# Topics in Algebra

## Lecture notes, Autumn 2021

Mikko Korhonen

# Contents

# 1 Introduction

These lecture notes will cover some of the fundamentals of group theory, with a particular focus on finite groups and their structure.

There are no formal prerequisites, but some previous exposure to basic algebra and group theory is expected. However, we will develop the theory from the beginning, starting with the basic definitions and examples.

**Definition 1.1.** A *group* is a pair $(G, *)$, where $G$ is a set and $* : G \times G \to G$ is a binary operation $(a, b) \mapsto a * b$ satisfying the following properties:

(i) Associativity: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$

(ii) There exists an *identity element* $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.

(iii) For all $a \in G$, there exists an *inverse* $b \in G$ such that $a * b = b * a = e$.

The cardinality $|G|$ of the set $G$ is called the *order* of the group $(G, *)$.

**Remark 1.2.** (a) Usually we will denote a group $(G, *)$ just by $G$.

(b) An identity element $e \in G$ is unique. For if $e'$ is another identity element, then $e' = e * e' = e$.

(c) Inverse elements are also unique. For if $b$ and $b'$ are inverses of $a$, then $b = e * b = (b' * a) * b = b' * (a * b) = b' * e = b'$.

(d) In general we use *multiplicative notation*. That is, the multiplication $a * b$ of two elements $a, b \in G$ is usually denoted by $ab$, and the identity element is usually denoted by 1 or $1_G$. The inverse of $a \in G$ is denoted by $a^{-1}$.

(e) For all $a, b \in G$ we have $(ab)^{-1} = b^{-1}a^{-1}$.

(f) Every group $G$ satisfies the following *cancellation laws*:

- If $ab = ac$, then $b = c$.
- If $ac = bc$, then $a = b$.

**Definition 1.3.** Let $G$ be a group. Two elements $a, b \in G$ are said to *commute* if $ab = ba$. A group $(G, *)$ is called *abelian* if all pairs of elements commute, i.e., if $ab = ba$ for all $a, b \in G$.

If $(G, *)$ is an abelian group, we will sometimes use *additive* notation: that is, we write $a * b$ as $a + b$ for $a, b \in G$, the inverse of $a \in G$ is denoted by $-a$ and the identity element is denoted by 0.

**Example 1.4.** Examples of abelian groups:

(i) $(\mathbb{R}, +)$: identity element is $0 \in \mathbb{R}$, the inverse of $x \in \mathbb{R}$ is $-x \in \mathbb{R}$. Similarly e.g. $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$.

(ii) $(\mathbb{R} \setminus \{0\}, \cdot)$: identity element is $1 \in \mathbb{R}$, inverse of $x \in \mathbb{R} \setminus \{0\}$ is $1/x$. Similarly e.g. $(\mathbb{C} \setminus \{0\}, \cdot)$ and $(\mathbb{R}_{>0}, \cdot)$.

**Example 1.5** (Integers modulo $n$)**.** Let $n > 0$ be an integer. For an integer $a \in \mathbb{Z}$, we denote by $\overline{a}$ the set of all integers $b \in \mathbb{Z}$ such that $b \equiv a \mod n$. In other words,

$$\overline{a} = a + n\mathbb{Z}.$$

Note that $\overline{a} = \overline{b}$ if and only if $a \equiv b \mod n$. We define the *integers modulo* $n$ as

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a} : a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

We define addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ by

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b} && \text{for all } a, b \in \mathbb{Z} \\ \overline{a} \cdot \overline{b} &= \overline{ab} && \text{for all } a, b \in \mathbb{Z} \end{aligned}$$

(These operations are well-defined: if $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$, then $\overline{a+b} = \overline{a'+b'}$ and $\overline{ab} = \overline{a'b'}$.) Then $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group of order $n$, called the *additive group of integers modulo* $n$.

Multiplication in $\mathbb{Z}/n\mathbb{Z}$ is associative and has multiplicative identity $\overline{1}$. But $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is not a group, since not every $\overline{a}$ has an inverse (for example $a = 0$). In general, for $\overline{a}$ there exists $\overline{b}$ such that $\overline{a} \cdot \overline{b} = \overline{1}$ if and only if $\gcd(a, n) = 1$. The set of invertible elements

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} : \gcd(a, n) = 1\}$$

forms a group $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$, which we call the *multiplicative group of integers modulo* $n$.

The order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is given by the number of integers $1 \leq a \leq n$ such that $\gcd(a, n) = 1$. In other words $|(\mathbb{Z}/n\mathbb{Z})^\times| = \phi(n)$, where $\phi$ is the Euler totient function.

**Remark 1.6.** Recall that for $p$ any prime number, we have $\phi(p) = p - 1$, and $\phi(p^k) = p^{k-1}(p-1)$ for all $k > 1$. More generally, for $n > 0$ with prime factorization $n = p_1^{k_1} \cdots p_t^{k_t}$, we have

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_t}\right).$$

As a consequence of this formula, for $n, m > 0$ with $\gcd(m, n) = 1$, we have $\phi(nm) = \phi(n)\phi(m)$.

**Example 1.7.** Recall that a *ring* is a triple $(R, +, \cdot)$, where $R$ is a set and $+$ and $\cdot$ are binary operations on $R$ such that the following hold:

- $(R, +)$ is an abelian group;
- Multiplication $\cdot$ is an associative binary operation on $R$ with identity $1 \in R$;
- Multiplication is distributive over $+$, in other words $(a + b)c = ac + bc$ and $a(b + c) = ab + ac$ for all $a, b, c \in R$.

A ring $R$ is *commutative* if $ab = ba$ for all $a, b \in R$. For a ring $R$, we denote the set of invertible elements in $R$ by $R^\times$, in other words

$$R^\times = \{x \in R : xy = yx = 1 \text{ for some } y \in R\}.$$

Then $(R^\times, \cdot)$ is a group, and called the *group of units* of $R$. A *field* is a commutative ring $(R, +, \cdot)$ such that every non-zero element has an inverse, in other words $R^\times = R \setminus \{0\}$.

For example, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a commutative ring with group of units $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$, and $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n$ is a prime number. Other examples of fields are $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, and $(\mathbb{C}, +, \cdot)$. The integers $(\mathbb{Z}, +, \cdot)$ form a commutative ring which is not a field.

**Definition 1.8** (Symmetric groups)**.** Let $\Omega$ be a set. The *symmetric group on* $\Omega$ is the group $(\mathrm{Sym}(\Omega), \circ)$, where

$$\mathrm{Sym}(\Omega) = \{f : \Omega \to \Omega \mid f \text{ is a bijection } \}$$

and $\circ$ is composition of functions. The identity element is the *identity map* $1 : \Omega \to \Omega$ defined by $1(x) = x$ for all $x \in \Omega$. If $\Omega = \{1, \ldots, n\}$ for some integer $n > 0$, we denote $\mathrm{Sym}(\Omega) = S_n$. In this case $|\mathrm{Sym}(\Omega)| = n!$ ($n$ factorial).

If $\Omega = \{\omega_1, \ldots, \omega_n\}$, then for $g \in \mathrm{Sym}(\Omega)$ we denote

$$g = \begin{pmatrix} \omega_1 & \omega_2 & \cdots & \omega_n \\ \omega_1' & \omega_2' & \cdots & \omega_n' \end{pmatrix},$$

where $g(\omega_i) = \omega_i'$ for $1 \leq i \leq n$.

**Definition 1.9.** Let $n > 0$ be an integer, and let $(i_1, \ldots, i_k)$ be a $k$-tuple of distinct integers from $\{1, 2, \ldots, n\}$. The *$k$-cycle* corresponding to $(i_1, \ldots, i_k)$ is the permutation $\sigma \in S_n$ defined by

$$\begin{aligned} \sigma(i_t) &= i_{t+1} \text{ for all } 1 \leq t < k, \\ \sigma(i_k) &= i_1, \\ \sigma(d) &= d \text{ for all } d \in \{1, 2, \ldots, n\} \setminus \{i_1, \ldots, i_k\}. \end{aligned}$$

We denote $\sigma = (i_1\ i_2\ \cdots\ i_k)$. A 2-cycle is called a *transposition*.

**Example 1.10.** In $S_3$, every element is a cycle: we have

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

With the group operation we have defined, we have e.g. $(1\ 2)(1\ 3) = (1\ 3\ 2)$ and $(1\ 2\ 3)(2\ 3) = (1\ 2)$. In $S_n$ for $n \geq 4$, you also have elements $\sigma \in S_n$ which are not cycles, for example $\sigma = (1\ 2)(3\ 4)$ and $\sigma = (1\ 2\ 3)(4\ 5)$.

**Example 1.11.** Exercise: If $|\Omega| \geq 3$, then $\mathrm{Sym}(\Omega)$ is not abelian.

**Definition 1.12** (General linear group)**.** Let $n > 0$ be an integer, and let $\mathbb{F}$ be a field (for example, $\mathbb{F} = \mathbb{Q}$ or $\mathbb{F} = \mathbb{C}$). The *general linear group of degree $n$* is the group $(\mathrm{GL}_n(\mathbb{F}), \cdot)$, where $\mathrm{GL}_n(\mathbb{F})$ is the set of invertible $(n \times n)$-matrices with entries in $\mathbb{F}$, and the group operation is matrix multiplication.

It is easy to check that $\mathrm{GL}_n(\mathbb{F})$ is a group, with the *identity matrix*

$$I_n := \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}$$

as the identity element.

**Example 1.13.** A square matrix with entries in a field is invertible if and only if it has nonzero determinant. Thus for example:

$$\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \text{ and } ad - bc \neq 0 \right\}.$$

**Example 1.14.** Let $p$ be a prime. An important example of a field is $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$, which we will denote by $\mathbb{F}_p$. We denote $\mathrm{GL}_n(p) := \mathrm{GL}_n(\mathbb{F}_p)$ for all $n > 0$. Then for example:

$$\mathrm{GL}_2(2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

## 1.1 Isomorphisms

**Definition 1.15.** Let $(G, *)$ and $(H, \star)$ be groups. A map $\varphi : G \to H$ is called an *isomorphism*, if $\varphi$ is a bijection and $\varphi(a * b) = \varphi(a) \star \varphi(b)$ for all $a, b \in G$. If there exists an isomorphism $G \to H$, we say that $G$ and $H$ are *isomorphic* and denote this by $G \cong H$.

If two distinct groups are isomorphic, they have the exact same multiplication table, just with different names for the elements (the different names are given by an isomorphism $\varphi$). Therefore as groups their internal structure is the same, and they have the same group-theoretical properties. For example, if $G \cong H$, then $G$ is abelian if and only if $H$ is abelian.

**Example 1.16.** Let $(G, *)$ be a group with $G = \{1, a, b\}$ and with the following multiplication table:

| $*$ | $1$ | $a$ | $b$ |
|---|---|---|---|
| $1$ | $1$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $1$ |
| $b$ | $b$ | $1$ | $a$ |

Suppose that $(H, \star)$ is a group such that $G \cong H$, and let $\varphi : G \to H$ be an isomorphism. Denote $1' := \varphi(1)$, $a' := \varphi(a)$, and $b' = \varphi(b)$. Then $H = \{1', a', b'\}$. Since $\varphi(x) \star \varphi(y) = \varphi(x * y)$ for all $x, y \in G$, we see that the multiplication table of $H$ is as follows:

| $\star$ | $1'$ | $a'$ | $b'$ |
|---|---|---|---|
| $1'$ | $1'$ | $a'$ | $b'$ |
| $a'$ | $a'$ | $b'$ | $1'$ |
| $b'$ | $b'$ | $1'$ | $a'$ |

So the table is exactly the same as for $(G, *)$, just the names of the elements are different. In this particular example, you can also check that $(G, *) \cong (\mathbb{Z}/3\mathbb{Z}, +)$.

**Example 1.17.** An isomorphism $\varphi : G \to G$ is called an *automorphism*. For any group $G$, the *identity map* $\varphi : G \to G$ defined by $\varphi(g) = g$ is an automorphism. If $G$ is an abelian group, then the inverse map $g \mapsto g^{-1}$ defines an automorphism of $G$.

**Example 1.18.** For any field $\mathbb{F}$, we have $\mathrm{GL}_1(\mathbb{F}) \cong \mathbb{F}^\times$.

**Example 1.19.** Let $V$ be an $n$-dimensional vector space over a field $\mathbb{F}$. Then the *general linear group on* $V$ is the group $(\mathrm{GL}(V), \circ)$, where $\mathrm{GL}(V)$ is the set of all bijective linear maps $V \to V$, and $\circ$ is composition of functions.

Fix a basis $e_1, \ldots, e_n$ of $V$. For $f \in \mathrm{GL}(V)$, let $A_f$ be the $(n \times n)$-matrix $A_f = (A_{ij})$, where $f(e_i) = \sum_{j=1}^n A_{ji} e_j$ for all $1 \leq i \leq n$. Then the map $f \mapsto A_f$ defines an isomorphism $\mathrm{GL}(V) \to \mathrm{GL}_n(\mathbb{F})$.

**Remark 1.20.** Isomorphism forms an equivalence relation in any nonempty collection $\mathcal{G}$ of groups. In other words, for all $A, B, C \in \mathcal{G}$ the following hold:

- $A \cong A$. (reflexivity)
- If $A \cong B$, then $B \cong A$. (symmetry)
- If $A \cong B$ and $B \cong C$, then $A \cong C$. (transitivity)

One type of problem that group theorists have studied since the early days of group theory are various *classification* problems, which are roughly speaking of the form "classify all groups $G$ with property $P$ up to isomorphism". A solution to such a problem would be a collection $\mathcal{G}$ (described as explicitly as possible) of groups such that:

- Every $X \in \mathcal{G}$ is a group with property $P$;
- If $X, Y \in \mathcal{G}$ and $X \neq Y$, then $X \ncong Y$;
- If $G$ is a group with property $P$, then $G \cong X$ for some $X \in \mathcal{G}$.

Here are two fundamental classification problems in finite group theory.

**Problem 1.21.** *Let $n \geq 0$ be an integer. Classify all groups of order $n$ up to isomorphism. In other words, describe a set $\mathcal{G}_n$ such that all of the following hold:*

(i) *$X$ is a finite group of order $n$ for all $X \in \mathcal{G}_n$;*

(ii) *If $X, Y \in \mathcal{G}_n$ and $X \neq Y$, then $X \ncong Y$;*

(iii) *If $G$ is a group of order $n$, then $G \cong X$ for some $X \in \mathcal{G}_n$.*

The cardinality of a set $\mathcal{G}_n$ as in Problem 1.21 is called the *group number of* $n$, and denoted by $\mathrm{gnu}(n) := |\mathcal{G}_n|$. (Exercise: show that $1 \leq \mathrm{gnu}(n) < \infty$ for all integers $n > 0$.)

**Problem 1.22.** *Let $n > 0$ be an integer. What is the value of* $\mathrm{gnu}(n)$*?*

There is no hope currently for a complete solution for these problems, except for specific values of $n$. The history goes back to Cayley[1], who in 1854 introduced the abstract definition of groups and classified groups of order 6. In modern notation, Cayley showed that if $G$ is a finite group of order 6, then $G \cong \mathbb{Z}/6\mathbb{Z}$ or $G \cong S_3$.

Currently the value of $\mathrm{gnu}(n)$ is known for $n < 2048$. It is known that

$$\mathrm{gnu}(2048) > 1774274116992170 \approx 1.77 \cdot 10^{15}$$

but the precise number of groups of order 2048 remains unknown[2,3]. The value of $\mathrm{gnu}(n)$ is also known for special values of $n$, such as prime powers $n = p^k$ with $k \leq 7$. For example, for any prime $p$, we have $\mathrm{gnu}(p) = 1$, $\mathrm{gnu}(p^2) = 2$, $\mathrm{gnu}(p^3) = 5$, and

$$\mathrm{gnu}(p^4) = \begin{cases} 14, & \text{if } p = 2; \\ 15, & \text{if } p \geq 3. \end{cases}$$

$$\mathrm{gnu}(p^5) = \begin{cases} 51, & \text{if } p = 2; \\ 67, & \text{if } p = 3; \\ 61 + 2p + 2\gcd(p-1,3) + 2\gcd(p-1,4), & \text{if } p \geq 5. \end{cases}$$

The results and the theory that we develop during this course will allow us to describe $\mathcal{G}_n$ and $\mathrm{gnu}(n)$ for some specific values of $n$. See Table 1 for a list of small values.[4]

Besides classifying various classes of groups up to isomorphism, another thing that we want to understand in group theory is the structure of a given group $G$. By "structure", we usually mean the various algebraic properties[5]

[1] A. Cayley. *On the theory of groups, as depending on the symbolic equation $\theta^n = 1$.* Philos. Mag., 4(7):40–47, 1854.

[2] J. H. Conway, H. Dietrich, E. A. O'Brien, *Counting groups: gnus, moas, and other exotica.* Math. Intelligencer 30 (2008), no. 2, 6–18.

[3] B. Eick, M. Horn, A. Hulpke, *Constructing groups of 'small' order: recent results and open problems.* Algorithmic and experimental methods in algebra, geometry, and number theory, 199–211, Springer, Cham, 2017.

[4] See for example https://oeis.org/A000001 for more values.

[5] Here is a formal definition: A property $P$ is an *algebraic property* (or *isomorphism-invariant*) if it is preserved under isomorphisms. In other words, if $G$ and $H$ are isomorphic groups, then $G$ has property $P$ if and only if $H$ has property $P$.

| $n$ | gnu($n$) | $n$ | gnu($n$) | $n$ | gnu($n$) | $n$ | gnu($n$) | $n$ | gnu($n$) |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 13 | 1 | 26 | 2 | 39 | 2 | 52 | 5 |
| 1 | 1 | 14 | 2 | 27 | 5 | 40 | 14 | 53 | 1 |
| 2 | 1 | 15 | 1 | 28 | 4 | 41 | 1 | 54 | 15 |
| 3 | 1 | 16 | 14 | 29 | 1 | 42 | 6 | 55 | 2 |
| 4 | 2 | 17 | 1 | 30 | 4 | 43 | 1 | 56 | 13 |
| 5 | 1 | 18 | 5 | 31 | 1 | 44 | 4 | 57 | 2 |
| 6 | 2 | 19 | 1 | 32 | 51 | 45 | 2 | 58 | 2 |
| 7 | 1 | 20 | 5 | 33 | 1 | 46 | 2 | 59 | 1 |
| 8 | 5 | 21 | 2 | 34 | 2 | 47 | 1 | 60 | 13 |
| 9 | 2 | 22 | 2 | 35 | 1 | 48 | 52 | 61 | 1 |
| 10 | 2 | 23 | 1 | 36 | 14 | 49 | 2 | 62 | 2 |
| 11 | 1 | 24 | 15 | 37 | 1 | 50 | 5 | 63 | 4 |
| 12 | 5 | 25 | 2 | 38 | 2 | 51 | 1 | 64 | 267 |

Table 1: Values of gnu($n$) for $0 \leq n \leq 64$.

that are associated with $G$ and its elements. The sections that follow will introduce some of the basic algebraic properties that are studied in group theory.

## 1.2 Order of an element

By associativity, we do not need to worry about brackets when multiplying elements in a group $G$. For example, for $n = 4$ and for any $a_1$, $a_2$, $a_3$, $a_4 \in G$ it is easy to see that the products

$$a_1(a_2(a_3a_4)), a_1((a_2a_3)a_4), (a_1a_2)(a_3a_4), (a_1(a_2a_3))a_4, ((a_1a_2)a_3)a_4$$

are all equal, and thus can be denoted by $a_1a_2a_3a_4$ without ambiguity.

More generally, we have *generalized associativity*: for $a_1$, $a_2$, ..., $a_n \in G$ the product $a_1a_2 \cdots a_n \in G$ is uniquely determined. That is, we get the same element regardless of the choice of brackets (Exercise: prove this by induction on $n$).

Thanks to generalized associativity, we can define powers of elements in a group.

**Definition 1.23.** Let $G$ be a group. For $a \in G$, we denote $a^0 = 1_G$, $a^1 = a$, and more generally $a^n = aa \cdots a$ ($n$ times) for an integer $n > 1$. We define $a^{-n} = (a^{-1})^n$ for all $n > 0$. It is easy to check that for all $a \in G$ and for all $m, n \in \mathbb{Z}$, we have $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

**Remark 1.24.** If $G$ is an abelian group and if we are using additive notation, we shall instead write $0a = 0$, $1a = a$, and $na = a + \cdots + a$ ($n$ times) for integers $n > 1$. Similarly $(-n)a = -(na)$ for all $n > 0$.

**Definition 1.25.** Let $G$ be a group and let $g \in G$. The *order* $|g|$ of $g$ is defined as follows. If the elements $g$, $g^2$, $g^3$, $g^4$, ... are all distinct, we say that $g$ has *infinite order* and define $|g| = \infty$. If there exist distinct integers $r, s$ such that $g^r = g^s$, then we say that $g$ has *finite order*. When $g$ has finite order, there exists $n > 0$ such that $g^n = 1$. In this case we call the smallest such $n$ the *order* of $g$ and define $|g| = n$.

**Example 1.26.** (i) Let $G = S_n$ and consider a $k$-cycle $\sigma = (i_1 \cdots i_k)$. Then $|\sigma| = k$.

(ii) Let $G = (\mathbb{Z}/n\mathbb{Z}, +)$. Then $\overline{1}$ has order $n$ in $G$.

(iii) Let $G = (\mathbb{Z}, +)$. Then every $a \in \mathbb{Z} \setminus \{0\}$ has infinite order in $G$.

**Lemma 1.27.** *Let $G$ be a group and let $g \in G$ be an element of finite order $|g| = n$.*

(i) *Let $m \in \mathbb{Z}$. Then $g^m = 1$ if and only if $n$ divides $m$.*

(ii) *Let $k \geq 0$. Then $|g^k| = \frac{n}{\gcd(n,k)}$.*

(iii) *Let $k \geq 0$ and suppose that $k \mid n$. Then $|g^k| = \frac{n}{k}$.*

(iv) $\{g^k : k \in \mathbb{Z}\} = \{1, g, \ldots, g^{n-1}\}$.

*Proof.* (i) By Euclidean division, we can write $m = qn + r$ with $q \in \mathbb{Z}$ and $0 \leq r < n$. Now $g^m = (g^n)^q g^r = g^r$ since $g^n = 1$, so we have $g^m = 1$ if and only if $g^r = 1$. Since $n$ is the smallest positive integer such that $g^n = 1$, we have $g^r = 1$ if and only if $r = 0$, which is equivalent to $n \mid m$.

(ii) First note that

$$(g^k)^{n/\gcd(k,n)} = (g^n)^{k/\gcd(k,n)} = 1.$$

Next consider $d \geq 0$ such that $(g^k)^d = 1$. Then by (i) we have $n \mid kd$, which implies

$$\frac{n}{\gcd(k,n)} \mid \frac{k}{\gcd(k,n)} d.$$

Since $\gcd(\frac{n}{\gcd(k,n)}, \frac{k}{\gcd(k,n)}) = 1$, it follows that

$$\frac{n}{\gcd(k,n)} \mid d.$$

Therefore $|g^k| = \frac{n}{\gcd(k,n)}$.

(iii) Immediate from (ii).

(iv) By (i), we have $g^i = g^j$ if and only if $i \equiv j \mod n$, from which the claim follows.

□

We end this section with some results about the order of the product $xy$ of two elements $x$ and $y$ in a group $G$.

**Lemma 1.28.** *Let $G$ be a group and let $x, y \in G$. Then $|xy| = |yx|$.*

*Proof.* We will show that for $n > 0$, we have $(xy)^n = 1$ if and only if $(yx)^n = 1$, from which the lemma follows. For this, we can write

$$(xy)^n = (xy)(xy)\cdots(xy) = x(yx)\cdots(yx)y = x(yx)^{n-1}y,$$

so $(xy)^n = 1$ if and only if $x(yx)^{n-1}y = 1$. Multiplying both sides on the left by $y$, we see that $x(yx)^{n-1}y = 1$ is equivalent to $(yx)^n y = y$, which in turn is equivalent to $(yx)^n = 1$, by cancelling out $y$. □

**Lemma 1.29.** *Let $G$ be a group and let $x, y \in G$ be elements of finite orders $|x| = m$ and $|y| = n$. Suppose that $xy = yx$ and that $\gcd(m, n) = 1$. Then $|xy| = mn$.*

*Proof.* Since $xy = yx$, it is easy to see that $(xy)^d = x^d y^d$ for all integers $d \in \mathbb{Z}$. In particular, we have $(xy)^{mn} = 1$ since $x^m = 1$ and $y^n = 1$. Suppose now that $(xy)^d = 1$. Then $x^d = y^{-d}$, and powering both sides by $n$ shows $x^{dn} = 1$. Therefore $m \mid dn$, which implies $m \mid d$ since $\gcd(m, n) = 1$. Similarly we have $y^d = x^{-d}$, and powering both sides by $m$ shows that $y^{dm} = 1$, which implies $n \mid d$. Therefore $m \mid d$ and $n \mid d$, which gives $mn \mid d$ since $\gcd(m, n) = 1$. Thus $|xy| = mn$. □

Note that both assumptions in Lemma 1.29 are necessary:

- Consider any nontrivial element $x \in G$ of finite order and let $y = x^{-1}$. Then $xy = yx$. But $|xy| = 1$, so $|xy| \neq |x||y|$.
- Consider $G = S_3$ and any $x, y \in G$ with $|x| = 2$ and $|y| = 3$. Then $\gcd(|x|, |y|) = 1$. But $|xy| = 2$, so $|xy| \neq |x||y|$.

In general, suppose that $x, y \in G$ are nontrivial elements of finite order. There are examples where $xy$ has infinite order (Exercise 1.3). If $xy$ has finite order, what do $|x|$ and $|y|$ tell us about $|xy|$? By the following result, the answer is "absolutely nothing".

**Theorem 1.30** (Miller, 1900)**.** *Let $m, n, \ell > 1$ be integers. Then there exists a finite group $G$ which contains elements $x$ and $y$ such that $|x| = m$, $|y| = n$, and $|xy| = \ell$.*

*Proof.* Omitted. □

As a historical note, the first proof of Theorem 1.30 was given in a paper of G. A. Miller[6] from 1900. Let $k = \max(m, n, \ell)$. In his paper, Miller constructs explicitly permutations $x, y \in S_{k+2}$ such that $|x| = m$, $|y| = n$, and $|xy| = \ell$. The proof by Miller is a somewhat lengthy calculation involving many different cases. Since 1900, the result has been rediscovered[7] several times and shorter proofs have been found.

## 1.3 Subgroups

One basic thing that we want to understand about a group $G$ is its *subgroup structure*, that is, the groups that are contained inside of $G$.

**Definition 1.31.** Let $(G, *)$ be a group. A subset $H \subseteq G$ is a *subgroup*, if $H$ is closed under the binary operation $*$ and $H$ equipped with $*$ is a group. We denote this by $H \leq G$.

Note that if $H$ is a subgroup $G$, then $H$ and $G$ must have the same identity element. Indeed, suppose that $x = 1_H$ is the identity element of $H$. Then $x^2 = x$, so multiplying both sides by $x^{-1}$ shows that $x = 1_G$. Throughout these notes, we will use the following lemma to check whether a subset $H \subseteq G$ is a subgroup.

**Lemma 1.32.** *Let $G$ be a group. A subset $H \subseteq G$ is a subgroup if and only if all of the following hold:*

(i) $1_G \in H$;

(ii) $ab \in H$ *for all* $a, b \in H$;

(iii) $a^{-1} \in H$ *for all* $a \in H$.

*Proof.* If $H$ is a subgroup of $G$, then $1_G \in H$ as seen above, so (i) holds. Property (ii) holds by definition, and (iii) holds since $H$ is a group and inverses are unique in $G$. Conversely if (i) — (iii) hold then $H$ is a subgroup; we only need to check associativity and this follows immediately from associativity in $G$. □

[6] G. A. Miller, *On the Product of Two Substitutions*, American Journal of Mathematics, Vol. 22, No. 2 (Apr., 1900), pp. 185-190.

[7] J. König, *A note on the product of two permutations of prescribed orders*, European J. Combin. 57 (2016), 50–56.

**Example 1.33.** Examples of subgroups:

(i) Let $G$ be a group. Then $G$ itself is a subgroup of $G$, and moreover the *trivial* subgroup $\{1\}$ is always a subgroup of $G$.

(ii) $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

(iii) $\mathrm{GL}_n(\mathbb{Q}) \leq \mathrm{GL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{C})$.

(iv) Let $n > 0$ be an integer and let $\mathbb{F}$ be a field. We define the *special linear group* $\mathrm{SL}_n(\mathbb{F})$ as

$$\mathrm{SL}_n(\mathbb{F}) = \{A \in \mathrm{GL}_n(\mathbb{F}) : \det(A) = 1\}.$$

Since $\det(AB) = \det(A)\det(B)$ and $\det(A^{-1}) = 1/\det(A)$, it follows that $\mathrm{SL}_n(\mathbb{F})$ is a subgroup of $\mathrm{GL}_n(\mathbb{F})$.

**Example 1.34.** If $G$ is finite and $H \subseteq G$ is a nonempty subset closed under products, then $H$ is a subgroup. This follows from the fact that a $g \in H$ has some finite order $n$, so $g^n = 1$ is in $H$, and $g^{n-1} = g^{-1}$ is also in $H$. (More generally, this works if every element of $G$ has finite order.)

However, in general closure under the group operation is not enough. Consider $H = \mathbb{Z}_{\geq 0}$ in $G = (\mathbb{Z}, +)$. Then $H$ equipped with $+$ contains the identity element and is closed under addition. But clearly $H$ is not closed under taking inverses, so $H$ is not a subgroup.

**Definition 1.35.** Let $H$ be a subgroup of a group $G$. If $H \lneqq G$, we say that $H$ is a *proper* subgroup. If $H \neq \{1\}$, we say that $H$ is a *nontrivial* subgroup.

**Lemma 1.36.** *Let $G$ be a group. Then the intersection of any collection of subgroups of $G$ is a subgroup.*

*Proof.* Any subgroup contains the identity, so the same is true for their intersection. The intersection is also closed under products and inverses since the subgroups are. □

**Definition 1.37.** Let $G$ be a group and $S \subseteq G$. We define the subgroup *generated by* $S$ as the intersection of all subgroups of $G$ that contain $S$. We denote the subgroup generated by $S$ with $\langle S \rangle := \cap_{S \subseteq H \leq G} H$. For $x_1$, …, $x_n \in G$, we denote $\langle x_1, \ldots, x_n \rangle := \langle \{x_1, \ldots, x_n\} \rangle$.

**Definition 1.38.** A group $G$ is said to be *finitely generated* if $G = \langle x_1, \ldots, x_n \rangle$ for some $x_1, \ldots, x_n \in G$.

**Lemma 1.39.** *Let $G$ be a subgroup and $S \subseteq G$. Then:*

(i) $\langle S\rangle$ *is the smallest subgroup of* $G$ *that contains* $S$*. In other words, if* $S \subseteq H \leq G$*, then* $\langle S\rangle \leq H$*.*

(ii) *We have*

$$\langle S\rangle = \{g \in G : g = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} \text{ for some } n \geq 0, s_i \in S \text{ and } \varepsilon_i \in \{1, -1\}\}.$$

*Here for* $n = 0$*, we interpret* $s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n} = 1$ *(empty product).*

*Proof.* (i) Since $\langle S\rangle$ is the intersection of some subgroups of $G$, it is itself a subgroup of $G$. For $S \subseteq H \leq G$, we have $\langle S\rangle \leq H$ by the definition of $\langle S\rangle$ as the intersection of all subgroups of $G$ that contain $S$.

(ii) Let $H = \{g \in G : g = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$ for some $s_i \in S$ and $\varepsilon_i \in \{1, -1\}\}$. We have $S \subseteq H$ and clearly $H$ is contained in every subgroup of $G$ that contains $S$, in particular $H \subseteq \langle S\rangle$. We will show that $H$ is a subgroup, from which it follows that $\langle S\rangle = H$. To this end, it is clear that $1 \in H$ and that $H$ is closed under multiplication. Closure under inverses follows from $(s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n})^{-1} = s_n^{-\varepsilon_n} \cdots s_1^{-\varepsilon_1}$, so $H$ is a subgroup. □

## 1.4 Cyclic groups

**Definition 1.40.** A group $G$ is said to be *cyclic* if $G = \langle g\rangle$ for some $g \in G$.

**Example 1.41.** For all $n > 0$, the group $\mathbb{Z}/n\mathbb{Z}$ is cyclic of order $n$, and $\mathbb{Z}$ is infinite cyclic.

In this section, we will describe the basic properties of cyclic groups.

**Lemma 1.42.** *Let* $G$ *be a group and* $g \in G$*.*

(i) $\langle g\rangle = \{g^k : k \in \mathbb{Z}\}$.

(ii) *If* $g$ *has finite order* $|g| = n$*, then* $\langle g\rangle$ *is a subgroup of order* $|g|$ *and* $\langle g\rangle = \{1, g, \ldots, g^{n-1}\}$.

*Proof.* (i) Follows from Lemma 1.39.

(ii) Follows from (i) and Lemma 1.27.

□

**Lemma 1.43.** *Let* $G$ *and* $H$ *be cyclic groups. Then* $G \cong H$ *if and only if* $|G| = |H|$*. In particular:*

(i) *If $G$ has finite order $n$, then $G \cong \mathbb{Z}/n\mathbb{Z}$.*

(ii) *If $G$ has infinite order, then $G \cong \mathbb{Z}$.*

*Proof.* If $G \cong H$, then $|G| = |H|$. Conversely if $G = \langle g \rangle$ and $H = \langle h \rangle$ are cyclic groups of equal order, check that $g^k \mapsto h^k$ defines an isomorphism $G \to H$. Then (i) follows since $\mathbb{Z}/n\mathbb{Z}$ is cyclic of order $n$, and (ii) since $\mathbb{Z}$ is infinite cyclic. □

Lemma 1.43 justifies the following notation.

**Definition 1.44.** We denote a cyclic group of order $n$ by $C_n$.

Next we will describe the subgroups of cyclic groups.

**Lemma 1.45.** *Every subgroup of a cyclic group is cyclic.*

*Proof.* Let $G = \langle g \rangle$ be cyclic and let $H \leq G$ be a subgroup. Then there exists $g^d \in H$ with $d \geq 0$, choose $d$ to be minimal. We will show that $H = \langle g^d \rangle$. It is clear that $\langle g^d \rangle \leq H$.

To show that $H \leq \langle g^d \rangle$, let $h \in H$ and write $h = g^k$ with $k \in \mathbb{Z}$. By Euclidean division, we can write $k = qd + r$ with $q \in \mathbb{Z}$ and $0 \leq r < d$. Then

$$g^k = (g^d)^q g^r,$$

which implies $g^r \in H$. By minimality of $d$ we have $r = 0$, so $h = g^{qd} \in \langle g^d \rangle$. □

**Lemma 1.46.** *Let $G = \langle g \rangle$ be a cyclic group of order $n > 0$.*

(i) *Let $k \in \mathbb{Z}$. Then $\langle g^k \rangle = \langle g^{\gcd(k,n)} \rangle$.*

(ii) *Every subgroup of $G$ has the form $\langle g^d \rangle$ for some $d \mid n$.*

(iii) *Let $d \mid n$. Then $G$ has a unique subgroup $H$ of order $d$, and $H = \langle g^{n/d} \rangle$.*

(iv) *Let $k \in \mathbb{Z}$. Then $\langle g^k \rangle = G$ if and only if $\gcd(k, n) = 1$.*

(v) *The number of generators of $G$ is equal to $\phi(n)$.*

*Proof.* (i) By Bézout's lemma, we can write $\lambda k + \mu n = \gcd(k, n)$ for some $\lambda, \mu \in \mathbb{Z}$. Since $g^n = 1$, this shows that $g^{\gcd(k,n)} = g^{\lambda k} \in \langle g^k \rangle$, so $\langle g^{\gcd(k,n)} \rangle \leq \langle g^k \rangle$. On the other hand $|g^k| = |g^{\gcd(k,n)}|$ by Lemma 1.27 (ii)–(iii), so $\langle g^{\gcd(k,n)} \rangle = \langle g^k \rangle$.

(ii) Since $\gcd(k, n)$ divides $n$, this is immediate from (i).

(iii) Let $H \leq G$ be a subgroup of order $d$, where $d \mid n$. By (ii) we have $H = \langle g^{d'} \rangle$ for some $d' \mid n$. Since $|g^{d'}| = n/d'$ by Lemma 1.27 (iii), it follows that $d = |H| = n/d'$, so $d' = n/d$.

(iv) We have $\langle g^k \rangle = G$ if and only if $|g^k| = n$, so this follows from Lemma 1.27 (ii).

(v) Follows from (iv).

□

**Remark 1.47.** Let $G = \langle g \rangle$ be cyclic of order $n$. By Lemma 1.46 (ii) – (iii), the number of subgroups of $G$ is equal to the number of divisors of $n$, with $d \mid n$ corresponding to the subgroup $\langle g^{n/d} \rangle$ of order $d$. For example if $G = \langle g \rangle$ is cyclic of order 6, then $G$ has a total of 4 subgroups: $\{1\}$, $\langle g^2 \rangle$, $\langle g^3 \rangle$, and $\langle g \rangle$.

**Lemma 1.48.** *Let $G = \langle g \rangle$ be a cyclic group of infinite order.*

(i) *Let $d \in \mathbb{Z} \setminus \{0\}$. Then $\langle g^d \rangle$ is infinite cyclic.*

(ii) *Every subgroup of $G$ has the form $\langle g^d \rangle$ for some $d \geq 0$.*

(iii) *$\langle g^d \rangle \leq \langle g^{d'} \rangle$ if and only if $d' \mid d$.*

(iv) *$\langle g^d \rangle = \langle g^{d'} \rangle$ if and only if $d = \pm d'$.*

(v) *$\langle g^d \rangle = G$ if and only if $d = \pm 1$.*

*Proof.* (i) Note first that since $g$ has infinite order, for all $k, \ell \in \mathbb{Z}$ we have $g^k = g^\ell$ if and only if $k = \ell$. If $\langle g^d \rangle$ is finite, we have $g^{dk} = 1 = g^0$ for some $k > 0$, which gives $dk = 0$ and thus $d = 0$.

(ii) By Lemma 1.45, every subgroup of $G$ is of the form $\langle g^k \rangle$ for some $k \in \mathbb{Z}$. If $k \geq 0$ we are done with $k = d$. If $d < 0$, then $\langle g^k \rangle = \langle g^{-k} \rangle$ and the claim follows with $d = -k$.

(iii) We have $\langle g^d \rangle \leq \langle g^{d'} \rangle$ if and only if $g^d \in \langle g^{d'} \rangle$. Now $g^d \in \langle g^{d'} \rangle$ if and only if $g^d = g^{d'k}$ for some $k \in \mathbb{Z}$, equivalently $d = d'k$ for some $k \in \mathbb{Z}$ since $g$ has infinite order. Therefore $g^d \in \langle g^{d'} \rangle$ if and only if $d' \mid d$.

(iv) By (iii), we have $\langle g^d \rangle = \langle g^{d'} \rangle$ if and only if $d' \mid d$ and $d \mid d'$, which is equivalent to $d = \pm d'$.

(v) Immediate from (iv).

□

## 1.5 On the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$

We will now apply the basic results on cyclic groups to describe the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$ in some cases.

**Definition 1.49.** Let $G$ be a group and $d > 0$ an integer. We denote by $o_d(G)$ the number of elements of order $d$ in $G$, in other words the cardinality of the set $\{x \in G : |x| = d\}$.

In this section, we will make use of the fact that will be proven later using Lagrange's theorem (Corollary 1.81): if $G$ is a finite group, the order of any $x \in G$ divides the order of $G$. It follows then for a finite group $G$ of order $n$, we have

$$n = |G| = \sum_{d|n} o_d(G).$$

We begin with an elementary result which does not involve any group theory, but can be proven using some basic properties of cyclic groups.

**Theorem 1.50.** *Let $n > 0$ be an integer. Then $n = \sum_{d|n} \phi(d)$.*

*Proof.* Let $G$ be a cyclic group of order $n$. Each element of order $d$ generates a subgroup of order $d$, and there is only such subgroup in $G$ by Lemma 1.46 (iii). Therefore $o_d(G)$ is equal to the number of generators for a cyclic group of order $d$, and so $o_d(G) = \phi(d)$ by Lemma 1.46 (v). We conclude then that

$$n = |G| = \sum_{d|n} o_d(G) = \sum_{d|n} \phi(d).$$

□

**Theorem 1.51.** *Let $G$ be a finite group such that for all $d > 0$, the number of solutions to $x^d = 1$ in $G$ is at most $d$. Then $G$ is cyclic.*

*Proof.* Denote $n = |G|$. We have $o_d(G) = \phi(d)s_d(G)$, where $s_d(G)$ is the number of cyclic subgroups of order $d$ in $G$. (This is because two different cyclic subgroups of order $d$ cannot have elements of order $d$ in common.)

Since $n = \sum_{d|n} o_d(G)$, we have

$$\sum_{d|n} \phi(d)s_d(G) = \sum_{d|n} \phi(d) \tag{1.1}$$

by Theorem 1.50. If we assume that $x^d = 1$ has at most $d$ solutions for all $d > 0$, then $s_d(G) \leq 1$ for all $d \mid n$. It follows then from (1.1) that $s_d(G) = 1$ for all $d \mid n$. In particular $s_n(G) = 1$, so $G$ is cyclic. □

For a field $\mathbb{F}$, recall that we denote the multiplicative group $(\mathbb{F} \setminus \{0\}, \cdot)$ by $\mathbb{F}^\times$. We will now apply Theorem 1.51 to prove the following fundamental result about finite fields.

**Theorem 1.52.** *Let $\mathbb{F}$ be a finite field. Then $\mathbb{F}^\times$ is cyclic.*

*Proof.* Over any field $\mathbb{F}$, a polynomial of degree $d > 0$ has at most $d$ roots. In particular, the polynomial $x^d - 1 \in \mathbb{F}[x]$ has at most $d$ roots, so there are at most $d$ solutions to $x^d = 1$ in $\mathbb{F}^\times$. By Theorem 1.51, the multiplicative group $\mathbb{F}^\times$ is cyclic. □

In particular, we have shown that $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic for any prime $p > 0$. In general $(\mathbb{Z}/n\mathbb{Z})^\times$ is not cyclic; for example $x^2 = 1$ for all $x \in (\mathbb{Z}/8\mathbb{Z})^\times$, so $(\mathbb{Z}/8\mathbb{Z})^\times$ does not have an element of order $4 = \phi(8)$. We now consider the question of when $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic for a prime number $p$. We will see that $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic if $p > 2$, and usually not if $p = 2$. First we need some notation and a lemma.

**Definition 1.53.** Let $n \neq 0$ be an integer and let $p$ be a prime. We denote by $\nu_p(n)$ the largest integer $\alpha \geq 0$ such that $p^\alpha \mid n$. (In other words, the unique integer $\alpha \geq 0$ such that $p^\alpha \mid n$ and $p^{\alpha+1} \nmid n$.)

For example, for $n = 60 = 2^2 \cdot 3 \cdot 5$ we have $\nu_2(n) = 2$, $\nu_3(n) = 1$, $\nu_5(n) = 1$, and $\nu_p(n) = 0$ for any prime $p > 5$.

**Lemma 1.54.** *Let $p > 2$ be a prime, and let $z \equiv 1 \mod p$. Then the following hold:*

(i) $\nu_p(z^p - 1) = \nu_p(z - 1) + 1$.

(ii) $\nu_p(z^{p^k} - 1) = \nu_p(z - 1) + k$ *for all* $k > 0$.

*Proof.* (i) Write $z = 1 + tp$, where $t \geq 1$. Then $\nu_p(z - 1) = \alpha + 1$, where $p^\alpha$ is the largest power of $p$ dividing $t$.

Applying the binomial formula, we get

$$z^p - 1 = (1+tp)^p - 1 = \binom{p}{1}tp + \binom{p}{2}t^2p^2 + \cdots + \binom{p}{p-1}t^{p-1}p^{p-1} + t^pp^p.$$

The first term in the sum is certainly divisible by $p^{\alpha+2}$, and not by $p^{\alpha+3}$. It is easy to see that all of the other terms in the sum are divisible by $p^{\alpha+3}$, so we conclude that $p^{\alpha+2}$ is the largest power of $p$ dividing $z^p - 1$. In other words $\nu_p(z^p - 1) = \nu_p(z - 1) + 1$.

