# Group Theory

J. S. Milne

January 27, 2022

## Contents

# 1 Basic Definitions and Results

## 1.1 Definitions and examples

The **order** $|G|$ of a group is its cardinality. A finite group whose order is a power of a prime $p$ is called a $p$**-group**

$C_n$ denote any cyclic group of order $n$

**Example 1.1** (The quaternion group $Q$)**.** Let $a = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then

$$a^4 = e, \quad a^2 = b^2, \quad bab^{-1} = a^3$$

The subgroup of $\mathrm{GL}_2(\mathfrak{C})$ generated by $a$ and $b$ is

$$Q = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

The group $Q$ can also be described as the subset $\{\pm 1, \pm i, \pm j, \pm k\}$ of the quaternion algebra $\mathbb{H}$. Recall that

$$\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

with the multiplication determined by

$$i^2 = -1 = j^2, \quad ij = k = -ji$$

The map

**Example 1.2.** Let $V$ be a finite-dimensional vector space over a field $F$. A bilinear form on $V$ is a mapping $\phi : V \times V \to F$ that is linear in each variable. An **automorphism** of such a $\phi$ is an isomorphism $\alpha : V \to V$ s.t.

$$\phi(\alpha v, \alpha w) = \phi(v, w) \text{ for all } v, w \in V$$

The automorphism of $\phi$ form a group Aut($\phi$). Let $\{e_1, \dots, e_n\}$ be a basis for $V$, and let

$$P = (\phi(e_i, e_j))_{1 \le i,j \le n}$$

be the matrix of $\phi$. The choice of the basis identifies Aut($\phi$) with the group of invertible matrices $A$ s.t.

$$A^T \cdot P \cdot A = P$$

When $\phi$ is symmetric, i.e.,

$$\phi(v, w) = \phi(w, v) \text{ all } v, w \in V$$

and nondegenerate, Aut($\phi$) is called the **orthogonal group** of $\phi$

**Theorem 1.1** (Cayley)**.** *There is a canonical injective homomorhism*

$$\alpha : G \to \mathrm{Sym}(G)$$

**Corollary 1.2.** *A finite group of order $n$ can be realized as a subgroup of $S_n$*

**Proposition 1.3.** *Let $H$ be a subgroup of a group $G$*

1. *An element $a \in G$ lies in a left coset $C$ of $H$ iff $C = aH$*
2. *Two left cosets are either disjoint or equal*
3. *$aH = bH$ iff $a^{-1}b \in H$*
4. *Any two left cosets have the same number of elements*

The **index** $(G : H)$ of $H$ in $G$ is defined to be the number of left cosets of $H$ in $G$. For example, $(G : 1)$ is the order of $G$

**Theorem 1.4** (Lagrange)**.** *If G is finite, then*

$$(G : 1) = (G : H)(H : 1)$$

*Proof.* The left cosets of $H$ in $G$ form a partition of $G$, there are $(G : H)$ of them □

**Corollary 1.5.** *The order of each element of a finite group divides the order of the group*

*Proof.* Consider $H = \langle g \rangle$ □

**Proposition 1.6.** *For any subgroups $H \supset K$ of $G$*

$$(G : K) = (G : H)(H : K)$$

*Proof.* $G = \coprod_{i \in I} g_i H$, and $H = \coprod_{j \in J} h_j K$ □

## 1.2 Normal subgroups

A subgroup $N$ of $G$ is **normal**, denoted $N \lhd G$, if $gNg^{-1} = N$ for all $g \in G$ it suffices to check that $gNg^{-1} \subset N$

**Example 1.3.** Let $G = \mathrm{GL}_2(\mathbb{Q})$ and let $H = \{\left(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}\right) \mid n \in \mathbb{Z}\}$. Then $H$ is a subgroup of $G$; in fact $H \cong \mathbb{Z}$. Let $g = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then

$$g \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} g^{-1} = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 5^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5n \\ 0 & 1 \end{pmatrix}$$

Hence $gHg^{-1} \subsetneq H$ and $g^{-1}Hg \not\subset H$

**Proposition 1.7.** *subgroup $N$ of $G$ is normal iff every left coset of $N$ in $G$ is also a right coset*

**Example 1.4.** 1. Every subgroup of index two is normal. Indeed, let $g \in G \setminus H$, then $G = H \coprod gH = H \coprod Hg$

A group $G$ is **simple** if it has no normal subgroups other than $G$ and $\{e\}$.

**Proposition 1.8.** *If $H$ and $N$ are subgroups of $G$ and $N$ is normal, then $HN$ is a subgroup of $G$. If $H$ is also normal, then $HN$ is a normal subgroup of $G$*

Intersection of normal subgroups of a group is again a normal subgroup. Therefore we can define the **normal subgroup generated by a subset** $X$ of a group $G$ to be the intersection of the normal subgroups containing $X$. We say that a subset $X$ of a group $G$ is **normal** if $gXg^{-1} \subset X$ for all $g \in G$

**Lemma 1.9.** *If $X$ is normal, then the subgroup $\langle X \rangle$ generated by it is normal*

**Lemma 1.10.** *For any subset $X$ of $G$, the subset $\bigcup_{g \in G} gXg^{-1}$ is normal, and it is the smallest normal set containing $X$*

**Proposition 1.11.** *The normal subgroup generated by a subset $X$ of $G$ is $\langle \bigcup_{g \in G} gXg^{-1} \rangle$*

**Proposition 1.12.** *The map $a \mapsto aN : G \to G/N$ has the following universal property: for any homomorhism $\alpha : G \to G'$ of groups s.t. $\alpha(N) = \{e\}$, there exists a unique homomorhism $G/N \to G'$ making the diagram*

$$\begin{tikzcd} G \arrow[r, "a \mapsto aN"] \arrow[dr, "\alpha"'] & G/N \arrow[d, dashed] \\ & G' \end{tikzcd}$$

*commute*

*Proof.* Define $\bar{\alpha} : G/N \to G'$, $\bar{\alpha}(gN) = \alpha(g)$ □

## 1.3 Theorems concerning homomorhisms

The kernel of the homomorhism $\det : \mathrm{GL}_n(F) \to F^\times$ is the group of $n \times n$ with determinant 1 - this group $\mathrm{SL}_n(F)$ is called the **special linear group of degree** $n$

**Theorem 1.13** (HOMOMORPHISM THEOREM)**.** *For any homomorhism $\alpha : G \to G'$ of groups, $\ker \alpha \lhd G$, $\operatorname{im} \alpha \leq G'$, and $\alpha$ factors in a natural way into the composite of a surjection, an isomorphism, and an injection*

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, two heads, "g \mapsto gN"] & G' \\ G/N \arrow[r, "\sim", "gN \mapsto \alpha(g)"'] & I \arrow[u, hook] \end{tikzcd}$$

**Theorem 1.14** (ISOMORPHISM THEOREM)**.** *$H \leq G$, $N \lhd G$. Then $HN \leq G$, $H \cap N \lhd G$*

$$h(H \cap N) \mapsto hN : H/H \cap N \to HN/N$$

*is an isomorphism*

link
$\overline{G}$ is a quotient group of $G$

**Theorem 1.15** (CORRESPONDENCE THEOREM)**.** *Let $\alpha : G \twoheadrightarrow \overline{G}$ be a surjective homomorhism, and let $N = \ker \alpha$. Then there is a one-to-one correspondence*

$$\{\textit{subgroups of } G \textit{ containing } N\} \leftrightarrow \{\textit{subgroups of } \overline{G}\}$$

*under which a subgroup $H$ of $G$ containing $N$ corresponds to $\overline{H} = \alpha(H)$ and a subgroup $\overline{H}$ of $\overline{G}$ corresponds to $H = \alpha^{-1}(\overline{H})$. Moreover, if $H \leftrightarrow \overline{H}$ and $H' \leftrightarrow \overline{H}'$, then*

