there exists $j \in \{0, \dots m\}$ such that $H_i = K_j$.

Proof. We induct on $|G| - \ell > 0$. If $|G| - \ell = 1$, then for all $1 \leqslant j \leqslant \ell$ we have $|H_{j-1}| = j$, so ℓ divides $|G| = \ell + 1$ hence $\ell = 1$, G is cyclic of order 2 and $\{1\} = H_0 < H_1 = G$ is a composition series. In general, if $\{1\} = H_0 < H_1 < \cdots < H_\ell = G$ is a composition series we are done, otherwise some factor H_i/H_{i-1} is not simple. By the Subgroup Correspondence Theorem 8.4, H_i has a normal subgroup K with $H_{i-1} < K < H_i$, and since $H_{i-1} \trianglelefteq H_i$, $H_{i-1} \trianglelefteq K$. By induction on $|G| - \ell$, this longer series refines to a composition series, hence so does the original series. $\square$

8.7 Corollary. Any nontrivial finite group G has a composition series, and is solvable if and only if it has a composition series whose factors are cyclic of prime order.

Indeed any $G \neq \{1\}$ has a subnormal series (e.g. $\{1\} < G$) which can be refined to a composition series. If the subnormal series has abelian factors, so does the refinement: if H_j/H_{j-1} is abelian and $H_{j-1} \leqslant K \leqslant H_j$, then $K/H_{j-1} \leqslant H_j/H_{j-1}$ is abelian, and so is the quotient $(H_j/H_{j-1})/(K/H_{j-1})$, hence H_j/K is abelian by the third isomorphism theorem 8.5. The factors in the refinement are simple abelian, i.e., cyclic of prime order. The converse is immediate as cyclic groups are abelian.

The Jordan–Hölder Theorem (see handout) asserts that the composition factors of a finite group G are essentially uniquely determined.

9 Finite simple groups

9.1 Definition. An action of a group G on a set X is *primitive* if it is transitive and also for any $x \in X$, $\operatorname{Stab}_G(x) \leqslant H \leqslant G$ implies $H = \operatorname{Stab}_G(x)$ or $H = G$.

9.2 Lemma. If an action of G on X is transitive and 2-transitive, then it is primitive.

Proof. Suppose $\mathrm{Stab}_G(x) < H \leqslant G$ so $\exists\, y = h \cdot x \neq x$ in $\mathrm{orb}_H(x)$. We want to show any $g \in G$ is in fact in H. If $g \in \mathrm{Stab}_G(x)$, there is nothing to prove, so suppose not, i.e., $g \cdot x = z \neq x$. Then by 2-transitivity of G, $\exists\, a \in G$ with $a \cdot (x, y) = (x, z)$, i.e., $a \in \mathrm{Stab}_G(x)$ and $a \cdot y = z$. Thus $g \cdot x = z = a \cdot y = a \cdot (h \cdot x) = (ah) \cdot x$ and so $g \in (ah)\,\mathrm{Stab}_G(x) \subseteq (ah)H = H$. □

9.3 Regular Normal Subgroup Theorem. Let G act primitively on X, let $N \trianglelefteq G$ and $x \in X$ with $N \not\subseteq G_x := \mathrm{Stab}_G(x)$, and let G_x act on N by conjugation. Then $G = NG_x$ and $\Phi\colon N \to X; n \mapsto n \cdot x$ is a surjective G_x-set morphism, which is an isomorphism if $N \cap G_x = \{1\}$.