(ii) For $k = 1$ the claim is just (i). Suppose that $k > 1$. Then

$$\nu_p(z^{p^k} - 1) = \nu_p((z^{p^{k-1}})^p - 1) = \nu_p(z^{p^{k-1}} - 1) + 1$$

by (i), so the claim follows by induction on $k$.

□

**Theorem 1.55.** *Let $p > 2$ be a prime. Then $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic for all $n \geq 1$.*

*Proof.* For $n = 1$, the claim follows from Theorem 1.52. Suppose then that $n > 1$. Our aim is to find an element of order $\phi(p^n) = p^{n-1}(p-1)$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. For this it will suffice to find an element of order $p^{n-1}$ and $(p-1)$, as then by Lemma 1.29 their product will have order $p^{n-1}(p-1)$.

Let $g \in \mathbb{Z}$ be such that the image of $g$ is a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$, in other words $g$ has order $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Then the order of $g$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$ must be divisible by $p-1$, so a suitable power of $g$ will have order $p-1$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

For an element of order $p^{n-1}$, we claim that the image of $z = 1 + p$ has order $p^{n-1}$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Indeed, by Lemma 1.54 (ii) we have $\nu_p(z^{p^k} - 1) = k + 1$ for all $k > 0$. Therefore $z^{p^{n-1}} \equiv 1 \mod p^n$ and $z^{p^{n-2}} \not\equiv 1 \mod p^n$, so $z$ has order $p^{n-1}$ in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. □

**Lemma 1.56.** *Let $z$ be an odd integer and $k > 0$. Then the following statements hold:*

(i) *If $z \equiv 1 \mod 4$, then $\nu_2(z^{2^k} - 1) = \nu_2(z - 1) + k$.*

(ii) *If $z \equiv 3 \mod 4$, then $\nu_2(z^{2^k} - 1) = \nu_2(z + 1) + k$.*

*Proof.* Exercise. □

**Theorem 1.57.** *If $n \geq 3$, then $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic.*

*Proof.* Exercise. (Apply Lemma 1.56.) □

## 1.6 Homomorphisms

**Definition 1.58.** Let $G$ and $H$ be groups. A map $\varphi : G \to H$ is called a *homomorphism*, if $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$.

Rather than only looking at structure-preserving maps which are bijective (isomorphisms), it is natural to consider structure-preserving maps which are not necessarily bijections (homomorphisms).

For example, note that if $\varphi : G \to H$ is an injective homomorphism, then it is easily shown that $\varphi(G)$ is a group and moreover that $\varphi$ provides an

isomorphism $G \cong \varphi(G)$ (see Lemma 1.63 (vi) below). In this case we say that $G$ *embeds into* $H$. The question whether a given group $G$ embeds into another group $H$ comes up all the time in group theory.

If $\varphi$ is not injective, a homomorphic image $\varphi(G)$ is still a group: the multiplication table of $\varphi(G)$ is like that of $G$, except some elements of $G$ are identified. For example, consider the map

$$\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ \varphi(x) = \overline{x} \text{ for all } x \in \mathbb{Z}.$$

This map is a surjective homomorphism; the image of $\mathbb{Z}$ is $\mathbb{Z}/n\mathbb{Z}$ which as a group is like $(\mathbb{Z}, +)$, except $a, b \in \mathbb{Z}$ with $a \equiv b \mod n$ are identified.

**Lemma 1.59.** *Let $G$ and $H$ be groups and let $\varphi : G \to H$ be a homomorphism. Then:*

(i) $\varphi(x_1 x_2 \cdots x_k) = \varphi(x_1)\varphi(x_2)\cdots\varphi(x_k)$ *for all* $x_1, x_2, \ldots, x_k \in G$;

(ii) $\varphi(1_G) = 1_H$;

(iii) $\varphi(x^{-1}) = \varphi(x)^{-1}$ *for all* $x \in G$;

(iv) $\varphi(x^n) = \varphi(x)^n$ *for all* $x \in G$ *and* $n \in \mathbb{Z}$;

*Proof.* (i) For $k = 2$ this is the definition of a homomorphism, for $k > 2$ apply $\varphi(x_1 x_2 \cdots x_k) = \varphi(x_1)\varphi(x_2 \cdots x_k)$ and induction on $k$.

(ii) We have $\varphi(1_G)\varphi(1_G) = \varphi(1_G 1_G) = \varphi(1_G)$; then multiplying both sides of $\varphi(1_G)\varphi(1_G) = \varphi(1_G)$ with $\varphi(1_G)^{-1}$ gives $\varphi(1_G) = 1_H$.

(iii) We have $\varphi(x)\varphi(x^{-1}) = \varphi(1_G) = 1_H$ by (ii); then multiplying both sides of $\varphi(x)\varphi(x^{-1}) = 1_H$ on the left with $\varphi(x)^{-1}$ gives $\varphi(x^{-1}) = \varphi(x)^{-1}$.

(iv) Follows from (i) – (ii) for $n \geq 0$. Then for $n < 0$ the claim follows from (iii), since $x^n = (x^{-n})^{-1}$.

□

**Definition 1.60.** Let $G$ and $H$ be groups and let $\varphi : G \to H$ be a homomorphism. The *kernel* of $\varphi$ is the set

$$\operatorname{Ker} \varphi = \{g \in G : \varphi(g) = 1\}.$$

**Example 1.61.** Let $G$ be any group and let $g \in G$. Since $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$, we have a homomorphism $\varphi : \mathbb{Z} \to G$ defined by $\varphi(k) = g^k$ for all $k \in \mathbb{Z}$. If $g$ has infinite order, then $\operatorname{Ker} \varphi = \{0\}$. If $g$ has finite order $|g| = n$, then $\operatorname{Ker} \varphi = n\mathbb{Z}$.

**Example 1.62.** Let $n > 0$ be an integer and let $\mathbb{F}$ be a field. We have $\det(AB) = \det(A)\det(B)$ for all $A, B \in \mathrm{GL}_n(\mathbb{F})$; in other words the determinant map $\det : \mathrm{GL}_n(\mathbb{F}) \to \mathbb{F} \setminus \{0\}$ is a group homomorphism. The kernel consists of $A \in \mathrm{GL}_n(\mathbb{F})$ with $\det(A) = 1$, in other words, the kernel is $\mathrm{SL}_n(\mathbb{F})$.

**Lemma 1.63.** *Let $G$ and $H$ be groups and let $\varphi : G \to H$ be a homomorphism. Then:*

(i) $\operatorname{Ker}\varphi$ *is a subgroup of* $G$.

(ii) *For $x, y \in G$ we have $\varphi(x) = \varphi(y)$ if and only if $xy^{-1} \in \operatorname{Ker}\varphi$.*

(iii) $\varphi$ *is injective if and only if* $\operatorname{Ker}\varphi = \{1\}$.

(iv) *If $X \leq G$, then $\varphi(X) \leq H$.*

(v) *If $Y \leq H$, then $\varphi^{-1}(Y) \leq G$.*

(vi) *If $\varphi$ is injective, then $\varphi(X) \cong X$ for all $X \leq G$, and in particular $\varphi(G) \cong G$.*

(vii) *If $\varphi$ is injective, then $|\varphi(g)| = |g|$ for all $g \in G$.*

*Proof.* (i) We have $1 \in \operatorname{Ker}\varphi$ by Lemma 1.59 (ii). If $x, y \in \operatorname{Ker}\varphi$ then $\varphi(xy) = \varphi(x)\varphi(y) = 1$ so $xy \in \operatorname{Ker}\varphi$. Furthermore $\varphi(x^{-1}) = \varphi(x)^{-1} = 1$ by Lemma 1.59 (iii), so $\operatorname{Ker}\varphi$ is a subgroup.

(ii) We have $\varphi(x) = \varphi(y)$ if and only if $\varphi(x)\varphi(y)^{-1} = 1$, which is equivalent to $\varphi(xy^{-1}) = 1$ by Lemma 1.59 (iii).

(iii) If $\varphi$ is injective, then $\operatorname{Ker}\varphi = \{1\}$ as otherwise $\varphi(x) = \varphi(1)$ for some $g \neq 1$. Conversely suppose that $\operatorname{Ker}\varphi = \{1\}$. Then $\varphi(x) = \varphi(y)$ implies $x = y$ by (ii), so $\varphi$ is injective.

(iv) Since $1_G \in X$, we have $\varphi(1_G) = 1_H \in \varphi(X)$ by Lemma 1.59 (ii). Closure under products follows from the definition of a homomorphism, and closure under inverses from Lemma 1.59 (iii).

(v) We have $1_G \in \varphi^{-1}(Y)$ since $\varphi(1_G) = 1_H \in Y$. If $x, y \in \varphi^{-1}(Y)$, then $\varphi(x), \varphi(y) \in Y$ and thus $\varphi(x)\varphi(y) = \varphi(xy) \in Y$, giving $xy \in \varphi^{-1}(Y)$. We also have $\varphi(y)^{-1} = \varphi(y^{-1}) \in Y$ by Lemma 1.59 (iii), so $y^{-1} \in \varphi^{-1}(Y)$. Thus $\varphi^{-1}(Y) \leq G$.

(vi) If $\varphi$ is injective, then the restriction of $\varphi$ to $X$ provides an isomorphism $X \to \varphi(X)$.

(vii) We have $\varphi(g)^n = \varphi(g^n)$ for all $g \in G$ by Lemma 1.59 (iv). Thus if $\varphi$ is injective, then $\varphi(g)^n = 1$ if and only if $g^n = 1$, so $|\varphi(g)| = |g|$.

□

**Definition 1.64.** Let $G$ be a group and $g \in G$. The *inner automorphism corresponding to* $g$ is the map $\gamma_g : G \to G$ defined by $\gamma_g(x) = gxg^{-1}$ for all $x \in G$.

**Lemma 1.65.** *Let $G$ be a group and $g \in G$. Then $\gamma_g : G \to G$ is an automorphism for all $g \in G$. In particular:*

(i) $(gxg^{-1})^k = gx^kg^{-1}$ *for all $x \in G$ and $k \in \mathbb{Z}$;*

(ii) $|gxg^{-1}| = |x|$ *for all $x \in G$.*

*Proof.* Let $g \in G$. We have

$$\gamma_g(xx') = gxx'g^{-1} = (gxg^{-1})(gx'g^{-1}) = \gamma_g(x)\gamma_g(x')$$

for all $x, x' \in G$, so $\gamma_g$ is a homomorphism. We have $gxg^{-1} = gyg^{-1}$ if and only if $x = y$ by the cancellation laws, so $\gamma_g$ is injective. Finally $\gamma_g$ is surjective, since $x = g(g^{-1}xg)g^{-1} = \gamma_g(g^{-1}xg)$ for all $x \in G$. Thus $\gamma_g$ is an automorphism. Now claims (i) and (ii) follow from Lemma 1.59 (iv) and Lemma 1.63 (vii). □

Next we will prove Cayley's theorem, which shows that every group is isomorphic to a subgroup of $\mathrm{Sym}(\Omega)$ with $|\Omega| = |G|$. In particular, it follows that a finite group $G$ can be embedded into $S_n$ with $n = |G|$. For most finite groups this is not optimal, in the sense that usually one can find smaller $n$ such that $G$ embeds into $S_n$. (Consider for example $G = S_n$, for which $|G| = n!$ is much bigger than $n$.)

**Theorem 1.66** (Cayley's theorem)**.** *Let $G$ be a group. For $g \in G$, define maps $L_g, R_g : G \to G$ by $L_g(x) = gx$ and $R_g(x) = xg$ for all $x \in G$. Then:*

(i) *$L_g$ and $R_g$ are bijections for all $g \in G$.*

(ii) *The map $\varphi : G \to \mathrm{Sym}(G)$ defined by $\varphi(g) = L_g$ for all $g \in G$ is an injective homomorphism.*

(iii) *The map $\psi : G \to \mathrm{Sym}(G)$ defined by $\varphi(g) = R_{g^{-1}}$ for all $g \in G$ is an injective homomorphism.*

*Proof.* (i) For $L_g$, injectivity follows from the cancellation laws (if $gx = gy$, then $x = y$); surjectivity follows from $x = g(g^{-1}x)$. In the same way we see that $R_g$ is a bijection.

(ii) We have $L_g L_h(x) = L_g(hx) = g(hx) = (gh)x = L_{gh}(x)$, so $L_{gh} = L_g L_h$ for all $g, h \in G$. Thus $\varphi$ is a homomorphism. For injectivity, if $L_g = L_h$, then in particular $L_g(1) = L_h(1)$, so $g = h$.

(iii) Similar to (ii).

□

The maps $L_g$ in Theorem 1.66 are called *left translation maps*, and the homomorphism $\varphi$ is called the *left regular representation*. Similarly the $R_g$ are called *right translations* and the homomorphism $\psi$ is called the *right regular representation*.

## 1.7 Dihedral groups

We have found that the structure of cyclic groups — that is, groups generated by one element — is fairly simple to describe. What about groups generated by two elements? In this case very little can be said in general, as is already hinted by Theorem 1.30. One special case where we can give a classification result is when $G$ is generated by two elements of order two.

**Definition 1.67.** A group $G$ is said to be *dihedral*, if $G = \langle a, b \rangle$ for some $a, b \in G$ with $|a| = |b| = 2$.

**Lemma 1.68.** *A group $G$ is dihedral if and only if $G = \langle x, y \rangle$ for some $x, y \in G$ such that $|x| = 2$, $xyx^{-1} = y^{-1}$, and $x \notin \langle y \rangle$.*

*Proof.* Suppose that $G$ is dihedral, say $G = \langle a, b \rangle$ with $|a| = |b| = 2$. We claim that $x = a$ and $y = ab$ works. It is clear that $G = \langle x, y \rangle$. Moreover $|x| = 2$, and $xyx^{-1} = a(ab)a = ba = y^{-1}$.

It remains to check that $x \notin \langle y \rangle$. To this end, if $x \in \langle y \rangle$, then $x$ and $y$ must commute, which implies $xyx^{-1} = y$. On the other hand $xyx^{-1} = y^{-1}$, so $y = y^{-1}$ and thus $y^2 = 1$. But since $|x| = 2$ and $x \in \langle y \rangle$, we must have $x = y$. In other words $a = ab$, which is impossible since $b \neq 1$.

For the other direction, suppose that $G = \langle x, y \rangle$ for some $x, y \in G$ such that $|x| = 2$, $xyx^{-1} = y^{-1}$, and $x \notin \langle y \rangle$. Let $a = x$ and $b = xy$. Then $b^2 = (xyx)y = y^{-1}y = 1$ and $b \neq 1$ since $x \notin \langle y \rangle$, so $|b| = 2$. Thus $G = \langle a, b \rangle$ with $|a| = |b| = 2$. □

**Lemma 1.69.** *Suppose that $G$ is a group such that $G = \langle x, y \rangle$ with $|x| = 2$, $xyx^{-1} = y^{-1}$, and $x \notin \langle y \rangle$. Then:*

(i) $G = \{x^i y^j : i \in \{0, 1\} \text{ and } j \in \mathbb{Z}\}$.

(ii) *For all* $i, i_0 \in \{0,1\}$ *and* $j, j_0 \in \mathbb{Z}$ *we have*

$$(x^i y^j)(x^{i_0} y^{j_0}) = x^{i+i_0} y^{(-1)^{i_0} j + j_0}.$$

(iii) *For all* $i, i_0 \in \{0,1\}$ *and* $j, j_0 \in \mathbb{Z}$ *we have* $x^i y^j = x^{i_0} y^{j_0}$ *if and only if* $i = i_0$ *and* $y^j = y^{j_0}$.

(iv) *If* $|y| < \infty$, *then* $|G| = 2|y|$.

*Proof.* The proof of (i) and (ii) is based on the following observation. We have $xyx^{-1} = y^{-1}$, so by Lemma 1.65 (i) we have $xy^k x^{-1} = y^{-k}$ and thus

$$xy^k = y^{-k}x \text{ for all } k \in \mathbb{Z}. \tag{1.2}$$

This relation will allow us to write any product of involving $x$, $y$, and $y^{-1}$ in the form $x^i y^j$.

(i) By Lemma 1.39, every $g \in G$ can be written in the form $g = s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}$, where $s_i \in \{x, y\}$ and $\varepsilon_i \in \{1, -1\}$ for all $1 \leq i \leq n$. We will show that $g$ can be written in the form $x^i y^j$ for some $i, j \in \mathbb{Z}$. If $n = 0$ or $n = 1$ this is clear, so we suppose that $n > 1$ and proceed by induction on $n$. Then
$$g = s_1^{\varepsilon_1} \cdots s_{n-1}^{\varepsilon_{n-1}} s_n^{\varepsilon_n} = x^i y^j s_n^{\varepsilon_n}$$
by induction. If $s_n = x$, then $g = x^i(y^j x) = x^{i+1} y^{-j}$ by (1.2). If $s_n = y$, then $g = x^i y^j y^{\varepsilon_n} = x^i y^{j+\varepsilon_n}$. This completes the proof of (i).

(ii) If $i_0 = 0$, then $(x^i y^j)(x^{i_0} y^{j_0}) = x^{i+i_0} y^{j+j_0}$ as claimed. If $i_0 = 1$, then
$$(x^i y^j)(x^{i_0} y^{j_0}) = x^i (y^j x) y^{j_0} = x^i (x y^{-j}) y^{j_0} = x^{i+i_0} y^{-j+j_0}$$
by (1.2).

(iii) Suppose that $x^i y^j = x^{i_0} y^{j_0}$ for some $i, i_0 \in \{0,1\}$ and $j, j_0 \in \mathbb{Z}$. Then $x^{i-i_0} = y^{j_0-j}$, so from $x \notin \langle y \rangle$ it follows that $x^{i-i_0} = 1$. This implies $i = i_0$, and then from $x^i y^j = x^{i_0} y^{j_0}$ we conclude that $y^j = y^{j_0}$.

(iv) Follows from (i) and (iii).

□

As a consequence of Lemma 1.69, the structure of a dihedral group $G = \langle x, y \rangle$ with $|x| = 2$, $xyx^{-1} = y^{-1}$, and $x \notin \langle y \rangle$ is determined by the order of $y$. More precisely, we have the following result.

**Lemma 1.70.** *Let $G = \langle x, y\rangle$ and $H = \langle z, w\rangle$ be groups such that the following hold:*

- $|x| = 2$, $xyx^{-1} = y^{-1}$, *and* $x \notin \langle y\rangle$;
- $|z| = 2$, $zwz^{-1} = w^{-1}$, *and* $z \notin \langle w\rangle$.

*Then $G \cong H$ if and only if $|y| = |w|$.*

*Proof.* Suppose first that $G \cong H$. Then in particular $|G| = |H|$. If $G$ and $H$ have infinite order, then by Lemma 1.69 (iv) we must have $|y| = |w| = \infty$. Similarly if $|G| = |H|$ is finite, then $|G| = 2|y|$ and $|H| = 2|w|$ by Lemma 1.69 (iv), so $|y| = |w|$.

For the other direction, suppose that $|y| = |w|$. Apply Lemma 1.69 (i) – (iv) to conclude that we can define an isomorphism $\varphi : G \to H$ by $\varphi(x^i y^j) = z^i w^j$ for all $i, j \in \mathbb{Z}$. (The details are left as an exercise.) □

At this point we have essentially classified the dihedral groups, but we have not yet shown that they exist. One way to do this would be to use the multiplication rule in Lemma 1.69 (ii), in which case the main thing to check is that this defines an associative binary operation. We will later see this as part of a more general construction (semidirect products), so we will instead proceed with the following construction using symmetric groups.

We construct groups $G = \langle x, y\rangle$ such that $|x| = 2$, $xyx^{-1} = y^{-1}$, $x \notin \langle y\rangle$; for all possible values of $|y|$. In view of Lemma 1.70, this provides us with all dihedral groups up to isomorphism.

- $|y| = 1$: Consider $x, y \in S_2$ with $x = (1\ 2)$ and $y = (1)$. We denote $D_2 = \langle x, y\rangle$.
- $|y| = 2$: Consider $x, y \in S_4$ with $x = (1\ 2)$ and $y = (3\ 4)$. We denote $D_4 = \langle x, y\rangle$.
- $3 \leq |y| < \infty$: write $n = |y|$. Consider $x, y \in S_n$, where bijections $x, y : \{1, \dots, n\} \to \{1, \dots, n\}$ are defined by

  $$x(i) = n + 1 - i \text{ for all } 1 \leq i \leq n,$$

  and $y$ is the $n$-cycle

  $$y = (1\ 2\ \cdots\ n).$$

  We denote $D_{2n} = \langle x, y\rangle$. (Note that $D_6 = \langle (1\ 3), (1\ 2\ 3)\rangle = S_3$.)

- $|y| = \infty$: Consider $x, y \in \mathrm{Sym}(\mathbb{Z})$, where the bijections $x, y : \mathbb{Z} \to \mathbb{Z}$ are defined by

$$x(i) = -i \text{ for all } i \in \mathbb{Z},$$
$$y(i) = i + 1 \text{ for all } i \in \mathbb{Z}.$$

  We denote $D_\infty = \langle x, y \rangle$.

In all of the cases above, it is readily checked that $|x| = 2$, $xyx^{-1} = y^{-1}$, $x \notin \langle y \rangle$, and that $|y|$ is as claimed. We call $D_\infty$ the *infinite dihedral group*, and for $n \geq 1$ we call $D_{2n}$ *the dihedral group of order* $2n$.

**Theorem 1.71.** *Let $G$ be a dihedral group, say $G = \langle a, b \rangle$ with $|a| = |b| = 2$. The following statements hold:*

(i) *If $|ab|$ is infinite, then $G \cong D_\infty$.*

(ii) *If $|ab| = n$ is finite, then $G \cong D_{2n}$.*

*Proof.* By the proof of Lemma 1.68, for $x = a$ and $y = ab$ we have $G = \langle x, y \rangle$ with $|x| = 2$, $xyx^{-1} = y^{-1}$, and $x \notin \langle y \rangle$. Then the theorem follows from Lemma 1.70 and the construction of $D_\infty$ and $D_{2n}$. □

## 1.8 Quaternion group $Q_8$

An important example of a non-abelian group is the quaternion group of order 8, which is denoted by $Q_8$. We construct $Q_8$ as a group of $2 \times 2$ complex matrices as follows:

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

with

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad i = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix},$$
$$j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad k = \begin{pmatrix} 0 & \mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix},$$

where $\mathbf{i}$ denotes the imaginary unit $\mathbf{i}^2 = -1$ in $\mathbb{C}$. A calculation shows that the following relations hold:

$$i^2 = j^2 = k^2 = -1$$

$$ij = k = -ji$$
$$jk = i = -kj$$
$$ki = j = -ik$$

from which it follows that $Q_8$ is a non-abelian[8] subgroup of $\mathrm{GL}_2(\mathbb{C})$.

**Remark 1.72.** This construction is closely related to the quaternion algebra $\mathbb{H}$, which is isomorphic to the following $\mathbb{R}$-algebra of matrices:

$$\mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k = \left\{ \begin{pmatrix} a + b\mathbf{i} & c + d\mathbf{i} \\ -c + d\mathbf{i} & a - b\mathbf{i} \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

**Remark 1.73.** We have previously seen that the dihedral group $D_8$ is another example of a non-abelian group of order 8. However, we have $Q_8 \ncong D_8$. One way to see this is to note that $D_8$ and $Q_8$ do not have the same number of elements of order 2. (Exercise: For $G = D_8$ and $G = Q_8$, determine the order of each element.)

## 1.9 Cosets and products of subsets

Let $G$ be a group and $S, T \subseteq G$. We define the product of the subsets $S$ and $T$ by

$$ST = \{st : s \in S, t \in T\}.$$

Since the group operation is associative, we also have associativity for products of subsets: $A(BC) = (AB)C$ for any subsets $A, B, C \subseteq G$. It follows then that for any finite number of subsets $A_1$, $A_2$, …, $A_k \subseteq G$ the product $A_1A_2 \cdots A_k$ is uniquely determined and equals $\{a_1a_2 \cdots a_k : a_i \in A_i\}$.

For $g \in G$ and $S \subseteq G$, we define the left and right translates of $S$ by $g$ as

$$gS = \{gs : s \in S\},$$
$$Sg = \{sg : s \in S\},$$

respectively. Recall from Cayley's theorem (Theorem 1.66) that the left translation maps $x \mapsto gx$ and right translation maps $x \mapsto xg$ are bijections for all $g \in G$. Thus $|gS| = |Sg| = |S|$ for all $S \subseteq G$ and $g \in G$; moreover $S = T$ if and only if $gS = gT$ if and only if $Tg = Sg$ for all $S, T \subseteq G$ and $g \in G$.

[8] Quaternions were discovered by Hamilton in 1843. Here is a quote from the paper where he first defined quaternions: "*… though it must, at first sight, seem strange and almost unallowable, to define that the product of two imaginary factors in one order differs (in sign) from the product of the same factors in the opposite order ($ji = -ij$).*."

**Definition 1.74.** Let $H$ be a subgroup of a group $G$. A *left coset* is a subset of the form $gH$, where $g \in G$. Similarly, a *right coset* is a subset of the form $Hg$, where $g \in G$.

For any $H \leq G$, it is clear that $G$ is the union of left cosets: we have

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

Moreover, it follows from the next two lemmas that the left cosets of $H$ are pairwise disjoint: for all $a, b \in G$ we have either $aH = bH$ or $aH \cap bH = \emptyset$.

**Lemma 1.75.** *Let $H$ be a subgroup of a group $G$ and let $a \in G$. Then $aH = H$ if and only if $a \in H$.*

*Proof.* If $aH = H$, then $a \in H$ since $1 \in H$ and $a = a1$. Conversely if $a \in H$, then $aH \subset H$ is clear and $H \subseteq aH$ follows from $h = a(a^{-1}h)$ for all $h \in H$. □

**Lemma 1.76.** *Let $H$ be a subgroup of a group $G$ and let $a, b \in G$. The following statements are equivalent:*

(i) $aH = bH$,

(ii) $b^{-1}a \in H$,

(iii) $a \in bH$,

(iv) $b \in aH$,

*Proof.* We prove (i) ⇒ (ii) ⇒ (iii) ⇒ (iv) ⇒ (i):

(i) ⇒ (ii): We have $a \in aH = bH$, so $a = bh$ for some $h \in H$; therefore $b^{-1}a \in H$.

(ii) ⇒ (iii): If $b^{-1}a = h \in H$, then $a = bh \in bH$.

(iii) ⇒ (iv): If $a = bh$ for some $h \in H$, then $b = ah^{-1} \in aH$.

(iv) ⇒ (i): If $b = ah$ for some $h \in H$, then $a^{-1}b \in H$. By Lemma 1.75 we have $a^{-1}bH = H$, so multiplying both sides by $a$ gives $bH = aH$.

□

Analogously to Lemma 1.76, for right cosets we have $Ha = Hb$ if and only if $ba^{-1} \in H$ if and only if $a \in Hb$ if and only if $b \in Ha$. Therefore the right cosets of $H$ are also pairwise disjoint.

**Definition 1.77.** Let $H$ be a subgroup of $G$. Then the cardinality of the set of left cosets $\{aH : a \in G\}$ is called the *index* of $H$ in $G$ and denoted by $[G : H]$. (It is possible that $[G : H]$ is infinite. For example, for $H = \{1\}$ we have $[G : H] = |G|$.)

**Remark 1.78.** By the axiom of choice[9], we can always find a subset $S \subseteq G$ such that $S$ contains precisely one element from every left coset of $H$ in $G$. In other words:

- Any left coset of $H$ in $G$ is of the form $aH$ for some $a \in S$;
- For all $a, b \in S$ we have $aH = bH$ if and only if $a = b$.

Then $|S| = [G : H]$, and $G$ can be written as the disjoint union

$$G = \bigcup_{x \in S} xH.$$

Such a subset $S$ is called a *set of left coset representatives for $H$ in $G$*, or a *left transversal for $H$ in $G$*. A *right transversal* for right cosets of $H$ is defined analogously.

**Example 1.79.** Let $G = S_3$ and let $H$ be the subgroup $H = \{(1), (1\ 2)\}$. Then $[G : H] = 3$, and the left cosets of $H$ are

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

The right cosets of $H$ are

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

Note that $H$ is both a left and right coset, but neither $H(1\ 3)$ nor $H(2\ 3)$ is a equal to a left coset.

[9] The use of axiom of choice in this remark is unavoidable. It was shown in Theorem 1 of "K. Keremedis, *Some equivalents of AC in algebra. II.*, Algebra Universalis 39 (1998), no. 3–4, 163–169." that the axiom of choice holds if and only if every subgroup of every abelian group has a left transversal.

We could also define the index of a subgroup using right cosets, since the set of left cosets and the set of right cosets have the same cardinality[10]. In any case, since $|aH| = |H|$ for all $a \in G$, in the case of finite groups we get Lagrange's theorem:

**Theorem 1.80** (Lagrange's theorem)**.** *Let $G$ be a finite group and let $H \leq G$. Then $|H| \cdot [G : H] = |G|$. In particular, the order of $H$ divides the order of $G$.*

**Corollary 1.81.** *Let $G$ be a finite group and $g \in G$. Then $|g|$ divides $|G|$.*

*Proof.* The claim follows from Lagrange's theorem with $H = \langle g \rangle$, since $|H| = |g|$ by Lemma 1.42 (ii). □

**Corollary 1.82.** *Let $G$ be a finite group. Then $g^{|G|} = 1$ for all $g \in G$.*

*Proof.* Since $g^{|g|} = 1$, the claim follows from Corollary 1.81. □

**Corollary 1.83.** *Let $G$ be a finite group of prime order. Then $G$ is cyclic.*

*Proof.* Let $x \in G$ be a nontrivial element. Since $|x| > 1$ divides $|G|$, we have $|x| = |G|$ since $|G|$ is a prime number. Since $\langle x \rangle$ is a subgroup of order $|x|$ (Lemma 1.42 (ii)), we conclude that $G = \langle x \rangle$. □

From Corollary 1.83 and Lemma 1.43, it follows that $\mathrm{gnu}(p) = 1$ for all primes $p$.

**Example 1.84.** Let $G = S_3$. By Lagrange's theorem, we know that any subgroup of $G$ has order 1, 2, 3, or 6. We see then that $G$ has a total of 6 subgroups:

- Order 1: trivial subgroup $\{(1)\}$;
- Order 2: three cyclic subgroups $\langle (1\ 2) \rangle$, $\langle (1\ 3) \rangle$, and $\langle (2\ 3) \rangle$;
- Order 3: one cyclic subgroup $\langle (1\ 2\ 3) \rangle$;
- Order 6: the group $G$ itself.

**Example 1.85.** Let $G = Q_8$. As in the previous example, we can apply Lagrange's theorem to see that $G$ has a total of 6 subgroups:

- Order 1: trivial subgroup $\{1\}$;

[10] You can check that $aH \mapsto Ha^{-1}$ is a well-defined bijection between the left cosets and the right cosets of $H$ in $G$.

- Order 2: cyclic subgroup $\{1, -1\}$;
- Order 4: three cyclic subgroups $\langle i \rangle$, $\langle j \rangle$, and $\langle k \rangle$;
- Order 8: the group $G$ itself.

**Lemma 1.86.** *Let $K \leq H \leq G$. Then:*

(i) *$[G : K]$ is finite if and only if both $[G : H]$ and $[H : K]$ are finite.*

(ii) *If $[G : K]$ is finite, then $[G : K] = [G : H][H : K]$.*

*Proof.* Let $X$ be a set of left coset representatives for $H$ in $G$, and let $Y$ be a set of left coset representative for $K$ in $H$ (Remark 1.78).

We will show that $Z = \{xy : x \in X, y \in Y\}$ is a set of left coset representatives for $K$ in $G$, and that $|Z| = |X \times Y|$. Indeed, consider a left coset $gK$, where $g \in G$. Then $g \in xH$ for some $x \in X$, so $g = xh$ for some $h \in H$. Now $h \in yK$ for some $y \in Y$, so $g \in xyK$. Thus every left coset of $H$ is of the form $zK$ for some $z \in Z$.

Next we show that if $xyK = x'y'K$ for some $x, x' \in X$ and $y, y' \in Y$, then $x = x'$ and $y = y'$. To this end, if $xyK = x'y'K$, then $xy \in x'y'K$, and thus $x \in x'H$ since $y, y' \in H$. Therefore $x = x'$ since $X$ is a set of left coset representatives for $H$ in $G$. Thus $xyK = xy'K$, which implies $yK = y'K$ and so $y = y'$ since $Y$ is a set of left coset representatives for $K$ in $H$.

We have seen that $Z$ is a set of left coset representatives for $K$, and moreover we have proven that $[G : K] = |Z| = |X \times Y|$. Since $|X| = [G : H]$ and $|Y| = [H : K]$, both claims (i) and (ii) follow. □

**Lemma 1.87.** *Let $H$ and $K$ be a subgroups of a group $G$. Suppose that $[G : H]$ and $[G : K]$ are finite. Then $[G : H \cap K]$ is finite, and $[G : H \cap K] \leq [G : H][G : K]$.*

*Proof.* Each left coset of $H \cap K$ is the intersection of a left coset of $H$ and a left coset of $K$, since $g(H \cap K) = gH \cap gK$ for all $g \in G$. Thus $H \cap K$ has only finitely many left cosets, and the total number is at most $[G : H][G : K]$. □

**Lemma 1.88.** *Let $G$ be a group and let $H$ and $K$ be finite subgroups of $G$. Then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

*Proof.* We have

$$HK = \bigcup_{h \in H} hK$$

and each left coset of $K$ has size $|K|$, so $|HK| = s|K|$, where $s$ is the number of left cosets of the form $hK$ with $h \in H$.

We show next that $s = [H : H \cap K]$. To this end, we can apply Lemma 1.76. For $x, y \in H$ we have $xK = yK$ if and only if $y^{-1}x \in H \cap K$. Therefore $xK = yK$ if and only if $x(H \cap K) = y(H \cap K)$, from which it follows that the sets $\{hK : h \in H\}$ and $\{h(H \cap K) : h \in H\}$ have the same size. In other words $s = [H : H \cap K]$, so by Lagrange's theorem

$$|HK| = [H : H \cap K]|K| = \frac{|H||K|}{|H \cap K|}.$$

as claimed. □

**Lemma 1.89.** *Let $H$ and $K$ be subgroups of a group $G$. Then $HK$ is a subgroup if and only if $HK = KH$.*

*Proof.* Exercise. □

## 1.10 Normal subgroups and quotient groups

Given a group $G$, we are interested in finding its subgroups and homomorphic images. Subgroups are found inside of the group $G$, and using *normal subgroups* we can construct all possible groups of the form $\varphi(G)$, where $\varphi : G \to H$ is a homomorphism.

**Definition 1.90.** Let $G$ be a group and let $N \leq G$. We say that $N$ is a *normal subgroup of $G$*, if $g^{-1}Ng = N$ for all $g \in G$. We denote this by $N \trianglelefteq G$.

**Example 1.91.** (a) In any group $G$, the trivial subgroup $\{1\}$ and the group $G$ itself are normal subgroups of $G$.

(b) Let $G$ be abelian. Then every subgroup of $G$ is a normal subgroup.

(c) Let $G = S_3$. Then the cyclic subgroup $\langle(1\ 2\ 3)\rangle$ of order 3 is a normal subgroup of $G$, but the cyclic subgroup $H = \langle(1\ 2)\rangle$ is not normal: we have $g^{-1}Hg = \langle(1\ 3)\rangle$ or $g^{-1}Hg = \langle(2\ 3)\rangle$ for $g \in G \setminus H$.

(d) Exercise: Show that if $H \leq G$ with $[G : H] = 2$, then $H \trianglelefteq G$.

(e) Exercise: Show that every subgroup of $Q_8$ is normal.

(f) The property of being a subgroup is transitive: $H \leq K \leq G$ implies $H \leq G$. The same is not true for normality. Let $G = D_8 = \langle x, y\rangle$ with $|x| = 2$, $|y| = 4$, and $xyx^{-1} = y^{-1}$. Then for $H = \langle x\rangle$ and $K = \langle x, y^2\rangle$ we have $H \trianglelefteq K \trianglelefteq G$ but $H \not\trianglelefteq G$.

**Lemma 1.92.** *Let $G$ be a group and let $N \leq G$. The following statements are equivalent:*

(i) *$N$ is a normal subgroup;*

(ii) *$gN = Ng$ for all $g \in G$;*

(iii) *$(xN)(yN) = xyN$ for all $x, y \in G$.*

(iv) *$g^{-1}Ng \subseteq N$ for all $g \in G$;*

*Proof.* We prove (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i):

(i) $\Rightarrow$ (ii): Since $g^{-1}Ng = N$ for all $g \in G$, we have $g(g^{-1}Ng) = gN$ and thus $Ng = gN$ for all $g \in G$.

(ii) $\Rightarrow$ (iii): By associativity and (ii), we have $(xN)(yN) = x(Ny)N = x(yN)N = xyNN = xyN$ for all $x, y \in G$.

(iii) $\Rightarrow$ (iv): For all $g \in G$, we have $(g^{-1}N)(gN) = N$, so $(g^{-1}Ng)N = N$, which implies $g^{-}Ng \subseteq N$.

(iv) $\Rightarrow$ (i): We have $g^{-1}Ng \subseteq N$ for all $g \in G$. Applying this with $g^{-1}$ this gives $gNg^{-1} \subseteq N$, so $N = g^{-1}(gNg^{-1})g \subseteq g^{-1}Ng$ for all $g \in G$. Thus $g^{-1}Ng = N$ for all $g \in G$.

□

**Lemma 1.93.** *Let $G$ and $H$ be groups and let $\varphi : G \to H$ be a homomorphism. The following statements hold:*

(i) *$\operatorname{Ker}\varphi$ is a normal subgroup of $G$.*

(ii) *If $N \trianglelefteq G$, then $\varphi(N) \trianglelefteq \varphi(G)$.*

(iii) *If $K \trianglelefteq H$, then $\varphi^{-1}(K) \trianglelefteq G$.*

*Proof.* (i) We know that $\operatorname{Ker}\varphi$ is a subgroup by Lemma 1.63 (i). It is a normal subgroup since $\varphi(x) = 1$ implies $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)\varphi(g^{-1}) = 1$ for all $g \in G$.

(ii) We have $\varphi(N) \leq \varphi(G)$ by Lemma 1.63 (iv). For all $g \in G$ we have $\varphi(g)^{-1}\varphi(N)\varphi(g) = \varphi(g^{-1}Ng) = \varphi(N)$, since $N$ is normal, so $\varphi(N) \trianglelefteq \varphi(G)$.

(iii) We have $\varphi^{-1}(K) \leq G$ by Lemma 1.63 (v). For all $g \in G$ and $x \in \varphi^{-1}(K)$, we have $\varphi(g^{-1}xg) = \varphi(g)^{-1}\varphi(x)\varphi(g) \in K$ since $\varphi(x)$ and $K \trianglelefteq G$. This shows that $g^{-1}xg \in \varphi^{-1}(K)$ for all $g \in G$ and $x \in \varphi^{-1}(K)$, so by Lemma 1.92 we have $\varphi^{-1}(K) \trianglelefteq G$.

□

The main importance of normal subgroups is they can be used to construct *quotient groups*, which turn out to be precisely the homomorphic images of a group[11]. This construction proceeds as follows. Let $N \trianglelefteq G$. We consider the set

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

of left cosets of $N$ in $G$. For $X, Y \in G/N$, the product $XY$ (product of subsets of $G$) is also in $G/N$ by Lemma 1.92 (iii). Thus we can define a binary operation $\cdot$ on $G/N$ by

$$X \cdot Y = XY \text{ for all } X, Y \in G/N.$$

Note that by Lemma 1.92 (iii), we have

$$(xN) \cdot (yN) = xyN$$

for all $x, y \in G$. This makes it clear that $(G/N, \cdot)$ is a group: associativity holds since it holds in $G$, the identity element is $N$, and $(xN)^{-1} = x^{-1}N$ for all $x \in G$.

**Definition 1.94.** Let $G$ be a group and $N \trianglelefteq G$. We call the group $(G/N, \cdot)$ the *quotient group of $G$ modulo $N$*.

Note that for $N \trianglelefteq G$ we have $|G/N| = [G : N]$, so by Lagrange's theorem $|G/N| = |G|/|N|$ if $G$ is finite.

**Remark 1.95.** We emphasize that the construction of the quotient group $G/N$ only makes sense when $N$ is a normal subgroup.

Indeed, consider a subgroup $H \leq G$ which is not normal. By Lemma 1.92 (iv), we can find a $g \in G$ be such that $g^{-1}Hg \not\subseteq H$. We claim then that the product of left cosets $(g^{-1}H)(gH)$ is not a left coset. If this were the case, then $g^{-1}HgH = xH$ for some $x \in G$. But $1 \in g^{-1}HgH$, so $1 \in xH$ which implies $x \in H$. Therefore $g^{-1}HgH = H$, from which we conclude that $g^{-1}Hg \subseteq H$, a contradiction. Therefore $(g^{-1}H)(gH)$ is not a left coset, which means that we cannot define the binary operation on $G/N$ as above.

[11] See Remark 1.99 below.

**Example 1.96.** (a) In Example 1.5, the construction of $\mathbb{Z}/n\mathbb{Z}$ is precisely the construction of the quotient group of $\mathbb{Z}$ by the normal subgroup $n\mathbb{Z}$.

(b) For $N = G$, the quotient $G/N = \{G\}$ is trivial.

(c) For $N = \{1\}$, the left cosets $N$ in $G$ are singletons $\{g\}$, $g \in G$. Multiplication in $G/N$ is defined as $\{g\} \cdot \{h\} = \{gh\}$ for all $g, h \in G$, so it is obvious that $G/N \cong G$.

(d) Let $G = S_3$ and consider the normal subgroup $N = \langle (1\ 2\ 3) \rangle$. Then $G/N = \{N, (1\ 2)N\}$, and $G/N \cong C_2$.

**Theorem 1.97.** *Let $G$ be a group and let $N$ be a normal subgroup of $G$. Then the map $\pi : G \to G/N$ defined by $x \mapsto xN$ is a surjective homomorphism with $\operatorname{Ker} \pi = N$.*

*Proof.* It is clear that $\pi$ is surjective, and $\pi$ is a homomorphism since we have $(xN)(yN) = xyN$ by definition. The fact that $\operatorname{Ker} \pi = N$ follows from Lemma 1.75. □

We will call the homomorphism $\pi : G \to G/N$ in Theorem 1.97 the *canonical homomorphism for $N$*.

**Theorem 1.98.** *Let $G$ be a group and let $\varphi : G \to H$ be a homomorphism. Then $G/\operatorname{Ker} \varphi \cong \varphi(G)$, with an isomorphism given by $x \operatorname{Ker} \varphi \mapsto \varphi(x)$.*

*Proof.* Consider the map $\psi : G/\operatorname{Ker} \varphi \to \varphi(G)$ defined by $\psi(x \operatorname{Ker} \varphi) = \varphi(x)$ for all $x \in G$. By Lemma 1.63 (ii) and Lemma 1.76, we have $x \operatorname{Ker} \varphi = y \operatorname{Ker} \varphi$ if and only if $\varphi(x) = \varphi(y)$, so $\psi$ is well-defined and injective. Moreover $\psi$ is clearly surjective, and it is a homomorphism since $\varphi$ is. Therefore $\psi$ is an isomorphism and $G/\operatorname{Ker} \varphi \cong \varphi(G)$. □

**Remark 1.99.** By Theorem 1.97 and Theorem 1.98, a group is isomorphic to a homomorphic image of $G$ if and only if it is isomorphic to $G/N$ for some $N \trianglelefteq G$.

Theorem 1.98 is sometimes called the *first isomorphism theorem*. We will next prove the rest of the standard isomorphism theorems for groups.

**Theorem 1.100.** *Let $G$ be a group, let $H \leq G$ and $K \trianglelefteq G$. Then $HK \leq G$, $H \cap K \trianglelefteq H$ and*

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

*Proof.* By Lemma 1.92 we have $hK = Kh$ for all $h \in H$. Therefore $HK = KH$, so $HK$ is a subgroup by Lemma 1.89. Since $H$ and $K$ are subgroups we have $H \cap K \leq H$, and moreover $H \cap K$ is a normal subgroup of $H$ since $h^{-1}(H \cap K)h = H \cap h^{-1}Kh = H \cap K$ for all $h \in H$.