1. *$\overline{H} \subset \overline{H}' \Leftrightarrow H \subset H'$, in which case $(\overline{H}' : \overline{H}) = (H' : H)$*
2. *$\overline{H} \lhd \overline{G} \Leftrightarrow H \lhd G$ , in which case $\alpha$ induces an isomorphism*

$$G/H \xrightarrow{\simeq} \overline{G}/\overline{H}$$

**Corollary 1.16.** *$N \lhd G$; then there is a one-to-one correspondence between the set of subgroups of $G$ containing $N$ and the set of subgroups of $G/N$, $H \leftrightarrow H/N$. Moreover $H \lhd G \Leftrightarrow H/N \lhd G/N$, in which case the homomorhism $g \mapsto gN : G \to G/N$ induces an isomorphism*

$$G/H \cong (G/N)/(H/N)$$

## 1.4 Direct products

Let $G$ be a group, and let $H_1, \dots, H_k$ be subgroups of $G$. $G$ is a **direct product** of the subgroups $H_i$ if the map

$$(h_1, \dots, h_k) \mapsto h_1 \dots h_k : H_1 \times \dots \times H_k \to G$$

is an isomorphism of groups

note that if $g = h_1 \dots h_k$ and $g' = h'_1 \dots h'_k$, then

$$gg' = (h_1 h'_1) \dots (h_k h'_k)$$

**Proposition 1.17.** *A group $G$ is a direct product of subgroups $H_1, H_2$ iff*

1. $G = H_1 H_2$
2. $H_1 \cap H_2 = \{e\}$
3. *every element of $H_1$ commutes with every element of $H_2$*

*Proof.* 3 shows that $(h_1, h_2) \to h_1 h_2$ is a homomorhism, 2 injective, 1 surjective □

**Proposition 1.18.** *A group $G$ is a direct product of subgroups $H_1, H_2$ iff*

1. $G = H_1 H_2$
2. $H_1 \cap H_2 = \{e\}$
3. $H_1, H_2 \lhd G$

*Proof.* The elements $h_1, h_2$ of a group commute iff their commutator

$$[h_1, h_2] := (h_1 h_2)(h_2 h_1)^{-1}$$

is $e$. But

$$(h_1 h_2)(h_2 h_1)^{-1} = h_1 h_2 h_1^{-1} h_2^{-2} = \begin{cases} (h_1 h_2 h_1^{-1}) \cdot h_2^{-1} \\ h_1 \cdot (h_2 h_1^{-1} h_2^{-1}) \end{cases}$$

which is in $H_2$ because $H_2$ is normal, and is in $H_1$ because $H_1$ is normal □

**Proposition 1.19.** *A group $G$ is a direct product of subgroups $H_1, \dots, H_k$ iff*

1. $G = H_1 \dots H_k$
2. *for each $j$, $H_j \cap (H_1 \dots H_{j-1} H_{j+1} \dots H_k) = \{e\}$*
3. $H_1, \dots, H_k \lhd G$

## 1.5 Commutative groups

Let $M$ be a commute group. The subgroup $\langle x_1, \dots, x_k \rangle$ of $M$ generated by the elements $x_1, \dots, x_k$ consists of the sums $\sum m_1 x_i$, $m_i \in \mathbb{Z}$. A subset $\{x_1, \dots, x_k\}$ of $M$ is a **basis** of $M$ if it generates $M$ and

$$\sum m_i x_i = 0, m_i \in \mathbb{Z} \Longrightarrow m_i x_i = 0 \text{ for every } i$$

then

$$M = \langle x_1 \rangle \oplus \cdots \oplus \langle x_k \rangle$$

**Lemma 1.20.** *Let $x_1, \dots, x_k$ generate $M$. For any $c_1, \dots, c_k \in \mathbb{N}$ with $\gcd(c_1, \dots, c_k) = 1$, there exist generators $y_1, \dots, y_k$ for $M$ s.t. $y_1 = c_1 x_1 + \cdots + c_k x_k$*

*Proof.* We argue by induction on $s = c_1 + \cdots + c_k$. The lemma certainly holds if $s = 1$, and so we assume $s > 1$. Then, at least two $c_i$ are nonzero, say, $c_1 \geq c_2 > 0$. Now

- $\{x_1, x_2 + x_1, x_3, \dots, x_k\}$ generates $M$
- $\gcd(c_1 - c_2, c_2, c_3, \dots, c_k) = 1$
- $(c_1 - c_2) + c_2 + \cdots + c_k < s$

and so, by induction, there exist generators $y_1, \dots, y_k$ for $M$ s.t.

$$\begin{aligned} y_1 &= (c_1 - c_2)x_1 + c_2(x_1 + x_2) + c_3 x_3 + \cdots + c_k x_k \\ &= c_1 x_1 + \cdots + c_k x_k \end{aligned}$$

□

**Theorem 1.21.** *Every finitely generated commutative group $M$ has a basis; hence it is a finite direct sum of cyclic groups*

*Proof.* Induction on the generators of $M$.

Among the generating sets $\{x_1, \dots, x_k\}$ for $M$ with $k$ elements there is one for which the order of $x_1$ is the smallest possible. We shall show that $M$ is the direct sum of $\langle x_1 \rangle$ and $\langle x_2, \dots, x_k \rangle$

If $M$ is not the direct sum of $\langle x_1 \rangle$ and $\langle x_2, \dots, x_k \rangle$, then there exists a relation

$$m_1 x_1 + \cdots + m_k x_k = 0$$

with $m_1 x_1 \neq 0$. After possibly changing the sign of some of the $x_i$, we may suppose that $m_1, \dots, m_k \in \mathbb{N}$ and $m_1 < \text{order}(x_1)$. Let $d = \gcd(m_1, \dots, m_k) >$

0, and let $c_i = m_i/d$. According to the lemma, there exists a generating set $y_1, \dots, y_k$ s.t. $y_1 = c_1x_1 + \dots + c_kx_k$. But

$$dy_1 = m_1x_1 + \dots + m_kx_k = 0$$

and $d \le m_1 < \text{order}(x_1)$, and so this contradicts the choice of $\{x_1, \dots, x_k\}$ $\square$

**Corollary 1.22.** *A finite commutative group is cyclic if, for each $n > 0$, it contains at most $n$ elements of order dividing $n$*

*Proof.* After Theorem 1.21, we may assume that $G = C_{n_1} \times \dots \times C_{n_r}$ with $n_i \in \mathbb{N}$. If $n$ divides $n_i$ and $n_j$ with $i \neq j$, then $G$ has more than $n$ elements of order dividing $n$ First consider $n = p$, then in $C_p$ there are $p-1$ elements of order dividing $p$ by Lagrange theorem.

Now consider $n = p_1p_2$. If $(k, p_1p_2) = 1$, then order of $k$ is $p_1p_2$. Hence there are at least $p_1p_2 - p_1 - p_2 - 1$ elements. Check THIS! Therefore the hypothesis implies that the $n_i$ are relatively prime. Let $a_i$ generate the $i$th factor. Then $(a_1, \dots, a_r)$ has order $n_1 \dots n_r$, and so generates $G$ $\square$

**Example 1.5.** Let $F$ be a field. The elements of order dividing $n$ in $F^\times$ are the roots of the polynomial $X^n - 1$. Because unique factorization holds in $F[X]$, there are at most $n$ of these, and so corollary shows that every finite subgroup of $F^\times$ is cyclic

**Theorem 1.23.** *A nonzero finitely generated commutative group $M$ can be expressed*

$$M \approx C_{n_1} \times \dots \times C_{n_s} \times C_\infty^r$$

*for certain integers $n_1, \dots, n_s \ge 2$ and $r \ge 0$. Moreover*

1. *$r$ is uniquely determined by $M$*
2. *the $n_i$ can be chosen so that $n_1 \ge 2$ and $n_1 \mid n_2, \dots, n_{s-1} \mid n_s$, and then they are uniquely determined by $M$*
3. *the $n_i$ can be chosen to be powers of prime numbers, and then they are uniquely determined by $M$*

The number $r$ is called the **rank** of $M$. By $r$ being uniquely determined by $M$, we mean that two decompositions of $M$ of the form , the number of copies of $C_\infty$ will be the same. The integers in (2) are called the **invariant factors** of $M$. Statement (3) says that $M$ can be expressed

$$M \approx C_{p_1^{e_1}} \times \dots \times C_{p_t^{e_t}} \times C_\infty^r, \quad e_i \ge 1$$

for certain prime powers $p_i^{e_i}$, and that the integers $p_1^{e_1}, \ldots, p_t^{e_t}$ are uniquely determined by $M$; they are called the **elementary divisors** of $M$

*Proof.* The first assertion is a restatement of Theorem 1.21

1. For a prime $p$ not dividing any of the $n_i$

$$M/pM \approx (C_\infty/pC_\infty)^r \cong (\mathbb{Z}/p\mathbb{Z})^r$$

   and so $r$ is the dimension of $M/pM$ as an $\mathbb{F}_p$-vector space suppose $C_n = \langle a \rangle$ and $f : C_n \to pC_n : a \mapsto a^p$. Since $(p, n) = 1$, $|a^p| = n$. Thus this is an isomorphism

2. 3. If $\gcd(m, n) = 1$, then $C_m \times C_n$ contains an element of order $mn$, and so

$$C_m \times C_n \approx C_{mn}$$

   In this way we can decomposite $C_{n_i}$ into products of cyclic groups of prime power order. Then we can construct what we want

   To prove the uniqueness of (2) and (3), we can replace $M$ with its torsion subgroup (and so assume $r = 0$).

   uniqueness of elementary divisors is clear.