Proof. Since $G_x < NG_x \leqslant G$, primitivity implies $G = NG_x$, and if $g = na$ with $n \in N$ and $a \in G_x$ then $g \cdot x = na \cdot x = n \cdot x$, so $\mathrm{orb}_N(x) = \mathrm{orb}_G(x) = X$ and Φ is surjective. It is a G_x-set morphism, since for any $a \in G_x$, $\Phi(a \cdot n) = \Phi(ana^{-1}) = ana^{-1} \cdot x = a \cdot (n \cdot x) = a \cdot \Phi(n)$. Now if $\Phi(n_1) = \Phi(n_2)$, then $n_1^{-1}n_2 \in N \cap G_x$, so if $N \cap G_x = \{1\}$ then $n_1 = n_2$, i.e., Φ is injective, hence a G_x-set isomorphism. □

9.4 Lemma. Let X be a set with $|X| = n$. Then the action of $\mathrm{Alt}(X)$ on X is m-transitive for all $m \leqslant n - 2$.

Proof. The action of $\mathrm{Sym}(X)$ on X is m-transitive for all $m \leqslant n$. Hence if $m \leqslant n - 2$, for any $x = (x_1, \ldots x_m)$ and $y = (y_1, \ldots y_m)$ with $x_i \neq x_j$ and $y_i \neq y_j$ for $i \neq j$, there exists $\sigma \in \mathrm{Sym}(X)$ with $\sigma \cdot x = y$, and there are at least two distinct $z_1, z_2 \in X$ which are not equal to any y_j. If $\sigma \in \mathrm{Alt}(X)$, we are done, otherwise $\sigma' := (z_1\ z_2) \circ \sigma \in \mathrm{Alt}(X)$ with $\sigma' \cdot x = (z_1\ z_2) \cdot y = y$. □

9.5 Theorem (Simplicity of Alternating Groups)**.** The group $\mathrm{Alt}(X)$ is simple for $|X| \geqslant 5$.

Proof. The result is true for $|X| = 5$ by Example 3.21, so suppose $|X| = n \geqslant 6$ and that $\mathrm{Alt}(Y)$ is simple when $|Y| = n - 1$. Since $n \geqslant 6$, the action of $\mathrm{Alt}(X)$ on X is m-transitive for $m \leqslant 4$ by Lemma 9.4, hence primitive by Lemma 9.2, and for $x \in X$, the action of $G_x := \mathrm{Stab}_G(x) \cong \mathrm{Alt}(X \smallsetminus \{x\})$ on $X \smallsetminus \{x\}$ is 3-transitive.

Let N be a proper nontrivial normal subgroup of $G = \mathrm{Alt}(X)$. Since G_x is not normal in G, we cannot have $G_x \leqslant N$ by primitivity. Hence $N \cap G_x = \{\mathrm{id}\}$ since G_x is simple, and so the Regular Normal Subgroup Theorem 9.3 implies $X \smallsetminus \{x\}$ and $N^* = N \smallsetminus \{\mathrm{id}\}$ are isomorphic G_x-sets. However, if $a_1 \in N^*$, $a_2 \in N^* \smallsetminus \{a_1, a_1^{-1}\}$, and $a_3 \in N^* \smallsetminus \{a_1, a_2, a_1a_2\}$, then no automorphism of N can map (a_1, a_2, a_1a_2) to (a_1, a_2, a_3), so the G_x action on N^* cannot be 3-transitive, a contradiction. □

9.6 Theorem. The (only) normal subgroups of S_n are $\{\mathrm{id}\}$, A_n, S_n, and, for $n = 4$, V_4.

Proof. If $N \trianglelefteq S_n$, then $N \cap A_n \trianglelefteq A_n$, and so if $n \neq 4$, $A_n \cap N = A_n$ or $A_n \cap N = \{\mathrm{id}\}$ as A_n is simple by Theorem 9.5. In the former case $A_n \leqslant N \leqslant S_n$, so $N = S_n$ or $N = A_n$. In the latter case, the cosets σN with $\sigma \in A_n$ are distinct, so $|N| \leqslant 2$. However N is a union of conjugacy classes of S_n, so either $N = \{\mathrm{id}\}$ or $n = 2$ and $N = S_2$. The Class Equation of S_4 is $24 = 1 + 3 + 8 + 6 + 6$, so $N = V_4$ is the only other possibility in this case. □

9.7 Corollary. S_n is solvable if and only if $n \leqslant 4$.