Finally consider the map $\varphi : H \to HK/K$ defined by $\varphi(x) = xK$ for all $x \in K$. It is clear that $\varphi$ is a homomorphism, and $\varphi$ is surjective since $hkK = hK = \varphi(h)$ for all $h \in H$ and $k \in K$ by Lemma 1.75. By Lemma 1.75 we have $\operatorname{Ker}\varphi = H \cap K$, so

$$H/H \cap K \cong HK/K$$

follows from Theorem 1.98. □

**Theorem 1.101.** *Let $G$ be a group and let $M$ and $N$ be normal subgroups of $G$ such that $M \leq N$. Then $M/N$ is a normal subgroup of $G/N$ and*

$$\frac{G/N}{M/N} \cong G/M.$$

*Proof.* Let $\pi : G \to G/N$ be the canonical homomorphism. We define

$$\varphi : G \to \frac{G/N}{M/N},\ \varphi(g) = \pi(g)(M/N) \text{ for all } g \in G.$$

We leave it as an exercise to check that $\varphi$ is a surjective homomorphism with $\operatorname{Ker}\varphi = M$. It follows then from Theorem 1.98 that

$$G/M \cong \frac{G/N}{M/N},$$

as claimed. □

**Theorem 1.102** (Correspondence theorem)**.** *Let $G$ be a group, $N \trianglelefteq G$, and let $\pi : G \to G/N$ be the canonical homomorphism. The following statements hold:*

(i) *For all $H \leq G$ we have $\pi(H) = HN/N$.*

(ii) *For all $N \leq M \leq G$, we have $\pi^{-1}(M/N) = M$.*

(iii) *If $N \leq M \leq G$, then $M/N \leq G/N$.*

(iv) *Every subgroup of $G/N$ is of the form $M/N$ for a unique subgroup $N \leq M \leq G$.*

(v) *Let $N \leq M \leq G$. Then $M \trianglelefteq G$ if and only if $M/N \trianglelefteq G/N$.*

*Proof.* (i) By Theorem 1.100 the product $HN$ is a group, so we can form the quotient $HN/N$. For all $h \in H$ and $n \in N$ we have $hnN = hN = \pi(h)$ by Lemma 1.75, so it follows that $HN/N = \pi(H)$.

(ii) It is clear that $M \subseteq \pi^{-1}(M/N)$. Conversely if $x \in \pi^{-1}(M/N)$, then $xN = yN$ for some $y \in M$. This implies $x \in yN$, which gives $x \in M$ by $N \leq M$. Therefore $\pi^{-1}(M/N) \subseteq M$.

(iii) By (i) $M/N$ is the image of $M$ under $\pi$, so it is a subgroup by Lemma 1.63 (iv).

(iv) Let $X \leq G/N$. Consider $M = \pi^{-1}(X)$. It is easy to see that $N \leq M \leq G$, and moreover we have $\pi(M) = \pi(\pi^{-1}(X)) = X$ since $\pi$ is surjective. Thus $X = \pi(M) = M/N$ by (i). Uniqueness of $M$ is immediate from (ii).

(v) If $M \trianglelefteq G$, then $M/N = \pi(M) \trianglelefteq G/N$ by (i) and Lemma 1.93 (ii). Conversely, if $M/N \trianglelefteq G/N$, then $M = \pi^{-1}(M/N) \trianglelefteq G$ by (ii) and Lemma 1.93 (iii).

□

**Definition 1.103.** A group $G$ is said to be *simple* if $G \neq \{1\}$ and the only normal subgroups of $G$ are $\{1\}$ and $G$.

**Example 1.104.** The abelian simple groups are known:

(a) If $G$ is cyclic of prime order, then $G$ has only two subgroups; $\{1\}$ and $G$ itself. Therefore $G$ is simple.

(b) Exercise: If $G$ is abelian, then $G$ is simple if and only if $G$ is cyclic of prime order.

**Remark 1.105.** Suppose that $G$ is a non-trivial finite group. Let $N_1 \triangleleft G$ be a proper normal subgroup such that $|N_1|$ is as large as possible. Then there are no normal subgroups of $G$ with $N_1 \leq M \trianglelefteq G$ other than $M = G$ and $M = N_1$, so by the correspondence theorem $G/N_1$ is simple. If $N_1 = \{1\}$ then $G$ is simple, otherwise by the same argument we can find a proper normal subgroup $N_2 \triangleleft N_1$ such that $N_1/N_2$ is simple. Continuing in this manner, we eventually construct a series

$$G = N_0 \triangleright N_1 \triangleright N_2 \triangleright \cdots \triangleright N_t \triangleright N_{t+1} = \{1\}$$

such that $N_i/N_{i+1}$ is simple for all $0 \leq i \leq t$. Such a series is called a *composition series*. (In a later section we will prove the Jordan-Hölder theorem, which states that the isomorphism types of the simple factors occurring in a composition series are unique.)

So a finite group is made up of simple groups, and this suggests an inductive approach towards understanding all finite groups ("Hölder program"):

(1) Determine all finite simple groups.

(2) (Extension problem) Given two finite groups $A$ and $B$, determine all finite groups $G$ with a normal subgroup $N$ such that $N \cong A$ and $G/N \cong B$.

One of the biggest achievements in group theory is the solution to (1): the classification of finite simple groups (CFSG). It has been shown that any finite simple group is isomorphic to one of the following:

- Cyclic of prime order;
- Alternating group $A_n$ with $n \geq 5$; (defined in a later section)
- A group of Lie type;
- One of the 26 *sporadic* simple groups. (See Table 2.)

The original proof of the classification consisted of hundreds of articles totalling tens of thousands of pages, starting from around 1955 with the Brauer–Fowler theorem and finishing in 2004 with the Aschbacher–Smith volume on quasithin groups. A second-generation proof led by Gorenstein–Lyons–Solomon is in progress, and as of 2021 a total of 9 volumes have been published (AMS Mathematical Surveys and Monographs).

What about the extension problem? This is completely infeasible in general, one reason being that we cannot even expect to classify all finite $p$-groups. However, there are many interesting things to be said about *extensions* of two groups $A$ and $B$ — meaning groups $G$ with a normal subgroup $N$ such that $N \cong A$ and $G/N \cong B$. We will later find various ways of constructing and recognizing such extensions.

| Group | Order | Year |
|---|---|---|
| $M_{11}$ | $2^4 \cdot 3^2 \cdot 5 \cdot 11$ | 1895 |
| $M_{12}$ | $2^6 \cdot 3^3 \cdot 5 \cdot 11$ | 1899 |
| $M_{22}$ | $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ | 1900 |
| $M_{23}$ | $2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ | 1900 |
| $M_{24}$ | $2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$ | 1900 |
| $J_1$ | $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$ | 1966 |
| $J_2$ | $2^7 \cdot 3^3 \cdot 5^2 \cdot 7$ | 1967 |
| $J_3$ | $2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$ | 1969 |
| $J_4$ | $2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$ | 1975 |
| $\mathrm{Co}_1$ | $2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$ | 1969 |
| $\mathrm{Co}_2$ | $2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$ | 1969 |
| $\mathrm{Co}_3$ | $2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$ | 1969 |
| $\mathrm{Fi}_{22}$ | $2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | 1969 |
| $\mathrm{Fi}_{23}$ | $2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$ | 1969 |
| $\mathrm{Fi}'_{24}$ | $2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$ | 1969 |
| HS | $2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$ | 1968 |
| McL | $2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$ | 1969 |
| He | $2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$ | 1969 |
| Ru | $2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$ | 1972 |
| Suz | $2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$ | 1969 |
| O'N | $2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$ | 1973 |
| HN | $2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$ | 1974 |
| Ly | $2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$ | 1971 |
| Th | $2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$ | 1974 |
| B | $2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$ | 1974 |
| M | $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$ | 1974 |

Table 2: The sporadic simple groups, their orders, and the year when they were first discovered.

## 1.11 Conjugacy classes of elements

**Definition 1.106.** Let $G$ be a group. We say that two elements $g, h \in G$ are *conjugate in* $G$, if there exists $x \in G$ such that $h = x^{-1}gx$. We will denote $g^x := x^{-1}gx$.

Two conjugate elements of a group are "similar" and many of their properties (as elements of $G$) are the same. For example, they must have the same order (Lemma 1.65 (ii)). As seen in the next example, in general linear groups conjugacy corresponds to the similarity of matrices and to change of basis.

**Example 1.107.** Let $V$ be a finite-dimensional vector space over a field $\mathbb{F}$. Let $f, g \in \mathrm{GL}(V)$. Let $e_1, \ldots, e_n$ be a basis of $V$ and let $(A_{ij})$ be the matrix of $f$ with respect to this basis, so $f(e_i) = \sum_{j=1}^n A_{ji}e_j$ for all $1 \leq i \leq n$.

Suppose that $g$ is conjugate to $f$, say $g = p^{-1}fp$ for some $p \in \mathrm{GL}(V)$. Let $e_1', \ldots, e_n'$ be the basis of $V$ defined by $e_i' := p^{-1}(e_i)$ for all $1 \leq i \leq n$. Then it is immediate that $g(e_i') = \sum_{j=1}^n A_{ji}e_j'$ for all $1 \leq i \leq n$. In other words, the matrix of $g$ is the same as that of $f$, just with respect to a different basis. Conversely, if $g$ is obtained from $f$ by a change of basis, then $g$ and $f$ are conjugate in $\mathrm{GL}(V)$.

For $g, h \in G$, denote $g \sim h$ if $g$ and $h$ are conjugate in $G$. It is easy to see that $\sim$ is an equivalence relation:

- $g \sim g$, since $g = x^{-1}gx$ for $x = 1_G$;
- If $g \sim g'$ with $g' = x^{-1}gx$, then $g = y^{-1}g'y$ with $y = x^{-1}$; thus $g' \sim g$;
- If $g \sim g'$ and $g' \sim g''$ with $g' = x^{-1}gx$ and $g'' = y^{-1}g'y$, then $g'' = (xy)^{-1}gxy$; thus $g \sim g''$.

The equivalence class of $g \in G$ under $\sim$ is called the *conjugacy class of* $x$ *in* $G$ and denoted by $x^G$. Then $G$ is partitioned into a disjoint union of conjugacy classes, and the conjugacy class of $x$ in $G$ is

$$x^G = \{g^{-1}xg : g \in G\}.$$

An element $y \in x^G$ is called a *representative* of the conjugacy class $x^G$.

**Example 1.108.** If $G$ is an abelian group, then $x^G = \{x\}$ for all $x \in G$.

**Example 1.109.** Let $G = S_n$ and consider a $k$-cycle $\sigma = (i_1 \ \cdots \ i_k)$. As an exercise, show that for all $g \in S_n$, we have

$$g(i_1 \ \cdots \ i_k)g^{-1} = (g(i_1) \ \cdots \ g(i_k)).$$

Conclude that $\sigma^G = \{g \in G : g \text{ is a } k\text{-cycle}\}$.

**Example 1.110.** Let $G = S_3$. Then $G$ has three conjugacy classes: $\{(1)\}$ (trivial element), $\{(1\ 2), (1\ 3), (2\ 3)\}$ (2-cycles), and $\{(1\ 2\ 3), (1\ 3\ 2)\}$ (3-cycles).

**Example 1.111.** Let $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Exercise: determine the conjugacy classes of $Q_8$ (there are a total of five).

**Lemma 1.112.** *Let $G$ be a group and $H \leq G$. Then $H \trianglelefteq G$ if and only if $H$ is a union of conjugacy classes of $G$.*

*Proof.* If $H$ is a union of conjugacy classes of $G$, then $H \trianglelefteq G$ since $g\mathscr{C}g^{-1} = \mathscr{C}$ for any conjugacy class $\mathscr{C}$ and $g \in G$. Conversely, suppose that $H \trianglelefteq G$. Then for all $x \in H$ we have $x^G \subseteq H$ since $gxg^{-1} \in H$ for all $g \in G$, and therefore $H$ is the union of the conjugacy classes of its elements. □

**Definition 1.113.** Let $G$ be a group and $x \in G$. The *centralizer of $x$ in $G$* is $C_G(x) = \{g \in G : gx = xg\}$, i.e., the set of all elements of $G$ that commute with $x$.

**Lemma 1.114.** *Let $G$ be a group. Then:*

(i) *$C_G(x)$ is a subgroup of $G$ for all $x \in G$.*

(ii) *$|x^G| = [G : C_G(x)]$ for all $x \in G$. In particular if $G$ is finite, then $|x^G|$ divides $|G|$.*

*Proof.* (i) It is clear that $1 \in C_G(x)$ for all $x \in G$. Suppose that $g, h \in C_G(x)$. Then $(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh)$, so $gh \in C_G(x)$ and $C_G(x)$ is closed under multiplication. We have $gx = xg$, and multiplying this equation from the left and the right with $g^{-1}$ gives $xg^{-1} = g^{-1}x$, in other words $g^{-1} \in C_G(x)$. Thus $C_G(x)$ is closed under taking inverses and is a subgroup.

(ii) For $a, b \in G$ we have $axa^{-1} = bxb^{-1}$ if and only if $(b^{-1}a)x = x(b^{-1}a)^{-1}$, i.e. $b^{-1}a \in C_G(x)$. Therefore $axa^{-1} = bxb^{-1}$ if and only if $aC_G(x) = bC_G(x)$, so the map $axa^{-1} \mapsto aC_G(x)$ is a well-defined bijection between the sets $x^G$ and $\{aC_G(x) : a \in G\}$. Thus $|x^G| = [G : C_G(x)]$.

□

**Definition 1.115.** Let $G$ be a group. The *center of $G$* is defined as

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

Note that $Z(G)$ is a subgroup, since it is the intersection of all centralizers of $G$.

**Lemma 1.116.** *Let $G$ be a group. Then $Z(G) \trianglelefteq G$, and any subgroup of $Z(G)$ is a normal subgroup of $G$.*

*Proof.* Follows from the fact that $g^{-1}xg = x$ for all $x \in Z(G)$. □

**Example 1.117.** Some basic facts:

(i) A group $G$ is abelian if and only if $G = Z(G)$.

(ii) For $g \in G$, we have $g \in Z(G)$ if and only if $g^G = \{g\}$.

(iii) Exercise: For all $n \geq 3$, we have $Z(S_n) = \{1\}$.

(iv) Let $G = S_3$. Then $C_G(x) = \langle x \rangle$ for all $x \in G \setminus \{1\}$. For $G = S_4$ and $x = (1\ 2)$, we have $C_G(x) = \{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$.

(v) Exercise: If $G/Z(G)$ is cyclic, then $G$ is abelian.

(vi) Exercise: Let $N \trianglelefteq G$ be such that $|N| = 2$. Prove that $N \leq Z(G)$.

**Definition 1.118.** For any subset $S \subset G$, we define the centralizer of $S$ as

$$C_G(S) = \{g \in G : gx = xg \text{ for all } x \in S\}.$$

Similarly to the center, we see that $C_G(S)$ is a subgroup since it is the intersection of the centralizers of elements of $S$. In particular, we have $C_G(H) \leq G$ for any $H \leq G$.

**Proposition 1.119** (Class equation)**.** *Let $G$ be a finite group. Let $x_1, \ldots, x_t$ be representatives for the conjugacy classes of $G$ with more than one element. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)].$$

*Proof.* Since a conjugacy class $x^G$ has size 1 if and only if $x \in Z(G)$, we have a disjoint union

$$G = Z(G) \cup \bigcup_{i=1}^{t} x_i^G.$$

Thus $|G| = |Z(G)| + \sum_{i=1}^{t} |x_i^G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)]$ by Lemma 1.114. □

## 1.12 Cauchy's theorem

As an application of the class equation, we will prove Cauchy's theorem.

**Theorem 1.120** (Cauchy's theorem)**.** *Let $p$ be a prime. If $G$ is a finite group such that $p \mid |G|$, then $G$ contains an element of order $p$.*

*Proof.* By induction on $|G|$, the theorem being vacuously true when $|G| = 1$. We can suppose then that $|G| > 1$ and $p \mid |G|$. By the class equation, we have

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)], \tag{1.3}$$

where $x_1, \ldots, x_t$ are representatives for the non-central conjugacy classes, i.e. $x_i \notin Z(G)$.

If $p \mid |C_G(x_i)|$ for some $1 \leq i \leq t$, then we are done by applying induction on $C_G(x_i)$.

Thus we may assume that $p \nmid |C_G(x_i)|$ for all $1 \leq i \leq t$, in which case we must have $p \mid [G : C_G(x_i)]$ for all $1 \leq i \leq t$. By (1.3) it follows that $p \mid |Z(G)|$. If $Z(G) \neq G$ we are again done by applying induction on $Z(G)$.

Thus we can assume that $G = Z(G)$, in which case $G$ is abelian. Let $x \in G$ be a non-identity element. If $p$ divides $|x|$, then a suitable power of $x$ will be an element of order $p$ (Lemma 1.27 (iii)). If $p$ does not divide $|x|$, then $p$ must divide the order of $G/\langle x \rangle$. In this case, by induction the image of some $g \in G$ in $G/\langle x \rangle$ has order $p$. Then $|g|$ is divisible by $p$, so a suitable power of $g$ will be an element of order $p$ in $G$. □

**Remark 1.121.** Can we generalize Cauchy's theorem? That is, suppose that $n$ is an integer that divides $|G|$, not necessarily a prime. Must $G$ contain an element of order $n$? Certainly this is not true in general, for example if $G$ is non-cyclic of order $n$. (Explicit example: $G = S_3$ has order divisible by 6, but $G$ does not contain an element of order 6.) Problem: Suppose that $n$ is not a prime number. Does there exist a finite group $G$ such that $n$ divides $|G|$, but $G$ has no element of order $n$?

As an example application of Cauchy's theorem, we will classify groups of order $2p$, where $p$ is a prime.

**Theorem 1.122.** *Let $G$ be a group such that $|G| = 2p$, where $p > 2$ is a prime. Then $G \cong C_{2p}$ or $G \cong D_{2p}$.*

*Proof.* By Cauchy's theorem, there exists $x, y \in G$ with $|x| = 2$ and $|y| = p$. We have $\langle y \rangle \triangleleft G$ since $\langle y \rangle$ has index 2 in $G$ (Example 1.91 (iv)), so $xyx^{-1} = y^i$ for some $i \in \mathbb{Z}$. Since $x^2 = 1$, we have

$$y = x^2 y x^{-2} = x y^i x^{-1} = (xyx^{-1})^i = y^{i^2},$$

so $i^2 \equiv 1 \mod p$. Since $p$ is prime, this implies $i \equiv \pm 1 \mod p$. If $i \equiv 1 \mod p$, then $xy = yx$. Thus $|xy| = 2p$ by Lemma 1.29, so $G = \langle xy \rangle \cong C_{2p}$. If $i \equiv -1 \mod p$, then $xyx^{-1} = y^{-1}$. In this case $G$ is dihedral (Lemma 1.68), so by Theorem 1.71 we have $G \cong D_{2p}$. □

Since $D_6 = S_3$, in particular we have proven the following result[12].

**Corollary 1.123** (Cayley, 1854)**.** *Let $G$ be a group such that $|G| = 6$. Then $G \cong C_6$ or $G \cong S_3$.*

Cauchy's theorem tells us that if $p$ is a prime dividing the order of a finite group $G$, then $G$ contains an element of order $p$. What can we say about the number of elements of order $p$?

**Theorem 1.124.** *Let $G$ be a finite group and let $p$ be a prime such that $p \mid |G|$. Then the number of $x \in G$ such that $x^p = 1$ is a multiple of $p$.*

*Proof.* By Cauchy's theorem, there exists an element of order $p$ in $G$, which generates subgroup $U \leq G$ of order $|U| = p$. We will use $U$ to partition the set $\Omega = \{x \in G : x^p = 1\}$ into pieces of size $p$, which implies $|\Omega| \equiv 0 \mod p$.

For $x \in G$, define

$$[x] := \begin{cases} xU, & \text{if } x \in C_G(U). \\ \{uxu^{-1} : u \in U\}, & \text{if } x \notin C_G(U). \end{cases}$$

It is an exercise (Exercise 1.33) to prove that the sets $[x]$ partition $G$, in other words for all $x, y \in G$ we have $[x] = [y]$ or $[x] \cap [y] = \emptyset$. Moreover, $[x]$ contains $p$ elements for all $x \in G$. Thus the sets $[x]$ partition $G$ into pieces of size $p$.

We now claim that the sets $[x]$ also partition $\Omega$, which proves the theorem. To this end, it will suffice to prove that for $x \in \Omega$, we have $[x] \subseteq \Omega$. Indeed, if $x \in C_G(U)$, then $(xu)^p = x^p u^p = 1$ for all $u \in U$, so $[x] = xU \subseteq \Omega$. If $x \notin C_G(U)$, then $(uxu^{-1})^p = ux^p u^{-1} = 1$, so $uxu^{-1} \in \Omega$ for all $u \in U$. Therefore $[x] = \{uxu^{-1} : u \in U\} \subseteq \Omega$. □

[12]Proven by Cayley in 1854. Two decades later, in a paper (American Journal of Mathematics , Vol. 1, No. 1 (1878), pp. 50–52) Cayley states (mistakenly) the following:

"*... if $n = 6$, there are three groups, a group 1, $\alpha$, $\alpha^2$, $\alpha^3$, $\alpha^4$, $\alpha^5$ ($\alpha^6 = 1$); and two groups 1, $\beta$, $\beta^2$, $\alpha$, $\alpha\beta$, $\alpha\beta^2$ ($\alpha^2 = 1$, $\beta^3 = 1$), viz: in the first of these $\alpha\beta = \beta\alpha$; while in the other of them we have $\alpha\beta = \beta^2\alpha$ ...*"

**Remark 1.125.** A more general result was proven by Frobenius in 1895. He showed that if $G$ is a finite group and $n \mid |G|$, then the number of $x \in G$ such that $x^n = 1$ is a multiple of $n$. There are several proofs of this Frobenius' theorem, but none of them are very short.

Frobenius also conjectured that if $n$ divides $|G|$ and if the number of solutions to $x^n = 1$ is exactly $n$, then the set of solutions forms a subgroup. Almost 100 years later, Frobenius' conjecture was proven by Iiyori and Yamaki (1991), using the classification of finite simple groups.

Recall the notation $o_d(G)$ for the number of elements of order $d$ in $G$.

**Corollary 1.126.** *Let $G$ be a finite group and let $p$ be a prime such that $p \mid |G|$. Then $o_p(G) \equiv -1 \mod p$.*

*Proof.* Follows from Theorem 1.124, since $x^p = 1$ if and only if $x = 1$ or $|x| = p$. □

**Remark 1.127.** Corollary 1.126 can also be improved in some cases. For example, if $p^2 \mid |G|$, then one can show[13] that $o_p(G) \equiv p - 1 \mod p^2$ or $o_p(G) \equiv -1 \mod p^2$. The precise value of $o_p(G)$ modulo $p^2$ depends on the structure of $p$-subgroups of $G$.

**Corollary 1.128.** *Let $G$ be a finite group and let $p$ be a prime such that $p \mid |G|$. Then the number of subgroups of order $p$ in $G$ is $\equiv 1 \mod p$.*

*Proof.* Let $r$ be the number of subgroups of order $p$ in $G$. Note that if $U$ and $V$ are subgroups of order $p$ in $G$, by Lagrange's theorem we have $U = V$ or $U \cap V = \{1\}$. Moreover, any element of $U \setminus \{1\}$ has order $p$. Thus the number of elements of order $p$ in $G$ is equal to $r(p-1)$, so $r \equiv 1 \mod p$ by Corollary 1.126. □

## 1.13 Number of conjugacy classes

Let $G$ be a finite group. Denote the number of conjugacy classes of $G$ by $k(G)$. What can we say about $k(G)$? Certainly $k(G) \leq |G|$, and $k(G) = |G|$ if and only if $G$ is abelian. What about lower bounds for $k(G)$? The first results go back to Landau[14], who showed in 1903 that $|G|$ can be bounded from above in terms of $k(G)$. Using Landau's method, one can find the following explicit bound[15].

[13] M. Herzog, *Counting group elements of order p modulo $p^2$*, Proc. Amer. Math. Soc. 66 (1977), 247–250.

[14] E. Landau, *Über die Klassenzahl der binären quadratischen Formen von negativer Discriminante.*, Math. Ann. 56 (1903), no. 4, 671–676.

[15] M. Newman, *A bound for the number of conjugacy classes in a group.*, J. London Math. Soc. 43 (1968), 108–110.

**Theorem 1.129.** *Let $G$ be a finite group of order $n$. Then $k(G) > \frac{\log \log n}{\log 2}$.*

*Proof.* Omitted. □

The bound in Theorem 1.129 is very weak, and later much better bounds have been found. But it does follow from Theorem 1.129 that $k(G) \to \infty$ as $|G| \to \infty$. Therefore for all $c > 0$, up to isomorphism there exist only finitely many finite groups $G$ with $k(G) = c$.

**Example 1.130.** Let $G$ be a finite group.

(a) It is clear that $k(G) = 1$ only if $G$ is trivial.

(b) Exercise: Show that $k(G) = 2$ if and only if $G \cong C_2$.

(c) Exercise: Show that $k(G) = 3$ if and only if $G \cong C_3$ or $G \cong S_3$.

(d) Currently the finite groups with $k(G) \leq 14$ have been classified[16].

(e) Denote by $f(c)$ the number of finite groups (up to isomorphism) with $k(G) = c$. Then we have the following values of $f(c)$:

| $c$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $f(c)$ | 1 | 1 | 2 | 4 | 8 | 8 | 12 | 21 | 26 | 38 | 35 | 32 |

**Remark 1.131.** For all $c > 1$, it is possible to construct an infinite group $G$ with $k(G) = c$.

## 1.14 Conjugacy classes of subgroups

Similarly to the conjugacy of elements, we will define conjugacy of subgroups.

**Definition 1.132.** Let $G$ be a group and $H, K \leq G$. A *conjugate* of $H$ is a subgroup of the form $g^{-1}Hg$ for $g \in G$. We say that the subgroups $H$ and $K$ are *conjugate*, if $K = g^{-1}Hg$ for some $g \in G$. We will denote $H^g := g^{-1}Hg$ for all $g \in G$.

We first observe that a conjugates of a subgroup $H$ are subgroups and isomorphic to $H$.

**Lemma 1.133.** *Let $G$ be a group and $H \leq G$. Then $g^{-1}Hg$ is a subgroup of $G$ and $g^{-1}Hg \cong H$ for all $g \in G$.*

[16] A. Vera-López, J. Sangroniz, *The finite groups with thirteen and fourteen conjugacy classes*, Mathematische Nachrichten, 280(5–6), 676–694, (2007).

*Proof.* Since the map $x \mapsto g^{-1}xg$ is an automorphism (Lemma 1.65), the lemma follows from Lemma 1.63 (iv) and (vi). □

**Example 1.134.** If $H$ and $K$ are conjugate subgroups of a group $G$, then $H \cong K$ by Lemma 1.133. The converse is not true, as seen by the following example. Let $G = S_4$ and consider $H = \{(1), (1\ 2)\}$ and $K = \{(1), (1\ 2)(3\ 4)\}$. Then $H$ and $K$ are both cyclic of order two, so $H \cong K$. However, $H$ and $K$ are not conjugate in $G$; for $\sigma \in G$ we have $\sigma H \sigma^{-1} = \{(1), (\sigma(1)\ \sigma(2))\} \neq K$.

Two isomorphic groups have the same multiplication table, so as groups we can think of them "as the same". But as subgroups, they might behave in very different ways; this is because any given group can usually be represented in many different ways. For subgroups, conjugacy is better notion of similarity than isomorphism.

**Example 1.135.** Consider $G = D_8$, so $G = \langle x, y \rangle$ with $|x| = 2$, $|y| = 4$, $xyx^{-1} = y^{-1}$ and $x \notin \langle y \rangle$. Consider $H = \langle x \rangle$ and $K = \langle y^2 \rangle$. Both $H$ and $K$ are cyclic of order 2, so $H \cong K$. Now $H$ is not a normal subgroup of $G$, but $K \trianglelefteq G$ since $K = Z(G)$.

**Definition 1.136.** Let $G$ be a group and $H \leq G$. The *normalizer of $H$ in $G$* is defined as

$$N_G(H) = \{g \in G : g^{-1}Hg = H\}.$$

**Lemma 1.137.** *Let $G$ be a group. Then:*

(i) *$N_G(H)$ is a subgroup of $G$ for all $H \leq G$.*

(ii) *The number of conjugates of $H$ in $G$ is equal to $[G : N_G(H)]$.*

*Proof.* The proofs of (i) is similar to the proofs of Lemma 1.114 (i). For (ii), show that $xN_G(H) = yN_G(H)$ if and only if $xHx^{-1} = yHy^{-1}$ and argue as in Lemma 1.114 (ii). The details are left as an exercise. □

**Remark 1.138.** Let $G$ be a group and $H \leq G$. It is clear that $H \trianglelefteq N_G(H)$, and moreover $N_G(H)$ is the largest subgroup of $G$ that contains $H$ as a normal subgroup. In particular $H \trianglelefteq G$ if and only if $N_G(H) = G$.

**Lemma 1.139.** *Let $G$ be a group and $N \trianglelefteq G$. Let $N \leq H \leq G$. Then $N_{G/N}(H/N) = N_G(H)/N$.*

*Proof.* Exercise. □

## 1.15 $p$-groups

**Definition 1.140.** Let $p$ be a prime. A group $G$ is said to be a *$p$-group*, if $|g|$ is a power of $p$ for all $g \in G$.

By Lagrange's theorem (Corollary 1.81) and Cauchy's theorem (Corollary 1.120), a finite group $G$ is a $p$-group if and only if $|G|$ is a power of $p$.

**Example 1.141.** Let $p$ be a prime.

(a) The cyclic group of order $p^k$ is a $p$-group for all $k \geq 0$.

(b) $Q_8$ is a 2-group of order 8.

(c) If $n$ is a power of 2, then $D_{2n}$ is a 2-group. The infinite dihedral group $D_\infty$ is not a 2-group, since it contains elements of infinite order.

(d) (Prüfer $p$-group) The following is an example of an infinite $p$-group. Consider the following set of complex numbers:

$$\mathbb{Z}(p^\infty) = \{z \in \mathbb{C} : z^{p^k} = 1 \text{ for some } k \geq 1\}.$$

Then $\mathbb{Z}(p^\infty)$ is a subgroup of $\mathbb{C}^\times$, and $\mathbb{Z}(p^\infty)$ is an infinite abelian $p$-group.

**Lemma 1.142.** *Let $G$ be a finite $p$-group and let $N \trianglelefteq G$. If $N \neq \{1\}$, then $N \cap Z(G) \neq \{1\}$.*

*Proof.* Since $N$ is a normal subgroup, it must be a union of conjugacy classes of $G$ (Lemma 1.112), say

$$N = \{1\} \cup C_1 \cup \cdots \cup C_t.$$

The order of a conjugacy class divides the order of the group (Lemma 1.114 (ii)), so $|C_i|$ is a power of $p$ for all $1 \leq i \leq t$. Thus we cannot have $|C_i| > 1$ for all $1 \leq i \leq t$, as otherwise $|N| = 1 + \sum_{i=1}^t |C_i|$ is not divisible by $p$. Therefore $C_i = \{x\}$ for some $1 \leq i \leq t$, in which case $x \in N \cap Z(G)$ and the lemma follows. □

The following is the special case $N = G$ of Lemma 1.142.

**Corollary 1.143.** *Let $G$ be a non-trivial finite $p$-group. Then $Z(G) \neq \{1\}$.*

**Proposition 1.144.** *Let $G$ be a finite $p$-group of order $p^2$. Then $G$ is abelian.*

*Proof.* By Corollary 1.143 we have $Z(G) \neq \{1\}$, so $G/Z(G)$ has order 1 or order $p$. Therefore $G/Z(G)$ is cyclic, which by an exercise implies that $G$ is abelian (Example 1.117 (v)).

□

**Example 1.145.** For any prime $p$, there exist non-abelian $p$-groups of order $p^3$. For this we can consider the *Heisenberg group*

$$H_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

Exercise: Show that $H_p$ is a non-abelian subgroup of $\mathrm{GL}_3(\mathbb{Z}/p\mathbb{Z})$ such that $|H_p| = p^3$. Is $H_2 \cong Q_8$ or $H_2 \cong D_8$?

**Proposition 1.146.** *Let $G$ be a finite $p$-group of order $|G| = p^\alpha$. Then for all $0 \leq \beta \leq \alpha$, there exists $N \trianglelefteq G$ with $|N| = p^\beta$.*

*Proof.* We proceed by induction on $|G|$, the case $|G| = 1$ being clear. Suppose then that $|G| > 1$. If $\beta = 0$, we can take $N = \{1\}$, so suppose that $\beta > 0$. By Corollary 1.143 there exists a non-identity element $x \in Z(G)$. Replacing $x$ with a suitable power of $x$, we can assume that $|x| = p$. Then $K = \langle x \rangle$ is subgroup of order $p$, and $K \trianglelefteq G$ since $x \in Z(G)$. By induction there exists $N/K \trianglelefteq G/K$ with $|N/K| = p^{\beta-1}$. Then $N \trianglelefteq G$ with $|N| = p^\beta$. (Remember Theorem 1.102.) □

**Proposition 1.147.** *["Normalizers grow"] Let $G$ be a finite $p$-group and $H$ be a proper subgroup of $G$. Then $H \lneqq N_G(H)$.*

*Proof.* By induction on $|G|$, the case $|G| = 1$ and $|G| = p$ are clear. Suppose then that $|G| > p$. By Corollary 1.143 we have $Z(G) \neq \{1\}$. Thus if $Z(G) \leq H$, then by induction

$$H/Z(G) \lneqq N_{G/Z(G)}(H/Z(G)) = N_G(H)/Z(G),$$

and thus $H \lneqq N_G(H)$. If $Z(G) \not\leq H$, then the claim follows since $Z(G) \leq N_G(H)$. □

**Proposition 1.148.** *Let $G$ be a finite $p$-group and $H \leq G$. If $[G : H] = p$, then $H \trianglelefteq G$.*

*Proof.* By Proposition 1.147, we have $H \lneqq N_G(H)$. If $[G : H] = p$, this implies $N_G(H) = G$, so $H \trianglelefteq G$. □

# 2 Symmetric and alternating Groups

In this section, we will establish some basic facts about finite symmetric groups $S_n$ and alternating groups $A_n$. For example, we will describe the conjugacy classes in both $S_n$ and $A_n$. We will also show that $A_n$ is a non-abelian simple group if $n \geq 5$.

## 2.1 Cycle decomposition

**Definition 2.1.** Let $\sigma = (i_1 \ \cdots \ i_k)$ and $\tau = (j_1 \ \cdots \ j_\ell)$ be cycles in $S_n$. We say that $\sigma$ and $\tau$ are *disjoint*, if $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_\ell\} = \emptyset$.

**Lemma 2.2.** *Let $\sigma = (i_1 \ \cdots \ i_k)$ and $\tau = (j_1 \ \cdots \ j_\ell)$ be cycles in $S_n$. If $\sigma$ and $\tau$ are disjoint, then $\sigma\tau = \tau\sigma$.*

*Proof.* Exercise. □

We will see that any permutation $\sigma \in S_n$ can be written as a product of pairwise disjoint cycles, and that this factorization is essentially unique.

**Definition 2.3.** Let $\sigma \in S_n$. For $1 \leq i \leq n$, the *orbit* of $i$ under $\sigma$ is the set $\mathrm{orb}_\sigma(i) = \{\sigma^k(i) : k \in \mathbb{Z}\}$.

**Lemma 2.4.** *Let $\sigma \in S_n$. Then any two orbits of $\sigma$ are either disjoint or equal. In particular, $\Omega = \{1, \ldots, n\}$ decomposes into a disjoint union*

$$\Omega = \mathrm{orb}_\sigma(i_1) \cup \cdots \cup \mathrm{orb}_\sigma(i_t)$$

*for some $i_1, \ldots, i_t \in \Omega$.*

*Proof.* Let $\mathrm{orb}_\sigma(i)$ and $\mathrm{orb}_\sigma(j)$ be two orbits of $\sigma$. If they are not disjoint, there exist some $k, \ell \in \mathbb{Z}$ such that $\sigma^k(i) = \sigma^\ell(j)$. Then $i = \sigma^{\ell-k}(j)$ which implies $\mathrm{orb}_\sigma(i) \subseteq \mathrm{orb}_\sigma(j)$, similarly $j = \sigma^{k-\ell}(i)$ which implies $\mathrm{orb}_\sigma(j) \subseteq \mathrm{orb}_\sigma(i)$. Therefore $\mathrm{orb}_\sigma(i) = \mathrm{orb}_\sigma(j)$. □

**Example 2.5.** For example, consider $\sigma \in S_3$. Then:

- $\sigma = (1)$ has three orbits: $\{1\}$, $\{2\}$, $\{3\}$.
- $\sigma = (1\ 2)$ has two orbits: $\{1, 2\}$, $\{3\}$.
- $\sigma = (1\ 3)$ has two orbits: $\{1, 3\}$, $\{2\}$.
- $\sigma = (2\ 3)$ has two orbits: $\{1\}$, $\{2, 3\}$.
- $\sigma = (1\ 2\ 3)$ and $\sigma = (1\ 3\ 2)$ have a single orbit: $\{1, 2, 3\}$.

**Lemma 2.6.** *Let $\sigma \in S_n$. Let $O = \mathrm{orb}_\sigma(i)$ be an orbit of $\sigma$. Let $k \geq 1$ be minimal such that $\sigma^k(i) = i$. Then:*

(i) *$|O| = k$ and $O = \{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$.*

(ii) *$\sigma(O) = O$, and the map $\sigma' : O \to O$ induced by $\sigma$ is the $k$-cycle $(i\ \sigma(i)\ \cdots\ \sigma^{k-1}(i))$ in $\mathrm{Sym}(O)$.*

*Proof.* (i) For any $\ell \in \mathbb{Z}$, we can write $\ell = r + qk$ for some $0 \leq r < k$. Then if $\sigma^\ell(i) = i$, we have $\sigma^r(i) = i$ since $\sigma^k(i) = i$. By minimality of $k$ this implies $r = 0$. Therefore $\sigma^\ell(i) = i$ if and only if $k \mid \ell$. As a consequence, for all $s, t \in \mathbb{Z}$ we have $\sigma^s(i) = \sigma^t(i)$ if and only if $s \equiv t \mod k$. Thus $O = \{i, \sigma(i), \ldots, \sigma^{k-1}(i)\}$ and $|O| = k$.

(ii) Immediate from (i).

□

**Proposition 2.7.** *Let $\sigma \in S_n$. Then $\sigma$ can be written as a product of pairwise disjoint cycles: we can write $\sigma = \pi_1 \cdots \pi_t$ such that:*

(i) *$\pi_i$ is a $k_i$-cycle for all $1 \leq i \leq t$;*

(ii) *The cycles $\pi_1$, …, $\pi_t$ are pairwise disjoint;*

(iii) *$k_1 + \cdots + k_t = n$.*

*This factorization is also unique, up to the order of factors: if $\sigma = \pi'_1 \cdots \pi'_s$ is another factorization satisfying properties (i) – (iii), then $t = s$ and $\{\pi_1, \ldots, \pi_t\} = \{\pi'_1, \ldots, \pi'_t\}$.*

*Proof.* Let $O_1 = \mathrm{orb}_\sigma(i_1)$, …, $O_t = \mathrm{orb}_\sigma(i_t)$ be the orbits of $\sigma$ on $\Omega = \{1, \ldots, n\}$, so by Lemma 2.4 we have a disjoint union $\Omega = O_1 \cup \cdots \cup O_t$. For $1 \leq r \leq t$, let $k_r = |O_r|$. It follows from Lemma 2.6 that $\sigma$ is equal to the following product of disjoint cycles:

$$\sigma = (i_1\ \sigma(i_1)\ \cdots\ \sigma^{k_1-1}(i_1)) \cdots (i_t\ \sigma(i_t)\ \cdots\ \sigma^{k_t-1}(i_t)).$$

Thus by defining $\pi_r = (i_r\ \sigma(i_r)\ \cdots\ \sigma^{k_r-1}(i_r))$ for $1 \leq r \leq t$, we have $\sigma = \pi_1 \cdots \pi_t$ such that conditions (i) – (iii) hold.

Suppose that $\sigma = \pi'_1 \cdots \pi'_s$ is another factorization satisfying properties (i) – (iii), say $\pi'_r = (j_1\ j_2\ \cdots\ j_{\ell_r})$ for $1 \leq r \leq s$. Then it is clear that each set $O'_r = \{j_1, j_2, \ldots, j_{\ell_r}\}$ is an orbit of $\sigma$ on $\Omega$, and $O'_1$, …, $O'_s$ are all the orbits of $\sigma$ by (iii). Since the orbits are uniquely determined by $\sigma$, it follows that $s = t$ and by reordering the factors (Lemma 2.2) we can assume that $O_1 = O'_1$, …, $O_t = O'_t$. Then by Lemma 2.6 (ii) we have $\pi_i = \pi'_i$ for all $1 \leq i \leq t$. □

**Definition 2.8.** By Proposition 2.7, for each $\sigma \in S_n$ there exist unique integers $k_1 \geq \cdots \geq k_t \geq 1$ such that $k_1 + \cdots + k_t = n$ and $\sigma$ is a product of pairwise disjoint cycles of lengths $k_1, \ldots, k_t$. We call $(k_1, \ldots, k_t)$ the *partition of $n$ corresponding to $\sigma$*.

**Example 2.9.** (a) In $S_3$, each element is a cycle.

(b) In $S_4$, the possible cycle decompositions are as follows, where $\{1,2,3,4\} = \{i,j,k,l\}$:

- $(i)(j)(k)(l) = (1)$ (trivial element). Partition $(1,1,1,1)$.
- $(i\ j)(k)(l) = (i\ j)$ (2-cycle). Partition $(2,1,1)$.
- $(i\ j)(k\ l)$ (product of disjoint 2-cycles). Partition $(2,2)$.
- $(i\ j\ k)(l) = (i\ j\ k)$ (3-cycle). Partition $(3,1)$.
- $(i\ j\ k\ l)$ (4-cycle). Partition $(4)$.

**Remark 2.10.** In the factorization $\sigma = \pi_1 \cdots \pi_t$ in Proposition 2.7, the cycles $\pi_i$ of length 1 correpond to the orbits of length 1, in other words, to the fixed points of $\sigma$. Thus we can write $\sigma = \pi_1 \cdots \pi_s$, where $s \geq 0$ and the $\pi_i$ are pairwise disjoint cycles of length $> 1$. By Proposition 2.7, this decomposition is unique up to the ordering of the factors.

**Corollary 2.11.** *The symmetric group $S_n$ is generated by cycles.*

*Proof.* Immediate from Proposition 2.7. □

On the other hand, any cycle can be written as a product of 2-cycles:

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_k)(a_1\ a_{k-1}) \cdots (a_1\ a_2).$$

Therefore we have the following corollary:

**Corollary 2.12.** *The symmetric group $S_n$ is generated by 2-cycles.*

Not all 2-cycles are needed to generate $S_n$, as for example $S_3 = \langle (1\ 2), (2\ 3) \rangle$.

**Example 2.13.** Some more examples on generators of $S_n$:

(a) Exercise: Show that $S_n$ is generated by $(1\ 2)$, $(1\ 3)$, …, $(1\ n)$.

(b) Exercise: Show that $S_n$ is generated by $(1\ 2)$, $(2\ 3)$, …, $(n-1\ n)$.

(c) Exercise: Show that $S_n = \langle (1\ 2), (1\ 2\ \cdots\ n) \rangle$.

## 2.2 Orders of permutations

The order of a permutation can be conveniently expressed in terms of its cycle decomposition.

**Lemma 2.14.** *Let $\sigma \in S_n$ be a $k$-cycle. Then:*

(i) $|\sigma| = k$.