   $n_s$ is the smallest integer $> 0$ s.t. $n_s M = 0$; $n_{s-1}$ is the smallest integer $> 0$ s.t. $n_{s-1}M$ is cyclic; $n_{s-2}$ is the smallest integer s.t. $n_{s-2}M$ can be expressed as a product of two cyclic groups, and so on

   in the end, we will get a factoring like

$$\begin{matrix} C_{p_1^{r_1}} & C_{p_1^{r_2}} & C_{p_1^{r_3}} & C_{p_1^{r_4}} \\ C_{p_2^{s_1}} & C_{p_2^{s_2}} & & \\ C_{p_3^{t_1}} & C_{p_3^{t_2}} & C_{p_3^{t_3}} & \end{matrix}$$

   and get out invariant factors

□

## 1.6 The order of $ab$

**Theorem 1.24.** *For any integers $m, n, r > 1$, there exists a finite group $G$ with elements $a$ and $b$ s.t. $a$ has order $m$, $b$ has order $n$, and $ab$ has order $r$*

*Proof.* We shall show that, for a suitable prime power $q$, there exist elements $a$ and $b$ of $\mathrm{SL}_2(\mathbb{F}_q)$ s.t. $a, b$ and $ab$ have orders $2m, 2n$ and $2r$ respectively. As $-I$ is the unique element of order 2 in $\mathrm{SL}_2(\mathbb{F}_q)$, the image of $a, b, ab$ in $\mathrm{SL}_2(\mathbb{F}_q)/\{\pm I\}$ will then have orders $m, n$ and $r$ as required.

Let $p$ be the prime number not dividing $2mnr$. Then $p$ is a unit in the finite ring $\mathbb{Z}/2mnr\mathbb{Z}$, and so some power of it, $q$ say, is 1 in the ring. This means that $2mnr$ divides $q-1$. As the group $\mathbb{F}_q^\times$ has order $q-1$ and is cyclic (1.5), there exist element $u, v, w \in \mathbb{F}_q^\times$ having orders $2m, 2n$ and $2r$ respectively. Let

$$a = \begin{pmatrix} u & 1 \\ 0 & u^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q) \quad b = \begin{pmatrix} v & 0 \\ t & v^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_q)$$

where $t$ has been chosen so that

$$uv + t + u^{-1}v^{-1} = w + w^{-1}$$

The characteristic polynomial of $a$ is $(X-u)(X-u^{-1})$ □

## 1.7 Exercises

*Exercise* 1.7.1. Let $n = n_1 + \cdots + n_r$ be a partition of the positive integer $n$. Use Lagrange's theorem to show that $n!$ is divisible by $\prod_{i=1}^r n_i!$

*Proof.* $n_1, \ldots, n_r$ is a partition of $n$ elements, and $S_{n_i}$ is the permutation group of each part.

Apparently each $S_{n_i}$ is normal. Thus $S_{n_1} \ldots S_{n_r}$ is a subgroup of $S$. Also $S_{n_i} \cap S_{n_j} = \{\mathrm{id}\}$. Therefore $S_{n_1} \ldots S_{n_r} \cong S_{n_1} \times \cdots \times S_{n_r}$ □

*Exercise* 1.7.2. Let $N \lhd G$ of index $n$. Show that $g \in G \Rightarrow g^n \in N$

*Proof.* Because the group $G/N$ has order $n$, $(gN)^n = 1$ for every $g \in G$. □

*Exercise* 1.7.3. A group $G$ is said to have **finite exponent** if there exists an $m > 0$ s.t. $a^m = e$ for every $a \in G$; the smallest such $m$ is then called the **exponent** of $G$

1. Show that every group of exponent 2 is commutative

2. Show that, for an odd prime $p$, the group of matrices

$$\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\}$$

has exponent $p$, but is not commutative

*Proof.* 1. $ba = (abab)ba = ab$

□

*Exercise* 1.7.4. Two subgroups $H$ and $H'$ of a group $G$ is **commensurable** if $H \cap H'$ is of finite index in both $H$ and $H'$. Show that commensurability is an equivalence relation on the subgroups of $G$

# 2 Free Groups and Presentations; Coxeter Groups

## 2.1 Free monoids

Let $X = \{a, b, c, \dots\}$. A **word** is a finite sequence of symbols from $X$. Empty sequence is denoted by $1$. Write $SX$ for the set of words together with the binary concatenation. Then $SX$ is a monoid, called the **free monoid** on $X$

$X \to SX$ has the following universal property: for any map of sets $\alpha : X \to S$ from $X$ to a monoid $S$, there exists a unique homomorhism $SX \to S$ making the diagram

$$\begin{tikzcd} X \arrow[r, "a \mapsto a"] \arrow[dr, "\alpha"'] & SX \arrow[d, dashed] \\ & S \end{tikzcd}$$

commute

## 2.2 Free groups

We want to construct a group $FX$ contianing $X$ and having the same universal property. Define

$$X' = \{a, a^{-1}, b, b^{-1}, \dots\}$$

Let $W'$ be the set of words using symbols from $X'$. A word is **reduced** if it contains no pairs of the form $aa^{-1}$ or $a^{-1}a$. Starting with a word $w$, we can perform a finite sequence of cancellations to arrive at a reduced word, which will be called the **reduced form** $w_0$ of $w$.

**Proposition 2.1.** *There is only one reduced form of a word*

*Proof.* Induction on the length of the word $w$. If $w$ is reduced, there is nothing to prove. Otherwise a pair of the form $a_0 a_0^{-1}$ or $a_0^{-1} a_0$ occurs - assume the first

Observe that any two reduced forms of $w$ obtained by a sequence of cancellations in which $a_0 a_0^{-1}$ is cancelled first are equal, because the induction hypothesis can be applied to the shorter word.

Next observed that any reduced forms of $w$ obtained by a sequence of cancellations where $a_0 a_0^{-1}$ is cancelled at some point are equal, because the result of such a sequence of cancellations will not be affected if $a_0 a_0^{-1}$ is cancelled first

finally consider a reduced form $w_0$ obtained by a sequence where no cancellation cancels $a_0 a_0^{-1}$ directly. Since $a_0 a_0^{-1}$ doesn't remain in $w_0$, at least one of $a_0$ or $a_0^{-1}$ is cancelled. But the word obtained after this cancellation is the same as if our original pair were cancelled $\square$

$w, w'$ are **equivalent**, denoted $w \sim w'$, if they have the same reduced form

**Proposition 2.2.** *products of equivalent words are equivalent, i.e.,*

$$w \sim w', v \sim v' \Rightarrow wv \sim w'v'$$

Let $FX$ be the set of equivalence classes of words. Proposition 2.2 shows that the binary operation on $W'$ defines a binary operation on $FX$, which obviously makes it into a monoid. It also has inverses. Thus $FX$ is a group, called the **free group**

**Proposition 2.3.** *For any map of sets $\alpha : X \to G$ from $X$ to a group $G$, there exists a unique homomorhism $FX \to G$ making the following diagram commute*

$$\begin{tikzcd} X \arrow[r, "a \mapsto a"] \arrow[dr, "\alpha"'] & FX \arrow[d, dashed] \\ & G \end{tikzcd}$$

*Proof.* Consider a map $\alpha : X \to G$, and extend it to $X' \to G$ letting $\alpha(a^{-1}) = \alpha(a)^{-1}$. Because $G$ is a monoid, $\alpha$ extends to a homomorhism of monoids $SX' \to G$. This map will send equivalent words to the same element of $G$, and so will factor through $FX = SX'/\sim$. $\square$