(ii) *Let $d \mid k$. Then $\sigma^d$ is a product of $d$ pairwise disjoint cycles of length $k/d$.*

*Proof.* Exercise. □

**Example 2.15.** The 4-cycle (1 2 3 4) has order 4 and $(1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4)$.

**Lemma 2.16.** *Let $\sigma \in S_n$, and suppose that $\sigma = \pi_1 \cdots \pi_t$ where $\pi_i$ are pairwise disjoint cycles, and $\pi_i$ is a $k_i$-cycle for $1 \leq i \leq t$. Then $|\sigma| = \operatorname{lcm}(k_1, \ldots, k_t)$.*

*Proof.* Since the cycles are pairwise disjoint, they commute pairwise, and therefore $\sigma^d = \pi_1^d \cdots \pi_t^d$ for all $d \in \mathbb{Z}$. By Lemma 2.14 and the uniqueness of the cycle decomposition, we have $\sigma^d = 1$ if and only if $\pi_i^d = 1$ for all $1 \leq i \leq t$. Since $|\pi_i| = k_i$ (Lemma 2.14), it follows that $\sigma^d = 1$ if and only if $k_i \mid d$ for all $1 \leq i \leq t$. Since $\operatorname{lcm}(k_1, \ldots, k_t)$ is precisely the smallest positive integer such that $k_i \mid \operatorname{lcm}(k_1, \ldots, k_t)$ for all $1 \leq i \leq t$, the lemma follows. □

**Example 2.17.** In $S_5$, the element (1 2)(3 4 5) has order 6, while (1 2)(3 4) has order 2.

**Example 2.18.** What is the largest order of an element of $S_n$? For example in $S_3$, the largest order is 3, for a 3-cycle. In $S_5$, the largest order is 6, for example for (1 2 3)(4 5). Denote the maximal order of an element of $S_n$ by $g(n)$. Below is a list of small values:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $g(n)$ | 1 | 2 | 3 | 4 | 6 | 6 | 12 | 15 | 20 | 30 | 30 | 60 | 60 | 84 |

Exercise: Using the values of $g(n)$ given above, find an element of largest order in $S_n$ for $1 \leq n \leq 14$.

## 2.3 Conjugacy classes in $S_n$

Another application of the cycle decomposition is the description of the conjugacy classes of $S_n$.

**Proposition 2.19.** *Let $\sigma, \tau \in S_n$. Then $\sigma$ and $\tau$ are conjugate if and only if they correspond to the same partitions of $n$.*

*Proof.* Suppose that $\sigma = \pi_1 \cdots \pi_t$ such that $\pi_i$ a $k_i$-cycle and that the cycles $\pi_i$ are pairwise disjoint. For conjugation of $k$-cycles in $S_n$, we have

$$g(i_1 \ \cdots \ i_k)g^{-1} = (g(i_1) \ \cdots \ g(i_k)) \tag{2.1}$$

for all $g \in S_n$. It follows from (2.1) that

$$g\sigma g^{-1} = (g\pi_1 g^{-1})(g\pi_2 g^{-1}) \cdots (g\pi_t g^{-1})$$

is a product of pairwise disjoint cycles of lengths $k_1$, ..., $k_t$. By uniqueness of the cycle decomposition (Proposition 2.7), we conclude that conjugate elements in $S_n$ correspond to the same partition of $n$.

Conversely, suppose that $\sigma, \tau \in S_n$ correspond to the same partitions of $n$. In other words, there exist integers $k_1 \geq \cdots \geq k_t > 0$ such that $k_1 + \cdots + k_t = n$ and

$$\begin{aligned}\sigma &= (a_{11} \ a_{12} \ \cdots \ a_{1k_1})(a_{21} \ \cdots \ a_{2k_2}) \cdots (a_{t1} \ \cdots \ a_{tk_t}) \\ \tau &= (b_{11} \ b_{12} \ \cdots \ b_{1k_1})(b_{21} \ \cdots \ b_{2k_2}) \cdots (b_{t1} \ \cdots \ b_{tk_t})\end{aligned}$$

are the decompositions of $\sigma$ and $\tau$ into a product of pairwise disjoint cycles. Define $g \in S_n$ by

$$g := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k_1} & a_{21} & \cdots & a_{2k_2} & \cdots & a_{t1} & \cdots & a_{tk_t} \\ b_{11} & b_{12} & \cdots & b_{1k_1} & b_{21} & \cdots & b_{2k_2} & \cdots & b_{t1} & \cdots & b_{tk_t} \end{pmatrix}.$$

By (2.1), we get

$$\begin{aligned} g\sigma g^{-1} &= g(a_{11} \ a_{12} \ \cdots \ a_{1k_1})g^{-1} g(a_{21} \ \cdots \ a_{2k_2})g^{-1} \cdots g(a_{t1} \ \cdots \ a_{tk_t})g^{-1} \\ &= (g(a_{11}) \ g(a_{12}) \ \cdots \ g(a_{1k_1}))(g(a_{21}) \ \cdots \ g(a_{2k_2})) \cdots (g(a_{t1}) \ \cdots \ g(a_{tk_t})) \\ &= \tau. \end{aligned}$$

Thus $\sigma$ and $\tau$ are conjugate in $S_n$. □

**Example 2.20.** With Proposition 2.19, it is straightforward to find representatives for the conjugacy classes for any given $n$. For example, in $S_4$ we have the following representatives for the 5 conjugacy classes:

| representative | partition | size of class |
|---|---|---|
| (1) | $(1,1,1,1)$ | 1 |
| (1 2) | $(2,1,1)$ | 6 |
| (1 2 3) | $(3,1)$ | 8 |
| (1 2)(3 4) | $(2,2)$ | 3 |
| (1 2 3 4) | $(4)$ | 6 |

The size of each class is counted by calculating the number of cycles with the corresponding decomposition. For example, the number of 3-cycles $(i\ j\ k)$ is $\frac{4\cdot3\cdot2}{3} = 8$. This is because there are $4\cdot3\cdot2$ choices for $i$, $j$, $k$; then we divide by 3 so that we do not count

$$(i\ j\ k) = (j\ k\ i) = (k\ i\ j)$$

three times. Similarly, the number of permutations $(i\ j)(k\ l)$ is $\frac{1}{2}(\frac{4\cdot3}{2}\cdot\frac{2\cdot1}{2}) = 3$. Indeed, there are $\frac{4\cdot3}{2}$ choices for $(i\ j)$, then $\frac{2\cdot1}{2}$ choices for $(k\ l)$; then divide by 2 to avoid counting $(i\ j)(k\ l) = (k\ l)(i\ j)$ twice. Similar arguments work for counting the size of any given conjugacy class in $S_n$.

## 2.4 Alternating groups

In this section, we will define alternating groups, and show that it is the unique subgroup of index 2 in $S_n$. There are multiple ways to define the alternating groups, all of which boil down identifying a notion of "parity" for permutations.

**Definition 2.21.** Let $\sigma \in S_n$. An unordered pair $\{i,j\}$ with $1 \le i < j \le n$ is an *inversion* of $\sigma$ if $\sigma(i) > \sigma(j)$. The set of all inversions of $\sigma$ is denoted by $I(\sigma)$.

**Lemma 2.22.** *Let $\sigma, \tau \in S_n$. Then $|I(\sigma\tau)| \equiv |I(\sigma)| + |I(\tau)| \mod 2$.*

*Proof.* The set $I(\sigma\tau)$ consists of $\{i,j\}$ with $1 \le i < j \le n$ such that either

- $\{i,j\} \notin I(\tau)$ and $\{\tau(i),\tau(j)\} \in I(\sigma)$; or
- $\{i,j\} \in I(\tau)$ and $\{\tau(i),\tau(j)\} \notin I(\sigma)$.

Thus $I(\sigma\tau) = (X \setminus Y) \cup (Y \setminus X)$, where

- $X = I(\tau)$
- $Y =$ set of pairs $\{i,j\}$ with $\{\tau(i),\tau(j)\} \in I(\sigma)$.

We have $|X \setminus Y| = |X| - |X \cap Y|$ and similarly $|Y \setminus X| = |Y| - |X \cap Y|$. Therefore $|I(\sigma\tau)| = |X| + |Y| - 2|X \cap Y|$. Moreover $|Y| = |I(\sigma)|$ (Exercise 2.5), so we conclude that $|I(\sigma\tau)| \equiv |I(\sigma)| + |I(\tau)| \mod 2$. □

Therefore the map $\operatorname{sgn} : S_n \to \{1, -1\}$ defined by

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

for all $\sigma \in S_n$ is a homomorphism. (Here $\{1, -1\}$ is a cyclic group of order 2 under multiplication.) We call sgn the *sign homomorphism*.

For $\sigma = (1\ 2)$ we have $I(\sigma) = \{\{1, 2\}\}$, so $\operatorname{sgn}(\sigma) = -1$ and thus sgn is a surjective homomorphism for $n \geq 2$.

**Definition 2.23.** The *alternating group of degree* $n$ is $A_n := \operatorname{Ker}(\operatorname{sgn})$, where $\operatorname{sgn} : S_n \to \{1, -1\}$ is the sign homomorphism. A permutation $\sigma \in S_n$ is said to be *even* if $\sigma \in A_n$, and *odd* if $\sigma \notin A_n$.

For $n \geq 2$ the sign homomorphism is surjective, so $|A_n| = n!/2$.

**Lemma 2.24.** *Any transposition is an odd permutation.*

*Proof.* Any transposition $\sigma$ is conjugate to $\tau = (1\ 2)$, say $\sigma = g\tau g^{-1}$ for some $g \in S_n$. Then $\operatorname{sgn}(\sigma) = \operatorname{sgn}(g)\operatorname{sgn}(\tau)\operatorname{sgn}(g)^{-1} = \operatorname{sgn}(\tau)$. As we have seen above $|I(\tau)| = 1$, so $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau) = -1$. □

**Remark 2.25.** Exercise: For $\sigma = (i\ j) \in S_n$ with $1 \leq i < j \leq n$, calculate $|I(\sigma)|$.

We know that every $\sigma \in S_n$ can be written as a product $\sigma = t_1 t_2 \cdots t_d$ of transpositions. Since the sign map is a homomorphism, by Lemma 2.24 we have that $\sigma$ is even if $d$ is even, and odd if $d$ is odd. Note that there might be multiple ways of writing a permutation as a product of transpositions, for example $(1\ 2\ 3) = (1\ 2)(2\ 3) = (1\ 3)(1\ 2) = (3\ 4)(3\ 4)(1\ 2)(2\ 3)$.

**Lemma 2.26.** *Let $n \geq 3$. Then $A_n$ is generated by 3-cycles.*

*Proof.* Any $\sigma \in A_n$ can be written as a product of even number of transpositions, say $\sigma = t_1 t_1' \cdots t_d t_d'$ for some transpositions $t_i, t_i' \in S_n$. Thus it will suffice to show that any product of two transpositions is contained in the subgroup generated by the 3-cycles. To this end, let $t = (i\ j)$ and $t' = (k\ l)$ be two transpositions. If $t$ and $t'$ are disjoint, then $tt' = (i\ j)(k\ l) = (i\ j\ k)(j\ k\ l)$. If $\{i, j\} = \{k, l\}$, then $tt' = 1$. The remaining possibility is that $\{i, j\}$ and $\{k, l\}$ have one element in common, say $t = (i\ j)$ and $t' = (j\ l)$. In this case $tt' = (i\ j\ l)$. □

**Proposition 2.27.** *Let $n \geq 2$. Suppose that $H < S_n$ is such that $[S_n : H] = 2$. Then $H = A_n$.*

*Proof.* If $n = 2$, then $S_2$ has order 2 and $A_2$ is trivial, so the claim is obvious. Suppose that $n \geq 3$. Since $H$ has index 2, it is a normal subgroup and $\sigma^2 \in H$ for all $\sigma \in S_n$. For a 3-cycle $(i\ j\ k)$ we have $(i\ j\ k) = (i\ k\ j)^2$, so $H$ contains every 3-cycle. It follows from Lemma 2.26 that $H = A_n$. □

**Example 2.28.** Arguing as in the proof of Proposition 2.27, we find that if $n \geq 3$, then $A_n$ contains no subgroup of index 2. This provides a counterexample to the converse of Lagrange's theorem: for example $|A_4| = 12$, so 6 divides the order of $A_4$, but $A_4$ has no subgroup of order 6.

**Lemma 2.29.** *Let $n \geq 2$ and $G \leq S_n$. Then either $G \leq A_n$, or $G \cap A_n$ is a normal subgroup of index 2 in $G$.*

*Proof.* Exercise. □

## 2.5 Conjugacy classes in $A_n$

What are the conjugacy classes in $A_n$? Since $A_n$ is a normal subgroup of $S_n$, we at least know that $A_n$ is a union of conjugacy classes $S_n$; namely it is the union of the conjugacy classes of even permutations.

Hence for $\sigma \in A_n$, we have $\sigma^{S_n} \subseteq A_n$. Are all elements of $\sigma^{S_n}$ conjugate in $A_n$? The answer is no in general. Consider for example $A_3$, which contains the conjugacy class $(1\ 2\ 3)^{S_3} = \{(1\ 2\ 3), (1\ 3\ 2)\}$. But $A_3$ is abelian, so $(1\ 2\ 3)$ and $(1\ 3\ 2)$ are not conjugate in $A_3$. An exercise shows that $(1\ 2\ 3)$ and $(1\ 3\ 2)$ are not conjugate in $A_4$ either, but they are conjugate in $A_n$ for $n \geq 5$.

In general it turns out that either $\sigma^{S_n} = \sigma^{A_n}$, or $\sigma^{S_n} = \sigma^{A_n} \cup (\sigma')^{A_n}$ is the union of two distinct $A_n$-conjugacy classes of equal size. In the latter case we say that the conjugacy class *splits* in $A_n$. When does a conjugacy class split? The answer is provided by the following lemma, in terms of centralizers.

**Lemma 2.30.** *Let $G$ be a finite group and let $N \triangleleft G$ be such that $[G : N] = 2$. Let $g \in N$. The following statements hold:*

(i) *If $C_G(g) \not\leq N$, then $g^N = g^G$.*

(ii) *If $C_G(g) \leq N$, then $g^G = g^N \cup (g')^N$ for some $g' \in N$, and moreover $|g^N| = |(g')^N| = |g^G|/2$.*

*Proof.* (i) Suppose that $C_G(g) \not\leq N$. It will suffice to prove that for $x \in G \setminus N$, we have $xgx^{-1} \in g^N$. Let $h \in C_G(g) \setminus N$. Since $x \notin N$ and $h \notin N$, we have $hx \in N$ because $G/N \cong C_2$. Since $hxh^{-1} = x$ we get $xgx^{-1} = (xh)g(xh)^{-1} \in g^N$.

(ii) Suppose that $C_G(g) \leq N$, so $C_G(g) = C_N(g)$. Then

$$|g^G| = [G : C_N(g)] = [G : N][N : C_N(g)] = 2|g^N|$$

by Lemma 1.114, so $|g^N| = |g^G|/2$. Let $g' \in g^G \setminus g^N$, say $g' = xgx^{-1}$. Then $C_G(g') = xC_G(g)x^{-1} \leq N$, so by the same argument $|(g')^N| = |g^G|/2$. Since distinct conjugacy classes of $N$ are disjoint, we conclude that $g^G = g^N \cup (g')^N$.

□

**Lemma 2.31.** *Suppose that $n \geq 5$. Then 3-cycles are conjugate in $A_n$.*

*Proof.* By Lemma 2.30, it will suffice to verify that for a 3-cycle $\sigma = (i\ j\ k) \in A_n$, we have $C_{S_n}(\sigma) \not\leq A_n$. For this, take $\tau = (l\ m)$ a transposition disjoint from $\sigma$. Then $\tau \in C_{S_n}(\sigma)$ (Lemma 2.2) and $\tau \notin A_n$. □

With the same proof, one can generalize Lemma 2.31 to show that for $k$ odd, the $k$-cycles for $k \leq n-2$ are conjugate in $A_n$. More generally, one can prove that for $\sigma \in A_n$ the conjugacy class $\sigma^{S_n}$ splits in $A_n$ if and only if the cycle decomposition of $\sigma$ consists of disjoint cycles with distinct odd lengths. (For example, in $A_4$ the 3-cycles split into two classes, since they are a product of a 3-cycle and a 1-cycle.)

## 2.6 $A_n$ is simple for $n \geq 5$

**Theorem 2.32.** *Let $n \geq 5$. Then $A_n$ is simple.*

*Proof.* Let $N \trianglelefteq A_n$ be a non-trivial normal subgroup. It will suffice to prove that $N$ contains a 3-cycle, since then $N$ will contain all 3-cycles by Lemma 2.31, and thus $N = A_n$ by Lemma 2.26.

Let $g \in N$ be a nontrivial element, and write its decomposition into a product of disjoint cycles as $g = \pi_1\pi_2 \cdots \pi_t$. We consider the different possibilities for the cycle decomposition, and show that in each case we can find a 3-cycle in $N$.

*Case 1: Some cycle has length $\geq 4$.* By replacing $g$ with a conjugate and rearranging the $\pi_i$, we can assume that $\pi_1 = (1\ 2\ 3\ \cdots\ s)$ with $s \geq 4$. Set $\sigma = (1\ 2\ 3)$. Then

$$\sigma g \sigma^{-1} = (\sigma\pi_1\sigma^{-1})(\sigma\pi_2\sigma^{-1}) \cdots (\sigma\pi_t\sigma^{-1})$$

$$\begin{aligned} &= (\sigma\pi_1\sigma^{-1})\pi_2\cdots\pi_t \\ &= (2\ 3\ 1\ 4\ \cdots\ s)\pi_2\cdots\pi_t. \end{aligned}$$

Here we have used the fact that $\sigma$ is disjoint from $\pi_2$, ..., $\pi_t$ and thus commutes with them. Since $\sigma g\sigma^{-1} \in N$ by normality of $N$, it follows that $\sigma g\sigma^{-1}g^{-1} = (2\ 3\ 1\ 4\ \cdots\ s)(1\ 2\ 3\ \cdots\ s)^{-1} = (1\ 2\ 4) \in N$.

*Case 2: Each cycle has length $\leq 3$, and there are at least two 3-cycles.* By replacing $g$ with a conjugate and rearranging the $\pi_i$, we can assume that $\pi_1 = (1\ 2\ 3)$ and $\pi_2 = (4\ 5\ 6)$. Set $\sigma = (1\ 5)(2\ 6\ 3\ 4)$. Then

$$\begin{aligned} \sigma g\sigma^{-1} &= (\sigma\pi_1\sigma^{-1})(\sigma\pi_2\sigma^{-1})(\sigma\pi_3\sigma^{-1})\cdots(\sigma\pi_t\sigma^{-1}) \\ &= (\sigma\pi_1\sigma^{-1})(\sigma\pi_2\sigma^{-1})\pi_3\cdots\pi_t \\ &= (1\ 3\ 2)(4\ 5\ 6)\pi_3\cdots\pi_t. \end{aligned}$$

Thus $\sigma g\sigma^{-1}g^{-1} = (1\ 2\ 3) \in N$.

*Case 3: There is exactly one 3-cycle, and rest of the cycles have length $\leq 2$.* By replacing $g$ with a conjugate and rearranging the $\pi_i$, we can assume that $g = (1\ 2\ 3)\pi_2\cdots\pi_t$, where $\pi_i$ are 2-cycles. Then $g^2 = (1\ 3\ 2)\pi_2^2\cdots\pi_t^2 = (1\ 3\ 2) \in N$.

*Case 4: All cycles have length $\leq 2$.* There must be at least 2 cycles since $g \in A_n$, so by replacing $G$ with a conjugate, we may assume that $g = (1\ 2)(3\ 4)\pi_3\cdots\pi_t$. Let $\sigma = (1\ 2\ 3)$. Calculating as in the previous cases shows that $\sigma g\sigma^{-1}g^{-1} = (1\ 3)(2\ 4) \in N$. Then for $\tau = (1\ 5\ 3)$, we have $\tau(1\ 3)(2\ 4)\tau^{-1}(1\ 3)(2\ 4) = (1\ 3\ 5) \in N$.

The cases above exhaust all possibilities, so we conclude that $N$ contains a 3-cycle and thus $N = A_n$. □

## 2.7 Group actions

Group actions are a convenient way to study the possible ways a group $G$ (or homomorphic images of $G$) can be realized as a group of permutations. Thanks to the orbit–stabilizer theorem (Theorem 2.40), group actions are also fundamental in various counting arguments that come up in finite group theory.

**Definition 2.33.** Let $G$ a group and let $X$ be a nonempty set. An *action of $G$ on $X$* is map $\alpha : G \times X \to X$, $(g, x) \mapsto g \cdot x$ such that:

(i) $1 \cdot x = x$ for all $x \in X$;

(ii) $(gh) \cdot x = g \cdot (h \cdot x)$ for all $g, h \in G$ and $x \in X$.

In this case we say that $G$ *acts on* $X$, and such an $X$ is called a $G$*-set*. We will often write $gx$ instead of $g \cdot x$ for $g \in G$ and $x \in X$. The *action* of an element $g \in G$ is the map $\alpha_g : X \to X$ defined by $\alpha_g(x) = gx$ for all $x \in X$.

**Example 2.34.** Let $G$ be a group.

(a) Let $H \leq G$ and consider the set $X = \{xH : x \in G\}$ of left cosets of $H$ in $G$. Then $G$ acts on $X$ via $g \cdot (xH) = gxH$.

(b) $G = S_n$ acts *naturally* on $X = \{1, 2, \ldots, n\}$, via $\sigma \cdot i = \sigma(i)$ for $\sigma \in S_n$ and $i \in X$.

(c) $G$ acts on itself by conjugation. That is, we have an action of $G$ on $X = G$ defined by $g \cdot x = gxg^{-1}$ for all $g, x \in G$.

The study of group actions of $G$ on a set $X$ is really the same thing as the study of group homomorphisms $G \to \mathrm{Sym}(X)$, which are called *permutation representations*. This is seen from the next lemma:

**Lemma 2.35.** *Let $G$ be a group. Then the following statements hold.*

(i) *If $G$ acts on a set $X$, then $\alpha_g : X \to X$ is a bijection for all $g \in G$.*

(ii) *If $G$ acts on a set $X$, then $\varphi(g)(x) := g \cdot x$ defines a homomorphism $\varphi : G \to \mathrm{Sym}(X)$.*

(iii) *If $\varphi : G \to \mathrm{Sym}(X)$ is a homomorphism, then $g \cdot x := \varphi(g)(x)$ defines an action of $G$ on $X$.*

*Proof.* (i) If $G$ acts on a set $X$, then it follows from (i) and (ii) in Definition 2.33 that $\alpha_g \alpha_{g^{-1}} = \mathrm{id}_X = \alpha_{g^{-1}} \alpha_g$ for all $g \in G$. Therefore $\alpha_g$ is a bijection with inverse $\alpha_{g^{-1}}$.

(ii) In other words, we have defined $\varphi(g) = \alpha_g$ for all $g \in G$. Thus $\varphi$ is a well-defined map $\varphi : G \to \mathrm{Sym}(X)$ by (i). Moreover, we have $\alpha_g \alpha_h = \alpha_{gh}$ for all $g, h \in G$ by (ii) in Definition 2.33, so $\varphi$ is a homomorphism.

(iii) In other words, we have defined a map $\alpha : G \times X \to X$ by $\alpha(g, x) = g \cdot x = \varphi(g)(x)$ for all $g \in G$ and $x \in X$, and we need to check that this is an action of $G$ on $X$. Definition 2.33 (i) is satisfied since $\varphi(1)$ must be the identity map (Lemma 1.59 (ii)). Definition 2.33 (ii) is satisfied since $\varphi(gh) = \varphi(g)\varphi(h)$ for all $g, h \in G$.

□

As is clear from Lemma 2.35, each action of $G$ on a set $X$ corresponds to a unique homomorphism $G \to \mathrm{Sym}(X)$, and conversely each homomorphism $G \to \mathrm{Sym}(X)$ corresponds to a unique action of $G$ on $X$. An action of $G$ on $X$ is *faithful* if the corresponding homomorphism is injective, equivalently if the kernel of the homomorphism is trivial.

**Definition 2.36.** Let $G$ be a group acting on a set $X$. The *orbit* of $x \in X$ under the action of $G$ is the set $Gx = \{g \cdot x : g \in G\}$. We will also sometimes denote $\mathrm{orb}_G(x) := Gx$.

**Lemma 2.37.** *Let $G$ be a group acting on a set $X$. For any two orbits $Gx$ and $Gy$, either $Gx = Gy$ or $Gx \cap Gy = \emptyset$.*

*Proof.* Note first that

$$Ggx = Gx \text{ for all } g \in G. \tag{2.2}$$

Suppose then that there exists $z \in Gx \cap Gy$, say $z = gx = hy$ for some $g, h \in G$. Then $Gx = Gz$ and $Gy = Gz$ by (2.2), so $Gx = Gy$. Thus any two orbits are either equal or disjoint, which proves the lemma. □

By Lemma 2.37, if a group $G$ acts on a set $X$, the orbits partition $X$. In other words, we have a disjoint union

$$X = \bigcup_{x \in S} Gx$$

where $S$ is a set of representatives for the orbits. If there is only one orbit, we say that the action of $G$ on $X$ is *transitive*. Note that $G$ acts transitively on any orbit $Gx$.

If $X$ is a finite set, say

$$X = Gx_1 \cup \cdots \cup Gx_t$$

with $x_1, \ldots, x_t \in X$ representatives for the orbits, then

$$|X| = |Gx_1| + \cdots + |Gx_t|.$$

We next explain how the sizes of the orbits are calculated.

**Definition 2.38.** Let $G$ be a group acting on a set $X$. The *stabilizer* of $x \in X$ is the set $G_x = \{g \in G : gx = x\}$. We will also sometimes denote $\mathrm{stab}_G(x) = G_x$.

For a group $G$ acting on a set $X$, the *kernel* of the action is the kernel of the corresponding homomorphism $G \to \mathrm{Sym}(X)$. It is clear that the kernel is equal to

$$\bigcap_{x \in X} G_x,$$

so the action of $G$ on $X$ is faithful if and only if $\bigcap_{x \in X} G_x = \{1\}$.

**Lemma 2.39.** *Let $G$ be a group acting on a set $X$. Then the following hold:*

(i) *$G_x \leq G$ for all $x \in X$.*

(ii) *$gG_xg^{-1} = G_{gx}$ for all $g \in G$ and $x \in X$.*

(iii) *Let $x \in X$. Then $gG_x = hG_x$ if and only if $gx = hx$.*

*Proof.* (i) Let $x \in X$. It is immediate from the definitions that $1 \in G_x$ and that $g, h \in G_x$ implies $gh \in G_x$. Moreover if $g \in G_x$, then $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = 1 \cdot x = x$, so $g^{-1} \in G_x$. Thus $G_x \leq G$.

(ii) Let $g \in G$ and $x \in X$. For $h \in G_x$, we have $ghg^{-1}(gx) = gh(g^{-1}gx) = ghx = gx$, so $gG_xg^{-1} \leq G_{gx}$. The same argument shows that $g^{-1}G_{gx}g \leq G_{g^{-1}gx} = G_x$, so $G_{gx} \leq gG_xg^{-1}$ and thus $gG_xg^{-1} = G_{gx}$.

(iii) We have $gG_x = hG_x$ if and only if $h^{-1}g \in G_x$, which is a equivalent to $h^{-1}gx = x$. Clearly $h^{-1}gx = x$ if and only if $gx = hx$.

□

**Theorem 2.40** (Orbit–Stabilizer theorem)**.** *Let $G$ be a group and suppose that $G$ acts on a set $X$. Let $x \in X$. Let $\Omega$ be the set of left cosets of $G_x$. Then the map*

$$\psi : \Omega \to Gx$$

*defined by $\psi(gG_x) = gx$ is a bijection. In particular $|\operatorname{orb}_G(x)| = [G : G_x]$.*

*Proof.* The fact that $\psi$ is well-defined and injective follows from Lemma 2.39 (iii). Since $\psi$ is clearly surjective, it is a bijection. Thus $|\Omega| = |Gx|$, so $[G : G_x] = |Gx|$.

□

**Remark 2.41.** Let $G$ be a group acting on two sets $X$ and $Y$. We say that $X$ and $Y$ are *equivalent* (isomorphic) as $G$-sets, if there exists a bijection $\psi : X \to Y$ such that $\psi(gx) = g\psi(x)$ for all $x \in X$. For equivalent $G$-sets $X$ and $Y$, the action of $G$ is essentially the same, just the names of the elements that $G$ acts on are different (and the different names or labels are provided

by the bijection $\psi$). This is analogous to the isomorphism of groups (recall e.g. Example 1.16).

It is clear that for the bijection $\psi : \Omega \to Gx$ in Theorem 2.40, we have $\psi(g\omega) = g\psi(\omega)$ for all $\omega \in \Omega$, so $\Omega$ and $Gx$ are equivalent as $G$-sets.

Thus any transitive $G$-set is equivalent to the action of $G$ on the left cosets of some subgroup of $G$. More precisely, if $G$ acts transitively on $X$, then the action of $G$ on $X$ is equivalent to the action of $G$ on the left cosets of $G_x$.

The orbit–stabilizer theorem tells us that the size of an orbit is the index of the stabilizer of a point. We will now see how many of the results and concepts are special cases of the orbit–stabilizer theorem. These include, for example, the fact that the size of a conjugacy class is the index of the centralizer.

**Example 2.42.** Let $G$ be a group. Some basic examples of group actions, along with the orbits and the stabilizers.

(a) Let $\sigma \in S_n$. Consider the natural action of $G = \langle \sigma \rangle$ on $X = \{1, 2, \ldots, n\}$.

- Orbits: $\mathrm{orb}_\sigma(i)$ for $1 \leq i \leq n$.
- Stabilizers: $\mathrm{stab}_G(i) = \langle \sigma^k \rangle$, where $k > 0$ is minimal such that $\sigma^k(i) = i$.

(b) Let $H \leq G$ and consider the set $X = \{xH : x \in G\}$ of left cosets of $H$ in $G$. Then $G$ acts on $H$ via $g \cdot (xH) = gxH$.

- Orbits: Only one orbit, $\mathrm{orb}_G(H) = X$.
- Stabilizers: Stabilizer of $xH$ is $\mathrm{stab}_G(xH) = xHx^{-1}$.

(c) $G$ acts on itself by left multiplication. That is, we have an action of $G$ on $X = G$ defined by $g \cdot x = gx$ for all $g, x \in G$. The corresponding homomorphism $G \to \mathrm{Sym}(G)$ is the left regular representation (Theorem 1.66).

- Orbits: Only one orbit, $\mathrm{orb}_G(x) = G$ for all $x \in G$.
- Stabilizers: $\mathrm{stab}_G(x) = \{1\}$ for all $x \in G$.

(d) Let $H \leq G$. We have $H$ acting on $X = G$ by left multiplication.

- Orbits: Cosets of $H$, with $\mathrm{orb}_H(x) = Hx$ for all $x \in G$.
- Stabilizers: $\mathrm{stab}_H(x) = \{1\}$ for all $x \in H$.

(e) $G$ acts on itself by conjugation; that is, we have an action of $G$ on $X = G$ via $g \cdot x = gxg^{-1}$ for all $g, x \in G$.

- Orbits: Conjugacy classes, i.e. $\mathrm{orb}_G(x) = x^G$.
- Stabilizers: Centralizers, i.e. $\mathrm{stab}_G(x) = C_G(x)$.

(f) $G$ acts on the set of its subgroup by conjugation; that is, we have an action of $G$ on $X = \{H : H \leq G\}$ via $g \cdot H = gHg^{-1}$ for all $g \in G$ and $H \leq G$.

- Orbits: Conjugacy classes of subgroups.
- Stabilizers: Normalizers, i.e. $\mathrm{stab}_G(H) = N_G(H)$.

(g) $G = S_n$ acts *naturally* on $X = \{1, 2, \ldots, n\}$, via $\sigma \cdot i = \sigma(i)$ for $\sigma \in S_n$ and $i \in X$.

- Orbits: Only one orbit, $\mathrm{orb}_G(i) = X$ for all $1 \leq i \leq n$.
- Stabilizers: $\mathrm{stab}_G(i)$ is isomorphic to $\mathrm{Sym}(X \setminus \{i\}) \cong S_{n-1}$.

(h) Let $V$ be a finite-dimensional vector space over a field $\mathbb{F}$, with $n = \dim V$. Then $G = \mathrm{GL}(V)$ as on $V$ via $g \cdot v = g(v)$ for all $g \in G$ and $v \in V$.

- Orbits: Two orbits, $\{0\}$ and $V \setminus \{0\}$.
- Stabilizers: $\mathrm{stab}_G(0) = G$, and for $v \in V \setminus \{0\}$ the stabilizer $\mathrm{stab}_G(v)$ is isomorphic to the group of matrices of the following form:

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & A & \\ 0 & & & \end{pmatrix},$$

where $A \in \mathrm{GL}_{n-1}(\mathbb{F})$.

**Lemma 2.43.** *Let $G$ be a finite group and let $H \leq G$ with $[G : H] = n$. Then the action of $G$ on the left cosets of $H$ induces a homomorphism $\varphi : G \to S_n$, with*

$$\mathrm{Ker}\,\varphi = \bigcap_{g \in G} gHg^{-1}.$$

*Proof.* The action of $G$ on the left cosets of $H$ induces a homomorphism $\varphi : G \to S_n$, as we have seen in Lemma 2.35. The kernel of this homomorphism is the intersection of all stabilizers. The stabilizer of a left coset $gH$ is equal to $gHg^{-1}$, so $\mathrm{Ker}\,\varphi = \cap_{g \in G} gHg^{-1}$. □

We finish this section with one more example. Consider $G = \mathrm{GL}_2(2)$ and let $V = \mathbb{F}_2^2$ with basis $e_1$, $e_2$. In this case, the action of $G$ on $V \setminus \{0\}$ provides a homomorphism

$$\varphi : \mathrm{GL}_2(2) \to S_3,$$

since there are only 3 non-zero vectors $V$; indeed $V \setminus \{0\} = \{e_1, e_2, e_1 + e_2\}$.

It is clear that the action of $G$ is faithful, so $\varphi$ must be injective. Since $|\mathrm{GL}_2(2)| = |S_3|$, the map $\varphi$ is an isomorphism, and so $\mathrm{GL}_2(2) \cong S_3$. Labelling the non-zero vectors $e_1$, $e_2$, $e_1 + e_2$ as 1, 2, 3 we have

$$\varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = (1) \qquad \varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) = (1\ 2)$$

$$\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right) = (1\ 2\ 3) \qquad \varphi\left(\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right) = (1\ 3)$$

$$\varphi\left(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right) = (1\ 3\ 2) \qquad \varphi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) = (2\ 3)$$

# 3 Linear groups

In this section, we will prove some basic results about the groups $\mathrm{GL}_n(\mathbb{F})$ and $\mathrm{SL}_n(\mathbb{F})$, where $\mathbb{F}$ is a field. Our focus is on the case where $\mathbb{F}$ is a finite field, but many of the methods described in this section will work over arbitrary fields as well.

## 3.1 On finite fields

The main example of a finite field of $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$, the field of integers modulo $p$, where $p$ is a prime.

Let $\mathbb{F}$ be a finite field. Let $p$ be the *characteristic* of $\mathbb{F}$, i.e., the smallest positive integer such that

$$p1 = \underbrace{1 + \cdots + 1}_{p \text{ summands}} = 0.$$

Since $\mathbb{F}$ is a field, it follows that $p$ is a prime number, and moreover

$$\{m1 : m \in \mathbb{Z}\}$$

is a subfield of $\mathbb{F}$ isomorphic to $\mathbb{F}_p$, called the *prime field*. Thus we can identify $\mathbb{F}_p = \{m1 : m \in \mathbb{Z}\}$.

Now $\mathbb{F}$ is a vector space over $\mathbb{F}_p$ (scalar multiplication is just multiplication by elements of $\mathbb{F}_p$). Let $\alpha_1, \ldots, \alpha_n$ be a basis for $\mathbb{F}$ over $\mathbb{F}_p$. Then any element of $\mathbb{F}$ is uniquely expressed as a linear combination $\sum_{i=1}^n c_i\alpha_i$ with $c_i \in \mathbb{F}_p$, so it follows that $|\mathbb{F}| = p^n$.

Thus every finite field has order equal to a prime power. Conversely, for any prime power there exists a finite field of that order.

**Theorem 3.1.** *Let $q = p^n$, where $p$ is a prime. Then there exists a field $\mathbb{F}$ with $|\mathbb{F}| = q$, and moreover $\mathbb{F}$ is unique up to isomorphism.*

*Proof.* Omitted. □

Thus for each prime power $q = p^n$ there exists a unique field of order $q$ up to isomorphism, and we denote such a field by $\mathbb{F}_q$. Note that in Theorem 1.52, we proved that the multiplicative group of a finite field is cyclic. In other words, we have $\mathbb{F}_q^\times \cong C_{q-1}$ for any prime power $q$.

**Example 3.2.** We know that $\mathbb{F}_4^\times$ is cyclic of order 3, say $\mathbb{F}_4^\times = \{1, \alpha, \alpha^2\}$, where $\alpha^3 = 1$. Then

$$0 = \alpha^3 - 1 = (\alpha - 1)(\alpha^2 + \alpha + 1),$$

so $\alpha^2 + \alpha + 1 = 0$ since $\alpha \neq 1$. Since $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, it is clear how to multiply elements in $\mathbb{F}_4$.

| $\cdot$ | $0$ | $1$ | $\alpha$ | $\alpha^2$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $\alpha$ | $\alpha^2$ |
| $\alpha$ | $0$ | $\alpha$ | $\alpha^2$ | $1$ |
| $\alpha^2$ | $0$ | $\alpha^2$ | $1$ | $\alpha$ |

The addition operator in $\mathbb{F}_4$ is determined by the fact that $\alpha^2+\alpha+1=0$, for example $\alpha^2+\alpha=1$ and $\alpha+1=\alpha^2$. Note that $(\mathbb{F}_4,+)$ is not cyclic, since $x+x=0$ for all $x\in\mathbb{F}_4$.

| $+$ | $0$ | $1$ | $\alpha$ | $\alpha^2$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $\alpha$ | $\alpha^2$ |
| $1$ | $1$ | $0$ | $\alpha^2$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $\alpha^2$ | $0$ | $1$ |
| $\alpha^2$ | $\alpha^2$ | $\alpha^2$ | $1$ | $0$ |

## 3.2 Basic properties of $\mathrm{GL}_n(q)$ and $\mathrm{SL}_n(q)$

Let $q$ be a power of a prime. For $\mathrm{GL}_n(\mathbb{F}_q)$ and $\mathrm{SL}_n(\mathbb{F}_q)$, we use notation $\mathrm{GL}_n(q):=\mathrm{GL}_n(\mathbb{F}_q)$ and $\mathrm{SL}_n(q):=\mathrm{SL}_n(\mathbb{F}_q)$.

**Lemma 3.3.** $|\mathrm{GL}_n(q)|=(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

*Proof.* An $n\times n$ matrix is invertible if and only if its columns are linearly independent, i.e. if they form a basis of the vector space $\mathbb{F}_q^n$. Thus $|\mathrm{GL}_n(q)|$ is equal to the number of ordered bases of $\mathbb{F}_q^n$, as a vector space over $\mathbb{F}_q$. Now vectors $(v_1,\dots,v_n)$ form a basis if and only if $v_1\neq 0$, and $v_i\notin\langle v_1,\dots,v_{i-1}\rangle$ for all $1<i\leq n$. Thus there are $q^n-1$ choices for $v_1$. For each such $v_1$ there are $q^n-q$ possible choice for $v_2$, since there are $q$ vectors in $\langle v_1\rangle$. Similarly for $v_3$ we have $q^n-q^2$ choices, since there are $q^2$ vectors in $\langle v_1,v_2\rangle$. Continuing in this manner, we see that there are a total of

$$(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$$

bases of $\mathrm{GL}_n(q)$. □

For the order of $\mathrm{SL}_n(q)$, we note that $\mathrm{SL}_n(q)$ is the kernel of the homomorphism $\det:\mathrm{GL}_n(q)\to\mathbb{F}_q^\times$. It is easy to see that this homomorphism is surjective, so by the first isomorphism theorem $\mathrm{GL}_n(q)/\mathrm{SL}_n(q)\cong\mathbb{F}_q^\times$ and $|\mathrm{SL}_n(q)|=|\mathrm{GL}_n(q)|/(q-1)$.

**Lemma 3.4.** *Let $n\geq 1$. Then the following hold:*

(i) $Z(\mathrm{GL}_n(q)) = \{\lambda I_n : \lambda \in \mathbb{F}_q^\times\}$, *the group formed by scalar matrices in* $\mathrm{GL}_n(q)$.

(ii) $Z(\mathrm{SL}_n(q)) = \{\lambda I_n : \lambda \in \mathbb{F}_q^\times, \lambda^n = 1\}$.

*Proof.* Exercise. □

The group $\mathrm{PGL}_n(q) := \mathrm{GL}_n(q)/Z(\mathrm{GL}_n(q))$ is called the *projective general linear group* (over $\mathbb{F}_q$), while $\mathrm{PSL}_n(q) := \mathrm{SL}_n(q)/Z(\mathrm{SL}_n(q))$ is called the *projective special linear group* (over $\mathbb{F}_q$). It can be proven that if $n \geq 2$, then $\mathrm{PSL}_n(q)$ is a non-abelian simple group, except for $\mathrm{PSL}_2(2) \cong S_3$ and $\mathrm{PSL}_2(3) \cong A_4$.

## 3.3 Polynomial rings

Let $\mathbb{F}$ be a field. The polynomial ring $\mathbb{F}[t]$ in the indeterminate $t$ (or variable) is a the vector space over $\mathbb{F}$ with basis 1, $t$, $t^2$, $t^3$, ... where multiplication is defined as

$$\left(\sum_{i\geq 0} a_i t^i\right) \cdot \left(\sum_{j\geq 0} b_j t^j\right) = \sum_{k\geq 0} \left(\sum_{i+j=k} a_i b_j\right) t^k.$$

(We denote $t^0 = 1$.) Then $(\mathbb{F}[t], +, \cdot)$ is a commutative ring with multiplicative identity 1.

Each non-zero $p(t) \in \mathbb{F}[t]$ can be written uniquely in the form

$$p(t) = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + a_n t^n$$

for some $n \geq 0$ and $a_0$, ..., $a_n \in \mathbb{F}$, where $a_n \neq 0$. In this case we call $n$ the *degree* of $p(t)$ and denote $\deg p(t) = n$. A polynomial $p(t)$ is *constant*, if $p(t) = 0$ or $\deg p(t) = 0$; in other words $p(t) = a_0$ for some $a_0 \in \mathbb{F}$.

The ring $\mathbb{F}[t]$ is an *Euclidean domain*, in other words, there is a division algorithm. Suppose that $f(t) \in \mathbb{F}[t]$ is non-zero. Then for all $p(t) \in \mathbb{F}[t]$ there exist unique $q(t), r(t) \in \mathbb{F}[t]$ such that

$$p(t) = q(t)f(t) + r(t), \text{ where } r(t) = 0 \text{ or } \deg r(t) < \deg f(t).$$

If $r(t) = 0$, we say that $f(t)$ divides $p(t)$ and denote $f(t) \mid p(t)$.

For every $p(t) \in \mathbb{F}[t]$ and $c \in \mathbb{F}$, the division algorithm gives

$$p(t) = q(t)(t - c) + d$$

for some $d \in \mathbb{F}$. Thus it follows that $p(c) = 0$ if and only if $t - c$ divides $p(t)$.

A non-constant polynomial $p(t)$ is *irreducible* (over $\mathbb{F}$), if $p(t)$ cannot be written as the product of two non-constant polynomials in $\mathbb{F}[t]$. In other

words, if $p(t) = a(t)b(t)$, then $a(t)$ or $b(t)$ is constant. For example $t^2 + 1$ is irreducible in $\mathbb{R}[t]$, but has factorization

$$t^2 + 1 = (t - \mathbf{i})(t + \mathbf{i})$$

in $\mathbb{C}[t]$.

We call a non-zero polynomial $p(t) \in \mathbb{F}[t]$ *monic* if it has leading coefficient 1, in other words

$$p(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0$$

for some $c_0, \ldots, c_{n-1} \in \mathbb{F}$.

Since $\mathbb{F}[t]$ is an Euclidean domain, greatest common divisors exist. Let $f(t), g(t) \in \mathbb{F}[t]$. Then $d(t) = \gcd(f(t), g(t))$ is the unique monic polynomial such that:

- $d(t) \mid f(t)$ and $d(t) \mid g(t)$;
- If $p(t)$ is such that $p(t) \mid f(t)$ and $p(t) \mid g(t)$, then $p(t) \mid d(t)$.

By Bézout's lemma there exist $a(t), b(t) \in \mathbb{F}[t]$ such that

$$a(t)f(t) + b(t)g(t) = \gcd(f(t), g(t)).$$

Since $\mathbb{F}[t]$ is Euclidean, it is a unique factorization domain, so we have unique factorization of polynomials into irreducibles. Let $p(t) \in \mathbb{F}[t]$ be non-constant. Then

$$p(t) = \alpha p_1(t)^{k_1} \cdots p_r(t)^{k_r}$$

for some $\alpha \in \mathbb{F}$, monic irreducible polynomials $p_1(t), \ldots, p_r(t)$, and integers $k_1, \ldots, k_r > 0$. Moreover, this factorization of $p(t)$ is unique, up to the ordering of the factors $p_1(t), \ldots, p_r(t)$. For example, the factorization of $t^3 - 1$ into irreducibles is

$$\begin{aligned}
t^3 - 1 &= (t-1)(t^2 + t + 1) && \text{in } \mathbb{F}_2[t], \\
t^3 - 1 &= (t-1)^3 && \text{in } \mathbb{F}_3[t], \\
t^3 - 1 &= (t-1)(t^2 + t + 1) && \text{in } \mathbb{F}_5[t], \\
t^3 - 1 &= (t-1)(t-2)(t-3) && \text{in } \mathbb{F}_7[t].
\end{aligned}$$

## 3.4 Characteristic polynomials and eigenvalues

Let $\mathbb{F}$ be a field and let $V$ be a finite-dimensional vector space over $\mathbb{F}$. For a linear map $f : V \to V$, recall that an *eigenvector of $f$ with eigenvalue $\alpha \in \mathbb{F}$* is a non-zero vector $v \in V$ such that $f(v) = \alpha v$. For $\alpha \in \mathbb{F}$, we denote by $V_\alpha$ the *eigenspace*

$$V_\alpha = \{v \in V : f(v) = \alpha v\}.$$

Let $A \in \mathrm{GL}_n(\mathbb{F})$. Recall that the *characteristic polynomial of $A$* is the monic polynomial $p_A(t) \in \mathbb{F}[t]$ defined by

$$p_A(t) = \det(tI_n - A).$$

(Here we are taking the determinant of a matrix with entries in $\mathbb{F}[t]$.)

**Example 3.5.** Let $A \in \mathrm{GL}_2(\mathbb{F})$, say $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then

$$\begin{aligned} p_A(t) = \det \begin{pmatrix} t-a & -b \\ -c & t-d \end{pmatrix} &= (t-a)(t-d) - bc \\ &= t^2 - (a+d)t + (ad - bc) \\ &= t^2 - \mathrm{tr}(A)t + \det(A). \end{aligned}$$

(Here $\mathrm{tr}(A)$ is the *trace* of the matrix $A$, which is defined the sum of the diagonal entries of $A$.)

We recall some basic properties of $p_A(t)$. First note that the characteristic polynomial is the same for any conjugate of $A$.

**Lemma 3.6.** *Let $A \in \mathrm{GL}_n(\mathbb{F})$. Then any conjugate of $A$ has the same characteristic polynomial as $A$.*

*Proof.* We have

$$\begin{aligned} p_{XAX^{-1}}(t) &= \det(tI_n - XAX^{-1}) \\ &= \det(X(tI_n - A)X^{-1}) \\ &= \det(X)\det(tI_n - A)\det(X)^{-1} \\ &= p_A(t) \end{aligned}$$

for all $X \in \mathrm{GL}_n(\mathbb{F})$. □

.

**Lemma 3.7.** *Let $A \in \mathrm{GL}_n(\mathbb{F})$. Then $A$ has an eigenvector in $\mathbb{F}^n$ with eigenvalue $\alpha \in \mathbb{F}$ if and only if $\alpha$ is a root of $p_A(t)$.*

*Proof.* There is an eigenvector in $\mathbb{F}^n$ with eigenvalue $\alpha \in \mathbb{F}$ if and only if $\alpha I_n - A$ has nontrivial kernel, which is equivalent to $\det(\alpha I_n - A) = 0$. Since $p_A(\alpha) = \det(\alpha I_n - A)$, the result follows. □

## 3.5 Conjugacy classes of $\mathrm{GL}_2(q)$

In section, we will give a description of the conjugacy classes of $\mathrm{GL}_2(q)$.

**Lemma 3.8.** *Let $V = (\mathbb{F}_q)^2$. Suppose that $A \in \mathrm{GL}_2(q)$ has an eigenvector in $V$ with eigenvalue $\alpha \in \mathbb{F}_q$. Then the following hold:*

(i) *If the eigenspace $V_\alpha$ is 2-dimensional, then*

$$A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$$

*is a scalar matrix.*

(ii) *If $A$ has another eigenvalue $\beta \neq \alpha$, then $A$ has characteristic polynomial $(t-\alpha)(t-\beta)$ and is conjugate to*

$$s_{\alpha,\beta} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

(iii) *If the eigenspace $V_\alpha$ is 1-dimensional and $\alpha$ is the only eigenvalue of $A$, then $A$ has characteristic polynomial $(t-\alpha)^2$ and is conjugate to*

$$u_\alpha = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}.$$

(iv) *Let $\alpha, \alpha', \beta, \beta' \in \mathbb{F}_q$. Then $s_{\alpha,\beta}$ and $s_{\alpha',\beta'}$ are conjugate in $\mathrm{GL}_2(q)$ if and only if $\{\alpha, \beta\} = \{\alpha', \beta'\}$.*

(v) *Let $\alpha, \alpha' \in \mathbb{F}_q$. Then $u_\alpha, u_{\alpha'}$ are conjugate in $\mathrm{GL}_2(q)$ if and only if $\alpha = \alpha'$.*

*Proof.* (i) In this case $V = V_\alpha$, so $Av = \alpha v$ for all $v \in V$ which makes it clear that $A = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$.

(ii) We are assuming that $\alpha$ and $\beta$ are eigenvalues of $A$, so there exist non-zero vectors $v_\alpha \in V_\alpha$ and $v_\beta \in V_\beta$. Now $v_\beta \notin V_\alpha$, so $\{v_\alpha, v_\beta\}$ is linearly independent and thus a basis of $V$. Then the matrix of $A$ with respect to this basis is

$$s_{\alpha,\beta} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix},$$

so $A$ is conjugate to $s_{\alpha,\beta}$ in $\mathrm{GL}_2(q)$.

(iii) Let $v \in V_\alpha$ be nonzero, and extend this to a basis $\{v, w\}$ of $V$. We have $Av = \alpha v$ and $Aw = \beta w + \gamma v$ for some $\beta, \gamma \in \mathbb{F}_q$, so the matrix of $A$ with respect to this basis is

$$\begin{pmatrix} \alpha & \gamma \\ 0 & \beta \end{pmatrix}.$$

Thus the characteristic polynomial of $A$ is $(t-\alpha)(t-\beta)$, and so $\beta = \alpha$ since $\alpha$ is the only eigenvalue of $A$.

Note that $\gamma \neq 0$, as otherwise $w$ would be an eigenvector. Thus we can replace $v$ by $v' = \gamma v$ to get another basis $\{v', w\}$, for which $Av' = \alpha v'$ and $Aw = \alpha w + v'$, so the matrix of $A$ is

$$u_\alpha = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

with respect to the basis $\{v', w\}$. Therefore $A$ is conjugate to $u_\alpha$ in $\mathrm{GL}_2(q)$.

(iv) Suppose that $s_{\alpha,\beta}$ and $u_{\alpha',\beta'}$ are conjugate. Then they must have the same characteristic polynomial. Since their characteristic polynomials are $(t-\alpha)(t-\beta)$ and $(t-\alpha')(t-\beta')$, we conclude $\{\alpha, \beta\} = \{\alpha', \beta'\}$.

Conversely, suppose that $\{\alpha, \beta\} = \{\alpha', \beta'\}$. If $\alpha = \alpha'$ and $\beta = \beta'$, then $s_{\alpha,\beta} = s_{\alpha',\beta'}$. Otherwise $\alpha = \beta'$ and $\beta = \alpha'$, and we should show that $s_{\alpha,\beta}$ is conjugate to $s_{\alpha',\beta'} = s_{\beta,\alpha}$. Let $e_1, e_2$ be the standard basis of column vectors. Then with respect to the basis $\{e_2, e_1\}$ the matrix of $s_{\beta,\alpha}$ is the same as that of $s_{\alpha,\beta}$, so they are conjugate in $\mathrm{GL}_2(q)$. (For example via the change of basis matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.)

(v) If $u_\alpha$ and $u_{\alpha'}$ are conjugate, they must have the same characteristic polynomial. The characteristic polynomials of $u_\alpha$ and $u_{\alpha'}$ are $(t-\alpha)^2$ and $(t-\alpha')^2$, respectively, so $\alpha = \alpha'$. Conversely if $\alpha = \alpha'$ then $u_\alpha = u_{\alpha'}$.

□

**Lemma 3.9.** *Suppose that $A \in \mathrm{GL}_2(q)$ has no eigenvectors in $(\mathbb{F}_q)^2$, and let $p(t) = t^2 + \beta t + \alpha$ be the characteristic polynomial of $A$. Then:*

(i) *The polynomial $p(t)$ is irreducible, and $A$ is conjugate to*

$$C_{p(t)} = \begin{pmatrix} 0 & -\alpha \\ 1 & -\beta \end{pmatrix}.$$

(ii) *For any polynomial* $p(t) \in \mathbb{F}_q[t]$*, the matrix* $C_{p(t)}$ *in (i) has characteristic polynomial equal to* $p(t)$*.*

(iii) *Let* $p(t), q(t) \in \mathbb{F}_q[t]$ *be irreducible monic polynomials of degree* 2*. Then* $C_{p(t)}$ *and* $C_{q(t)}$ *are conjugate if and only if* $p(t) = q(t)$*.*

*Proof.* (i) As a degree two polynomial $p(t)$ is irreducible if and only if it has no roots in $\mathbb{F}_q$. This is the case since $A$ has no eigenvectors in $V = (\mathbb{F}_q)^2$.

Now pick a non-zero vector $v \in V$. Then $Av \notin \langle v \rangle$ since $A$ has no eigenvectors, so $\{v, Av\}$ is a basis of $V$. Thus we can write $A^2 v = -\alpha' v - \beta' Av$ for some $\alpha', \beta' \in \mathbb{F}_q$. Then with respect to the basis $\{v, Av\}$ the matrix of $A$ is

$$C = \begin{pmatrix} 0 & -\alpha' \\ 1 & -\beta' \end{pmatrix},$$

so $A$ is conjugate to $C$ in $\mathrm{GL}_2(q)$. The characteristic polynomial of $C$ is equal to $t^2 + \beta' t + \alpha'$. Since conjugate matrices have the same characteristic polynomial, we have $p(t) = t^2 + \beta' t + \alpha'$ and thus $\alpha' = \alpha$ and $\beta' = \beta$. In other words $C = C_{p(t)}$.

(ii) Straightforward calculation.

(iii) If $C_{p(t)}$ and $C_{q(t)}$ are conjugate, they must have the same characteristic polynomial, so $p(t) = q(t)$ by (ii). Conversely if $p(t) = q(t)$, then $C_{p(t)} = C_{q(t)}$.

□

In view of Lemma 3.9, to calculate the total number of conjugacy classes, we should count the number of irreducible polynomials $t^2 + \beta t + \alpha \in \mathbb{F}_q[t]$.

**Lemma 3.10.** *Let* $q$ *be a prime power. The number of irreducible polynomials in* $\mathbb{F}_q[t]$ *of the form* $t^2 + \beta t + \alpha$ *is equal to* $q(q-1)/2$*.*

*Proof.* Exercise. □

With Lemma 3.8 and Lemma 3.9, we have found representatives for all conjugacy classes of $\mathrm{GL}_2(q)$.

- $q - 1$ classes corresponding to scalar matrices (Lemma 3.8 (i)).
- $(q-1)(q-2)/2$ classes consisting of diagonal matrices with distinct eigenvalues (Lemma 3.8 (ii));

- $q-1$ classes consisting of non-diagonalizable matrices with an eigenvalue (Lemma 3.8 (iii));
- $q(q-1)/2$ classes with an irreducible characteristic polynomial (Lemma 3.9 and 3.10);

Thus there are a total of $k(G) = q^2 - 1$ conjugacy classes in $G$. We will now calculate the size of each conjugacy class $g^G$, which is equal to $[G : C_G(g)]$. A scalar matrix $g \in G$ is central, so $|g^G| = 1$. For diagonal matrices with distinct eigenvalues, we have $|C_G(g)| = (q-1)^2$, so $|g^G| = q(q+1)$. For $g \in G$ non-diagonalizable with one eigenvalue, we have $|C_G(g)| = q(q-1)$ and so $|g^G| = (q-1)(q+1)$. Finally for $g \in G$ with irreducible characteristic polynomial we have $|C_G(g)| = (q-1)(q+1)$ and so $|g^G| = q(q-1)$. (The details of these calculations are left as an exercise.) We summarize the information about the conjugacy classes in Table 2.

**Example 3.11.** Here is an illustration in the smallest case, $G = \mathrm{GL}_2(2)$. We have following representatives for the conjugacy classes:

- Scalar: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- Non-diagonalizable with one eigenvalue: $u_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
- Irreducible characteristic polynomial: $C_{p(t)} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ with irreducible characteristic polynomial $p(t) = t^2 + t + 1$ (This is the only irreducible degree 2 polynomial in $\mathbb{F}_2[t]$.)

Thus there are a total of 3 conjugacy classes. (One could also deduce this from the fact that $G \cong S_3$.)

**Example 3.12.** Exercise: Determine similarly representatives for the conjugacy classes of $\mathrm{GL}_2(3)$, and the size of each conjugacy class. (There are 8 conjugacy classes.)

**Example 3.13.** Exercise: Describe representatives for the conjugacy classes of elements of order 3 in $\mathrm{GL}_2(7)$. (There are 5 conjugacy classes of elements of order 3 in $\mathrm{GL}_2(7)$.)

| Type | Number of classes | Representatives | Characteristic polynomial | Size of class |
|---|---|---|---|---|
| Scalar | $q-1$ | $\begin{pmatrix}\alpha & 0\\ 0 & \alpha\end{pmatrix}$ | $(t-\alpha)^2$ | 1 |
| Diagonalizable | $(q-1)(q-2)/2$ | $\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}$, $\alpha \neq \beta$ | $(t-\alpha)(t-\beta)$ | $q(q+1)$ |
| Non-diagonal, one eigenvalue | $q-1$ | $\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}$ | $(t-\alpha)^2$ | $(q-1)(q+1)$ |
| Irreducible characteristic polynomial | $q(q-1)/2$ | $\begin{pmatrix}0 & -\alpha\\ 1 & -\beta\end{pmatrix}$ | $t^2+\beta t+\alpha$ (irreducible) | $q(q-1)$ |

Table 3: Conjugacy classes in $G = \mathrm{GL}_2(q)$.

## 3.6 Minimal polynomials

For $A \in \mathrm{GL}_n(\mathbb{F})$ and a polynomial $f(t) \in \mathbb{F}[t]$ with $f(t) = a_k t^k + a_{k-1}t^{k-1} + \cdots + a_1 t + a_0$, we denote by $f(A)$ the polynomial evaluated at the matrix $A$; in other words

$$f(A) = a_k A^k + a_{k-1}A^{k-1} + \cdots + a_1 A + a_0 I_n.$$

**Theorem 3.14** (Cayley–Hamilton theorem)**.** *Let $A \in \mathrm{GL}_n(\mathbb{F})$ with characteristic polynomial $p_A(t) \in \mathbb{F}[t]$. Then $p_A(A) = 0$.*

*Proof.* Omitted. (The usual proof is an application of the Jordan normal form.) □

For our purposes, we will mostly need the Cayley–Hamilton theorem in degree $n = 2$, in which case it is easy to prove. For $A \in \mathrm{GL}_2(\mathbb{F})$, we have

$$p_A(t) = t^2 - \mathrm{tr}(A)t + \det(A),$$

where $\mathrm{tr}(A)$ is the trace of $A$. It is straightforward to verify that

$$A^2 - \mathrm{tr}(A)A + \det(A)I_2 = 0.$$

A *minimal polynomial* for $A \in \mathrm{GL}_n(\mathbb{F})$ is a monic polynomial $m(t) \in \mathbb{F}[t]$ of minimal degree such that $m(A) = 0$.

**Lemma 3.15.** *Let $m(t)$ be a minimal polynomial of $A \in \mathrm{GL}_n(\mathbb{F})$. Let $f(t) \in \mathbb{F}[t]$. Then $f(A) = 0$ if and only if $m(t)$ divides $f(t)$.*

*Proof.* If $m(t)$ divides $q(t)$ the lemma is clear. For the other direction, use the division algorithm to write $f(t) = q(t)m(t) + r(t)$ where $\deg r(t) < \deg m(t)$; by minimality of $m(t)$ we must have $r(t) = 0$. □

It follows from Lemma 3.15 that a minimal polynomial of $A$ is unique. We will denote it by $m_A(t)$. By the Cayley–Hamilton theorem, $m_A(t)$ divides the characteristic polynomial $p_A(t)$.

**Lemma 3.16.** *Let $A \in \mathrm{GL}_n(\mathbb{F})$. Then any conjugate of $A$ has the same minimal polynomial as $A$.*

*Proof.* Let $g \in \mathrm{GL}_n(\mathbb{F})$. For any polynomial $p(t)$, we have $p(gAg^{-1}) = gp(A)g^{-1}$, so $p(A) = 0$ if and only if $p(gAg^{-1}) = 0$. The lemma follows. □

**Lemma 3.17.** *Let $A \in \mathrm{GL}_n(\mathbb{F})$. Then $\deg m_A(t) \leq n$.*

*Proof.* By Cayley–Hamilton $m_A(t)$ divides $p_A(t)$, from which the result follows. □

In degree $n = 2$, by the Cayley–Hamilton theorem the minimal polynomial of $A \in \mathrm{GL}_2(\mathbb{F})$ has either degree 2 or degree 1. Moreover, it is clear that the degree is 1 if and only if $A$ is equal to a scalar matrix

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$$

for some $\alpha \in \mathbb{F}^\times$. Thus if $A$ is not a scalar matrix, then by Cayley–Hamilton the minimal polynomial of $A$ is the characteristic polynomial of $A$. We record this observation in the following lemma.

**Lemma 3.18.** *Let $A \in \mathrm{GL}_2(\mathbb{F})$ be a non-scalar matrix. Then the minimal polynomial of $A$ is the characteristic polynomial $p_A(t) = t^2 - \mathrm{tr}(A)t + \det(A)I_2$ of $A$.*

**Example 3.19.** Let $\mathbb{F}$ be a field of characteristic $p > 0$. Suppose that $A \in \mathrm{GL}_2(\mathbb{F})$ is such that $|A| = p$. Since $p$ is prime, this is equivalent to $A^p = I_2$ and $A \neq I_2$. On the other hand, by the binomial theorem

$$(A - I_2)^p = \sum_{i=0}^{p} \binom{p}{i} A^i (-1)^{p-i} = A^p - I_2 = 0$$

since $\binom{p}{i} \equiv 0 \mod p$ for all $0 < i < p$. Therefore the minimal polynomial of $A$ divides $(A - I_2)^p$. Since the minimal polynomial has degree $\leq 2$ by Cayley–Hamilton, we conclude that $m_A(t) = (t - 1)^2$.

Therefore the only eigenvalue of $A$ is 1, and by Lemma 3.8 we conclude that $A$ is conjugate to the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

In particular, there is a unique conjugacy class of elements of order $p$ in $\mathrm{GL}_2(\mathbb{F})$.

## 3.7 Orders of elements

Let $q$ be a prime power. Using the minimal polynomial, we can describe the order of $A \in \mathrm{GL}_n(q)$. Indeed, we have $A^k = I_n$ if and only if $A^k - I_n = 0$, which by Lemma 3.15 is equivalent to $m_A(t)$ dividing the polynomial $t^k - 1$. Thus we have the following result.

**Lemma 3.20.** *Let $A \in \mathrm{GL}_n(q)$. Then $|A|$ is the smallest integer $k > 0$ such that $m_A(t)$ divides $t^k - 1$.*

We now illustrate this in degree $n = 2$ for matrices of determinant 1, and as an application give a proof of a theorem of Miller on the order of a product of two elements (Theorem 1.30). First we need a lemma.

**Lemma 3.21.** *Let $\mathbb{F}$ be a field of characteristic $\neq 2$. Let $A \in \mathrm{SL}_2(\mathbb{F})$ be such that $A$ has order 2. Then $A = -I_2$.*

*Proof.* Exercise. □

**Theorem 3.22** (Miller, 1900)**.** *Let $m, n, \ell > 1$ be integers. Then there exists a finite group $G$ which contains elements $x$ and $y$ such that $|x| = m$, $|y| = n$, and $|xy| = \ell$.*

*Proof.* Pick a prime $p$ such that $p$ does not divide $2mn\ell$. The image of $p$ in $(\mathbb{Z}/2mn\ell\mathbb{Z})^\times$ has some finite order $d$, so $q = p^d$ is equal to 1 modulo $2mn\ell$. We will construct elements $x, y \in \mathrm{SL}_2(q)$ such that $|x| = 2m$, $|y| = 2n$, and $|xy| = 2\ell$. Then since $-I_2$ is the unique element of order 2 in $\mathrm{SL}_2(q)$ (Lemma 3.21), we conclude that the images of $x$, $y$, $xy$ in $\mathrm{PSL}_2(q) = \mathrm{SL}_2(q)/\langle -I_2 \rangle$ have orders $m, n, \ell$, respectively.

The basic idea is that if $A \in \mathrm{SL}_2(q)$ is non-scalar, then the minimal polynomial and the characteristic polynomial of $A$ are equal (Lemma 3.18), and given by

$$m_A(t) = t^2 - \mathrm{tr}(A)t + 1.$$

Thus by Lemma 3.20, the order of a non-scalar matrix $A \in \mathrm{SL}_2(q)$ is completely determined by its trace.

Now $2m$, $2n$, $2\ell$ divide $|\mathbb{F}_q^\times| = q-1$, so since $\mathbb{F}_q^\times$ is cyclic (Theorem 1.52), we can find $\alpha, \beta, \gamma \in \mathbb{F}_q^\times$ with orders $|\alpha| = 2m$, $|\beta| = 2n$, and $|\gamma| = 2\ell$. Let $\delta \in \mathbb{F}_q$ and define

$$x = \begin{pmatrix} \alpha & 0 \\ \delta & \alpha^{-1} \end{pmatrix}, \qquad y = \begin{pmatrix} \beta & 1 \\ 0 & \beta^{-1} \end{pmatrix}.$$

Now $x$ has characteristic polynomial $(t-\alpha)(t-\alpha^{-1})$ and is thus similar to a diagonal matrix with entries $\alpha$, $\alpha^{-1}$. Therefore $|x| = 2m$, and similarly $|y| = 2n$. We have

$$xy = \begin{pmatrix} \alpha\beta & \alpha \\ \delta\beta & \delta + (\alpha\beta)^{-1} \end{pmatrix}.$$

Now with a suitable choice of $\delta$ we can make $\operatorname{tr}(xy)$ equal to any element of $\mathbb{F}_q$ we wish, in particular we can choose $\delta$ such that $xy$ has order $2\ell$.

Indeed, take $\delta = \gamma + \gamma^{-1} - \alpha\beta - (\alpha\beta)^{-1}$, in which case $\operatorname{tr}(xy) = \gamma + \gamma^{-1}$ and $xy$ has characteristic polynomial $(t-\gamma)(t-\gamma^{-1})$. Then $xy$ is similar to a diagonal matrix with entries $\gamma$, $\gamma^{-1}$, so $|xy| = 2\ell$. □

## 3.8 Factorizations of polynomials

In general, when classifying the conjugacy classes of $\mathrm{GL}_n(\mathbb{F})$, one can reduce to the case where the characteristic polynomial is equal to $p(t)^k$ for some irreducible polynomial $p(t)$ and integer $k > 0$. This is a consequence of the following lemma.

**Lemma 3.23.** *Let $A \in \mathrm{GL}_n(\mathbb{F})$. Suppose that $p(t), q(t) \in \mathbb{F}[t]$ are polynomials such that $\gcd(p(t), q(t)) = 1$ and $p(A)q(A) = 0$. Then $V = \mathbb{F}^n$ decomposes as a direct sum*

$$V = \operatorname{Ker} p(A) \oplus \operatorname{Ker} q(A).$$

*Proof.* Since $\gcd(p(t), q(t)) = 1$, by Bézout's identity in $\mathbb{F}[t]$ we have

$$a(t)p(t) + b(t)q(t) = 1$$

for some $a(t), b(t) \in \mathbb{F}[t]$. Thus for all $v \in V$ we have

$$v = I_n v = a(A)p(A)v + b(A)q(A)v. \tag{3.1}$$

Since $p(A)q(A) = 0$, we have $p(A)b(A)q(A) = b(A)p(A)q(A) = 0$, so we conclude that $b(A)q(A)v \in \operatorname{Ker} p(A)$. Similarly $a(A)p(A) \in \operatorname{Ker} q(A)$, so we have shown that $V = \operatorname{Ker} p(A) + \operatorname{Ker} q(A)$. To show that the sum is direct, we need to verify that $\operatorname{Ker} p(A) \cap \operatorname{Ker} q(A) = 0$. To this end, if $v \in \operatorname{Ker} p(A) \cap \operatorname{Ker} q(A)$, then it is immediate from (3.1) that $v = 0$. □

We illustrate Lemma 3.23 for $\mathrm{GL}_3(2)$. Now $|\mathrm{GL}_3(2)| = 168 = 2^3 \cdot 3 \cdot 7$. By Cauchy's theorem there exist elements of order 3 and 7 in $\mathrm{GL}_3(2)$. How to find such elements, and how to classify them up to conjugacy?

We consider elements of order 3 first. Suppose that $A \in \mathrm{GL}_3(2)$ is such that $|A| = 3$. Then the minimal polynomial of $A$ divides $t^3 - 1$, which factorizes as

$$t^3 - 1 = (t-1)(t^2 + t + 1).$$

Since $A \neq 1$, the minimal polynomial must be divisible by $t^2 + t + 1$, and thus the characteristic polynomial is divisible by $t^2+t+1$. The characteristic polynomial has degree 3, so it must be the product of $t^2 + t + 1$ and a factor of degree 1. This factor cannot be $t$ since $A$ does not have zero as eigenvalue, so it is $t - 1$ and so $p_A(t) = (t-1)(t^2 + t + 1) = t^3 - 1$.

The polynomials $t - 1$ and $t^2 + t + 1$ are coprime, so by Lemma 3.23 we have

$$\mathbb{F}_2^3 = \mathrm{Ker}(A - 1) \oplus \mathrm{Ker}(A^2 + A + 1).$$

Since 1 is a root of $p_A(t)$, we have $\dim \mathrm{Ker}(A-1) \geq 1$. A straightforward check shows that $\dim \mathrm{Ker}(A - 1) = 1$, so $\dim \mathrm{Ker}(A^2 + A + 1) = 2$. Let $v \in \mathrm{Ker}(A - 1)$ be non-zero, so $A(v) = v$. The linear map induced by $A$ on $\mathrm{Ker}(A^2+A+1)$ must have minimal polynomial and characteristic polynomial $A^2 + A + 1$, so by Lemma 3.9 it has a basis $\{w, w'\}$ such that $A(w) = w'$ and $A(w') = w + w'$.

We conclude then that with respect to the basis $\{v, w, w'\}$, the matrix of $A$ is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

and so $A$ is conjugate to this matrix. In particular we have shown that there is a unique conjugacy class of elements of order 3 in $\mathrm{GL}_3(2)$, with a representative given by the matrix above.

It turns out there are two conjugacy classes of elements of order 7 in $\mathrm{GL}_3(2)$. Let $A \in \mathrm{GL}_3(2)$ be such that $|A| = 7$. Then $A^7 = 1$, so the minimal polynomial of $A$ divides $t^7 - 1 \in \mathbb{F}_2[t]$, which has a factorization into irreducible polynomials as

$$t^7 - 1 = (t-1)(t^3 + t + 1)(t^3 + t^2 + 1)$$

in $\mathbb{F}_2[t]$.

Since the minimal polynomial of $A$ has degree at most 3 (Lemma 3.17), it follows that the minimal polynomial of $A$ is either $t - 1$, $t^3 + t + 1$, or $t^3 + t^2 + 1$. It cannot be $t - 1$ since $A \neq 1$, so $m_A(t) = t^3 + t + 1$ or $t^3 + t^2 + 1$.

Both possibilities can be realized, and these correspond to the two conjugacy classes of elements of order 7. This is seen from the next lemma.

**Lemma 3.24.** *Let $A \in \mathrm{GL}_3(q)$ with minimal polynomial $p(t) = t^3 + \gamma t^2 + \beta t + \alpha$ irreducible in $\mathbb{F}_q[t]$. Then:*

(i) *We have $p_A(t) = p(t)$, and $A$ is conjugate to the matrix*

$$C_{p(t)} = \begin{pmatrix} 0 & 0 & -\alpha \\ 1 & 0 & -\beta \\ 0 & 1 & -\gamma \end{pmatrix}$$

(ii) *For any irreducible polynomial $p(t) \in \mathbb{F}_q[t]$, the matrix $C_{p(t)}$ as in (i) has its characteristic and minimal polynomial equal to $p(t)$.*

(iii) *Let $p(t), q(t) \in \mathbb{F}_q[t]$ be irreducible monic polynomials of degree 3. Then $C_{p(t)}$ and $C_{q(t)}$ are conjugate in $\mathrm{GL}_3(q)$ if and only if $p(t) = q(t)$.*

*Proof.* (i) Since the minimal polynomial divides $p_A(t)$ and $\deg p_A(t) = 3$, it follows that $p_A(t) = p(t)$.

Let $V = \mathbb{F}_q^3$ and pick a non-zero vector $v \in V$. Now $A$ has no eigenvalues since $p_A(t) = p(t)$ is irreducible, so $Av \notin \langle v \rangle$. Thus $\{v, Av\}$ is linearly independent. We claim that $A^2 v \notin \langle v, Av \rangle$. For if we had $A^2 v \in \langle v, Av \rangle$, then the action of $A$ on $W = \langle v, Av \rangle$ would induce a linear map $A' : W \to W$. Now $\dim W = 2$, so $A'$ has minimal polynomial $m_{A'}(t)$ of degree $\leq 2$. On the other hand $p(A') = 0$, so $m_{A'}(t) \mid p(t)$, a contradiction since $p(t)$ is irreducible.

Thus $A^2 \notin \langle v, Av \rangle$. Then $\{v, Av, A^2 v\}$ is a basis of $V$, and we can write $A^3 v = -\alpha' v - \beta' Av - \gamma' A^2 v$ for some $\alpha', \beta', \gamma' \in \mathbb{F}_q$. Then with respect to the basis $\{v, Av, A^2 v\}$, the matrix of $A$ is

$$C = \begin{pmatrix} 0 & 0 & -\alpha' \\ 1 & 0 & -\beta' \\ 0 & 1 & -\gamma' \end{pmatrix},$$

so $A$ is conjugate to $C$ in $\mathrm{GL}_3(q)$. A straightforward calculation shows that $C$ has characteristic polynomial equal to $q(t) = t^3 + \gamma' t^2 + \beta' t + \alpha'$. Since $A$ and $C$ have the same characteristic polynomial we get $q(t) = p(t)$, and so $C = C_{p(t)}$.

(ii) A calculation shows that the characteristic polynomial is equal to $p(t)$. Since the minimal polynomial divides the characteristic polynomial and since $p(t)$ is irreducible, we conclude that $p(t)$ is also the minimal polynomial.

(iii) If $C_{p(t)}$ and $C_{q(t)}$ are conjugate, they have the same characteristic polynomial, so $p(t) = q(t)$ by (ii). Conversely if $p(t) = q(t)$, then $C_{p(t)} = C_{q(t)}$.

□

As we saw before, for an element $A \in \mathrm{GL}_3(2)$ of order 7, the minimal polynomial $m_A(t)$ is irreducible and equal to $t^3 + t + 1$ or $t^3 + t^2 + 1$. Thus it follows from Lemma 3.24 that $A$ is conjugate to

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

if $m_A(t) = t^3 + t + 1$, and $A$ is conjugate to

$$Q = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

if $m_A(t) = t^3 + t^2 + 1$. Note that by Lemma 3.24, we have $m_P(t) = t^3 + t + 1$ and $m_Q(t) = t^3 + t^2 + 1$.

**Example 3.25.** Exercise: We have $|\mathrm{GL}_3(7)| = 2^6 \cdot 3^4 \cdot 7^3 \cdot 19$. Find representatives for conjugacy classes of elements of order 19 in $\mathrm{GL}_3(7)$. (There are 6 classes. Use the factorization $t^{19} - 1 = (t-1)(t^3 + 2t - 1)(t^3 + 3t^2 + 3t - 1)(t^3 + 4t^2 + t - 1)(t^3 + 4t^2 + 4t - 1)(t^3 + 5t^2 - 1)(t^3 + 6t^2 + 3t - 1)$ in $\mathbb{F}_7[t]$.)

## 3.9 Generators for $\mathrm{GL}_2(\mathbb{F})$ and $\mathrm{SL}_2(\mathbb{F})$

Let $\mathbb{F}$ be a field. In $\mathrm{GL}_2(\mathbb{F})$, a *transvection* is a matrix which has one of the following forms:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \qquad\qquad \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$$

where $x, y \in \mathbb{F}^\times$.

We have the following result.

**Lemma 3.26.** *Any two transvections are conjugate in* $\mathrm{GL}_2(\mathbb{F})$.

*Proof.* Immediate from Lemma 3.8 (iii). □

**Lemma 3.27.** *The special linear group* $\mathrm{SL}_2(\mathbb{F})$ *is generated by transvections.*

*Proof.* Let $A \in \mathrm{SL}_2(\mathbb{F})$, say $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. We note first that multiplying $A$ on the left with a transvection corresponds to row operations; and similarly multiplying $A$ on the right with a transvection corresponds to column operations. That is, for all $\lambda \in \mathbb{F}$:

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a + \lambda c & b + \lambda d \\ c & d \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c + \lambda a & d + \lambda b \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b + \lambda a \\ c & d + \lambda c \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \lambda & 1 \end{pmatrix} = \begin{pmatrix} a + \lambda b & b \\ c + \lambda d & d \end{pmatrix}$$

Suppose that $c \neq 0$. Then with row and column operations, we can reduce $A$ into the identity matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} 1 & b' \\ c & d \end{pmatrix} \to \begin{pmatrix} 1 & b' \\ 0 & d' \end{pmatrix} \to \begin{pmatrix} 1 & 0 \\ 0 & d' \end{pmatrix}$$

where $d' = 1$ since row and column operations do not change the determinant. Thus there exist transvections $x_1, \ldots, x_t, y_1, \ldots, y_s$ such that

$$x_1 \cdots x_t A y_1 \cdots y_s = I_2$$

which implies that $A$ is contained in the subgroup generated by transvections.

If $c = 0$, then we must have $a \neq 0$. Then adding the first row to the second changes $A$ into a matrix where the entry corresponding to $c$ is non-zero. It follows from the previous case that $A$ is contained in the subgroup generated by transvections. □

**Remark 3.28.** In general for $\mathrm{GL}_n(\mathbb{F})$, a transvection is defined as follows. For $1 \leq i, j \leq n$, let $E_{i,j}$ be the $(n \times n)$ matrix with 1 as the $(i, j)$ entry (row $i$, column $j$) and zeroes elsewhere. Then in $\mathrm{GL}_n(\mathbb{F})$, a *transvection* is a matrix of the form $I_n + \lambda E_{i,j}$, where $\lambda \in \mathbb{F}$ and $i \neq j$. Similarly to the proof of Lemma 3.27, with Gaussian elimination one can show that $\mathrm{SL}_n(\mathbb{F})$ is generated by transvections.

**Lemma 3.29.** *The general linear group* $\mathrm{GL}_2(\mathbb{F})$ *is generated by the set of transvections, together with matrices of the form* $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$, *where* $\lambda \in \mathbb{F}^\times$.

*Proof.* Exercise. □

Let $q$ be a prime power. The set of generators for $\mathrm{SL}_2(q)$ provided by Lemma 3.27 has size $2q$, while the set of generators for $\mathrm{GL}_2(q)$ in Lemma 3.29 has size $3q$. It turns out we can find a much smaller set of generators, and indeed both groups can always be generated by two elements. For example, suppose that $q \neq 2$ and let $\zeta \in \mathbb{F}_q^\times$ be a generator for $\mathbb{F}_q^\times \cong C_{q-1}$. Then for

$$x = \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix} \qquad x' = \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \qquad y = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

we have $\mathrm{GL}_2(q) = \langle x, y \rangle$ and $\mathrm{SL}_2(q) = \langle x', y \rangle$. This follows from a 1962 result of Steinberg.

## 3.10 Simplicity of $\mathrm{PSL}_2(q)$

Let $q$ be a prime power. We know that $\mathrm{PSL}_2(2) \cong S_3$ and $\mathrm{PSL}_2(3) \cong A_4$ are not simple. In this section, we will prove that $\mathrm{PSL}_2(q)$ is simple for $q > 3$. We will first do this for $q = 4$ and $q > 5$. After that we will prove that $\mathrm{PSL}_2(5) \cong A_5$, so then $\mathrm{PSL}_2(5)$ is simple since $A_5$ is (Theorem 2.32).

**Lemma 3.30.** *Let $\alpha \in \mathbb{F}_q^\times$ be such that $\alpha \neq \pm 1$. Suppose that $A \in \mathrm{SL}_2(q)$ has characteristic polynomial $p_A(t) = (t - \alpha)(t - \alpha^{-1})$. Then $A$ is conjugate to*

$$S = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$$

*in $\mathrm{SL}_2(q)$.*

*Proof.* By Lemma 3.9 we know that $A$ is conjugate to $S$ in $\mathrm{GL}_2(q)$, in other words $XAX^{-1} = S$ for some $X \in \mathrm{GL}_2(q)$. Let $\lambda = \det(X)$. Now $S$ commutes with the diagonal matrix

$$D = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{pmatrix},$$

so $DXA(DX)^{-1} = S$. Now $\det(DX) = \det(D)\det(X) = 1$, so $DX \in \mathrm{SL}_2(q)$ conjugates $A$ into $S$ in $\mathrm{SL}_2(q)$. □

**Lemma 3.31.** *Suppose that $q = 4$ or $q > 5$ and let $A \in \mathrm{SL}_2(q)$ be a non-scalar matrix. Then there exists $B \in \mathrm{SL}_2(q)$ such that $ABA^{-1}B^{-1}$ is conjugate to a matrix of the form*

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

*for some $\lambda \in \mathbb{F}_q^\times$ with $\lambda \neq \pm 1$.*

*Proof.* Let $V = \mathbb{F}_q^2$. Since $A$ is non-scalar, there exists a vector $v \in V \setminus \{0\}$ which is not an eigenvector of $A$ (Exercise 3.18). In other words we have $Av \notin \langle v \rangle$, so $\{v, Av\}$ is a basis of $V$. Write $A^2 v = \alpha v + \beta Av$. Then with respect to the basis $\{v, Av\}$, the matrix of $A$ is

$$\begin{pmatrix} 0 & \alpha \\ 1 & \beta \end{pmatrix}.$$

Since $A$ has determinant 1, we must have $\alpha = -1$. Thus by replacing $A$ with a conjugate, we may assume that

$$A = \begin{pmatrix} 0 & -1 \\ 1 & \beta \end{pmatrix}.$$

Define

$$B = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix}.$$

Then $B \in \mathrm{SL}_2(q)$, and $ABA^{-1}B^{-1}$ is equal to

$$\begin{pmatrix} 0 & -1 \\ 1 & \beta \end{pmatrix} \begin{pmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{pmatrix} \begin{pmatrix} \beta & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \mu^{-1} & 0 \\ 0 & \mu \end{pmatrix} = \begin{pmatrix} \mu^{-2} & 0 \\ \beta - \beta\mu^{-2} & \mu^2 \end{pmatrix}.$$

Hence $ABA^{-1}B^{-1}$ has characteristic polynomial $(t - \mu^2)(t - \mu^{-2})$, so by Lemma 3.30 it is conjugate to

$$\begin{pmatrix} \mu^2 & 0 \\ 0 & \mu^{-2} \end{pmatrix}$$

in $\mathrm{SL}_2(q)$. Since we are assuming $q = 4$ or $q > 5$, there exists $\mu \in \mathbb{F}_q^\times$ such that $\mu^2 \neq \pm 1$, so the lemma follows. □

**Theorem 3.32.** *Suppose that $q = 4$ or $q > 5$, and let $N$ be a normal subgroup of $\mathrm{SL}_2(q)$. Then $N = \{1\}$, $N = Z(\mathrm{SL}_2(q)) = \{\pm I_2\}$, or $N = \mathrm{SL}_2(q)$.*

*Proof.* Let $N \trianglelefteq \mathrm{SL}_2(q)$ be such that $N \neq \{1\}$ and $N \neq Z(\mathrm{SL}_2(q))$. We will show that $N$ contains every transvection, which by Lemma 3.27 implies that $N = \mathrm{SL}_2(q)$.

Since $N$ is not contained in $Z(\mathrm{SL}_2(q))$, there exists a non-scalar matrix $A \in N$. Then by Lemma 3.31, we can find $B \in \mathrm{SL}_2(q)$ such that $ABA^{-1}B^{-1}$ is conjugate in $\mathrm{SL}_2(q)$ to a diagonal matrix

$$D = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

for some $\lambda \in \mathbb{F}_q^\times$ with $\lambda \neq \pm 1$. Now $ABA^{-1}B^{-1} \in N$ since $N$ is a normal subgroup, so we conclude that $D \in N$. By Lemma 3.30, we find that $N$ contains every matrix in $\mathrm{SL}_2(q)$ with characteristic polynomial $(t-\lambda)(t-\lambda^{-1})$. Therefore

$$\begin{pmatrix} \lambda & x\lambda^{-1} \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in N$$

for all $x \in \mathbb{F}_q$. Similarly by taking transposes

$$\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \in N$$

for all $x \in \mathbb{F}_q$. This completes the proof of the theorem. □

**Corollary 3.33.** *Suppose that $q = 4$ or $q > 5$. Then $\mathrm{PSL}_2(q)$ is simple.*

*Proof.* By Theorem 3.32, there only normal subgroups $N \trianglelefteq \mathrm{SL}_2(q)$ with $Z(\mathrm{SL}_2(q)) \leq N \leq \mathrm{SL}_2(q)$ are $N = Z(\mathrm{SL}_2(q))$ and $N = \mathrm{SL}_2(q)$. Thus by the correspondence theorem $\mathrm{PSL}_2(q) = \mathrm{SL}_2(q)/Z(\mathrm{SL}_2(q))$ is simple. □

**Theorem 3.34.** $\mathrm{PGL}_2(5) \cong S_5$.

*Proof.* For $\mathrm{GL}_2(5)$, we have a natural action on a 2-dimensional vector space $V = \mathbb{F}_5^2$ over $\mathbb{F}_5$. Let $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ be the standard basis of column vectors. Since $\mathrm{GL}_2(5)$ acts on $V$, it also acts on the set of 1-dimensional subspaces of $V$:

$$\Omega = \{\langle v \rangle : v \in V \setminus \{0\}\}.$$

(The action is the obvious one: $g \cdot \langle v \rangle = \langle gv \rangle$ for all $g \in \mathrm{GL}_2(5)$ and $v \in V \setminus \{0\}$.) The set $\Omega$ is known as the projective line $\mathbb{P}^1(\mathbb{F}_5)$ over $\mathbb{F}_5$, or the Grassmannian $\mathrm{Gr}(1, V)$.