**Corollary 2.4.** *Every group is a quotient of a free group*

*Proof.* Choose a set $X$ of generators for $G$ (e.g. $X = G$), and let $F$ be the free group generated by $X$. According to 2.3 the map $a \mapsto a : X \to G$ extends to a homomorhism $F \to G$, and the image, being a subgroup containing $X$, must equal $G$ □

**Theorem 2.5** (Nielsen-Schreier)**.** *Subgroups of free groups are free*

Two free groups $FX$ and $FY$ are isomorphic iff $|X| = |Y|$. Thus **rank** of a free group $G$ to be the cardinality of any free generating set (subset $X$ of $G$ for which the homomorhism $FX \to G$ given by 2.3 is an isomorphism)

## 2.3 Generators and relations

Consider a set $X$ and a set $R$ of words made up of symbols in $X'$. Each element of $R$ represents an element of the free group $FX$, and the quotient $G$ of $FX$ by the normal subgroup generated by these elements is said to have $X$ as **generators** and $R$ as **relations**. $(X, R)$ is a **presentation** for $G$, and denotes $G$ by $\langle X \mid R \rangle$

**Proposition 2.6.** $G = \langle X \mid R \rangle$*, for any group $H$ and map $\alpha : X \to H$ sending each element of $R$ to 1, there exists a unique homomorhism $G \to H$ making the diagram commute*

$$\begin{tikzcd} X \arrow[r, "a\mapsto a"] \arrow[dr, "\alpha"'] & G \arrow[d, dashed] \\ & H \end{tikzcd}$$

*Proof.*
$$\begin{tikzcd} X \arrow[r, "\iota"] \arrow[dr] & FX \arrow[r] \arrow[d, dashed] & FX/(\iota R) = G \arrow[dl, dashed] \\ & H & \end{tikzcd}$$

□

## 2.4 Finitely presented groups

A group is **finitely presented** if it admits a presentation $(X, R)$ with both $X$ and $R$ finite

**Example 2.1.** Consider a finite group $G$. Let $X = G$, and let $R$ be the set of words

$$\{abc^{-1} \mid ab = c\}$$

$(X, R)$ is a presentation of $G$, and so $G$ is finitely presented: let $G' = \langle X \mid R \rangle$. The extension of $a \mapsto a : X \to G$ to $FX$ sends each element of $R$ to 1, and therefore defines a homomorhism $G' \to G$, which is obviously surjective. But every element of $G'$ is represented by an element of $X$, and so $|G'| \le |G|$. Therefore the homomorhism is bijective

### 2.5 Coxeter groups

A **Coxeter system** is a pair $(G, S)$ consisting of a group $G$ and a set of generators $S$ for $G$ subject only to relations of the form $(st)^{m(s,t)} = 1$

$$\begin{cases} m(s,s) = 1 \text{ for all } s \\ m(s,t) \ge 2 \\ m(s,t) = m(t,s) \end{cases} \tag{1}$$

When no relation occurs between $s$ and $t$, we set $m(s,t) = \infty$. Thus a Coxeter system is defined by a set $S$ and a mapping

$$m : S \times S \to \mathbb{N} \cup \{\infty\}$$

satisfying (1), and the group $G = \langle S \mid R \rangle$ where

$$R = \{(st)^{m(s,t)} \mid m(s,t) \neq \infty\}$$

The **Coxeter groups** are those that arise as part of a Coxeter system. The cardinality of $S$ is called the **rank** of the Coxeter system

### 2.6 Exercises

*Exercise* 2.6.1. Let $D_n = \langle a, b \mid a^n, b^2, abab \rangle$ be the $n$th dihedral group. If $n$ is odd, prove that $D_{2n} \approx \langle a^n \rangle \times \langle a^2, b \rangle$, and hence that $D_{2n} \approx C_2 \times D_n$

*Proof.* first, $ab(b^{-1}a^{-1}) = ab(b^{-1}a^{-1})(abab) = abab = e$, hence $D_n$ is commutative for any $n$. Since $n$ is odd, $(n, 2) = 1$ and so $D_{2n} \approx C_2 \times C_n$ □

## 3 Automorphisms and Extensions

### 3.1 Automorphisms of groups

For $g \in G$, the map $i_g$ "conjugation by $g$"

$$x \mapsto gxg^{-1} : G \to G$$

is an automorphism of $G$, called an **inner automorphism** and others are called **outer**

As $i_{gh}(x) = (i_g \circ i_h)(x)$ and so the map $g \mapsto i_g : G \to \mathrm{Aut}(G)$ is a homomorhism, its image is denoted by $\mathrm{Inn}(G)$. It's kernel is the center of $G$

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

and so

$$G/Z(G) \cong \mathrm{Inn}(G)$$

$\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$: for $g \in G$ and $\alpha \in \mathrm{Aut}(G)$, we have

$$\alpha \circ i_g \circ \alpha^{-1} = i_{\alpha(g)}$$

**Example 3.1.**

1. $G = \mathbb{F}_p^n$. The automorphisms of $G$ as a commutative group are just the automorphisms of $G$ as a vector space over $\mathbb{F}_p$; thus $\mathrm{Aut}(G) = \mathrm{GL}_n(\mathbb{F}_p)$

2. As a particular case of (1), we see that

$$\mathrm{Aut}(C_2 \times C_2) = \mathrm{GL}_2(\mathbb{F}_2)$$

**Definition 3.1.** A group $G$ is **complete** if the map $g \mapsto i_g : G \to \mathrm{Aut}(G)$ is an isomorphism

$G$ is complete iff

1. $Z(G)$ is trivial

2. every automorphism of $G$ is inner

Let $G$ be a cyclic group of order $n$, say $G = \langle a \rangle$. Let $m$ be an integer $\geq 1$. The smallest multiple of $m$ divisible by $n$ is $m \cdot \frac{n}{\gcd(m,n)}$. Therefore $a^m$ has order $\frac{n}{\gcd(m,n)}$, and so the generators of $G$ are exactly the elements $a^m$ with $\gcd(m,n) = 1$. An automorphism $\alpha$ of $G$ must send $a$ to another generator of $G$, and so $\alpha(a) = a^m$ for some $m$ relatively prime to $n$. The map $\alpha \mapsto m$ defines an isomorphism

$$\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

where

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\text{units in } \mathbb{Z}/n\mathbb{Z}\} = \{m + n\mathbb{Z} \mid \gcd(m,n) = 1\}$$

If $n = p_1^{r_1} \dots p_s^{r_s}$ is the factorization of $n$ into a product of powers of distinct primes, then

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}, \quad m \mod n \leftrightarrow (m \mod p^{r_1}, \dots)$$

by the Chinese remainder theorem. This is an isomorphism of rings, and so

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})^\times$$

It remains to consider the case $n = p^r$, $p$ prime

Suppose first that $p$ is odd. Then $\{0, 1, \dots, p^r - 1\}$ is a complete set of representatives for $\mathbb{Z}/p^r\mathbb{Z}$, and one $p$th of its elements are divisible by $p$. Hence $(\mathbb{Z}/p^r\mathbb{Z})^\times$ has order $p^r - \frac{p^r}{p} = p^{r-1}(p-1)$. The homomorhism

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$$

is surjective with kernel of order $p^{r-1}$, and we know that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. Let $G = (\mathbb{Z}/p\mathbb{Z})^\times$ and suppose $G$ is not cyclic. Suppose each $i$ has order $m_i$. Let $d = [m_1, \dots, m_{p-1}]$. Then there is an element $c$ with order $d$ and $d < p-1$. Now if we consider $X^d - 1$, it has $p-1$ roots in $G$. A contradiction. link

Let $a \in (\mathbb{Z}/p^r\mathbb{Z})^\times$ map to a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $a^{p^r(p-1)} = 1$ and $a^{p^r}$ again maps to a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Therefore $(\mathbb{Z}/p^r\mathbb{Z})^\times$ contains an element $\xi := a^{p^r}$ of order $p-1$. Using the binomial theorem, one finds that $1+p$ has order $p^{r-1}$ in $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Therefore $(\mathbb{Z}/p^r\mathbb{Z})^\times$ is cyclic with generators $\xi \cdot (1+p)$ and every element can be written uniquely in the form

$$\xi^i \cdot (1+p)^j, \quad 0 \le i < p-1, \quad 0 \le j < p^{r-1}$$

On the other hand

$$(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} = \langle \bar{3}, \bar{5} \rangle \approx C_2 \times C_2$$

is not cyclic

reference

**Summary**

1. For a cyclic group of $G$ of order $n$, $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. The automorphism of $G$ corresponding to $[m] \in (\mathbb{Z}/n\mathbb{Z})^\times$ is $a \mapsto a^m$
2. If $n = p_1^{r_1} \dots p_s^{r_s}$ with the $p_i$ distinct primes, then
$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})^\times$$
3. For a prime $p$
$$(\mathbb{Z}/p^r\mathbb{Z})^\times \approx \begin{cases} C_{(p-1)p^{r-1}} & p \text{ odd} \\ C_2 & p^r = 2^2 \\ C_2 \times C_{2^{r-2}} & p = 2, r > 2 \end{cases}$$

## 3.2 Characteristic subgroups

**Definition 3.2.** A **characteristic subgroup** of a group $G$ is a subgroup $H$ s.t. $\alpha(H) = H$ for all automorphism $\alpha$ of $G$

*Remark.*
1. Consider a group $G$ and $N \lhd G$. An inner automorphism of $G$ restricts to an automorphism of $N$, which may be outer. Thus a normal subgroup of $N$ need not be a normal subgroup of $G$. However, a characteristic subgroup of $N$ will be a normal subgroup of $G$. Also a characteristic subgroup of a characteristic subgroup is a characteristic subgroup
2. The center $Z(G)$ of $G$ is a characteristic subgroup
3. If $H$ is the only subgroup of $G$ of order $m$, then it must be characteristic, because $\alpha(G)$ is again a subgroup of $G$ of order $m$
4. Every subgroup of a commutative group is normal but not necessarily characteristic. For example, every subspace of dimension 1 in $\mathbb{F}_p^2$ is a subgroup of $\mathbb{F}_p^2$, but it is not characteristic because it is not stable under $\mathrm{Aut}(\mathbb{F}_p^2) = \mathrm{GL}_2(\mathbb{F}_p)$

## 3.3 Semidirect products

$N \lhd G$. Each element $g \in G$ defines an automorphism of $N$, $n \mapsto gng^{-1}$, and this defines a homomorhism

$$\theta : G \to \mathrm{Aut}(N), \quad g \mapsto i_g \mid N$$

If there is a subgroup $Q$ of $G$ s.t. $G \to G/N$ maps $Q$ isomorphically onto $G/N$, then we can construct $G$ from $N, Q$ and the restriction of $\theta$ to $Q$. Indeed, an element $g$ of $G$ can be written uniquely in the form

$$g = nq, \quad n \in N, \quad q \in Q$$

Thus we have a one-to-one correspondence

$$G \leftrightarrow N \times Q$$

If $g = nq$ and $g' = n'q'$, then

$$gg' = (nq)(n'q') = n(qn'q^{-1})qq' = n\theta(q)(n')qq'$$

**Definition 3.3.** A group $G$ is a **semidirect product** of its subgroups $N$ and $Q$ if $N \lhd G$ and $G \to G/N$ induces an isomorphism $Q \to G/N$

Equivalently, $G$ is a semidirect product of subgroup $N$ and $Q$ if

$$N \lhd G; \quad NQ = G; \quad N \cap Q = \{1\}$$

written as $G = N \rtimes Q$ (or $N \rtimes_\theta Q$, where $\theta : Q \to \mathrm{Aut}(N)$ gives the action of $Q$ on $N$ by inner automorphism)

**Example 3.2.** 1. In $D_n$, $n \geq 2$, let $C_n = \langle r \rangle$ and $C_2 = \langle s \rangle$; then

$$D_n = \langle r \rangle \rtimes_\theta \langle s \rangle = C_n \rtimes_\theta C_2$$

where $\theta(s)(r^i) = r^{-i}$

From a semidirect product $G = N \rtimes Q$, we obtain a triple

$$(N, Q, \theta : Q \to \mathrm{Aut}(N))$$

and that the triple determines $G$. We now prove that every such triple arises from a semidirect product. As a set, let $G = N \times Q$, and define

$$(n, q)(n', q') = (n\theta(q)(n', qq'))$$

**Proposition 3.4.** *The composition law above makes $G$ into a group, in fact, the semidirect product of $N$ and $Q$*

**Example 3.3** (Groups of order 6)**.** Both $S_3$ and $C_6$ are semidirect products of $C_3$ by $C_2$.

Note that $\mathrm{Aut}(C_3) \cong (\mathbb{F}_3)^\times \cong C_2$ and there are two homomorhism of $C_2 \to C_2$, the identity function and the constant function. If $\theta$ is the constant function, then $C_6 \cong C_3 \rtimes_\theta C_2$. Otherwise, suppose $C_2 = \{1, b\}$ and $C_3 = \{1, a, a^2\}$, $\theta(b) = a \mapsto a^2$. Then $abab = a\theta(b)(a)bb = a^3b^2 = 1$. Hence $C_3 \rtimes_\theta C_2 = D_3 \cong S_3$.

**Example 3.4** (Groups of order $p^3$ (element of order $p^2$))**.** Let $N = \langle a \rangle$ be cyclic of order $p^2$ and let $Q = \langle b \rangle$ be cyclic of order $p$, where $p$ is an odd prime. Then $\mathrm{Aut}(N) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times \cong C_{(p-1)p} \cong C_p \times C_{p-1}$, and $C_p$ is generated by $\alpha : a \mapsto a^{1+p}$. Define $Q \to \mathrm{Aut}\, N$ by $b \mapsto \alpha$. The group $G := N \rtimes_\theta Q$ has generators $a, b$ and defining relations

$$a^{p^2} = 1, \quad b^p = 1, \quad bab^{-1} = a^{1+p}$$

It is a noncommutative group of order $p^3$, and possesses an element of order $p^2$

**Example 3.5** (Groups of order $p^3$ without element of order $p^2$)**.** Let $N = \langle a, b\rangle$ be the product of two cyclic groups $\langle a\rangle$ and $\langle b\rangle$ of order $p$, and let $Q = \langle c\rangle$ be a cyclic group of order $p$. Define $\theta : Q \to \mathrm{Aut}(N)$ to be the homomorhism s.t.

$$\theta(c^i)(a) = ab^i, \quad \theta(c^i)(b) = b$$

If we regard $N$ as the additive group $N = \mathbb{F}_p^2$ with $a$ and $b$ the standard basis elements, then $\theta(c^i)$ is the automorphism of $N$ defined by the matrix $\left(\begin{smallmatrix} 1 & 0 \\ i & 1 \end{smallmatrix}\right)$. The group $G := N \rtimes_\theta Q$ is a group of order $p^3$, with generators $a, b, c$ and defining relations

$$a^p = b^p = c^p = 1, \quad ab = cac^{-1}, \quad [b, a] = 1 = [b, c]$$

**Lemma 3.5.** *Given two triples $(N, Q, \theta)$ and $(N, Q, \theta')$, if there exists an $\alpha \in$ Aut$(N)$ s.t.*

$$\theta'(q) = \alpha \circ \theta(q) \circ \alpha^{-1}, \quad \text{all } q \in Q$$

*then the map*

$$(n, q) \mapsto (\alpha(n), q) : N \rtimes_\theta Q \to N \rtimes_{\theta'} Q$$

*is an isomorphism*

**Lemma 3.6.** *If $\theta = \theta' \circ \alpha$ with $\alpha \in$ Aut$(Q)$, then the map*

$$(n, q) \mapsto (n, \alpha(q)) : N \rtimes_\theta Q \approx N \rtimes_{\theta'} Q$$

*is an isomorphism*

**Lemma 3.7.** *If $Q$ is finite and cyclic and the subgroup $\theta(Q)$ of Aut$(N)$ is conjugate to $\theta'(Q)$, then*

$$N \rtimes_\theta Q \approx N \rtimes_{\theta'} Q$$

**Summary**. Let $G$ be a group with subgroups $H_1$ and $H_2$ s.t. $G = H_1H_2$ and $H_1 \cap H_2 = \{e\}$, so that each element $g$ of $G$ can be written uniquely as $g = h_1h_2$ with $h_1 \in H_1$ and $h_2 \in H_2$