It is readily seen that there are 6 subspaces in $\Omega$; hence there is a homomorphism $\varphi : \mathrm{GL}_2(5) \to S_6$ corresponding to this action. By Exercise 3.18 the kernel $\operatorname{Ker}\varphi$ consists of the scalar matrices, thus $\varphi(\mathrm{GL}_2(5)) \cong \mathrm{PGL}_2(5)$ by the first isomorphism theorem.

We label the points in $\Omega$ by 1,2,3,4,5,6 as follows:

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| $\langle e_1 \rangle$ | $\langle e_2 \rangle$ | $\langle e_1 + e_2 \rangle$ | $\langle 2e_1 + e_2 \rangle$ | $\langle 3e_1 + e_2 \rangle$ | $\langle 4e_1 + e_2 \rangle$ |

Then for example $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is mapped to (2 3 4 5 6) by $\varphi$. For $S_5$ we will find a faithful action on 6 points, such that for the corresponding homomorphism $\psi : S_5 \to S_6$ we have $\psi(S_5) = \varphi(\mathrm{GL}_2(5))$. Then $S_5 \cong \varphi(G) \cong \mathrm{PGL}_2(5)$ and the theorem follows.

To this end, let $\Omega'$ be the set of subgroups of order 5 in $S_5$, and consider the action of $S_5$ on $\Omega'$ by conjugation. Each subgroup in $\Omega'$ is generated by a 5-cycle, and there are a total of

$$\frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{5} = 24$$

5-cycles in $S_5$. In each subgroup of order 5 there are a total of four 5-cycles, and distinct subgroups of order 5 have no elements of order 5 in common. Therefore the total number of subgroups of order 5 in $S_5$ is

$$|\Omega'| = 24/4 = 6.$$

Let $\psi : S_5 \to S_6$ be the homomorphism corresponding to the action of $S_5$ on $\Omega'$. We label the elements of $\Omega'$ has $H_1$, $H_2$, $H_3$, $H_4$, $H_5$, $H_6$ as follows:

| $H_1$ | $H_2$ | $H_3$ | $H_4$ | $H_5$ | $H_6$ |
|---|---|---|---|---|---|
| $\langle(1\ 2\ 3\ 4\ 5)\rangle$ | $\langle(1\ 2\ 3\ 5\ 4)\rangle$ | $\langle(1\ 5\ 2\ 3\ 4)\rangle$ | $\langle(1\ 3\ 4\ 5\ 2)\rangle$ | $\langle(1\ 3\ 2\ 4\ 5)\rangle$ | $\langle(1\ 2\ 4\ 3\ 5)\rangle$ |

We have chosen this labeling so that for $\sigma = (1\ 2\ 3\ 4\ 5) \in H_1$ we have

$$\psi(\sigma) = (2\ 3\ 4\ 5\ 6) = \varphi\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right).$$

Note that this implies that $\operatorname{Ker}\psi = \{(1)\}$ since the only normal subgroups of $S_5$ are $\{(1)\}$, $A_5$, and $S_5$ (Exercise 2.12). Thus $S_5 \cong \psi(S_5)$.

For $\tau = (1\ 2)$ and $\sigma = (1\ 2\ 3\ 4\ 5)$ we have $S_5 = \langle \tau, \sigma \rangle$ (Exercise 2.2), so $S_5 \cong \psi(S_5) = \langle \psi(\tau), \psi(\sigma) \rangle$. A calculation shows that $\psi(\tau) = (1\ 4)(2\ 3)(5\ 6)$ and we know that $\psi(\sigma) = (2\ 3\ 4\ 5\ 6)$, so

$$\psi(S_5) = \langle (1\ 4)(2\ 3)(5\ 6), (2\ 3\ 4\ 5\ 6) \rangle.$$

Next we will show that $\psi(S_5) \leq \varphi(\mathrm{GL}_2(5))$ and thus $\psi(S_5) = \varphi(\mathrm{GL}_2(5))$ since $|S_5| = 120$ and $|\varphi(\mathrm{GL}_2(5))| = |\operatorname{PGL}_2(5)| = 120$. To this end, it will suffice to prove that $\psi(\tau), \psi(\sigma) \in \varphi(\mathrm{GL}_2(5))$. We already saw that $\psi(\sigma)$ is the image of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. For $\psi(\tau)$ we would need a matrix $A \in \mathrm{GL}_2(5)$ that maps the first basis vector $e_1$ to a scalar multiple of $2e_1 + e_2$ (and vice versa), and the second basis vector $e_2$ to a scalar multiple of $e_1 + e_2$ (and vice versa). This determines $A$ up to a scalar, and indeed a straightforward calculation shows that

$$\varphi\left(\begin{pmatrix} 2 & 3 \\ 1 & 3 \end{pmatrix}\right) = (1\ 4)(2\ 3)(5\ 6) = \psi(\tau).$$

This completes the proof of the theorem. □

**Corollary 3.35.** $\mathrm{PSL}_2(5) \cong A_5$. *In particular,* $\mathrm{PSL}_2(5)$ *is simple.*

*Proof.* We note that $\mathrm{PSL}_2(5)$ can be embedded as a normal subgroup of $\mathrm{PGL}_2(5)$. Indeed, this is true in general: let $\pi : \mathrm{GL}_n(q) \to \mathrm{PGL}_n(q)$ be the natural quotient map, so $\operatorname{Ker}\pi$ is the set of scalar matrices in $\mathrm{GL}_n(q)$ by Lemma 3.4. Then $\pi(\mathrm{SL}_n(q)) \trianglelefteq \mathrm{PGL}_n(q)$ since $\mathrm{SL}_n(q) \trianglelefteq \mathrm{GL}_n(q)$, and $\pi(\mathrm{SL}_n(q)) \cong \mathrm{PSL}_n(q)$ by the first isomorphism theorem and Lemma 3.4.

Now $|\mathrm{PSL}_2(5)| = 60$ and $|\mathrm{PGL}_2(5)| = 120$, so $\mathrm{PSL}_2(5)$ is a normal subgroup of index 2 in $\mathrm{PGL}_2(5)$. Since $A_5$ is the unique subgroup of index 2 in $S_5$ (Proposition 2.27), by Theorem 3.34 we have $\mathrm{PSL}_2(5) \cong A_5$. Since $A_5$ is simple (Theorem 2.32), we conclude that $\mathrm{PSL}_2(5)$ is simple. □

Here is a list of some exceptional isomorphisms involving $\mathrm{PSL}_2(q)$ and $\mathrm{PGL}_2(q)$:

$$\begin{aligned}
\mathrm{PSL}_2(2) &\cong S_3 \\
\mathrm{PGL}_2(3) &\cong S_4 \\
\mathrm{PSL}_2(3) &\cong A_4 \\
\mathrm{PSL}_2(4) &\cong A_5 \\
\mathrm{PGL}_2(5) &\cong S_5 \\
\mathrm{PSL}_2(5) &\cong A_5 \\
\mathrm{PSL}_2(7) &\cong \mathrm{PSL}_3(2) \\
\mathrm{PSL}_2(9) &\cong A_6 \\
\mathrm{PSL}_4(2) &\cong A_8
\end{aligned}$$

# 4 Normal series

## 4.1 Characteristic subgroups

**Definition 4.1.** Let $G$ be a group. A subgroup $H \leq G$ is a *characteristic subgroup*, if $\varphi(H) = H$ for every automorphism $\varphi : G \to G$. We denote this by $H \operatorname{char} G$.

**Example 4.2.** Some basic examples:

(a) In any group $G$, the trivial subgroup $\{1\}$ and the group $G$ itself are characteristic subgroups.

(b) For any group $G$, we have $Z(G) \operatorname{char} G$.

(c) If $G$ is a finite group such that $G$ has exactly one subgroup $N$ with $|N| = d$, then $N \operatorname{char} G$. This is because for any automorphism $\varphi : G \to G$, the image $\varphi(N)$ is also a subgroup of order $d$. Thus if $G$ is finite cyclic, then every subgroup of $G$ is characteristic.

**Lemma 4.3.** *Let $G$ be a group. Then the following statements hold:*

(i) *Suppose that $H \operatorname{char} G$. Then $H \trianglelefteq G$.*

(ii) *Suppose that $H \operatorname{char} K \operatorname{char} G$. Then $H \operatorname{char} G$.*

(iii) *Suppose that $H \operatorname{char} K \trianglelefteq G$. Then $H \trianglelefteq G$.*

*Proof.* (i) Let $g \in G$ and consider the inner automorphism $\gamma_g : G \to G$ defined by $\gamma_g(x) = gxg^{-1}$. Since $H$ is characteristic in $G$, we have $H = \gamma_g(H) = gHg^{-1}$. Therefore $H \trianglelefteq G$.

(ii) Let $\varphi : G \to G$ be an automorphism of $G$. Since $K$ is characteristic in $G$, we have $\varphi(K) = K$ and so the restriction of $\varphi$ to $K$ is an automorphism $\varphi' : K \to K$ of $K$. Since $H$ is characteristic in $K$, we have $\varphi'(H) = H$, and thus $\varphi(H) = H$.

(iii) Let $g \in G$. Since $K$ is a normal subgroup, the inner automorphism $\gamma_g : G \to G$ restricts to an automorphism $\gamma_g' : K \to K$ of $K$. Because $H$ is characteristic in $K$, we have $\gamma_g'(H) = H$, in other words $gHg^{-1} = H$. Thus $H \trianglelefteq G$.

□

**Example 4.4.** Not all normal subgroups are characteristic. For example, consider the subgroup $G = \langle (1\ 2), (3\ 4) \rangle$ of $S_4$. One checks that conjugation by $g = (1\ 3\ 2\ 4)$ gives an automorphism $\varphi : G \to G$, where $\varphi(x) = gxg^{-1}$ for all $x \in G$. Then $\varphi((1\ 2)) = (3\ 4)$ and $\varphi((3\ 4)) = (1\ 2)$, so the normal subgroups $\langle (1\ 2) \rangle$ and $\langle (3\ 4) \rangle$ are not characteristic in $G$.

## 4.2 Commutator subgroups and solvability

Let $G$ be a group. For $x, y \in G$ we have $xy = yx$ if and only if $x^{-1}y^{-1}xy = 1$. We call $x^{-1}y^{-1}xy$ the *commutator* of $x$ and $y$, and denote it by

$$[x, y] := x^{-1}y^{-1}xy.$$

**Definition 4.5.** Let $G$ be a group. The *commutator subgroup* of $G$ is the subgroup $[G, G] := \langle [x, y] : x, y \in G \rangle$; in other words, the subgroup generated by the commutators in $G$. More generally, for subgroups $H, K \leq G$, we define the *commutator subgroup of $H$ and $K$* as

$$[H, K] := \langle [x, y] : x \in H, y \in K \rangle.$$

**Remark 4.6.** In general it is not true that the set of commutators is a subgroup. In other words, it may happen that $[G, G]$ is not the set of commutators in $G$. Later in this section we will provide an example for $G = \mathrm{SL}_2(\mathbb{R})$. (For finite groups, the smallest example has order $|G| = 96$.)

At this point we provide the following example which shows that for $H, K \leq G$ the subgroup $[H, K]$ is not necessarily equal to the set of commutators $[h, k]$ with $h \in H$ and $k \in K$. Let $G = A_4$ and consider $H = \langle (1\ 2)(3\ 4) \rangle$ and $K = \langle (1\ 2\ 3) \rangle$. Then

$$\{[h, k] : h \in H, k \in K\} = \{(1), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$
$$[H, K] = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

There are also many examples where $[G, G]$ is equal to the set of all commutators, this holds for example for $G = S_n$ or $G = A_n$. The *Ore conjecture* states that every element of a finite non-abelian simple group is a commutator. The Ore conjecture is now a theorem, and its proof was completed by Liebeck, O'Brien, Shalev, and Tiep (J. Eur. Math. Soc., 2010) using the classification of finite simple groups.

Recall that for elements $g$ and $x$ in a group $G$, we denote $g^x = x^{-1}gx$. Thus $[g, x] = g^{-1}g^x$ for all $g, x \in G$.

**Lemma 4.7.** *Let $G$ be a group and $x, y, z \in G$. Then the following identities hold:*

(i) $[x, y]^{-1} = [y, x]$.

(ii) $xy = yx[x, y]$.

(iii) $[xy, z] = [x, z]^y[y, z]$.

(iv) $[x, yz] = [x, z][x, y]^z$.

(v) $[x, y]^z = [x^z, y^z]$.

*Proof.* Exercise. □

Note that by Lemma 4.7, we have $[H, K] = [K, H]$ for any subgroups $H$ and $K$ of a group $G$.

**Lemma 4.8.** *Let $G$ be a group and $x, y \in G$. Suppose that $x$ and $y$ commute with $[x, y]$. Then*

$$(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$$

*for all $n \in \mathbb{Z}_{\geq 0}$.*

*Proof.* Exercise. □

**Lemma 4.9.** *Let $G$ be a group and $H \leq G$. Then $H \trianglelefteq G$ if and only if $[H, G] \leq H$.*

*Proof.* Suppose that $H \trianglelefteq G$. Then $[h, g] = h^{-1}g^{-1}hg \in H$ for all $h \in H$ and $g \in G$, since $g^{-1}hg \in H$ by normality. Thus $[H, G] \leq H$. Conversely, suppose that $[H, G] \leq G$. Then in particular $[h, g] = h^{-1}g^{-1}hg \in H$ for all $h \in H$ and $g \in G$, so $h[h, g] = g^{-1}hg \in H$ for all $g \in G$ and $h \in H$. Thus $H \trianglelefteq G$. □

**Lemma 4.10.** *Let $G$ be group. Then the following statements hold:*

(i) *$G$ is abelian if and only if $[G, G] = \{1\}$.*

(ii) *If $[G, G] \leq N \leq G$, then $N \trianglelefteq G$. In particular $[G, G] \trianglelefteq G$.*

(iii) *$G/[G, G]$ is abelian. For $N \trianglelefteq G$, the quotient $G/N$ is abelian if and only if $[G, G] \leq N$.*

*Proof.* (i) Clear.

(ii) Suppose that $[G, G] \leq N \leq G$. Let $g \in G$ and $n \in N$. Then $g^{-1}ng = n(n^{-1}g^{-1}ng) = n[n, g] \in N$ because $[n, g] \in G$. Therefore $N \trianglelefteq G$.

(iii) We have $[x[G, G], y[G, G]] = [x, y][G, G] = [G, G]$ in $G/[G, G]$, so $G/[G, G]$ is abelian. If $N \trianglelefteq G$, then by (i) the quotient $G/N$ is abelian if and only if $[xN, yN] = N$ for all $x, y \in G$, which is equivalent to $[x, y] \in N$ for all $x, y \in G$.

□

**Example 4.11.** (i) For any abelian group $G$, we have $[G, G] = \{1\}$.

(ii) For $G = S_3$, we have $[G, G] = \langle(1\ 2\ 3)\rangle$. More generally $[S_n, S_n] = A_n$ for $n \geq 3$.

(iii) Exercise: Let $p$ be a prime and let $G$ be a non-abelian $p$-group of order $p^3$. Show that $[G, G]$ has order $p$ and $[G, G] = Z(G)$.

(iv) Let $q$ be a power of a prime and $n \geq 2$. For $G = \mathrm{GL}_n(q)$, the determinant provides a homomorphism $\det : G \to \mathbb{F}_q^\times$. Since $\mathbb{F}_q^\times$ is abelian, so is $G/\operatorname{Ker}(\det) = G/\operatorname{SL}_n(q)$, so it follows from Lemma 4.10 (ii) that $[G, G] \leq \mathrm{SL}_n(q)$. (It is also easy to check directly that $\det([x, y]) = 1$ for all $x, y \in \mathrm{GL}_n(q)$.)

**Lemma 4.12.** *Let $\mathbb{F}$ be a field and $|\mathbb{F}| > 3$. Then $\mathrm{SL}_2(\mathbb{F}) = [\mathrm{SL}_2(\mathbb{F}), \mathrm{SL}_2(\mathbb{F})]$.*

*Proof.* (This lemma would follow from the fact that $\mathrm{PSL}_2(\mathbb{F})$ is simple when $|\mathbb{F}| > 3$, but we will give the following computational proof.) We know that $\mathrm{SL}_2(\mathbb{F})$ is generated by transvections (Lemma 3.27), i.e., matrices of the form $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}$ for $x, y \in \mathbb{F}$. Thus it will suffice to prove that every transvection is contained in the commutator subgroup. To this end, we have

$$\begin{aligned}\left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}\right] &= \begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \\ &= \begin{pmatrix} 1 & (a^2-1)x \\ 0 & 1 \end{pmatrix}\end{aligned}$$

for all $a \in \mathbb{F}^\times$ and $x \in \mathbb{F}$. Since $|\mathbb{F}| > 3$, we can choose $a \in \mathbb{F}^\times$ such that $a \neq \pm 1$, so $(a^2 - 1) \neq 0$. Then choosing $x = \frac{x'}{a^2-1}$ gives

$$\left[\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix}\right] = \begin{pmatrix} 1 & x' \\ 0 & 1 \end{pmatrix} \in [\mathrm{SL}_2(\mathbb{F}), \mathrm{SL}_2(\mathbb{F})]$$

for any $x' \in \mathbb{F}$. Taking transposes shows that $\begin{pmatrix} 1 & 0 \\ x' & 1 \end{pmatrix} \in [\mathrm{SL}_2(\mathbb{F}), \mathrm{SL}_2(\mathbb{F})]$, which completes the proof of the lemma. □

**Lemma 4.13.** *Let $\mathbb{F}$ be a field and $|\mathbb{F}| \geq 3$. Then $[\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})] = \mathrm{SL}_2(\mathbb{F})$.*

*Proof.* Exercise. (Argue as in Lemma 4.12.) □

We now give an example of an element in the commutator subgroup which is not equal to a commutator. By Lemma 4.12 we have $\mathrm{SL}_2(\mathbb{R}) = [\mathrm{SL}_2(\mathbb{R}), \mathrm{SL}_2(\mathbb{R})]$, and we will show that $-I_2 \in \mathrm{SL}_2(\mathbb{R})$ is not a commutator in $\mathrm{SL}_2(\mathbb{R})$.

**Lemma 4.14.** *The matrix $-I_2 \in \mathrm{SL}_2(\mathbb{R})$ is not a commutator in $\mathrm{SL}_2(\mathbb{R})$.*

*Proof.* Suppose that $[A, B] = A^{-1}B^{-1}AB = -I_2$ for some $A, B \in \mathrm{SL}_2(\mathbb{R})$. Then $B^{-1}AB = -A$, so $\mathrm{tr}(A) = \mathrm{tr}(-A)$ and thus $\mathrm{tr}(A) = 0$. Thus the characteristic polynomial of $A$ is

$$p_A(t) = t^2 - \mathrm{tr}(A)t + \det(A) = t^2 + 1,$$

which is an irreducible polynomial in $\mathbb{R}[t]$. As in the proof of Lemma 3.9, it follows that $A$ is conjugate to the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

in $\mathrm{GL}_2(\mathbb{R})$. For every $g \in \mathrm{GL}_2(\mathbb{R})$ we have $[A^g, B^g] = [A, B]^g = -I_2$ and $A^g, B^g \in \mathrm{SL}_2(\mathbb{R})$, so without loss of generality we may assume that $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

It follows from $A^{-1}B^{-1}AB = -I_2$ that

$$A^{-1}BA = -B.$$

With $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, this implies that $B$ is of the form $B = \begin{pmatrix} x & y \\ y & -x \end{pmatrix}$ for some $x, y \in \mathbb{R}$. But then $\det(B) = -(x^2 + y^2)$, which cannot be equal to 1 for $x, y \in \mathbb{R}$, a contradiction. □

**Remark 4.15.** However, note that $-I_2$ is a commutator in $\mathrm{SL}_2(\mathbb{C})$: for example for

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} \mathbf{i} & 0 \\ 0 & -\mathbf{i} \end{pmatrix}$$

we have $[A, B] = -I_2$. (We have seen these matrices before in Section 1.8, where they appeared in the definition of the quaternion group $Q_8$.)

Suppose that $G$ is a group generated by a subset $S$, say $G = \langle S \rangle$. In general it is not true that $[G, G]$ is generated by the commutators $[x, y]$ with $x, y \in S$. For example, let $n \geq 4$ and consider the symmetric group $G = S_n$. Then $G$ is generated by $S = \{(1\ 2), (1\ 2\ \cdots\ n)\}$, and it is an exercise to check that $\{[x, y] : x, y \in S\}$ does not generate $[G, G]$. The correct result in this direction is given by the following lemma.

**Lemma 4.16.** *Let $G$ be a group and suppose that $G = \langle S \rangle$ for some $S \subseteq G$. Then*

$$[G, G] = \langle [x, y]^g : x, y \in S \text{ and } g \in G \rangle.$$

*Proof.* Exercise. □

**Definition 4.17.** Let $G$ be a group. We define the *derived series* of $G$ as the following series of subgroups: $G^{(0)} = G$, $G^{(1)} = [G, G]$, $G^{(2)} = [G^{(1)}, G^{(1)}]$, ... and in general $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$ for $k > 1$.

For any group $G$, we have

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \trianglerighteq G^{(3)} \trianglerighteq \cdots$$

and $G^{(i)}/G^{(i+1)}$ is an abelian group for all $i \geq 0$. If there exists an integer $k \geq 0$ such that $G^{(k)} = \{1\}$, then we say that $G$ is *solvable*.

**Example 4.18.** The following groups are solvable: any abelian group, finite dihedral groups $D_{2n}$, infinite dihedral group $D_\infty$, quaternion group $Q_8$, symmetric groups $S_3$ and $S_4$, any finite $p$-group.

**Example 4.19.** A group $G$ is said to be *perfect* if $G = [G, G]$. It is clear that a non-trivial perfect group cannot be solvable, since the $G^{(k)} = G$ for all $k \geq 0$. By Lemma 4.12, the special linear groups $\mathrm{SL}_2(\mathbb{F})$ are perfect whenever $\mathbb{F}$ is a field with $|\mathbb{F}| > 3$.

**Lemma 4.20.** *Let $\varphi : G \to H$ be a homomorphism between two groups $G$ and $H$. Then $\langle \varphi(S) \rangle = \varphi(\langle S \rangle)$ for any $S \subseteq G$.*

*Proof.* Exercise. □

**Lemma 4.21.** *Let $\varphi : G \to H$ be a homomorphism between two groups $G$ and $H$. Then the following statements hold:*

(i) $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ *for all* $x, y \in G$.

(ii) $\varphi([A, B]) = [\varphi(A), \varphi(B)]$ *for all* $A, B \leq G$.

(iii) $\varphi(G^{(k)}) = \varphi(G)^{(k)}$ *for all* $k \geq 0$.

*Proof.* Claim (i) is an exercise, while (ii) follows from Lemma 4.20 and (i). Claim (iii) follows from (ii), by induction on $k$. □

**Lemma 4.22.** *Let $G$ be a group. Then $G^{(k)} \operatorname{char} G$ for all $k \geq 0$, and in particular $G^{(k)} \trianglelefteq G$.*

*Proof.* Follows from Lemma 4.21 (iii) and Lemma 4.3 (i). □

**Lemma 4.23.** *Let $G$ be a group. Then the following hold:*

(i) *If $G$ is solvable, then every subgroup of $G$ is solvable.*

(ii) *Let $N \trianglelefteq G$. Then $G$ is solvable if and only if both $N$ and $G/N$ are solvable.*

*Proof.* (i) For any $H \leq G$ we have $H^{(k)} \leq G^{(k)}$ for all $k \geq 0$. Thus if $G$ is solvable and $G^{(k)} = \{1\}$, then $H^{(k)} = \{1\}$ and so $H$ is solvable as well.

(ii) Let $\pi : G \to G/N$ be the canonical homomorphism. Suppose first that $G$ is solvable, say $G^{(k)} = \{1\}$. Then $N$ is solvable by (i). We have $\pi(G)^{(k)} = \pi(G^{(k)}) = \{1\}$ by Lemma 4.21, so $\pi(G) = G/N$ is also solvable.

Conversely, suppose that both $N$ and $G/N$ are solvable. Let $k \geq 0$ be such that $(G/N)^{(k)}$ is trivial. Since $\pi(G)^{(k)} = \pi(G^{(k)})$, it follows that $G^{(k)} \leq \operatorname{Ker}\pi = N$. Now let $\ell \geq 0$ be such that $N^{(\ell)} = \{1\}$. Then $G^{(k+\ell)} \leq N^{(\ell)} = \{1\}$, so $G^{(k+\ell)} = \{1\}$ and $G$ is solvable.

□

**Lemma 4.24.** *Let $G$ be a group and let $H, K \leq G$ be solvable subgroups such that $H \trianglelefteq G$. Then $HK$ is solvable.*

*Proof.* Exercise. □

**Remark 4.25.** Suppose that $H, K \leq G$ are solvable subgroups such that $HK$ is a subgroup. Then it is not in general true that $HK$ is solvable, an example is provided by $G = A_5$ which is not solvable, but $G = HK$ for $H = A_4$ and $K$ cyclic of order 5.

## 4.3 Jordan–Hölder theorem

**Definition 4.26.** Let $G$ be a group. A *series* is a sequence

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1\}$$

of subgroups such that $G_{i+1} \trianglelefteq G_i$ for all $1 \leq i \leq s$. We call $s$ the *length* of the series. The subgroups $G_i$ are called the *terms* of the series, and the groups $G_i/G_{i+1}$ are called *quotients* or *factors* of the series.

For example, if $G$ is a solvable group with $G^{(k)} = \{1\}$, then the derived series is a series

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq \cdots \trianglerighteq G^{(k-1)} \trianglerighteq G^{(k)} = \{1\}$$

where the quotients $G^{(i)}/G^{(i+1)}$ are abelian groups. In fact, the existence of a series with abelian quotients is equivalent to solvability, as we will prove next.

**Lemma 4.27.** *Let $G$ be a group. Then $G$ is solvable if and only if there exists a series*

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1\}$$

*such that $G_i/G_{i+1}$ is abelian for all $1 \leq i \leq s$.*

*Proof.* If $G$ is solvable, then as noted before the lemma, the derived series provides a series of subgroups in $G$ with abelian quotients. Conversely, suppose that

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1\}$$

is a series of subgroups such that $G_i/G_{i+1}$ is abelian for all $1 \leq i \leq s$. It follows from Lemma 4.10 (iii) that $[G, G] = G^{(1)} \leq G_2$.

In general, we claim that

$$G^{(k)} \leq G_{k+1}$$

for all $1 \leq k \leq s$. We prove this by induction on $k$, the case $k = 1$ having been proven already. Suppose that $1 < k \leq s$. By induction $G^{(k-1)} \leq G_k$. Now $G_k/G_{k+1}$ is abelian, so by Lemma 4.10 (iii) we have

$$G_{k+1} \geq [G_k, G_k] \geq [G^{(k-1)}, G^{(k-1)}] = G^{(k)}.$$

This completes the proof of the claim. With $k = s$ we get $G^{(s)} \leq G_{s+1} = \{1\}$, so $G^{(s)} = \{1\}$ and $G$ is solvable. □

**Definition 4.28.** Let $G$ be a nontrivial group. A series

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1\}$$

is called a *composition series*, if $G_i/G_{i+1}$ is simple for all $1 \leq i \leq s$.

**Example 4.29.** Examples of composition series:

(a) Exercise: Let $G = C_{p^k}$, where $p$ is a prime. Show that $G$ has only one composition series.

(b) Exercise: Let $G = C_{pq}$, where $p$ and $q$ are distinct primes. How many composition series does $G$ have?

(c) Let $G = D_8 = \langle x, y \rangle$ with $|x| = 2$, $|y| = 4$ and $xyx^{-1} = y^{-1}$. Then $G$ has several composition series:

$$\begin{aligned}
&G \rhd \langle y \rangle \rhd \langle y^2 \rangle \rhd \{1\} \\
&G \rhd \langle x, y^2 \rangle \rhd \langle x \rangle \rhd \{1\} \\
&G \rhd \langle x, y^2 \rangle \rhd \langle xy^2 \rangle \rhd \{1\} \\
&G \rhd \langle x, y^2 \rangle \rhd \langle y^2 \rangle \rhd \{1\} \\
&G \rhd \langle xy, y^2 \rangle \rhd \langle xy \rangle \rhd \{1\} \\
&G \rhd \langle xy, y^2 \rangle \rhd \langle xy^3 \rangle \rhd \{1\} \\
&G \rhd \langle xy, y^2 \rangle \rhd \langle y^2 \rangle \rhd \{1\}
\end{aligned}$$

(d) If $G \neq \{1\}$ is simple, then $G$ has a unique composition series $G \rhd \{1\}$.

(e) Exercise: Show that $\mathbb{Z}$ does not admit a composition series.

**Definition 4.30.** Let $G$ be a group. Two series

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1\}$$

and

$$G = H_1 \trianglerighteq H_2 \trianglerighteq \cdots \trianglerighteq H_t \trianglerighteq H_{t+1} = \{1\}$$

are said to be *equivalent*, if $s = t$ and there exists a permutation $(\pi(1), \ldots, \pi(s))$ of $(1, \ldots, s)$ such that $G_i/G_{i+1} \cong H_{\pi(i)}/H_{\pi(i)+1}$ for all $1 \leq i \leq s$.

**Lemma 4.31.** *Let $G$ be a group. Suppose that $B \trianglelefteq A \leq G$ and $C \trianglelefteq G$. Then:*

(i) *$B \cap C \trianglelefteq A \cap C$ and $\frac{A \cap C}{B \cap C} \cong \frac{B(A \cap C)}{B} \trianglelefteq \frac{A}{B}$.*

(ii) *$BC \trianglelefteq AC$ and $\frac{AC}{BC} \cong \frac{A}{B(A \cap C)}$.*

*Proof.* (i) Let $g \in A \cap C$. Then $(B \cap C)^g = B^g \cap C^g = B \cap C$, because $B^g = B$ by $B \trianglelefteq A$ and $C^g = C$ by $C \trianglelefteq G$. Moreover, we have $B \trianglelefteq B(A \cap C)$ since $B \trianglelefteq A$. Thus

$$\frac{B(A \cap C)}{B} \cong \frac{A \cap C}{(A \cap C) \cap B} = \frac{A \cap C}{B \cap C}$$

by Theorem 1.100. Since $B$ and $A \cap C$ are normal subgroups of $A$, the product $B(A \cap C)$ is a normal subgroup of $A$, and so by the correspondence theorem

$$\frac{B(A \cap C)}{B} \trianglelefteq \frac{A}{B}.$$

(ii) For all $a \in A$, we have $(BC)^a = B^a C^a = BC$ since $B \trianglelefteq A$ and $C \trianglelefteq G$. We also have $(BC)^c = BC$ for all $c \in C$, since $C \leq BC$. Thus $BC^g = BC$ for all $g \in AC$, in other words $BC \trianglelefteq AC$. For the isomorphism, we have

$$\frac{AC}{BC} = \frac{A(BC)}{BC} \cong \frac{A}{A \cap BC}$$

by Theorem 1.100. Now the claim follows from Exercise 4.18, where it is shown that $A \cap BC = B(A \cap C)$.

□

**Lemma 4.32.** *Let $G$ be a group that has a composition series. If $N$ is a nontrivial proper normal subgroup of $G$, then both $N$ and $G/N$ have a composition series.*

*Proof.* Let

$$G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s \triangleright G_{s+1} = \{1\}$$

be a composition series for $G$, so $G_i/G_{i+1}$ is simple for all $1 \leq i \leq s$.

For $N$, taking intersections gives the following series:

$$N = G_1 \cap N \trianglerighteq G_2 \cap N \trianglerighteq \cdots \trianglerighteq G_s \cap N \trianglerighteq G_{s+1} \cap N = \{1\}.$$

Now

$$\frac{G_i \cap N}{G_{i+1} \cap N} \cong \frac{(G_i \cap N)G_{i+1}}{G_{i+1}} \trianglelefteq \frac{G_i}{G_{i+1}}$$

by Lemma 4.31 (i), so for all $1 \leq i \leq s$, the quotient $(G_i \cap N)/(G_{i+1} \cap N)$ is isomorphic to a normal subgroup of $G_i/G_{i+1}$. Since each $G_i/G_{i+1}$ is simple, we conclude that each quotient $(G_i \cap N)/(G_{i+1} \cap N)$ is either trivial or simple, and thus $N$ admits a composition series.

For $G/N$, taking the images of $G_i$ in $G/N$ we get the following series:

$$G/N = G_1N/N \trianglerighteq G_2N/N \trianglerighteq \cdots \trianglerighteq G_sN/N \trianglerighteq G_{s+1}N/N = \{1\}.$$

For the quotients, for all $1 \leq i \leq s$ we have

$$\frac{G_iN/N}{G_{i+1}N/N} \cong \frac{G_iN}{G_{i+1}N} \cong \frac{G_i}{G_{i+1}(N \cap G_i)} \cong \frac{G_i/G_{i+1}}{G_{i+1}(N \cap G_i)/G_{i+1}}$$

by Lemma 4.31 (ii) and Theorem 1.101. Thus each quotient $\frac{G_iN/N}{G_{i+1}N/N}$ is isomorphic to a quotient of $G_i/G_{i+1}$. Since $G_i/G_{i+1}$ is simple, each quotient $\frac{G_iN/N}{G_{i+1}N/N}$ must be trivial or simple. Therefore $G/N$ admits a composition series. □

**Theorem 4.33** (Jordan-Hölder theorem)**.** *Let $G$ be a nontrivial group. Suppose that $G$ has a composition series. Then any two composition series of $G$ are equivalent.*

*Proof.* Denote by $\ell(G)$ the minimal length of a composition series of $G$. We will prove the theorem by induction on $\ell(G)$. If $\ell(G) = 1$, then $G$ is simple and the result is obvious. Suppose then that $\ell(G) > 1$, and let

$$G = G_1 \rhd G_2 \rhd \cdots \rhd G_s \rhd G_{s+1} = \{1\}$$

and

$$G = H_1 \rhd H_2 \rhd \cdots \rhd H_t \rhd H_{t+1} = \{1\}$$

be two composition series of $G$. It suffices to prove the claim in the case where $s = \ell(G)$.

If $G_2 = H_2$, then the result follows by applying induction on $G_2$, since $\ell(G_2) \leq \ell(G_1) - 1$. Thus we can assume that $G_2 \neq H_2$. Then

$$G \trianglerighteq G_2H_2 \rhd G_2,$$

so it follows from simplicity of $G/G_2$ that $G = G_2H_2$. Moreover, the intersection $K_2 = G_2 \cap H_2$ is a normal subgroup of $G$. By isomorphism theorems, we have

$$G/G_2 = G_2H_2/G_2 \cong H_2/K_2,$$

and similarly $G/H_2 = G_2H_2/H_2 \cong G_2/K_2$.

By Lemma 4.32 we can find some composition series of $K_2$, say

$$K_2 \rhd K_3 \rhd \cdots \rhd K_u \rhd K_{u+1} = \{1\}.$$

Now we have several composition series of $G = G_1$:

$$G_1 \rhd G_2 \rhd G_3 \rhd \cdots \rhd G_s \rhd G_{s+1} = \{1\} \tag{4.1}$$
$$G_1 \rhd G_2 \rhd K_2 \rhd \cdots \rhd K_u \rhd K_{u+1} = \{1\} \tag{4.2}$$
$$G_1 \rhd H_2 \rhd K_2 \rhd \cdots \rhd K_u \rhd K_{u+1} = \{1\} \tag{4.3}$$
$$G_1 \rhd H_2 \rhd H_3 \rhd \cdots \rhd H_t \rhd K_{t+1} = \{1\} \tag{4.4}$$

Applying induction on $G_2$, it follows that the series (4.1) and (4.2) are equivalent. Since $G_1/G_2 \cong H_2/K_2$ and $G_1/H_2 \cong G_2/K_2$, the series (4.2) and (4.3) are equivalent. Applying induction on $H_2$, it follows that the series (4.3) and (4.4) are equivalent. We conclude then that series (4.1) and (4.4) are equivalent, as claimed. □

## 4.4 Nilpotent groups

An important class of solvable groups is that of *nilpotent groups*. (Among finite groups, the typical example is a finite $p$-group.) There are multiple ways to define nilpotent groups, we will use the following definition.

**Definition 4.34.** Let $G$ be a group. We define the *lower central series* of $G$ as the following series of subgroups: $\gamma_1(G) = G$, and $\gamma_k(G) = [\gamma_{k-1}(G), G]$ for all $k > 1$. (So for example $\gamma_2(G) = G^{(1)} = [G, G]$, and $\gamma_3(G) = [[G, G], G]$.) If there exists an integer $k \geq 1$ such that $\gamma_k(G) = \{1\}$, then we say that $G$ is *nilpotent*.

**Lemma 4.35.** *Let $G$ be a group. Then:*

(i) *For any homomorphism $\varphi : G \to H$, we have $\varphi(\gamma_k(G)) = \gamma_k(\varphi(G))$ for all $k \geq 1$.*

(ii) *$\gamma_k(G)$ char $G$ for all $k \geq 1$, so in particular $\gamma_k(G) \trianglelefteq G$.*

*Proof.* (i) By induction on $k$. For $k = 1$ the claim is clear, and for $k > 1$ the claim follows by applying Lemma 4.21 (ii) and induction.

(ii) Follows from (i).

□

**Lemma 4.36.** *Let $G$ be a nilpotent group. Then every subgroup and quotient group of $G$ is nilpotent.*

*Proof.* Suppose that $G$ is nilpotent and let $k \geq 1$ be such that $\gamma_k(G) = \{1\}$. For any subgroup $H \leq G$ we have $\gamma_k(H) \leq \gamma_k(G)$, so $\gamma_k(H) = \{1\}$ and $H$ is nilpotent. For quotients, let $N \trianglelefteq G$ be a normal subgroup. Applying Lemma 4.35 (i) to the canonical homomorphism $\pi : G \to G/N$, we see that $\gamma_k(G/N) = \gamma_k(G)N/N = \{1\}$. Thus $G/N$ is also nilpotent. □

**Lemma 4.37.** *Let $G$ be a group. Then $G^{(k)} \leq \gamma_{k+1}(G)$ for all $k \geq 0$. In particular if $G$ is nilpotent, then $G$ is solvable.*

*Proof.* By induction on $k$. For $k = 0$ we have $G^{(0)} = G = \gamma_1(G)$. Suppose then that $k > 0$. Then

$$G^{(k)} = [G^{(k-1)}, G^{(k-1)}] \leq [\gamma_k(G), \gamma_k(G)] \leq [\gamma_k(G), G] = \gamma_{k+1}(G),$$

since $G^{(k-1)} \leq \gamma_k(G)$ by induction. □

By Lemma 4.37, we know that nilpotent groups are solvable. The converse is not true: for example $G = S_3$ is solvable since $G^{(2)} = \{(1)\}$, but $\gamma_k(G) = [G, G]$ for all $k \geq 2$, so $G$ is not nilpotent. Another example is provided by the following subgroup of $\mathrm{GL}_2(\mathbb{F})$, where $\mathbb{F}$ is a field:

$$B = \left\{ \begin{pmatrix} \lambda & \zeta \\ 0 & \mu \end{pmatrix} : \lambda, \mu \in \mathbb{F}^\times, \zeta \in \mathbb{F} \right\}.$$

Assuming that $|\mathbb{F}| > 2$, a calculation shows that $B$ is solvable but not nilpotent.

Another characterization of nilpotent groups can be given in terms of series. We know by Lemma 4.35 that for any group, in the lower central series

$$G = \gamma_1(G) \trianglerighteq \gamma_2(G) \trianglerighteq \gamma_3(G) \trianglerighteq \cdots$$

the terms $\gamma_i(G)$ are characteristic subgroups in $G$. Thus each quotient $\gamma_i(G)/\gamma_{i+1}(G)$ is a normal subgroup of $G/\gamma_{i+1}(G)$ by the correspondence theorem. Moreover, we have $[\gamma_i(G), G] = \gamma_{i+1}(G)$, so in fact $\gamma_i(G)/\gamma_{i+1}(G)$ is contained in the center $Z(G/\gamma_{i+1}(G))$ of $G/\gamma_{i+1}(G)$. The existence of a series with this property characterizes nilpotent groups.

**Lemma 4.38.** *Let $G$ be a group. Then $G$ is nilpotent if and only if there exists a series*

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1\}$$

*such that $G_i \trianglelefteq G$ for all $1 \leq i \leq s+1$, and $G_i/G_{i+1} \leq Z(G/G_{i+1})$ for all $1 \leq i \leq s$. (Such a series is called a* central series*.)*

*Proof.* If $G$ is nilpotent, then as noted before the lemma, the lower central series is such a series. Conversely, suppose that there exists a series

$$G = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1\}$$

such that $G_i \trianglelefteq G$ for all $1 \leq i \leq s+1$, and $G_i/G_{i+1} \leq Z(G/G_{i+1})$ for all $1 \leq i \leq s$.

We claim that for all $2 \leq k \leq s+1$, we have $\gamma_k(G) \leq G_k$. First note that $G/G_2 = G_1/G_2 \leq Z(G/G_2)$, so $G/G_2$ is abelian, and thus $\gamma_2(G) = [G, G] \leq G_2$. For $k > 2$ we proceed by induction on $k$. We have $G_{k-1}/G_k \leq Z(G/G_k)$, or equivalently $[G_{k-1}, G] \leq G_k$. By induction $\gamma_{k-1}(G) \leq G_{k-1}$, so then

$$\gamma_k(G) = [\gamma_{k-1}(G), G] \leq [G_{k-1}, G] \leq G_k$$

as claimed. Applying this with $k = s+1$, we get $\gamma_{s+1}(G) \leq G_{s+1} = \{1\}$, so $\gamma_{s+1}(G) = \{1\}$ and $G$ is nilpotent. □

**Lemma 4.39.** *Let $G$ be a nilpotent group and $N \trianglelefteq G$ such that $N \neq \{1\}$. Then $N \cap Z(G) \neq \{1\}$.*

*Proof.* Let $k \geq 1$ be the largest integer such that $N \cap \gamma_k(G) \neq \{1\}$, so then $N \cap \gamma_{k+1}(G) = \{1\}$. (Such an integer exists since $N$ is nontrivial, and since $G$ is nilpotent.)

Then $[N \cap \gamma_k(G), G] \leq [N, G] \leq N$ since $N$ is a normal subgroup, and $[N \cap \gamma_k(G), G] \leq [\gamma_k(G), G] = \gamma_{k+1}(G)$. Thus $[N \cap \gamma_k(G), G] \leq N \cap \gamma_{k+1}(G) = \{1\}$, and so $[G, N \cap \gamma_k(G)] = \{1\}$. Therefore $N \cap \gamma_k(G)$ is in the center of $G$, and in particular $N \cap Z(G) \neq \{1\}$. □

Applying Lemma 4.39 with $G = N$, we get the following corollary.

**Corollary 4.40.** *Let $G$ be a nontrivial nilpotent group. Then $Z(G) \neq \{1\}$.*

For solvable groups, we have seen that they are closed under extensions: in other words if $N \trianglelefteq G$ is such that $N$ and $G/N$ are both solvable, then $G$ is solvable. This fails for nilpotent groups: for example $G = S_3$ has a normal subgroup $N$ with $N \cong C_3$ and $G/N \cong C_2$, but $G$ is not nilpotent. However, we can now prove the following result.

**Lemma 4.41.** *Let $G$ be a nilpotent group and $N \leq Z(G)$. Then $G$ is nilpotent if and only if $G/N$ is nilpotent. In particular, $G$ is nilpotent if and only if $G/Z(G)$ is nilpotent.*

*Proof.* If $G$ is nilpotent, then $G/N$ is nilpotent by Lemma 4.36. Conversely, suppose that $G/N$ is nilpotent, say $\gamma_k(G/N) = \{1\}$. By Lemma 4.21 applied to the canonical homomorphism $G \to G/N$, we have $\gamma_k(G/N) = \gamma_k(G)N/N$. Therefore $\gamma_k(G) \leq N$, and then $\gamma_{k+1}(G) = [\gamma_k(G), G] = \{1\}$ since $N$ is central. □

As a corollary, we prove that finite $p$-groups are nilpotent.