1. If $H_1$ and $H_2$ are both normal, then $G$ is the direct product of $H_1$ and $H_2$, $G = H_1 \times H_2$ (1.18)
2. If $H_1 \lhd G$, then $G$ is the semidirect product of $H_1$ and $H_2$, $G = H_1 \rtimes H_2$
3. If neither $H_1$ nor $H_2$ is normal, then $G$ is the Zappa-Szép product of $H_1$ and $H_2$

### 3.4 Extensions of groups

$$1 \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} Q \longrightarrow 1$$

An exact sequence is called an **extension of** $Q$ **by** $N$. An extension is **central** if $\iota(N) \subset Z(G)$. For example, a semidirect product $N \rtimes_\theta Q$ give rise to an extension of $Q$ by $N$

$$1 \longrightarrow N \longrightarrow N \rtimes_\theta Q \longrightarrow Q \longrightarrow 1$$

which is central iff $\theta$ is the trivial homomorhism and $N$ is commutative

The extensions of $Q$ by $N$ are said to be **isomorphic** if there exists a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & Q & \longrightarrow & 1 \\ & & \| & & \downarrow{\approx} & & \| & & \\ 1 & \longrightarrow & N & \longrightarrow & G' & \longrightarrow & Q & \longrightarrow & 1 \end{array}$$

An extension of $Q$ by $N$ is **split** if it is isomorphic to the extension defined by a semidirect product. Equivalently

1. there is a subgroup $Q' \subset G$ s.t. $\pi$ induces an isomorphism $Q' \to Q$; or

2. there exists a homomorhism $s : Q \to G$ s.t. $\pi \circ s = \mathrm{id}$

**Theorem 3.8** (Schur-Zassenhaus)**.** *An extension of finite groups of relatively prime order is split*

### 3.5 The Hölder program

### 3.6 Exercises

*Exercise* 3.6.1. $\mathrm{GL}_2(\mathbb{F}_2) \approx S_3$

*Proof.* In $\mathbb{F}_2^2$, the vectors are $\{0, u, v, w\}$ and there are three bases $\{u, v\}, \{u, w\}, \{v, w\}$. An element $A \in \mathrm{GL}_2(\mathbb{F}_2)$ is an automorphism of $\mathbb{F}_2^2$ and also that two linear map are the same if they carry one basis to another. □

*Exercise* 3.6.2. Find the automorphism groups of $C_\infty$ and $S_3$

# 4 Groups Acting on Sets

## 4.1 Definition and examples

**Definition 4.1.** Let $X$ be a set and let $G$ be a group. A **left action** of $G$ on $X$ is a mapping $(g, x) \mapsto gx : G \times X \to X$ s.t.

1. $1x = x$, for all $x \in X$
2. $(g_1 g_2)x = g_1(g_2 x)$, all $g_1, g_2 \in X$, $x \in X$

A set together with a (left) action of $G$ is called a (left) $G$**-set**. An action is **trivial** if $gx = x$ for all $g \in G$

The condition imply that, for each $g \in G$, left translation by $g$,

$$g_L : X \to X, \quad x \mapsto gx$$

has $(g^{-1})_L$ as an inverse, and therefore $g_L$ is a bijection, i.e., $g_L \in Sym(X)$. Axiom (2) now says that

$$g \mapsto g_L : G \to \text{Sym}(X) \tag{2}$$

is a homomorhism. Conversely, every such homomorhism defines an action of $G$ on $X$. The action is **faithful** (or **effective**) if the homomorhism (2) is injective, i.e., if

$$gx = x \text{ for all } x \in X \Rightarrow g = 1$$

**Example 4.1.** 1. Every subgroup of the symmetric group $S_n$ acts faithfully on $\{1, 2, \ldots, n\}$

2. Every subgroup $H$ of a group $G$ acts faithfully on $G$ by left translation

$$H \times G \to G, \quad (h, x) \mapsto hx$$

3. Let $H$ be a subgroup of $G$. The group $G$ acts on the set of left cosets of $H$,

$$G \times G/H \to G/H, \quad (g, C) \mapsto gC$$

The action is faithful if, for example, $H \neq G$ and $G$ is simple

4. Every group $G$ acts on itself by conjugation. For any $N \lhd G$, $G$ acts on $N$ and $G/N$ by conjugation

A **right action** $X \times G \to X$ is defined similarly. To turn a right action into a left action, set $g{*}x = xg^{-1}$. For example, there is a natural right action of $G$ on the set of right cosets of a subgroup $H$ in $G$, namely $(C, g) \mapsto Cg$, which can be turned into a left action $(g, C) \mapsto Cg^{-1}$

A **map of $G$-sets** ($G$**-map**, $G$**-equivariant map**) is a map $\varphi : X \to Y$ s.t.

$$\varphi(gx) = g\varphi(x), \quad \text{all } g \in G, \quad x \in X$$

### 4.1.1 Orbits

Let $G$ act on $X$. A subset $S \subset X$ is **stable** under the action of $G$ if

$$g \in G, x \in S \Rightarrow gx \in S$$

The action of $G$ on $X$ then induces an action of $G$ on $S$

Write $x \sim_G y$ if $y = gx$ for some $g \in G$. This is an equivalence relation. The equivalence classes are called $G$**-orbits**. Thus the $G$-orbits partition $X$. Write $G\backslash X$ for the set of orbits

By definition, the $G$-orbit containing $x_0$ is

$$Gx_0 = \{gx_0 \mid g \in G\}$$

It is the smallest $G$-stable subset of $X$ containing $x_0$

**Example 4.2.**

1. Suppose $G$ acts on $X$, and let $\alpha \in G$ be an element of order $n$. Then the orbits of $\langle\alpha\rangle$ are the set of the form

$$\{x_0, \alpha x_0, \dots, \alpha^{n-1}x_0\}$$

2. The orbits for a subgroup $H$ of $G$ acting on $G$ by left multiplication are the right cosets of $H$ in $G$. We write $H\backslash G$ for the set of right cosets. Note that the group law on $G$ will **not** induce a group law on $G/H$ unless $H$ is normal

3. For a group $G$ acting on itself by conjugation, the orbits are called **conjugacy classes**: for $x \in G$, the conjugacy class of $x$ is the set

$$\{gxg^{-1} \mid g \in G\}$$

of conjugates of $x$.

A subset of $X$ is stable iff it is a union of orbits. For example, a subgroup $H$ of $G$ is normal iff it is a union of conjugacy classes

The action of $G$ on $X$ is said to be **transitive**, and $G$ is said to act **transitively** on $X$ if there is only one orbit. The set $X$ is called a **homogeneous** $G$-set. For example, $S_n$ acts transitively on $\{1, 2, \dots, n\}$. For any subgroup $H$ of a group $G$, $G$ acts transitively on $G/H$, but the action of $G$ on itself is never transitive if $G \neq 1$ because $\{1\}$ is always a conjugacy class

The action of $G$ on $X$ is **doubly transitive** if for any two pairs $(x_1, x_2)$, $(y_1, y_2)$ of elements of $X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$, there exists a (single) $g \in G$ s.t. $gx_1 = y_1$ and $gx_2 = y_2$. Define **$k$-fold transitivity** for $k \geq 3$ similarly

#### 4.1.2 Stabilizers

Let $G$ acts on $X$. The **stabilizer** (or **isotropy group**) of an element $x \in X$ is

$$\text{Stab}(x) = \{g \in G \mid gx = x\}$$

It is a subgroup, but it need not be a normal subgroup. The action is **free** if $\text{Stab}(x) = \{e\}$ for all $x$

**Lemma 4.2.** *For any $g \in G$ and $x \in X$*

$$\text{Stab}(gx) = g \cdot \text{Stab}(x) \cdot g^{-1}$$

$$\bigcap_{x \in X} \text{Stab}(x) = \ker(G \to \text{Sym}(X))$$

which is a normal subgroup of $G$. The action is faithful iff $\bigcap \text{Stab}(x) = \{1\}$

**Example 4.3.**

1. Let $G$ act on itself by conjugation. Then

   $$\text{Stab}(x) = \{g \in G \mid gx = xg\}$$

   This group is called the **centralizer** $C_G(x)$ of $x$ in $G$. It consists of all elements of $G$ that commute with, i.e., centralize, $x$. The intersection

   $$\bigcap_{x \in G} C_G(x) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

   is the centre of $G$

2. Let $G$ act on $G/H$ by left multiplication. Then $\text{Stab}(H) = H$,and the stabilizer of $gH$ is $gHg^{-1}$

For $S \subseteq X$, we define the **stabilizer** of $S$ to be

$$\text{Stab}(S) = \{g \in G \mid gS = S\}$$

Then $\text{Stab}(S)$ is a subgroup of $G$, and the same argument as in the proof of 4.2 shows that

$$\text{Stab}(gS) = g \cdot \text{Stab}(S) \cdot g^{-1}$$

**Example 4.4.** Let $G$ act on $G$ by conjugation, and let $H$ be a subgroup of $G$. The stablizer of $H$ is called the **normalizer** $N_G(H)$ of $H$ in $G$

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

Clearly $N_G(H)$ is the largest subgroup of $G$ containing $H$ as a normal subgroup

It is possible for $gS \subset S$ but $g \notin \text{Stab}(S)$ 1.3

### 4.1.3 Transitive actions

**Proposition 4.3.** *If G acts transitively on $X$, then for any $x_0 \in X$, the map*

$$g\,\text{Stab}(x_0) \mapsto gx_0 : G/\,\text{Stab}(x_0) \to X$$

*is an isomorphism of G-sets*

*Proof.* $G$-equivariant □

Thus every homogeneous $G$-set $X$ is isomorphic to $G/H$ for some subgroup $H$ of $G$, but such a realization of $X$ is *not canonical*: it depends on the choice of $x_0 \in X$. The $G$-set $G/H$ has a preferred point, namely, the coset $H$; to give a homogeneous $G$-set $X$ together with a preferred point is essentially the same as to give a subgroup of $G$

**Corollary 4.4.** *Let G act on $X$, and let $O = Gx_0$ be the orbit containing $x_0$. Then the cardinality of O is*

$$|O| = (G : \text{Stab}(x_0))$$

For example, the number of conjugates $gHg^{-1}$ of a subgroup $H$ of $G$ is $(G : N_G(H))$

*Proof.* The action of $G$ on $O$ is transitive □

**Proposition 4.5.** *Let $x_0 \in X$. If $G$ acts transitively on $X$, then*

$$\ker(G \to \mathrm{Sym}(X))$$

*is the largest normal subgroup contained in* $\mathrm{Stab}(x_0)$

*Proof.*

$$\ker(G \to \mathrm{Sym}(X)) = \bigcap_{x \in X} \mathrm{Stab}(x) = \bigcap_{g \in G} \mathrm{Stab}(gx_0) = \bigcap g \cdot \mathrm{Stab}(x_0) \cdot g^{-1}$$

Hence the proposition is a consequence of the following lemma □

**Lemma 4.6.** *For any subgroup $H$ of a group $G$, $\bigcap_{g \in G} gHg^{-1}$ is the largest normal subgroup contained in $H$*

*Proof.* $N_0 := \bigcap_{g \in G} gHg^{-1}$ is still a subgroup. It is normal since

$$g_1 N_0 g_1^{-1} = \bigcap_{g \in G} (g_1 g) H (g_1 g)^{-1} = N_0$$

If $N$ is a second such group, then

$$N = gNg^{-1} \subset gHg^{-1}$$

for all $g \in G$, and so $N \subset N_0$ □

#### 4.1.4 The class equation

When $X$ is finite, it is a disjoint union of a finite number of orbits:

$$X = \bigcup_{i=1}^{m} O_i$$

hence

**Proposition 4.7.**

$$|X| = \sum_{i=1}^{m} |O_i| = \sum_{i=1}^{m} (G : \mathrm{Stab}(x_i)), \quad x_i \in O_i$$

When $G$ acts on itself by conjugation, this formula becomes

**Proposition 4.8** (Class equation)**.**

$$|G| = \sum (G : C_G(x))$$

*(*$x$ *runs over a set of representatives for the conjugacy classes), or*

$$|G| = |Z(G)| + \sum (G : C_G(y))$$

*(*$y$ *runs over set of representatives for the conjugacy classes containing more than one element)*

**Theorem 4.9** (Cauchy)**.** *If the prime* $p$ *divides* $|G|$*, then* $G$ *contains an element of order* $p$

*Proof.* Induction on $|G|$. If for some $y$ not in the center of $G$, $p$ doesn't divide $(G : C_G(y))$, then $p$ divides the order of $C_G(y)$ and we can apply induction to find an element of order $p$ in $C_G(y)$. Thus we may suppose that $p$ divides all of the terms $(G : C_G(y))$ in the class equation (second form), and so also divides $Z(G)$. But $Z(G)$ is commutative and it follows from the structure theorem[1] of such groups that $Z(G)$ will contain an element of order $p$ □

**Corollary 4.10.** *A finite group* $G$ *is a* $p$*-group iff every element has order a order a power of* $p$

*Proof.* If $|G|$ is a power of $p$, then Lagrange's theorem shows that the order of every element is a power of $p$. The converse follows from Cauchy's theorem □

**Corollary 4.11.** *Every group of order* $2p$*,* $p$ *an odd prime, is cyclic or dihedral*

*Proof.* From Cauchy's theorem, we know that such a $G$ contains elements $s$ and $r$ of orders 2 and $p$ respectively. Let $H = \langle r \rangle$. Then $H$ is of index 2, and so is normal. Obviously $s \notin H$, and so $G = H \cup Hs$:

$$G = \{1, r, \ldots, r^{p-1}, s, rs, \ldots, r^{p-1}s\}$$

As $H$ is normal, $srs^{-1} = r^i$, some $i$. Because $s^2 = 1$, $r = s^2rs^{-2} = s(srs^{-1})s^{-1} = r^{i^2}$ and so $i^2 \equiv 1 \mod p$. Because $\mathbb{Z}/p\mathbb{Z}$ is a field, its only elements with square 1 are $\pm 1$, and so $i \equiv 1$ or $-1 \mod p$. In the first case, the group is commutative; in the second case $srs^{-1} = r^{-1}$ and we have the dihedral group □

[1] Here is a direct proof that the theorem holds for an abelian group $Z$ . We use inducftion on the order of $Z$. It suffices to show that $Z$ contains an element whose order is divisible by $p$. Let $g \neq 1$ be an element of $Z$. If $p$ doesn't divide the order of $g$, then it divides the order of $Z/\langle g \rangle$, in which case there exists an element of $G$ whose order in $Z/\langle g \rangle$ is divisible by $p$. But the order of such an element must itself be divisible by $p$

### 4.1.5 $p$-groups

**Theorem 4.12.** *Every nontrivial finite $p$-group has nontrivial center*

*Proof.* By assumption, $(G : 1)$ is a power of $p$, and so $(G : C_G(y))$ is a power of $p$ for all $y$ not in the center of $G$. Thus $p \mid |Z(G)|$ $\square$

**Corollary 4.13.** *A group of order $p^n$ has normal subgroups of order $p^m$ for all $m \leq n$*

*Proof.* Induction on $n$. The center of $G$ contains an element of order $p$, and so $N = \langle g \rangle$ is a normal subgroup of $G$ of order $p$. Now the induction hypothesis allows us to assume the result for $G/N$, and the correspondence theorem 1.15 then gives it to use for $G$ $\square$

**Proposition 4.14.** *Every group of order $p^2$ is commutative, and hence is isomorphic to $C_p \times C_p$ or $C_{p^2}$*

*Proof.* We know that the center $Z$ is nontrivial, and that $G/Z$ is therefore has order 1 or $p$. In either case it is cyclic, and the next result implies that $G$ is commutative $\square$

**Lemma 4.15.** *Suppose $G$ contains a subgroup $H$ in its center* (*hence $H$ is normal*) *s.t. $G/H$ is cyclic. Then $G$ is commutative*

*Proof.* Let $a$ be an element of $G$ whose image in $G/H$ generates it. Then every element of $G$ can be written $g = a^i h$ with $h \in H$, $i \in \mathbb{Z}$. Now

$$a^i h \cdot a^{i'} h' = a^i a^{i'} h h' = a^{i'} h' \cdot a^i h$$

$\square$

The above proof shows that if $H \subset Z(G)$ and $G$ contains a set of representatives for $G/H$ whose elements commute, then $G$ is commutative