**Lemma 4.42.** *Let $G$ be a finite $p$-group. Then $G$ is nilpotent.*

*Proof.* By induction on $|G|$. The case $|G| = 1$ is trivial, so suppose that $|G| > 1$. By Corollary 1.143 we have $Z(G) \neq \{1\}$. Thus by induction $G/Z(G)$ is nilpotent, and then $G$ is nilpotent by Lemma 4.41. □

As we have seen already, several of the results we have proven before for finite $p$-groups hold more generally for nilpotent groups. The following proposition is a generalization of Proposition 1.147.

**Proposition 4.43.** *["Normalizers grow"] Let $G$ be a nilpotent group and $H$ be a proper subgroup of $G$. Then $H \lneq N_G(H)$.*

*Proof.* Exercise. (Hint: Show that there exists $k \geq 1$ such that $\gamma_k(G) \not\leq H$ and $\gamma_{k+1}(G) \leq H$.) □

## 4.5 Upper central series

Let $G$ be a group. By the correspondence theorem, there exists a normal subgroup $Z(G) \leq Z^2(G) \leq G$ such that $Z^2(G)/Z(G) = Z(G/Z(G))$. By definition, we have

$$g \in Z^2(G) \text{ if and only if } [g, x] \in Z(G) \text{ for all } x \in G.$$

Similarly, we define $Z^3(G)$ to be unique subgroup $Z^2(G) \leq Z^3(G) \trianglelefteq G$ such that $Z^3(G)/Z^2(G) = Z(G/Z^2(G))$. Then

$$g \in Z^3(G) \text{ if and only if } [g, x] \in Z^2(G) \text{ for all } x \in G.$$

Continuing in this manner, we can define the *upper central series*, which gives another way of defining nilpotent groups. The upper central series is the series

$$1 = Z^0(G) \leq Z^1(G) \leq Z^2(G) \leq Z^3(G) \leq \cdots$$

of normal subgroups of $G$, such that $Z^0(G) = \{1\}$, $Z^1(G) = Z(G)$, and for $k > 1$ we have $Z^k(G) \leq Z^{k-1}(G) \trianglelefteq G$ and $Z^k(G)/Z^{k-1}(G) = Z(G/Z^{k-1}(G))$. Then for all $k \geq 1$, we have

$$g \in Z^k(G) \text{ if and only if } [g, x] \in Z^{k-1}(G) \text{ for all } x \in G.$$

**Lemma 4.44.** *Let $G$ be a group. Then $Z^k(G) \operatorname{char} G$ for all $k \geq 0$.*

*Proof.* Exercise. □

**Lemma 4.45.** *Let $G$ be a nilpotent group, and let $c \geq 1$ be such that $\gamma_{c+1}(G) = \{1\}$. Then $\gamma_{c-i+1}(G) \leq Z^i(G)$ for all $1 \leq i \leq c$. In particular $Z^c(G) = G$.*

*Proof.* Exercise. □

**Lemma 4.46.** *Let $G$ be a group and suppose that $Z^c(G) = G$ for some $c \geq 1$. Then $\gamma_{c-i+1}(G) \leq Z^i(G)$ for all $1 \leq i \leq c$. In particular $\gamma_{c+1}(G) = \{1\}$.*

*Proof.* Exercise. □

By Lemma 4.45 and Lemma 4.46, a group $G$ is nilpotent if and only if $Z^c(G) = G$ for some $c \geq 1$. Moreover, we have $Z^c(G) = G$ if and only if $\gamma_{c+1}(G) = \{1\}$. We will call the smallest integer $c \geq 1$ such that $\gamma_{c+1}(G) = \{1\}$ the *class* of a nilpotent group $G$.

## 4.6 Higher commutators

Let $G$ be a group. For $n \geq 3$, we define the *higher commutator* of elements $x_1, x_2, \ldots, x_n \in G$ recursively as

$$[x_1, x_2, \ldots, x_n] := [[x_1, \ldots, x_{n-1}], x_n].$$

Therefore for example

$$[x, y, z] = [[x, y], z]$$

and

$$[x, y, z, w] = [[[x, y], z], w]$$

for all $x, y, z, w \in G$. Similarly for subgroups $H_1, \ldots, H_n \leq G$ we define the *higher commutator subgroup* of $H_1, \ldots, H_n$ as

$$[H_1, \ldots, H_n] := [[H_1, \ldots, H_{n-1}], H_n].$$

Thus for example

$$[H, K, L] = [[H, K], L]$$

and for $k \geq 2$ we have

$$\gamma_k(G) = \underbrace{[G, G, \ldots, G]}_{k \text{ times}}.$$

In our definition we have used "left-normed" commutators. Taking commutators is not associative, in the sense that for $x, y, z \in G$ it is possible that

$$[[x, y], z] \neq [x, [y, z]]$$

and for $H, K, L \leq G$ it is possible that

$$[[H, K], L] \neq [H, [K, L]].$$

(Examples can be found already in the smallest non-abelian group, $G = S_3$.)

**Lemma 4.47.** *Let $G$ be a group and $k \geq 2$. Then*

$$\gamma_k(G) = \langle [x_1, x_2, \ldots, x_k] : x_1, x_2, \ldots, x_k \in G \rangle$$

*Proof.* Exercise. □

By Lemma 4.47, we have yet another definition of nilpotence: a group $G$ is nilpotent if and only if there exists $k \geq 1$ such that

$$[x_1, x_2, \ldots, x_k] = 1$$

for all $x_1, \ldots, x_k \in G$. For example:

$$\begin{aligned}
G \text{ is nilpotent of class } 1 &\Leftrightarrow [x,y] = 1 \text{ for all } x,y \in G.\\
G \text{ is nilpotent of class } &\leq 2 \Leftrightarrow [x,y,z] = 1 \text{ for all } x,y,z \in G.\\
G \text{ is nilpotent of class } &\leq 3 \Leftrightarrow [x,y,z,w] = 1 \text{ for all } x,y,z,w \in G.\\
&\cdots\\
G \text{ is nilpotent of class } &\leq c \Leftrightarrow [x_1,x_2,\ldots,x_{c+1}] = 1 \text{ for all } x_1,x_2,\ldots,x_{c+1} \in G.
\end{aligned}$$

**Lemma 4.48.** *Let $H, K, L \trianglelefteq G$. Then $[HK, L] = [H, L][K, L]$ and $[H, KL] = [H, K][H, L]$.*

*Proof.* Exercise. □

**Lemma 4.49.** *Let $H_1, \ldots, H_k, A, B \trianglelefteq G$, where $k \geq 1$. Then*

$$\begin{aligned}
&[H_1, \ldots, H_{r-1}, AB, H_{r+1}, \ldots, H_k]\\
&\quad = [H_1, \ldots, H_{r-1}, A, H_{r+1}, \ldots, H_k][H_1, \ldots, H_{r-1}, B, H_{r+1}, \ldots, H_k]
\end{aligned}$$

*for all $1 \leq r \leq k$.*

*Proof. Case 1: $r = 1$.* Applying Lemma 4.48 repeatedly, we get

$$\begin{aligned}
[AB, H_2, \ldots, H_k] &= [[AB, H_2], H_3, \ldots, H_k] && \text{(definition)}\\
&= [[A, H_2][B, H_2], H_3, \ldots, H_k] && \text{(by Lemma 4.48)}\\
&= [[[A, H_2][B, H_2], H_3], H_4, \ldots, H_k] && \text{(definition)}\\
&= [[[A, H_2, H_3][B, H_2, H_3], H_4, \ldots, H_k] && \text{(by Lemma 4.48)}\\
&= \cdots\\
&= [A, H_2, \ldots, H_k][B, H_2, \ldots, H_k]
\end{aligned}$$

as claimed.

*Case 2: $r = k$.* In this case

$$[H_1, \ldots, H_{k-1}, AB] = [H_1, \ldots, H_{k-1}, A][H_1, \ldots, H_{k-1}, B]$$

by Lemma 4.48.

*Case 3: $1 < r < k$.* In this case

$$\begin{aligned}
&[H_1, \ldots, H_{r-1}, AB, H_{r+1}, \ldots, H_k]\\
&= [[H_1, \ldots, H_{r-1}, AB], H_{r+1}, \ldots, H_k] && \text{(definition)}
\end{aligned}$$

$$
\begin{aligned}
&= [[H_1, \ldots, H_{r-1}, A][H_1, \ldots, H_{r-1}, B], H_{r+1}, \ldots, H_k] && \text{(by Case 2)}\\
&= [[H_1, \ldots, H_{r-1}, A], H_{r+1}, \ldots, H_k][[H_1, \ldots, H_{r-1}, B], H_{r+1}, \ldots, H_k] && \text{(by Case 1)}\\
&= [H_1, \ldots, H_{r-1}, A, H_{r+1}, \ldots, H_k][H_1, \ldots, H_{r-1}, B, H_{r+1}, \ldots, H_k] && \text{(definition)}
\end{aligned}
$$

This completes the proof of the lemma in all cases. □

**Lemma 4.50.** *Let $H_1$, $H_2$, …, $H_k$, $A$ be normal subgroups of $G$. Suppose that among the $H_i$'s there are at least $d$ which are equal to $A$. Then*

$$[H_1, H_2, \ldots, H_k] \leq \gamma_d(A).$$

*Proof.* By induction on $k$. If $k = 1$ the claim is clear, and for $k = 2$ we have $[H_1, A] \leq A$ and $[A, H_2] \leq A$ since $A$ is a normal subgroup. Suppose then that $k > 2$. Note that $\gamma_t(A)$ char $A$ (Lemma 4.35), so $\gamma_t(A)$ is a normal subgroup of $G$ for all $t \geq 1$ by Lemma 4.3 (iii). Thus if $H_k \neq A$, then by induction

$$
\begin{aligned}
[H_1, \ldots, H_k] &= [[H_1, \ldots, H_{k-1}], H_k]\\
&\leq [\gamma_d(A), H_k]\\
&\leq \gamma_d(A).
\end{aligned}
$$

Similarly if $H_k = A$, then by induction

$$
\begin{aligned}
[H_1, \ldots, H_k] &= [[H_1, \ldots, H_{k-1}], A]\\
&\leq [\gamma_{d-1}(A), A]\\
&= \gamma_d(A).
\end{aligned}
$$

This completes the proof of the lemma. □

**Proposition 4.51** (Fitting's theorem)**.** *Let $G$ be a group and let $A, B \trianglelefteq G$ be nilpotent. Then $AB$ is nilpotent normal subgroup of $G$.*

*Proof.* Since $A$ and $B$ are normal subgroups, it follows that $AB$ is a normal subgroup. For nilpotence, let $a$ and $b$ be such that $\gamma_{a+1}(A) = \{1\}$ and $\gamma_{b+1}(B) = \{1\}$. Now for any $k \geq 2$, applying Lemma 4.49 repeatedly we get

$$
\begin{aligned}
&\gamma_k(AB)\\
&= \underbrace{[AB, AB, \ldots, AB]}_{(k \text{ times })}\\
&= [A, AB, \ldots, AB][B, AB, \ldots, AB]\\
&= [A, A, AB, \ldots, AB][A, B, AB \ldots, AB][B, A, AB \ldots, AB][B, B, AB, \ldots, AB]
\end{aligned}
$$

$$= \cdots$$
$$= \prod_{X_i \in \{A,B\}} [X_1, X_2, \ldots, X_k]$$

In other words, $\gamma_k(AB)$ is the product of the $2^k$ higher commutator subgroups $[X_1, X_2, \ldots, X_k]$ with $X_i$ equal to $A$ or $B$ for each $1 \leq i \leq k$.

Consider one such commutator subgroup $[X_1, \ldots, X_k]$. Let $k = d + e$, where $d$ is the number of $X_i$'s which are equal to $A$, and $e$ is the number of $X_i$'s equal to $B$. By Lemma 4.50 we have

$$[X_1, \ldots, X_k] \leq \gamma_d(A) \cap \gamma_e(B).$$

Suppose that $k > a+b$. Then $d > a$ or $e > b$, so $\gamma_d(A) = \{1\}$ or $\gamma_e(B) = \{1\}$, and therefore $[X_1, \ldots, X_k] = \{1\}$. Thus we conclude that $\gamma_{a+b+1}(AB) = \{1\}$, in other words, $AB$ is nilpotent. □

As a consequence of Proposition 4.51, a subgroup generated by finitely many nilpotent normal subgroups is nilpotent. In particular for a finite group $G$, this implies the existence of a unique maximal nilpotent normal subgroup.

Indeed, suppose that $G$ is finite and let $M$ be a nilpotent normal subgroup of $G$ such that $|M|$ is maximal. Then if $N \trianglelefteq G$ is nilpotent, then $MN$ is nilpotent by Proposition 4.51. Thus $MN = M$ by maximality of $M$, so in fact $N \leq M$ and $M$ contains every nilpotent normal subgroup of $G$. This of course implies that $M$ is unique[17]. We call $M$ the *Fitting subgroup* of $G$ and denote it by $F(G)$. In summary, the Fitting subgroup is characterized by the following properties:

- $F(G) \trianglelefteq G$ and $F(G)$ is nilpotent;
- For all $N \trianglelefteq G$ nilpotent, we have $N \leq F(G)$.

As a straightforward consequence, the Fitting subgroup is a characteristic subgroup of $G$.

**Lemma 4.52.** *Let $G$ be a finite group. Then $F(G)$ $\operatorname{char} G$.*

*Proof.* Exercise. □

[17]For if $M'$ is another nilpotent normal subgroup of maximal order, then $M' \leq M$, and thus $M' = M$ by maximality of $M'$.

# 5 Constructing groups

In this section, we will consider various ways of constructing new groups from old ones.

## 5.1 Direct products

**Definition 5.1.** Let $G_1$, ..., $G_n$ be groups, where $n \geq 2$. The *direct product* of $G_1$, ..., $G_n$ is the cartesian product $G_1 \times \cdots \times G_n$ equipped with the following product:

$$(g_1, \ldots, g_n)(g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n')$$

where $g_i, g_i' \in G_i$ for all $1 \leq i \leq n$. Then $G_1 \times \cdots \times G_n$ equipped with this operation is a group. The identity element is $(1_{G_1}, \ldots, 1_{G_n})$ and the inverse of $(g_1, \ldots, g_n) \in G_1 \times \cdots \times G_n$ is the element $(g_1^{-1}, \ldots, g_n^{-1})$.

**Lemma 5.2.** *Let $G_1$, ..., $G_n$ be groups.*

(i) *If $|G_i| < \infty$ for all $1 \leq i \leq n$, then $|G_1 \times \cdots \times G_n| = |G_1| \cdots |G_n|$.*

(ii) *$(A \times B) \times C \cong A \times (B \times C)$ for any groups $A$, $B$, and $C$.*

(iii) *Let $(\pi(1), \ldots, \pi(n))$ be a permutation of $\{1, \ldots, n\}$. Then*

$$G_{\pi(1)} \times \cdots \times G_{\pi(n)} \cong G_1 \times \cdots \times G_n.$$

(iv) *Let $\widehat{G_i} := \{1\} \times \cdots \times \{1\} \times G_i \times \{1\} \times \cdots \times \{1\}$. Then $\widehat{G_i} \trianglelefteq G_1 \times \cdots \times G_n$ and*

$$(G_1 \times \cdots \times G_n)/\widehat{G_i} \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

*Proof.* Exercise. □

**Definition 5.3.** Let $G$ be a group and let $H_1$, ..., $H_n$ be subgroups of $G$. We say that $G$ is the direct product of $H_1$, ..., $H_n$ if the map

$$H_1 \times \cdots \times H_n \to G, \ (h_1, \ldots, h_n) \mapsto h_1 \cdots h_n \text{ for all } h_i \in H_i$$

is an isomorphism.

**Lemma 5.4.** *Let $G$ be a group and let $H, K \trianglelefteq G$. Suppose that $H \cap K = \{1\}$. Then $hk = kh$ for all $h \in H$ and $k \in K$.*

*Proof.* Exercise. □

**Lemma 5.5.** *Let $G$ be a group and let $H_1$, ..., $H_n$ be subgroups of $G$. Then $G$ is the direct product of $H_1$, ..., $H_n$ if and only if all of the following conditions hold:*

(i) $G = H_1 \cdots H_n$;

(ii) $H_i$ *is a normal subgroup of* $G$ *for all* $1 \leq i \leq n$;

(iii) $H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n) = \{1\}$ *for all* $1 \leq i \leq n$.

*Proof.* Suppose first that $G$ is the direct product of $H_1$, ..., $H_n$; in other words, we assume that the map $\varphi : H_1 \times \cdots \times H_n \to G$ defined by $\varphi(h_1, \ldots, h_n) = h_1 \cdots h_n$ is an isomorphism. Then (i) holds since $\varphi$ is surjective. For (ii), note that we have

$$\varphi(\{1\} \times \cdots \times \{1\} \times H_i \times \{1\} \times \cdots \times \{1\}) = H_i.$$

Since $\varphi$ is a surjective homomorphism and since $\{1\} \times \cdots \times \{1\} \times H_i \times \{1\} \times \cdots \times \{1\}$ is a normal subgroup of $H_1 \times \cdots \times H_n$ (Lemma 5.2 (iv)), it follows from Lemma 1.93 that $H_i$ is a normal subgroup of $G$. For statement (iii), let $h \in H_i \cap (H_1 \cdots H_{i-1} H_{i+1} \cdots H_n)$, say $h = h_i = h_1 \cdots h_{i-1} h_{i+1} \cdots h_n$ with $h_j \in H_j$ for all $1 \leq j \leq n$. Then

$$h = \varphi(1, \ldots, 1, h_i, 1, \ldots, 1) = \varphi(h_1, \ldots, h_{i-1}, 1, h_{i+1}, \ldots, h_n),$$

so $h_j = 1$ for all $1 \leq j \leq n$ since $\varphi$ is injective. Thus $h = 1$, and we conclude that (iii) holds.

For the other direction, suppose that (i), (ii), and (iii) hold. We will show that $\varphi$ is an isomorphism. First note that by (iii) we have $H_i \cap H_j = \{1\}$ for all $i \neq j$, so by (ii) and Lemma 5.4 we have $h_i h_j = h_j h_i$ for all $h_i \in H_i$ and $h_j \in H_j$. It follows then that we have

$$(h_1 h_2 \cdots h_n)(h_1' h_2' \cdots h_n') = (h_1 h_1')(h_2 h_2') \cdots (h_n h_n')$$

for all $h_i, h_i' \in H_i$. In other words

$$\varphi(h_1, \ldots, h_n)\varphi(h_1', \ldots, h_n') = \varphi(h_1 h_1', \ldots, h_n h_n')$$

for all $h_i, h_i' \in H_i$, so $\varphi$ is a homomorphism. It follows from (i) that $\varphi$ is surjective. For injectivity, by Lemma 1.63 (iii) it will suffice to check that $\operatorname{Ker} \varphi = \{1\}$. Suppose that $\varphi(h_1, \ldots, h_n) = h_1 \cdots h_n = 1$. Since $h_i h_j = h_j h_i$ for $i \neq j$, it follows that $h_i^{-1} = h_1 \cdots h_{i-1} h_{i+1} \cdots h_n$ for all $1 \leq i \leq n$. Therefore $h_i = 1$ for all $1 \leq i \leq n$ by (iii). This proves that $\operatorname{Ker} \varphi = \{1\}$ and completes the proof of the lemma. □

The special case of Lemma 5.5 with two factors ($n = 2$) is the one that comes up most often, so we state it in the following lemma.

**Lemma 5.6.** *Let $G$ be a group and let $H, K \leq G$. Then $G$ is the direct product of $H$ and $K$ if and only if $G = HK$ and $H, K \trianglelefteq G$, and $H \cap K = \{1\}$.*

**Example 5.7.** (a) Consider the dihedral group $G = D_4 = \langle (12), (34) \rangle$. Then $G$ is the direct product of $H = \langle (12) \rangle$ and $K = \langle (12) \rangle$, so $G \cong C_2 \times C_2$.

(b) Let $G = (\mathbb{Z}/8\mathbb{Z})^\times$. Then $G = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$, and an easy calculation shows that $G$ is the direct product of $H = \langle \overline{3} \rangle$ and $K = \langle \overline{5} \rangle$. Thus $G \cong C_2 \times C_2$.

(c) Consider $G = S_3$ and the subgroups $H = \langle (12) \rangle$ and $K = \langle (123) \rangle$. Then $G = HK$, $H \cap K = \{1\}$, and $K$ is a normal subgroup of $G$. But $H$ is not a normal subgroup, so $G$ is not the direct product of $H$ and $K$. (This is also clear since $H \times K$ is abelian, and $G$ is non-abelian.)

**Example 5.8.** Let $n \geq 3$. Then as we have seen in an exercise (Theorem 1.57, Exercise 1.15), the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic. In fact, we can now prove that

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong C_{2^{n-2}} \times C_2.$$

To this end, Exercise 1.15 (d) shows that $H = \langle \overline{5} \rangle$ is a cyclic subgroup of order $2^{n-2}$ in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. We claim then that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is the direct product of $H$ and $K = \langle \overline{-1} \rangle$, from which the isomorphism follows since $K$ is cyclic of order 2.

Since $H$ and $K$ are normal subgroups, it will suffice to prove that $H \cap K = 1$, for then $|HK| = |H||K| = 2^{n-1} = |(\mathbb{Z}/2^n\mathbb{Z})^\times|$ and thus $(\mathbb{Z}/2^n\mathbb{Z})^\times = HK$. In other words, we should show that $\overline{-1} \notin \langle \overline{5} \rangle$. If we had $-1 \equiv 5^k \mod 2^n$, then in particular $-1 \equiv 5^k \mod 4$. But $5^k \equiv 1 \mod 4$ for all $k$, so this is a contradiction. Thus $H \cap K = 1$ and we get the isomorphism

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong C_{2^{n-2}} \times C_2.$$

Previously (Theorem 1.55) we proved that for any odd prime $p$, the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic for all $n > 0$. Moreover, it can be shown using the Chinese remainder theorem that if $a, b > 0$ are integers with $\gcd(a, b) = 1$, then

$$(\mathbb{Z}/ab\mathbb{Z})^\times \cong (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times.$$

Applying this on an integer $k > 0$ with prime factorization $k = p_1^{n_1} \cdots p_t^{n_t}$, we can describe the structure of $(\mathbb{Z}/k\mathbb{Z})^\times$, since the structure of $(\mathbb{Z}/p_i^{n_i}\mathbb{Z})^\times$ is now known for all $1 \leq i \leq t$.

**Lemma 5.9.** *Let $G = H \times K$. Then for any $A \leq H$ and $B \leq K$, the product $A \times B$ is a subgroup of $G$.*

*Proof.* Exercise. □

**Remark 5.10.** The converse of Lemma 5.9 fails; in general it is not true that every subgroup of $H \times K$ is of the form $A \times B$ for some $A \leq H$ and $B \leq K$. Example: Let $G$ be nontrivial and consider the direct product $G \times G$ and the diagonal subgroup $\Delta = \{(g, g) : g \in G\}$.

**Lemma 5.11.** *Let $H$ and $K$ be finite groups such that $\gcd(|H|, |K|) = 1$. If $N \leq H \times K$, then $N = A \times B$ for some $A \leq H$ and $B \leq K$.*

*Proof.* Exercise. □

**Lemma 5.12.** *Let $G$ and $H$ be groups. Then the following hold:*

(i) *$(G \times H)^{(k)} = G^{(k)} \times H^{(k)}$ for all $k \geq 0$.*

(ii) *$\gamma_k(G \times H) = \gamma_k(G) \times \gamma_k(H)$ for all $k \geq 1$.*

(iii) *$Z^k(G \times H) = Z^k(G) \times Z^k(H)$ for all $k \geq 0$.*

(iv) *The direct product $G \times H$ is solvable if and only if $G$ and $H$ are solvable.*

(v) *The direct product $G \times H$ is nilpotent if and only if $G$ and $H$ are nilpotent.*

*Proof.* Exercise. □

**Lemma 5.13.** *Let $G$ and $H$ be finite groups. Then the Fitting subgroup $F(G \times H) = F(G) \times F(H)$.*

*Proof.* Exercise. □

## 5.2 Classification of finitely generated abelian groups

In this section, we will provide the classification theorem of finitely generated abelian groups, thus in particular we classify the finite abelian groups. In the finite case, the first proof was given in 1870 by Kronecker.

The classification theorem could be proven naturally as part of the theory involving the Smith normal form and the classification of finitely generated modules over principal ideal domains. To keep these notes self-contained, we shall instead follow a short proof due to Rado[18].

[18] R. Rado, *A proof of the basis theorem for finitely generated Abelian groups.* J. London Math. Soc. 26 (1951), 74–75.

The key result is that any finitely generated abelian groups is a direct product of cyclic groups. For this we first need a lemma. (Note that throughout this section we will use additive notation for abelian groups.)

**Lemma 5.14.** *Let $G = \langle x_1, \ldots, x_k \rangle$ be an abelian group. Let $c_1$, …, $c_k \geq 0$ be integers such that $\gcd(c_1, \ldots, c_k) = 1$. Then there exists $y_1, \ldots, y_k \in G$ such that both of the following hold:*

(i) $G = \langle y_1, \ldots, y_k \rangle$;

(ii) $y_1 = c_1 x_1 + \cdots + c_k x_k$.

*Proof.* Let $s = c_1 + \cdots + c_k$. If $s = 1$, then $c_i = 1$ for some $1 \leq i \leq k$ and $c_j = 0$ for all $j \neq i$; in this case we can choose $y_1 = x_i$ and $\{y_2, \ldots, y_k\} = \{x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k\}$.

Suppose then $s > 1$ and proceed by induction on $s$. At least two of the $c_i$ are non-zero, and without loss of generality we can assume $c_1 \geq c_2 > 0$. Clearly $G = \langle x_1, x_1 + x_2, x_3, \ldots, x_k \rangle$ and $\gcd(c_1 - c_2, c_2, c_3, \ldots, c_k) = 1$. Now by induction there exist $y_1, \ldots, y_k \in G$ such that $G = \langle y_1, \ldots, y_k \rangle$ and

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

which proves the lemma. □

**Theorem 5.15.** *Let $G$ be a finitely generated abelian group, and suppose that $G$ is generated by $k$ elements. Then $G$ is isomorphic to a direct product of $\leq k$ cyclic groups.*

*Proof.* Let $k \geq 1$ be the smallest possible size of a generating set for $G$. If $k = 1$, then $G$ is cyclic and there is nothing to prove; assume $k > 1$ in what follows.

Choose generators $G = \langle x_1, x_2, \ldots, x_k \rangle$ such that $|x_1|$ is as small as possible. We will show that $G$ is the direct product of $\langle x_1 \rangle$ and $\langle x_2, \ldots, x_k \rangle$. If this is not the case, then by Lemma 5.6 their intersection is not trivial; thus there exist $a_1$, …, $a_k \in \mathbb{Z}$ such that $a_1 x_1 \neq 0$ and

$$a_1 x_1 + a_2 x_2 + \cdots + a_k x_k = 0.$$

We can assume that $0 < a_1 < |x_1|$. Moreover, by replacing some of the $x_i$ with $-x_i$ if necessary, we can assume $a_2, \ldots, a_k \geq 0$ without loss of generality.

Let $d = \gcd(a_1, a_2, \ldots, a_k)$. Since $\gcd(a_1/d, a_2/d, \ldots, a_k/d) = 1$, by Lemma 5.14 we can find $y_1, \ldots, y_k \in G$ such that $G = \langle y_1, \ldots, y_k \rangle$ and

$$y_1 = \frac{a_1}{d} x_1 + \frac{a_2}{d} x_2 + \cdots + \frac{a_k}{d} x_k.$$

But then we have $dy_1 = a_1x_1 + a_2x_2 + \cdots + a_kx_k = 0$, and thus

$$|y_1| \leq d \leq a_1 < |x_1|,$$

which contradicts the minimality of $|x_1|$.

Therefore $G$ is the direct product of $\langle x_1 \rangle$ and $\langle x_2, \ldots, x_k \rangle$. The theorem follows by applying induction on $\langle x_2, \ldots, x_k \rangle$. □

**Remark 5.16.** The assumption that $G$ is finitely generated is essential in Theorem 5.15. For example, an exercise shows that $G = (\mathbb{Q}, +)$ is not a direct product of cyclic groups.

**Definition 5.17.** Let $G$ be a group. We will use the following notation: $G^0 = \{1\}$ (trivial group), $G^1 = G$, and for $n > 1$ we denote $G^n = G \times \cdots \times G$ ($n$ times). Clearly $G^n \times G^m \cong G^{n+m}$ for all integers $n, m \geq 0$.

We have seen that any finitely generated abelian group is isomorphic to a direct product $C_{n_1} \times \cdots \times C_{n_k} \times \mathbb{Z}^n$ for some integers $n_1, \ldots, n_k > 1$ and $n \geq 0$. This decomposition is not unique, as is seen by the following lemma.

**Lemma 5.18.** *Let $m, n > 0$ be such that $\gcd(m, n) = 1$. Then $C_{mn} \cong C_m \times C_n$.*

*Proof.* Clearly $C_m \times C_n$ contains elements $x$ and $y$ with $|x| = m$ and $|y| = n$. Since $xy = yx$, by Lemma 1.29 we have $|xy| = mn$, so $C_m \times C_n$ is generated by $xy$. □

For example, we have $C_{15} \cong C_3 \times C_5$ by Lemma 5.18, so the decomposition of $C_{15}$ into a direct product of cyclic groups is not unique. However, if we assume that the integers $n_i$ in the decomposition $C_{n_1} \times \cdots \times C_{n_k} \times \mathbb{Z}^n$ are prime powers, we do get the following uniqueness result.

**Theorem 5.19.** *Let $G$ be a finitely generated abelian group. Then:*

(i) *$G \cong C_{n_1} \times \cdots \times C_{n_k} \times \mathbb{Z}^r$ for some $k \geq 0$, prime powers $n_1, \ldots, n_k > 1$, and $r \geq 0$.*

(ii) *The integers $n_1, \ldots, n_k$, $r$ are unique*[19].

[19] To be more precise, this means that if $G \cong C_{m_1} \times \cdots \times C_{m_\ell} \times \mathbb{Z}^s$ for some prime powers $m_1, \ldots, m_\ell > 1$ and $s \geq 0$; then $s = r$, $k = \ell$, and $(m_1, \ldots, m_k)$ is a permutation of $(n_1, \ldots, n_k)$.

*Proof.* For an integer $n > 1$ with prime factorization $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, we have

$$C_n \cong C_{p_1^{\alpha_1}} \times \cdots \times C_{p_t^{\alpha_t}}$$

by Lemma 5.18. This together with Theorem 5.15 proves (i).

Thus we can assume $G \cong C_{n_1} \times \cdots \times C_{n_k} \times \mathbb{Z}^r$ where $k \geq 0$, $n_1, \ldots, n_k > 1$ are prime powers, and $r \geq 0$. An exercise shows that the set

$$\operatorname{tor}(G) = \{g \in G : |g| < \infty\}$$

of elements of finite order is a subgroup of $G$, and moreover

$$\begin{aligned} \operatorname{tor}(G) &\cong C_{n_1} \times \cdots \times C_{n_k}, \\ G/\operatorname{tor}(G) &\cong \mathbb{Z}^r. \end{aligned}$$

Therefore if $G \cong C_{m_1} \times \cdots \times C_{m_\ell} \times \mathbb{Z}^s$ for some other prime powers $m_1, \ldots, m_\ell > 1$ and $s \geq 0$, we must have

$$\begin{aligned} C_{m_1} \times \cdots \times C_{m_\ell} &\cong C_{n_1} \times \cdots \times C_{n_k}, \\ \mathbb{Z}^s &\cong \mathbb{Z}^r. \end{aligned}$$

By an exercise $\mathbb{Z}^r \cong \mathbb{Z}^s$ if and only if $r = s$, so $r$ is uniquely determined by $G$. Next let $p$ be a prime. Consider $G(p^t) := \{g \in G : g^{p^t} = 1\}$, for $t \geq 1$. Then $G(p^t)$ is a subgroup of $G$, and for all $t \geq 1$ we have

$$G(p^t)/G(p^{t-1}) \cong (C_p)^{c_t},$$

where $c_t$ is the number of $n_j$ such that $n_j = p^\alpha$ for some $\alpha \geq t$ (Exercise). Then for $t \geq 1$, we have that $c_t - c_{t+1}$ is the number of $n_j$ such that $n_j = p^t$. On the other hand, by the same argument $c_t - c_{t+1}$ is the number of $m_j$ such that $m_j = p^t$. We conclude then that $k = \ell$ and $(m_1, \ldots, m_k)$ is a permutation of $(n_1, \ldots, n_k)$, so the integers $n_1$, ..., $n_k$ are uniquely determined by $G$. □

**Example 5.20.** By Theorem 5.19, we have a complete classification of all finite abelian groups. As an illustration, in Table 4 we provide a list of all finite abelian groups of order at most 12, up to isomorphism.

**Example 5.21.** In general, what is the number of finite abelian groups of order $n$? Write the prime factorization of $n$ as $n = p_1^{k_1} \cdots p_t^{k_t}$. Exercise: Use Theorem 5.19 to show that up to isomorphism, the number of finite abelian groups of order $n$ is $p(k_1) \cdots p(k_t)$, where $p(k)$ denotes the number of *partitions* of an integer $k > 0$.

For example $p(4) = 5$, since the partitions of 4 are 4, $1+3$, $2+2$, $1+1+2$, and $1+1+1+1$. And for any prime number $p$, there are a total of 5 abelian groups of order $p^4$ up to isomorphism:

$$C_{p^4} \quad C_p \times C_{p^3} \quad C_{p^2} \times C_{p^2} \quad C_p \times C_p \times C_{p^2} \quad C_p \times C_p \times C_p \times C_p$$

| $n$ | Abelian groups of order $n$ |
|---|---|
| 1 | $C_1$ |
| 2 | $C_2$ |
| 3 | $C_3$ |
| 4 | $C_4$, $C_2 \times C_2$ |
| 5 | $C_5$ |
| 6 | $C_2 \times C_3$ |
| 7 | $C_7$ |
| 8 | $C_8$, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$ |
| 9 | $C_9$, $C_3 \times C_3$ |
| 10 | $C_2 \times C_5$ |
| 11 | $C_{11}$ |
| 12 | $C_4 \times C_3$, $C_2 \times C_2 \times C_3$ |

Table 4: Abelian groups of order $1 \leq n \leq 12$.

**Lemma 5.22.** *Let $G$ be a finite abelian group of order $n > 0$. Let $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ be the prime factorization of $n$. Then the following hold.*

(i) *$G$ contains a unique subgroup $P_k$ of order $p_k^{\alpha_k}$ for all $1 \leq k \leq t$.*

(ii) *$G$ is the direct product of $P_1$, ..., $P_t$.*

*Proof.* (i) By Theorem 5.19, we can assume that

$$G = (C_{p_1^{m(1,1)}} \times \cdots \times C_{p_1^{m(1,r_1)}}) \times \cdots \times (C_{p_t^{m(t,1)}} \times \cdots \times C_{p_t^{m(t,r_t)}})$$

for some integers $m(i,j) > 0$, where $\sum_{j=1}^{r_k} m(k,j) = \alpha_k$ for all $1 \leq k \leq t$. Define

$$P_k = C_{p_k^{m(k,1)}} \times \cdots \times C_{p_k^{m(k,r_k)}}$$

for $1 \leq k \leq t$. Then $P_k$ is a subgroup of order $p^{\alpha_k}$ in $G$, and $G = P_1 \times \cdots \times P_t$. Since $P_i$ for $i \neq k$ have order coprime to $p_k$, we have

$$P_k = \{x \in G : x^{p^{\alpha_k}} = 1\}.$$

In other words, $P_k$ is the set of elements with order dividing $p^{\alpha_k}$, and thus it is the only subgroup of order $p_k^{\alpha_k}$ in $G$.

(ii) Clear from the description of $P_k$ in the proof of (i).

□

**Example 5.23.** Let $G$ be a finite abelian $p$-group, say $G \cong C_{p^{\alpha_1}} \times \cdots \times C_{p^{\alpha_t}}$ with $\alpha_1 \geq \cdots \geq \alpha_t > 0$.

(a) Exercise: For $H \leq G$, we have $H \cong C_{p^{\beta_1}} \times \cdots \times C_{p^{\beta_t}}$ for some $\beta_1 \geq \cdots \geq \beta_t \geq 0$.

(b) Exercise: In (a), we have $\beta_i \leq \alpha_i$ for all $1 \leq i \leq t$.

(c) Exercise: Prove that results analogous to (a) and (b) hold for the quotient $G/H$.

(d) Exercise: Let $H \leq G$. Show that there exists a subgroup of $G$ that is isomorphic to $G/H$.

(e) Exercise: Show that $Q_8$ does not have a subgroup isomorphic to $Q_8/Z(Q_8)$.

## 5.3 Automorphisms

Let $G$ be a group. Recall (Example 1.17) that an *automorphism* of $G$ is an isomorphism $\varphi : G \to G$. We will denote the set of all automorphisms of $G$ by $\mathrm{Aut}(G)$. It is easily seen that if $\varphi, \psi \in \mathrm{Aut}(G)$; then so is $\varphi\psi \in \mathrm{Aut}(G)$ and $\varphi^{-1} \in \mathrm{Aut}(G)$. Moreover, the identity map $I : G \to G$ defined by $I(g) = g$ for all $g \in G$ is always an automorphism of $G$.

Thus we conclude that $\mathrm{Aut}(G)$ is a subgroup of $\mathrm{Sym}(G)$. We call the group $\mathrm{Aut}(G)$ the *automorphism group* of $G$.

**Remark 5.24.** Exercise: Show that if $G \cong H$, then $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$.

Recall (Lemma 1.65) also that each element $g \in G$ defines an *inner automorphism* $\gamma_g : G \to G$ by $\gamma_g(x) = gxg^{-1}$ for all $x \in G$. Note that $\gamma_1$ is the identity map, and moreover $\gamma_{gh} = \gamma_g\gamma_h$ and $\gamma_g^{-1} = \gamma_{g^{-1}}$ for all $g, h \in G$. Therefore the set of all inner automorphisms forms a subgroup of $\mathrm{Aut}(G)$. We denote $\mathrm{Inn}(G) = \{\gamma_g : g \in G\}$ and call $\mathrm{Inn}(G)$ the *inner automorphism group of* $G$. The quotient $\mathrm{Aut}(G)/\mathrm{Inn}(G)$ is called the *outer automorphism group of* $G$ and denoted by $\mathrm{Out}(G)$.

**Lemma 5.25.** *Let $G$ be a group. Then the following hold:*

(i) $\mathrm{Inn}(G)$ *is a normal subgroup of* $\mathrm{Aut}(G)$*;*

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

*Proof.* (i) Let $\varphi \in \mathrm{Aut}(G)$. A calculation shows that $\varphi\gamma_g\varphi^{-1} = \gamma_{\varphi(g)}$ for all $g \in G$, thus $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

(ii) We define a map $\psi : G \to \mathrm{Inn}(G)$ by $\psi(g) = \gamma_g$. Since $\gamma_{gh} = \gamma_g\gamma_h$ for all $g, h \in G$, it is clear that $\psi$ is a surjective homomorphism. We have $\psi(g) = 1$ if and only if $gxg^{-1} = x$ for all $x \in G$; equivalently $g \in Z(G)$. Thus $\operatorname{Ker}\psi = Z(G)$, so $G/Z(G) \cong \mathrm{Inn}(G)$.

□

**Remark 5.26.** The following observation is easy but often useful. Suppose that $G$ is generated by some set $S$. Then any automorphism $\varphi$ is determined by its values on $S$. That is, if $\varphi, \varphi' \in \mathrm{Aut}(G)$ are such that $\varphi(x) = \varphi'(x)$ for all $x \in S$, then $\varphi = \varphi'$. This is easily seen for example with Lemma 1.39.

We now calculate automorphism groups for some examples of groups.

**Lemma 5.27.** *Let $G = \langle g \rangle$ be cyclic of order $n > 0$.*

(i) *For $k \in \mathbb{Z}$, define the map $\psi_k : G \to G$ by $x \mapsto x^k$. Then $\mathrm{Aut}(G) = \{\psi_k : \gcd(k, n) = 1\}$.*

(ii) $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

*Proof.* (i) It is clear that $\psi_k$ is a homomorphism for all $k \in \mathbb{Z}$. If $\gcd(k, n) = 1$, then by Lemma 1.46 (iv) we have $\langle g \rangle = \langle g^k \rangle$, so $\psi_k$ is surjective and thus a bijection since $G$ is finite. Therefore $\psi_k \in \mathrm{Aut}(G)$ for all $k \in \mathbb{Z}$ with $\gcd(k, n) = 1$.

Conversely, let $\varphi \in \mathrm{Aut}(G)$. Then $G = \langle \varphi(g) \rangle$, so by Lemma 1.46 (iv) we have $\varphi(g) = g^k$ for some $k \in \mathbb{Z}$ such that $\gcd(k, n) = 1$. Then it is clear that $\varphi(x) = x^k$ for all $x \in G$, so $\varphi = \psi_k$. This completes the proof of (i).

(ii) We have $\psi_k = \psi_{k'}$ if and only if $g^k = g^{k'}$, which is equivalent to $k \equiv k' \bmod n$. Thus we have an injective map defined by

$$\psi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G), \psi(\overline{k}) = \psi_k \text{ for all } k \in \mathbb{Z} \text{ with } \gcd(k, n) = 1.$$

It is clear $\psi$ is also surjective, so $\psi$ is a bijection. For all $k, k' \in \mathbb{Z}$ we have $\psi_k\psi_{k'} = \psi_{kk'}$, so we conclude that $\psi$ is an isomorphism and $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

□

**Lemma 5.28.** *Let $G = \langle g \rangle$ be infinite cyclic. Then $\mathrm{Aut}(G) \cong C_2$.*

*Proof.* Similar to Lemma 5.27. Since the only generators of $G$ are $g$ and $g^{-1}$ (Lemma 1.48), it is easy to see that the only nontrivial automorphism of $G$ is the inverse map $x \mapsto x^{-1}$. □

**Lemma 5.29.** $\mathrm{Aut}(S_3) \cong S_3$.

*Proof.* Let $G = S_3$. Consider $\varphi \in \mathrm{Aut}(G)$. We have $S_3 = \langle (12), (123) \rangle$, so $\varphi$ is determined by the images of (12) and (123). Since an automorphism must map an element to another element with the same order (Lemma 1.63 (vii)), we have

$$\varphi((12)) \in \{(12), (13), (23)\},$$
$$\varphi((123)) \in \{(123), (132)\}.$$

Thus $|\mathrm{Aut}(G)| \leq 3 \cdot 2 = 6$. On the other hand, by Lemma 5.25 we have $|\mathrm{Inn}(G)| = |G/Z(G)| = 6$ since $Z(G) = \{1\}$. Therefore $\mathrm{Aut}(G) = \mathrm{Inn}(G) \cong G/Z(G) \cong G$. □

**Lemma 5.30.** *Let $G$ and $H$ be finite groups such that* $\gcd(|G|, |H|) = 1$. *Then* $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

*Proof.* Exercise. □

**Example 5.31.** (a) The automorphism group of a cyclic group is not necessarily cyclic; for example $\mathrm{Aut}(C_8) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$.

(b) The automorphism group of an abelian group is not necessarily abelian. Exercise: $\mathrm{Aut}(C_2 \times C_2) \cong S_3$.

(c) Exercise: $\mathrm{Aut}(S_4) \cong S_4$.

**Theorem 5.32.** *Let $G$ be a group and let $H \leq G$. For $g \in N_G(H)$, define $f_g : H \to H$ by $f_g(x) = gxg^{-1}$ for all $x \in H$.*

(i) *$f_g$ is an automorphism of $H$ for all $g \in N_G(H)$.*

(ii) *The map $N_G(H) \to \mathrm{Aut}(H)$ defined by $g \mapsto f_g$ is a homomorphism with kernel $C_G(H)$. In particular $C_G(H) \trianglelefteq N_G(H)$, and $N_G(H)/C_G(H)$ is isomorphic to a subgroup of* $\mathrm{Aut}(H)$.

*Proof.* (i) By Lemma 1.65, each $f_g$ is an injective homomorphism. For $g \in N_G(H)$ we have $gHg^{-1} = H$, so $f_g$ is also surjective. Thus $f_g$ is an automorphism of $H$ for all $g \in N_G(H)$.

(ii) Similarly to Lemma 5.25 (ii).

□

Theorem 5.32 is sometimes called the "$N/C$-theorem" (normalizer-centralizer theorem).