For $p$ odd, it is now not difficult to show that any noncommutative group of order $p^3$ is isomorphic to exactly one of the groups constructed in 3.4 3.5

*Proof.* Suppose $|G| = p^3$. Then $|Z(G)|$ is either $p$ or $p^2$. If $|Z(G)| = p$. Then $G/Z(G)$ is commutative. $Z(G)$ is also cyclic

If $|Z(G)| = p^2$, then $\square$

**Example 4.5.** Let $G$ be a noncommutative group of order 8. Then $G$ must contain an element $a$ of order 4 (1.7.3). If $G$ contains an element $b$ of order 2 not in $\langle a \rangle$, then $G \simeq \langle a \rangle \rtimes_\theta \langle b \rangle$ where $\theta$ is the unique isomorphism $\mathbb{Z}/2\mathbb{Z} \to (\mathbb{Z}/4\mathbb{Z})^\times$, and so $G \approx D_4$. If not, any element $b$ of $G$ not in $\langle a \rangle$ must have order 4, and $a^2 = b^2$. Now $bab^{-1}$ is an element of order 4 in $\langle a \rangle$. It can't equal $a$, because otherwise $G$ would be commutative, and so $bab^{-1} = a^3$. Therefore $G$ is the quaternion group

### 4.1.6 Action on the left cosets

Let $X = G/H$. Recall that

$$\text{Stab}(gH) = g\,\text{Stab}(1 \cdot H)g^{-1} = gHg^{-1}$$

and the kernel of

$$G \to \text{Sym}(X)$$

is the largest normal subgroup $\bigcap_{g \in G} gHg^{-1}$ of $G$ contained in $H$

*Remark.*

1. Let $H$ be a subgroup of $G$ not containing a normal subgroup of $G$ other than 1. Then $G \to \text{Sym}(G/H)$ is injective, and we have realized $G$ as a subgroup of a symmetric group of order much smaller than $(G : 1)!$.

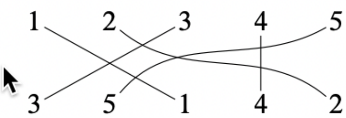
### 4.1.7 Permutation groups

Consider a permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

The ordered pairs $(i, j)$ with $i < j$ and $\sigma(i) > \sigma(j)$ are called the **inversions** of $\sigma$, and $\sigma$ is said to be **even** or **odd** according as the number of inversions is even or odd. The **signature**, $\text{sgn}(\sigma)$ of $\sigma$ is 1 or $-1$ according as $\sigma$ is even or odd.

*Remark.* To compute the signature of $\sigma$, connect each element $i$ in the top row to the element $i$ in the bottom row, and count the number of times that the lines cross. For example, is even




For a permutation $\sigma$, consider the products

$$\begin{aligned} V = \prod_{1 \le i < j \le n} (j - i) = (2-1)(3-1) \dots (n-1) \\ (3-2) \dots (n-2) \\ \dots \\ (n-(n-1)) \end{aligned}$$

$$\begin{aligned} \sigma V = \prod_{1 \le i < j \le n} (\sigma(j) - \sigma(i)) = (\sigma(2)-\sigma(1))(\sigma(3)-\sigma(1)) \dots (\sigma(n)-\sigma(1)) \\ (\sigma(3)-\sigma(2)) \dots (\sigma(n)-\sigma(2)) \\ \dots \\ (\sigma(n)-\sigma(n-1)) \end{aligned}$$

Both products run over the 2-element subsets $\{i, j\}$ of $\{1, 2, \dots, n\}$ and the terms corresponding to a subset are the same except that each inversion introduces a negative sign. Therefore

$$\sigma V = \mathrm{sgn}(\sigma) V$$

Now let $P$ be the additive group of maps $\mathbb{Z}^n \to \mathbb{Z}$. For $f \in P$ and $\sigma \in S_n$, let $\sigma f$ denote the element of $P$ defined by

$$(\sigma f)(z_1, \dots, z_n) = f(z_{\sigma(1)}, \dots, z_{\sigma(n)})$$

For $z \in \mathbb{Z}^n$ and $\sigma \in S_n$, let $z^\sigma$ denote the element of $\mathbb{Z}^n$ s.t. $(z^\sigma)_i = z_{\sigma(i)}$. Then $(z^\sigma)^\tau = z^{\sigma\tau}$. By definition, $(\sigma f)(z) = f(z^\sigma)$, and so $((\sigma\tau)f)(z) = f(z^{\sigma\tau}) = f((z^\sigma)^\tau) = (\tau f)(z^\sigma) = (\sigma(\tau f))(z)$, i.e.

$$\sigma(\tau f) = (\sigma\tau) f$$

Let $p \in P$ defined by

$$p(z_1, \dots, z_n) = \prod_{1 \le i < j \le n} (z_j - z_i)$$

The same argument as above shows that

$$\sigma p = \mathrm{sgn}(\sigma) p$$

On putting $f = p$, we finds that

$$\mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau) = \mathrm{sgn}(\sigma\tau)$$

Therefore "sign" is a homomorhism $S_n \to \{\pm 1\}$. When $n \geq 2$, it is surjective, and so its kernel is a normal subgroup of $S_n$ of order $\frac{n!}{2}$, called the **alternating group** $A_n$

*Remark.* We show shown that there exists a homomorhism sgn : $S_n \to \{\pm 1\}$ s.t. $\mathrm{sgn}(\sigma) = -1$ for every transposition. The transposition generate $S_n$, and so sign is uniquely determined by this property. Now let $G = \mathrm{Sym}(X)$, where $X$ is a set with $n$ elements. The choice of an ordering of $X$ determines an isomorphism of $G$ with $S_n$ sending transpositions to transpositions. Therefore $G$ also admits a unique isomorphism $\epsilon : G \to \{\pm 1\}$ s.t. $\epsilon(\sigma) = -1$ for every transposition $\sigma$. Once we have chosen an ordering of $X$, we can speak of the inversions of an element $\sigma$ of $G$, and define a sign homomorhism $G \to \{\pm 1\}$ as before. This must agree with $\epsilon$, and so $\epsilon(\sigma)$ equals 1 or $-1$ according as $\sigma$ has an even or an odd number of inversions.

A **cycle** is a permutation of the following form

$$i_1 \mapsto i_2 \mapsto i_3 \mapsto \cdots \mapsto i_r \mapsto i_1$$

The $i_j$ are required to be distinct. We denote this cycle by $(i_1 i_2 \ldots i_r)$ and call $r$ its **length**. The **support of the cycle** $(i_1 \ldots i_r)$ is the set $\{i_1, \ldots, i_r\}$ and cycles are **disjoint** if their supports are disjoint. Disjoint cycles commute

**Proposition 4.16.** *Every permutation can be written as a product of disjoint cycles*

*Proof.* $\sigma \in S_n$, and let $O \subset \{1, \ldots, n\}$ be an orbit for $\langle\sigma\rangle$. If $|O| = r$, then for any $i \in O$,

$$O = \{i, \sigma(i), \ldots, \sigma^{r-1}(i)\}$$

Therefore $\sigma$ and the cycle $(i \ \ \sigma(i) \ldots \sigma^{r-1}(i))$ have the same action on any element of $O$. Let

$$\{1, 2, \ldots, n\} = \bigcup_{j=1}^{m} O_j$$

be the decomposition of $\{1, \ldots, n\}$ into a disjoint union of orbits for $\langle\sigma\rangle$, and let $\gamma_j$ be the cycle associated with $O_j$. Then

$$\sigma = \gamma_1 \ldots \gamma_m$$

is a decomposition of $\sigma$ into a product of disjoint cycles. $\square$

**Corollary 4.17.** *Each permutation $\sigma$ can be written as a product of transpositions; the number of transpositions in such a product is even or odd according as $\sigma$ is even or odd*

*Proof.*

$$(i_1 i_2 \dots i_r) = (i_1 i_2) \dots (i_{r-2} i_{r-1})(i_{r-1} i_r)$$

Because sign is a homomorhism, and the signature of a transposition is -1, $\mathrm{sgn}(\sigma) = -1^{\#\text{transpositions}}$ $\square$

# 5 TODO skip and problems

$$1.6 \quad 2.5 \quad 4.1.6$$