## 5.4 Elementary abelian $p$-groups

Let $p$ be a prime, and $G$ be a finite $p$-group of order $|G| = p^n$. We say that $G$ is *elementary abelian*, if $G \cong C_p \times C_p \times \cdots \times C_p$ ($n$ times).

**Lemma 5.33.** *Let $G$ be a finite group. Then $G$ is an elementary abelian $p$-group if and only if $G$ is abelian and $x^p = 1$ for all $x \in G$.*

*Proof.* Exercise. □

Suppose now that $(G, +)$ is an elementary abelian $p$-group, with additive notation. The $(G, +)$ becomes a vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ as follows. Let $\overline{\lambda} \in \mathbb{F}_p$, where $\lambda \in \mathbb{Z}$. We define scalar multiplication by $\overline{\lambda}$ on $G$ by

$$\overline{\lambda} \cdot g = \lambda g$$

for all $g \in G$. Since $pg = 0$ for all $g \in G$, this operation is well defined. An exercise shows this makes $(G, +)$ into a vector space over $\mathbb{F}_p$. Since $G$ is finite, we have $|G| = p^n$, where $n$ is the dimension of $G$ as an $\mathbb{F}_p$-vector space.

Let $g_1, \ldots, g_n$ be a basis for $G$ has an $\mathbb{F}_p$-vector space. Then each $g \in G$ can be expressed uniquely in the form

$$g = \alpha_1 g_1 + \cdots + \alpha_n g_n$$

with $\alpha_i \in \mathbb{F}_p$. Thus $G = \langle g_1, \ldots, g_n \rangle$ and $G$ is the direct product of $\langle g_1 \rangle$, $\ldots$, $\langle g_n \rangle$.

If $\varphi : G \to G$ is a homomorphism, then $\varphi(x + y) = \varphi(x) + \varphi(y)$ for all $x, y \in G$. Moreover, we have $\varphi(kx) = k\varphi(x)$ for all $x \in G$ and $k \in \mathbb{Z}$, so in fact $\varphi$ is also a $\mathbb{F}_p$-linear map. In particular, this shows us that $\mathrm{Aut}(G)$ is precisely the set of $\mathbb{F}_p$-linear bijections $G \to G$, in other words $\mathrm{Aut}(G) = \mathrm{GL}(G)$. We have proven the following result.

**Lemma 5.34.** *Let $G$ be an elementary abelian $p$-group of order $p^n$. Then $\mathrm{Aut}(G) \cong \mathrm{GL}_n(p)$.*

We illustrate the identification of $\mathrm{Aut}(G)$ with $\mathrm{GL}_n(p)$ in the case where $n = 2$. Let $G$ be an elementary abelian $p$-group of order $p^2$. Let $g_1$, $g_2$ be a basis of $G$. Consider $\varphi \in \mathrm{Aut}(G)$. Then

$$\varphi(g_1) = g_1^a g_2^c$$
$$\varphi(g_2) = g_1^b g_2^d$$

for some $a, b, c, d \in \mathbb{Z}$. With the isomorphism $\mathrm{Aut}(G) \to \mathrm{GL}_2(p)$ (corresponding to the basis $g_1$, $g_2$), the automorphism $\varphi$ corresponds to the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in $\mathrm{GL}_2(p)$.

For example, we have $\mathrm{Aut}(C_2 \times C_2) \cong GL_2(2)$ and $\mathrm{Aut}(C_3 \times C_3) \cong \mathrm{GL}_2(3)$ by Lemma 5.34.

## 5.5 Semidirect products

By Lemma 5.6, a group $G$ is the direct product of two subgroups $H$ and $K$ precisely when the following two conditions hold:

(a) $G = HK$ and $H \cap K = \{1\}$. Equivalently, every $g$ factors as $g = hk$ for unique $h \in H$ and $k \in K$.

(b) Both $H$ and $K$ are normal in $G$.

If we assume that (a) holds (so $G = HK$ with unique factorization), but only assume that $H$ is a normal subgroup, we say that $G$ is a *semidirect product* of $H$ and $K$.

**Example 5.35.** (a) The direct product of any two groups is also a semidirect product.

(b) For $G = S_3$, consider $H = \langle (1\ 2\ 3) \rangle$ and $K = \langle (1\ 2) \rangle$. Then $G = HK$, $H \cap K = \{(1)\}$, and $H$ is a normal subgroup. Thus $G$ is the semidirect product of $H$ and $K$, and in this case $K$ is not a normal subgroup.

(c) More generally, $G = S_n$ is the semidirect product of $H = A_n$ and $K = \langle (1\ 2) \rangle$.

(d) $G = S_4$ is the semidirect product of

$$V = \{(1), (1\ 4)(2\ 3), (1\ 3)(2\ 4), (1\ 2)(3\ 4)\}$$

and $S_3$.

(e) Any dihedral group $G$ is a semidirect product of cyclic subgroups $H = \langle y \rangle$ and $K = \langle x \rangle$, where $|x| = 2$, $xyx^{-1} = y^{-1}$, and $x \notin \langle y \rangle$. (See Lemma 1.68 and Lemma 1.69.)

(f) The quaternion group $G = Q_8$ is not the semidirect product of two nontrivial subgroups $H$ and $K$, since $H \cap K$ contains $Z(Q_8) = \{1, -1\}$.

Given two groups $H$ and $K$, up to isomorphism there is only one group which is the direct product of $H$ and $K$. But for semidirect products there can be several possibilities. We know from Example 5.35 (b) that $S_3$ is isomorphic to a semidirect product of $C_2$ and $C_3$. But the direct product $C_2 \times C_3$ is also a semidirect product of $C_2$ and $C_3$, and certainly $C_2 \times C_3 \ncong S_3$.

So how can we construct all possible semidirect products of two groups? There is a natural way to do this, which is motivated by looking at the group operation in a semidirect product more closely.

Consider a group $G$ with subgroups $H$ and $K$ such that the following hold:

- $G = HK$,
- $H \cap K = \{1\}$,
- $H \trianglelefteq G$.

Given two elements $g = hk$ and $g' = h'k'$ with $h, h' \in H$ and $k, k' \in K$, their product should also be of the form $gg' = h''k''$ for unique $h'' \in H$ and $k'' \in K$. We can determine $h''$ and $k''$ as follows. We have

$$gg' = hkh'k' = (hkh'k^{-1})kk' \tag{5.1}$$

and here $kh'k^{-1} \in H$ since $H$ is a normal subgroup. Therefore $h'' = hkh'k^{-1}$ and $k'' = kk'$. In other words, $h'' = hf_k(h')$ and $k'' = kk'$ where $f_k$ is an automorphism of $H$ as in Theorem 5.32. Moreover by Theorem 5.32, the map $\psi : K \to \mathrm{Aut}(H)$ defined by $\psi(k) = f_k$ is a homomorphism.

So any semidirect product $G = HK$ with $H \trianglelefteq G$ comes with a homomorphism $\psi : K \to \mathrm{Aut}(H)$ which determines group operation of $G$: we have

$$(hk)(h'k') = (h\psi(k)(h'))(kk')$$

for all $h, h' \in H$ and $k, k' \in K$. This motivates the definition of an *external semidirect product* of $H$ and $K$, which we define as follows.

Let $H$ and $K$ be groups and let $\psi : K \to \mathrm{Aut}(H)$ be a homomorphism. The external semidirect product $H \rtimes_\psi K$ of $H$ and $K$ (corresponding to the homomorphism $\psi$) is the cartesian product

$$H \rtimes_\psi K := H \times K$$

equipped with the following group operation:

$$(h, k) \cdot (h', k') = (h\psi(k)(h'), kk')$$

for all $h, h' \in H$ and $k, k' \in K$.

We will next verify the the external semidirect product is indeed a group, and that it is the semidirect product of $H$ and $K$ with the various properties that we expect from it.

**Theorem 5.36.** *Let $H$ and $K$ be groups, and let $\psi : K \to \mathrm{Aut}(H)$ be a homomorphism. Then $H \rtimes_\psi K$ is a group. Moreover for $\widehat{H} = \{(h, 1) : h \in H\}$ and $\widehat{K} = \{(1, k) : k \in K\}$ the following hold:*

(i) *$\widehat{H}$ is a normal subgroup of $H \rtimes_\psi K$, and $H \cong \widehat{H}$ with an isomorphism given by $h \mapsto (h, 1)$.*

(ii) *$\widehat{K}$ is a subgroup of $H \rtimes_\psi K$, and $K \cong \widehat{K}$ with an isomorphism given by $k \mapsto (1, k)$.*

(iii) *$H \rtimes_\psi K = \widehat{H}\widehat{K}$ and $\widehat{H} \cap \widehat{K} = \{1\}$.*

*In particular $H \rtimes_\psi K$ is the semidirect product of $\widehat{H} = \{(h, 1) : h \in H\}$ and $\widehat{K} = \{(1, k) : k \in K\}$.*

*Proof.* We begin by showing that the binary operation on $H \rtimes_\psi K$ is associative. Let $h, h', h'' \in H$ and $k, k', k'' \in K$. Then

$$\begin{aligned}(h, k) \cdot ((h', k') \cdot (h'', k'')) &= (h, k) \cdot (h' \cdot \psi(k')(h''), k'k'') \\ &= (h \cdot \psi(k)(h' \cdot \psi(k')(h'')), k(k'k'')) \\ &= (h \cdot \psi(k)(h') \cdot (\psi(k) \circ \psi(k'))(h''), k(k'k'')) \quad (5.2) \\ &= (h \cdot \psi(k)(h') \cdot \psi(kk')(h''), k(k'k'')) \quad (5.3)\end{aligned}$$

where (5.2) holds since $\psi(k)$ is a homomorphism, and (5.3) holds since $\psi$ is a homomorphism. Similarly

$$\begin{aligned}((h, k) \cdot (h', k')) \cdot (h'', k'') &= (h \cdot \psi(k)(h'), kk') \cdot (h'', k'') \\ &= (h \cdot \psi(k)(h') \cdot \psi(kk')(h''), kk'(k'')).\end{aligned}$$

Therefore $(h, k) \cdot ((h', k') \cdot (h'', k'')) = ((h, k) \cdot (h', k')) \cdot (h'', k'')$ for all $h, h', h'' \in H$ and $k, k', k'' \in K$.

For all $h \in H$ and $k \in K$ we have $(h, k) \cdot (1, 1) = (h \cdot \psi(k)(1), k) = (h, k)$ and $(1, 1) \cdot (h, k) = (1 \cdot \psi(1)(h), k) = (h, k)$; therefore $(1, 1)$ is the identity element.

For inverse elements, the correct element is suggested by the formula (5.1). Indeed, we have $(hk)^{-1} = k^{-1}h^{-1} = h''k''$ with $h'' = k^{-1}h^{-1}k$ and $k'' = k^{-1}$.

This suggests that $(\psi(k^{-1})(h^{-1}), k^{-1})$ should be the inverse of $(h, k)$. We check that this is indeed the case. Now

$$\begin{aligned}(h,k)\cdot(\psi(k^{-1})(h^{-1}),k^{-1}) &= (h\cdot\psi(k)(\psi(k^{-1})(h^{-1}),kk^{-1})\\ &= (h\cdot\psi(kk^{-1})(h^{-1}),1)\\ &= (h\cdot h^{-1},1) = (1,1)\end{aligned}$$

and similarly

$$\begin{aligned}(\psi(k^{-1})(h^{-1}),k^{-1})\cdot(h,k) &= (\psi(k^{-1})(h^{-1})\cdot\psi(k^{-1})(h),k^{-1}k)\\ &= (\psi(k^{-1})(h^{-1}h),1)\\ &= (1,1).\end{aligned}$$

Therefore $(h, k)$ is invertible with inverse $(\psi(k^{-1})(h^{-1}), k^{-1})$. We conclude that $H \rtimes_\psi K$ is a group.

Since $(h, k) \mapsto k$ is a surjective homomorphism $H \rtimes_\psi K \to K$ with kernel equal to $\widehat{H}$, we conclude that $\widehat{H}$ is a normal subgroup. It is easily seen that the map $h \mapsto (h, 1)$ is an isomorphism $H \to \widehat{H}$, so $H \cong \widehat{H}$ and claim (i) holds. A similar calculation shows that $k \mapsto (k, 1)$ is an injective homomorphism with image equal to $\widehat{K}$, so (ii) holds. For (iii), we have $H \rtimes_\psi K = \widehat{H}\widehat{K}$ since $(h, k) = (h, 1) \cdot (1, k)$ for all $h \in H$ and $k \in K$. It is obvious that $\widehat{H} \cap \widehat{K} = \{(1, 1)\}$. This completes the proof of (i) – (iii) and the theorem. □

**Remark 5.37.** Note that if $\psi : K \to \mathrm{Aut}(H)$ is the *trivial homomorphism* defined by $\psi(k)(h) = h$ for all $k \in K$ and $h \in H$, then $H \rtimes_\psi K = H \times K$.

**Lemma 5.38.** *Let $G = H \rtimes_\psi K$ be an external semidirect product, where $\psi : K \to \mathrm{Aut}(H)$ is a homomorphism. Let $\widehat{H}$ and $\widehat{K}$ be as in Theorem 5.36. Then the following statements are equivalent:*

(i) $G = H \times K$.

(ii) $\psi : K \to \mathrm{Aut}(H)$ *is trivial.*

(iii) $\widehat{K}$ *is a normal subgroup of* $G$.

*Proof.* Exercise. □

Let $H \rtimes_\psi K$ be an external semidirect product of $H$ and $K$. Then it is clear that

$$\begin{aligned}(h,1)\cdot(h',1) &= (hh',1),\\ (1,k)\cdot(1,k') &= (1,kk'),\end{aligned}$$

$$(h,1)\cdot(1,k)=(h,k),$$
$$(1,k)\cdot(h,1)\cdot(1,k)^{-1}=(\psi(k)(h),1),$$

for all $h,h'\in H$ and $k,k'\in K$. Thus in practice when working with an external semidirect product $H\rtimes_\psi K$, we can denote $(h,k)$ by $hk$, $(h,1)$ by $h$, and $(1,k)$ by $k$ for all $h\in H$ and $k\in K$.

**Example 5.39.** Using Theorem 5.36 we can construct the dihedral groups as follows. Let $H=\langle y\rangle$ be cyclic, and let $K=\langle x\rangle$ be cyclic of order 2. We have a homomorphism $\psi: K\to \mathrm{Aut}(H)$, where $\psi(x): H\to H$ is the inverse map $h\mapsto h^{-1}$ on $H$. Let $G=H\rtimes_\psi K$. Then in $G$ we have the following (writing $y$ for $(y,1)$ and $x$ for $(1,x)$):

$$|x|=2, xyx^{-1}=y^{-1}, x\notin\langle y\rangle.$$

Therefore $G$ is dihedral (Lemma 1.68). If $H$ is finite cyclic of order $n$, then $G\cong D_{2n}$, and if $H$ is infinite cyclic, then $G\cong D_\infty$.

**Theorem 5.40.** *Suppose that $G=HK$, where $H\trianglelefteq G$, $K\leq G$, and $H\cap K=\{1\}$. Then the following hold:*

(i) *$G\cong H\rtimes_\psi K$, where $\psi: K\to\mathrm{Aut}(H)$ is the homomorphism defined by $\psi(k)(h)=khk^{-1}$ for all $h\in H$ and $k\in K$.*

(ii) *Suppose that $H\cong H'$ and $K\cong K'$. Then any external semidirect product $H\rtimes_\psi K$ is isomorphic to $H'\rtimes_{\psi'}K'$ for some homomorphism $\psi': K'\to\mathrm{Aut}(H')$.*

*Proof.* (i) We define $\varphi: H\rtimes_\psi K\to G$ by $\varphi(h,k)=hk$ for all $h\in H$ and $k\in K$. As in (5.1), for all $h,h'\in H$ and $k,k'\in K$ we have

$$\varphi(h,k)\varphi(h',k')=(hk)(h'k')=(h\cdot\psi(k)(h))(kk')=\varphi(h\cdot\psi(k)(h),kk'),$$

so $\varphi$ is a homomorphism. Moreover $\varphi$ is a bijection since $G=HK$ and $H\cap K=\{1\}$, so $\varphi$ is an isomorphism and $G\cong H\rtimes_\psi K$.

(ii) Exercise.

□

By Theorem 5.36 and Theorem 5.40, we have at least on some level a systematic way of studying semidirect products of two groups $H$ and $K$ up to isomorphism. Theorem 5.40 tells us that all possible semidirect products of two groups $H$ and $K$ can be constructed as an external semidirect product. However, there are many examples where $H\rtimes_\psi K\cong H\rtimes_{\psi'}K$ for $\psi\neq\psi'$.

.

**Example 5.41.** Let $H$ be a non-abelian group. Consider the direct product $G = H \times H$. Then $G$ is the direct product of $H \times \{1\}$ and $\{1\} \times H$, so $G = H \rtimes_\psi H$ with $\psi$ as the trivial map.

Now consider the diagonal subgroup

$$K = \{(h, h) : h \in H\}.$$

It is clear that $K \leq G$ and that $K \cong H$. Furthermore, we have that $G$ is the semidirect product of $H \times \{1\}$ and $K$, since $(x, y) = (xy^{-1}, 1)(y, y)$ for all $x, y \in H$. By Theorem 5.40, we have $G \cong H \rtimes_{\psi'} H$, where $\psi' : H \to \mathrm{Aut}(H)$ is defined by $\psi'(x)(y) = xyx^{-1}$ for all $x, y \in H$. Therefore

$$H \times H = H \rtimes_\psi H \cong H \rtimes_{\psi'} H,$$

and here $\psi' \neq \psi$ since $H$ is non-abelian.

**Example 5.42.** Any group $G$ is a semidirect product in a trivial way, since $G \cong G \rtimes_\psi \{1\} \cong \{1\} \rtimes_{\psi'} G$. But there are many examples of groups which can be written non-trivially as a semidirect product in many different ways. That is, we can have $H \rtimes_\psi K \cong H' \rtimes_{\psi'} K'$ with $H, K, H', K'$ non-trivial and pairwise non-isomorphic.

Consider the dihedral group $G = D_{12}$ of order 12, with generators $G = \langle x, y \rangle$ such that $|x| = 2$, $|y| = 6$, $xyx^{-1} = y^{-1}$. Then $G$ is the semidirect product of $H = \langle y \rangle$ and $K = \langle x \rangle$, so $G \cong C_6 \rtimes_\psi C_2$. On the other hand, an exercise shows that $G$ is also the semidirect product of $H' = \langle y^2 \rangle$ and $K' = \langle x, y^3 \rangle$, so $G \cong C_3 \rtimes_{\psi'} (C_2 \times C_2)$.

**Lemma 5.43.** *Let $H$ and $K$ be groups and let $\psi, \psi' : K \to \mathrm{Aut}(H)$ be homomorphisms. Then the following hold:*

(i) *Suppose that $\psi' = \psi\varphi$ for some $\varphi \in \mathrm{Aut}(K)$. Then $H \rtimes_\psi K \cong H \rtimes_{\psi'} K$.*

(ii) *Suppose that there exists $\phi \in \mathrm{Aut}(H)$ such that $\psi'(x) = \phi\psi(x)\phi^{-1}$ for all $x \in K$. Then $H \rtimes_\psi K \cong H \rtimes_{\psi'} K$.*

*Proof.* (i) Exercise: check that the map $H \rtimes_\psi K \to H \rtimes_{\psi'} K$ defined by $(h, k) \mapsto (h, \varphi^{-1}(k))$ is an isomorphism.

(ii) Exercise: check that the map $H \rtimes_\psi K \to H \rtimes_{\psi'} K$ defined by $(h, k) \mapsto (\phi(h), k)$ is an isomorphism.

□

**Remark 5.44.** Besides direct products and semidirect products, there are various other generalizations that have been studied in group theory. Suppose that $G$ is a group and $G = HK$ for some subgroups $H$ and $K$. Here are some notions that appear in the literature.

(a) **Factorizations:** Without any further assumptions, we say that $G = HK$ is a *factorization* of $G$. Even this level of generality has been studied. Factorizations of finite non-abelian almost simple[20] groups has been studied extensively, and is still an active area of research[21]. Factorizations of almost simple groups come up very naturally in permutation group theory, and have also found applications in the study of Cayley graphs.

(b) **Zappa-Szép products:** If $H \cap K = \{1\}$, we say that the factorization $G = HK$ is *exact*. In this case $G$ is called the *Zappa-Szép product* of $H$ and $K$. One has the notion of an *external Zappa-Szép product*, for which the analogue of Theorem 5.40 holds. A result of Douglas[22] gives a complete classification of Zappa-Szép products of finite cyclic groups $H \cong C_m$ and $K \cong C_n$.

(c) **Central products:** If $hk = kh$ for all $h \in H$ and $k \in K$, we say that $G$ is the *central product* of $H$ and $K$. In this case $H$ and $K$ are normal subgroups, $H \cap K \leq Z(G)$, and we are not necessarily assuming that $H \cap K$ is trivial. (If $H \cap K = \{1\}$, we get the direct product of $H$ and $K$.)

There is a notion of an *external central product* and an analogue of Theorem 5.40, which allows us to construct all possible central products of $H$ and $K$. The construction requires two subgroups $H_0 \leq Z(H)$, $K_0 \leq Z(K)$, and an isomorphism $\psi : H_0 \to K_0$.

One defines an external central product as

$$H \circ_\psi K = (H \times K)/N,$$

where $N$ is the normal subgroup $N = \{(h, k) \in H_0 \times K_0 : \psi(h) = k^{-1}\}$ of $H \times K$.

Let $\widehat{H}$ and $\widehat{K}$ be the images of $H \times \{1\}$ and $\{1\} \times K$ in $H \circ_\psi K$, respectively. Then the following hold:

- $H \cong \widehat{H}$

[20] A non-abelian simple group $G$ has trivial center, so $G \cong \mathrm{Inn}(G)$ and we can identify $G$ as a normal subgroup of $\mathrm{Aut}(G)$. A finite group $X$ is *almost simple* if $G \leq X \leq \mathrm{Aut}(G)$ for some non-abelian finite simple group $G$.

[21] See for example "T. C. Burness, C. H. Li, *On solvable factors of almost simple groups.*, Adv. Math. 377 (2021)"

[22] J. Douglas, *On finite groups with two independent generators. I–IV.*, Proc. Nat. Acad. Sci. U.S.A. 37 (1951).

- $K \cong \widehat{K}$
- $H \circ_\psi K$ is the central product of $\widehat{H}$ and $\widehat{K}$, with $\widehat{H} \cap \widehat{K} \cong H_0$.

Given a central product $G = HK$, one has $G \cong H \circ_\psi K$ with $H_0 = H \cap K = K_0$ and $\psi$ the identity map; thus the analogue of Theorem 5.40 holds[23].

## 5.6 Application: Groups of order $pq$ ($p$, $q$ primes)

Let $p$ and $q$ be distinct primes. What are the groups of order $pq$?

**Lemma 5.45.** *Let $G$ be a group such that $|G| = pq$, where $p > q$ are primes. Then $G \cong C_p \rtimes_\psi C_q$ for some $\psi : C_q \to \mathrm{Aut}(C_p)$.*

*Proof.* By Cauchy's theorem, there exist subgroups $H \leq G$ and $K \leq G$ with $|H| = p$ and $|K| = q$. We will show that $H \trianglelefteq G$. If this is not the case, then $H \neq g^{-1}Hg$ for some $g \in G$. But then $H \cap g^{-1}Hg = \{1\}$, so $|Hg^{-1}Hg| = p^2 > |G|$ by Lemma 1.88, a contradiction. Now the lemma follows from Theorem 5.40. □

**Proposition 5.46.** *Let $G$ be a group such that $|G| = pq$, where $p > q$ are primes. If $q \nmid p - 1$, then $G$ is cyclic.*

*Proof.* We have $\mathrm{Aut}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$ by Lemma 5.27 and Theorem 1.52. Thus if $q \nmid p - 1$, then every homomorphism $\psi : C_q \to \mathrm{Aut}(C_p)$ is trivial, and consequently $C_p \rtimes_\psi C_q = C_p \times C_q \cong C_{pq}$. □

**Proposition 5.47.** *Let $G$ be a group such that $|G| = pq$, where $p > q$ are primes. Suppose that $q \mid p - 1$. Then the following hold:*

(i) *There exists a non-trivial homomorphism $\psi : C_q \to \mathrm{Aut}(C_p)$, so that $X_{p,q} = C_p \rtimes_\psi C_q$ is non-abelian.*

(ii) *Any group of order $pq$ is isomorphic to $C_{pq}$ or $X_{p,q}$.*

*Proof.* (i) Let $C_q = \langle x \rangle$. Since $q \mid p - 1$, there exists an element $\sigma$ order $q$ in $\mathrm{Aut}(C_p) \cong C_{p-1}$ (Lemma 5.27 and Theorem 1.52). Thus there exists a homomorphism $\psi : C_q \to \mathrm{Aut}(C_p)$ such that $\psi(x) = \sigma$. Then $X_{p,q} := C_p \rtimes_\psi C_q$ is non-abelian, since $\psi$ is nontrivial.

[23] For details, see for example M. Suzuki's book "Group Theory I", Proposition 4.17, p. 138.

(ii) By Lemma 5.45, any group of order $pq$ is isomorphic to $C_p \rtimes_{\psi'} C_q$ for some homomorphism $\psi' : C_q \to \mathrm{Aut}(C_p)$.

If $\psi'$ is trivial, then $C_p \rtimes_{\psi'} C_q = C_p \times C_q \cong C_{pq}$.

If $\psi'$ is non-trivial, then $\psi'(x)$ is an element of order $q$ in $\mathrm{Aut}(C_p)$. Since $\mathrm{Aut}(C_p)$ is cyclic, it has a unique subgroup of order $q$, and so $\psi'(x) = \sigma^k = \psi(x)^k$ for some $k \in \mathbb{Z}$ coprime to $q$. Thus $\psi' = \psi\psi_k$, where $\psi_k : C_q \to C_q$ is the automorphism of $C_q$ defined by $\psi_k(x) = x^k$ (Lemma 5.27 (i)). It follows then from Lemma 5.43 (i) that $C_p \rtimes_{\psi'} C_q \cong C_p \rtimes_{\psi} C_q$. □

With Proposition 5.46 and Proposition 5.47, we have completed the classification of groups of order $pq$, where $p$ and $q$ are distinct primes. We summarize them in the following.

**Theorem 5.48.** *Let $p$ and $q$ be primes and assume that $p > q$. Then the following hold:*

*(a) If $q \nmid p - 1$, there is a unique group of order $pq$ up to isomorphism, the cyclic group $C_{pq}$.*

*(b) If $q \mid p - 1$, there are two groups of order $pq$ up to isomorphism, the cyclic group $C_{pq}$ and a non-trivial semidirect product $C_p \rtimes_\psi C_q$.*

**Remark 5.49.** As seen in the proof of Proposition 5.47, if $q \mid p - 1$ and we access to an automorphism of order $q$ in $\mathrm{Aut}(C_p)$, a non-trivial semidirect product $C_p \rtimes_\psi C_q$ can be described explicitly.

First note that due to the isomorphism $\mathrm{Aut}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, finding an automorphism of order $q$ in $\mathrm{Aut}(C_p)$ is equivalent to finding an integer $t$ such that $t \not\equiv 1 \mod p$ and $t^q \equiv 1 \mod p$. Indeed, then the powering map $g \mapsto g^t$ on $C_p$ defines an automorphism of order $q$.

Now writing $C_p = \langle x \rangle$ and $C_q = \langle y \rangle$, we have $x^p = y^q = 1$, and $yxy^{-1} = x^t$. Moreover, these relations determine the group operation on $C_p \rtimes_\psi C_q$ completely.

**Example 5.50.** Some special cases:

(i) Every group of order 33 is cyclic.

(ii) There are two groups of order 21 up to isomorphism. The cyclic group of order 21, and a non-trivial semidirect product $G = C_7 \rtimes_\psi C_3$. We have $2 \not\equiv 1 \mod 7$ and $2^3 \equiv 1 \mod 7$, so as in Remark 5.49, the map $x \mapsto x^2$ defines an automorphism of order 3 for $C_7$. It follows that there exist $x, y \in G$ such that $G = \langle x, y \rangle$, where $|x| = 7$, $|y| = 3$, and $yxy^{-1} = x^2$.

(iii) As special case of Theorem 5.48, we recover Theorem 1.122. If $p > 2$ is prime, then any group of order $2p$ is isomorphic to $C_{2p}$ or $D_{2p}$.

## 5.7 Application: $p$-groups of order $p^3$

Let $p$ be a prime. There is only one group of order $p$ up to isomorphism, the cyclic group $C_p$ of order $p$ (Corollary 1.83). We have seen (Proposition 1.144) that every group of order $p^2$ is abelian, and in this case by Theorem 5.19 we have the following result.

**Theorem 5.51.** *Let $p$ be a prime. There are only two groups of order $p^2$ up to isomorphism, the cyclic group $C_{p^2}$ and the direct product $C_p \times C_p$.*

In this section, we will apply the results on semidirect products to classify all groups of order $p^3$. By Theorem 5.19 there are exactly three abelian groups of order $p^3$ up to isomorphism: $C_{p^3}$, $C_p \times C_{p^2}$, and $C_p \times C_p \times C_p$.

We will next see that there are two non-abelian groups of order $p^3$ up to isomorphism, so in total we have $\mathrm{gnu}(p^3) = 5$ groups of order $p^3$. Thus the number of groups does not depend on $p$. However, we will have to deal with the cases $p = 2$ and $p > 2$ separately, and we begin with the case $p = 2$.

**Theorem 5.52.** *Let $G$ be a non-abelian group of order 8. Then $G \cong D_8$ or $G \cong Q_8$.*

*Proof.* Note first that $G$ must contain an element $y \in G$ of order 4. For otherwise $x^2 = 1$ for all $x \in G$, which is only possible if $G$ is abelian. We now consider the elements in $G \setminus \langle y \rangle$. Clearly any $x \in G \setminus \langle y \rangle$ must have order 2 or order 4, and moreover $G = \langle x, y \rangle$. Now $\langle y \rangle$ is a normal subgroup of $G$ since it has index 2, so $xyx^{-1} \in \langle y \rangle$. Since $|xyx^{-1}| = |y|$, we have $xyx^{-1} \in \{y, y^{-1}\}$. We cannot have $xyx^{-1} = y$ since otherwise $G = \langle x, y \rangle$ would be abelian, so $xyx^{-1} = y^{-1}$ for all $x \in G \setminus \langle y \rangle$.

*Case 1: There exists $x \in G \setminus \langle y \rangle$ with $|x| = 2$.*
In this case $G = \langle x, y \rangle$ with $|x| = 2$, $|y| = 4$, $xyx^{-1} = y^{-1}$, and $x \notin \langle y \rangle$. Thus $G$ is dihedral by Lemma 1.68, and $G \cong D_8$ by Theorem 1.71.

*Case 2: For all $x \in G \setminus \langle y \rangle$, we have $|x| = 4$.*
In this case, any element of order 2 must be contained in $\langle y \rangle$, so $\eta = y^2$ is the unique element of order 2 in $G$. In particular $\eta \in Z(G)$. Let $x \in G \setminus \langle y \rangle$. Then $|x| = 4$, so $x^2 = \eta$ and $xyx^{-1} = y^{-1}$. Similarly for $z = xy$ we have $|z| = 4$, $z^2 = \eta$, and $zyz^{-1} = y^{-1}$. The elements $1, \eta, x^{\pm 1}, y^{\pm 1}, z^{\pm 1}$ are distinct, so $G = \{1, \eta, x^{\pm 1}, y^{\pm 1}, z^{\pm 1}\}$.

Moreover $x^{-1} = \eta x$, $y^{-1} = \eta y$, and $z^{-1} = \eta z$, so we conclude that

$$G = \{1, \eta, x, \eta x, y, \eta y, z, \eta y\}.$$

One can check that the elements of $G$ satisfy the following relations:

$$\begin{aligned} x^2 = y^2 = z^2 &= \eta \\ xy = z &= \eta(yx) \\ yz = x &= \eta(zy) \\ zx = y &= \eta(xz) \\ \eta g &= g\eta \text{ for all } g \in G \end{aligned}$$

Which may remind you of the relations established for the quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, with $-1$, $i$, $j$, $k$ corresponding to $\eta$, $x$, $y$, $z$ respectively. At this point the theory of generators and relations would easily allow us to prove that the bijection $Q_8 \to G$ defined by

$$\begin{aligned} 1 &\mapsto 1 & -1 &\mapsto \eta \\ i &\mapsto x & -i &\mapsto \eta x \\ j &\mapsto y & -j &\mapsto \eta y \\ k &\mapsto z & -k &\mapsto \eta z \end{aligned}$$

is an isomorphism. This could also be checked manually.

Alternatively, we can compute the left regular representation $\varphi : G \to \mathrm{Sym}(G)$ and calculate

$$\begin{aligned} \varphi(x) &= \begin{pmatrix} 1 & \eta & x & \eta x & y & \eta y & z & \eta z \\ x & \eta x & \eta & 1 & z & \eta z & \eta y & y \end{pmatrix} \\ \varphi(y) &= \begin{pmatrix} 1 & \eta & x & \eta x & y & \eta y & z & \eta z \\ y & \eta y & \eta z & z & \eta & 1 & x & \eta x \end{pmatrix} \end{aligned}$$

Relabeling the elements of $G$ as 1, 2, …, 8, we find that

$$G \cong \varphi(G) = \langle \varphi(x), \varphi(y) \rangle \cong \langle (1\ 3\ 2\ 4)(5\ 7\ 6\ 8), (1\ 5\ 2\ 6)(3\ 8\ 4\ 7) \rangle.$$

These arguments also apply for $Q_8$ since it is a non-abelian group and all elements of $Q_8 \setminus \langle i \rangle$ have order 4, so we conclude

$$Q_8 \cong \langle (1\ 3\ 2\ 4)(5\ 7\ 6\ 8), (1\ 5\ 2\ 6)(3\ 8\ 4\ 7) \rangle$$

and thus $G \cong Q_8$.

□

**Lemma 5.53.** *Let $p$ be a prime, and let $G$ be a non-abelian group of order $p^3$. Then $|Z(G)| = p$, $G/Z(G) \cong C_p \times C_p$, and $Z(G) = [G, G]$.*

*Proof.* By Corollary 1.143 the center of $G$ is nontrivial, so $|Z(G)| = p$ or $|Z(G)| = p^2$. Since $G$ is non-abelian, $G/Z(G)$ cannot be cyclic (Exercise 1.31), so we must have $|Z(G)| = p$. Thus $G/Z(G)$ is a non-cyclic group of order $p^2$, which implies $G/Z(G) \cong C_p \times C_p$ by Theorem 5.51. In particular $G/Z(G)$ is abelian, so $[G, G] \leq Z(G)$. Because $[G, G] \neq 1$ and $|Z(G)| = p$, we conclude that $Z(G) = [G, G]$. □

**Lemma 5.54.** *Let $p > 2$ be a prime, and let $G$ be a non-abelian group of order $p^3$. Then $(xy)^p = x^p y^p$ for all $x, y \in G$.*

*Proof.* By Theorem 5.53 the commutator subgroup is central of order $p$, so by Lemma 4.8 we have

$$(xy)^p = x^p y^p [y, x]^{\frac{p(p-1)}{2}}$$

for all $x, y \in G$. Since $[G, G]$ has order $p$ and since $\frac{p(p-1)}{2}$ is a multiple of $p$, we have $[y, x]^{\frac{p(p-1)}{2}} = 1$. Thus $(xy)^p = x^p y^p$ for all $x, y \in G$. □

**Lemma 5.55.** *Let $p > 2$ be a prime, and let $G$ be a non-abelian group of order $p^3$. Then one of the following holds:*

(i) *$G$ contains an element of order $p^2$, and $G \cong C_{p^2} \rtimes_\psi C_p$ for some $\psi : C_p \to \mathrm{Aut}(C_{p^2})$.*

(ii) *$x^p = 1$ for all $x \in G$, and $G \cong (C_p \times C_p) \rtimes_\psi C_p$ for some $\psi : C_p \to \mathrm{Aut}(C_p \times C_p)$.*

*Proof.* By Lemma 5.54, the map $\varphi : G \to G$ defined by $\varphi(x) = x^p$ for all $x \in G$ is a homomorphism. Since $G/Z(G) \cong C_p \times C_p$ by Lemma 5.53, we have $\varphi(G) \leq Z(G)$. Now $|Z(G)| = p$, so by the first isomorphism theorem either $|\operatorname{Ker}\varphi| = p^2$ or $|\operatorname{Ker}\varphi| = p^3$. We consider the two possibilities.

*Case 1:* $|\operatorname{Ker}\varphi| = p^2$.
In this case, there exists $y \in G$ such that $y^p \neq 1$. Then we must have $|y| = p^2$, and $H = \langle y \rangle$ is a normal subgroup of $G$ by Proposition 1.148. Now $H \cap \operatorname{Ker}\varphi = \langle y^p \rangle$ has order $p$, so there exists $x \in \operatorname{Ker}\varphi$ such that $x \notin H$. Then for $K = \langle x \rangle$ we have $H \cap K = \{1\}$ and $G = HK$, so $G$ is the semidirect product of $H$ and $K$. By Theorem 5.40, (i) holds.

*Case 2:* $|\operatorname{Ker}\varphi| = p^3$.
In this case, we have $x^p = 1$ for all $x \in G$. By Proposition 1.146 there exists a

normal subgroup $H \trianglelefteq G$ with $|H| = p^2$, and by Theorem 5.51 we must have $H \cong C_p \times C_p$. Now choose $y \in G \setminus H$, and let $K = \langle y \rangle$, so $K \cong C_p$. Then $H \cap K = \{1\}$, and $G$ is the semidirect product of $H$ and $K$. By Theorem 5.40, (ii) holds. □

In view of Lemma 5.55, for $p > 2$ what remains is to classify the possible semidirect products $C_{p^2} \rtimes_\psi C_p$ and $(C_p \times C_p) \rtimes_\psi C_p$.

**Proposition 5.56.** *Let $p > 2$ be a prime. There exists a unique non-abelian semidirect product $C_{p^2} \rtimes_\psi C_p$ up to isomorphism.*

*Proof.* Let $C_p = \langle x \rangle$ and $C_{p^2} = \langle y \rangle$. First we note that a semidirect product $C_{p^2} \rtimes_\psi C_p$ is non-abelian if and only if $\psi : C_p \to \mathrm{Aut}(C_{p^2})$ is non-trivial, equivalently $\psi$ is injective.

By Theorem 1.55 and Lemma 5.27, we have $\mathrm{Aut}(C_{p^2}) \cong C_{p(p-1)}$. Thus we can find a homomorphism $\psi : C_p \to \mathrm{Aut}(C_{p^2})$ such that $\psi(x)$ has order $p$. Then $C_{p^2} \rtimes_\psi C_p$ is non-abelian.

Consider any non-trivial map $\psi' : C_p \to \mathrm{Aut}(C_{p^2})$. Then $\psi'(x)$ is an automorphism of order $p$. Since $\mathrm{Aut}(C_{p^2})$ is cyclic of order $p(p-1)$, it has a unique subgroup of order $p$, and therefore $\psi'(x) = \psi(x)^k$ for some $k \in \mathbb{Z}$ coprime to $p$. Thus $\psi' = \psi\psi_k$, where $\psi_k \in \mathrm{Aut}(C_p)$ is the automorphism defined by $\psi_k(x) = x^k$ (Lemma 5.27 (i)). By Lemma 5.43 (i), we conclude that $C_{p^2} \rtimes_\psi C_p \cong C_{p^2} \rtimes_{\psi'} C_p$. □

**Proposition 5.57.** *Let $p > 2$ be a prime. There exists a unique non-abelian semidirect product $(C_p \times C_p) \rtimes_\psi C_p$ up to isomorphism.*

*Proof.* Let $C_p = \langle g \rangle$, and suppose that $C_p \times C_p = \langle x, y \rangle$. We can identify $\mathrm{Aut}(C_p \times C_p) = \mathrm{GL}_2(p)$, where a matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ corresponds to the automorphism defined by $x \mapsto x^a y^c$, $y \mapsto x^b y^d$.

The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has order $p$ in $\mathrm{GL}_2(p)$, so there exists a homomorphism $\psi : C_p \to \mathrm{Aut}(C_p \times C_p)$ such that $\psi(g) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

By Example 3.19 any element of order $p$ in $\mathrm{GL}_2(p)$ is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Thus if $\psi' : C_p \to \mathrm{Aut}(C_p \times C_p)$ is a non-trivial homomorphism, then there exists $\phi \in \mathrm{Aut}(C_p \times C_p)$ such that $\psi'(g) = \phi\psi(g)\phi^{-1}$. Then $\psi'(g_0) = \phi\psi(g_0)\phi^{-1}$ for all $g_0 \in C_p$, so by Lemma 5.43 (ii), we have $(C_p \times C_p) \rtimes_\psi C_p \cong (C_p \times C_p) \rtimes_{\psi'} C_p$. □

Thus for any prime $p$, there are exactly two non-abelian groups $G$ of order $p^3$, up to isomorphism:

- If $p = 2$, we have $G \cong D_8$ or $G \cong Q_8$.
- For $p > 2$, we have $G \cong C_{p^2} \rtimes_\psi C_p$ or $G \cong (C_p \times C_p) \rtimes_{\psi'} C_p$, where the semidirect products are non-trivial.

For $p > 2$, we will realize the nontrivial semidirect products in the following examples. This amounts to finding automorphisms of order $p$ in $\mathrm{Aut}(C_{p^2})$ and $\mathrm{Aut}(C_p \times C_p)$.

**Example 5.58.** First note that $\mathrm{Aut}(C_{p^2}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times$, with $\overline{k} \in (\mathbb{Z}/p^2\mathbb{Z})^\times$ corresponding to the automorphism $\psi_k : g \mapsto g^k$ of $C_{p^2}$. We saw in the proof of Theorem 1.55 that $\overline{1+p}$ has order $p$ in $(\mathbb{Z}/p^2\mathbb{Z})^\times$, so the map $\psi_{p+1}$ is an automorphism of order $p$ for $C_{p^2}$. Consider then $C_{p^2} = \langle x \rangle$ and $C_p = \langle y \rangle$. We have a homomorphism $\psi : C_p \to \mathrm{Aut}(C_{p^2})$ defined by $\psi(y) = \psi_{1+p}$. Then

$$C_{p^2} \rtimes_\psi C_p = \langle x, y \rangle \text{ with } |x| = p^2,\ |y| = p, \text{ and } yxy^{-1} = x^{p+1}.$$

Moreover, the group operation in $C_{p^2} \rtimes_\psi C_p$ is completely determined by these relations.

**Example 5.59.** Let $x, y$ be a basis of $C_p \times C_p$, and let $C_p = \langle z \rangle$ be another cyclic group of order $p$. As we have seen Section 5.4, we have $\mathrm{Aut}(C_p \times C_p) \cong \mathrm{GL}_2(p)$, with matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ corresponding to the automorphism of $C_p \times C_p$ defined by $x \mapsto x^a y^c$ and $y \mapsto x^b y^d$. The matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(p)$ has order $p$, so the map $x \mapsto x$, $y \mapsto xy$ defines an automorphism $\varphi : C_p \times C_p \to C_p \times C_p$ of order $p$.

Thus we have a homomorphism $\psi' : C_p \to \mathrm{Aut}(C_p \times C_p)$ defined by $\psi(z) = \varphi$. Then $(C_p \times C_p) \rtimes_{\psi'} C_p = \langle x, y, z \rangle$ such that:

$$\begin{cases} |x| = |y| = |z| = p \\ xy = yx \\ \langle x, y \rangle \cong C_p \times C_p \\ zxz^{-1} = x \text{ and } zyz^{-1} = xy \end{cases}$$

The group operation in $(C_p \times C_p) \rtimes_\psi C_p$ is completely determined by these relations.

Alternatively, a nontrivial semidirect product $(C_p \times C_p) \rtimes_\psi C_p$ can be realized as the *Heisenberg group*

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

As seen in Exercise 1.37, for $p > 2$ the group $H_p$ is non-abelian of order $p^3$, and $x^p = 1$ for all $x \in H_p$.

## 5.8 Application: Groups of order $2n$ ($n$ odd)

**Lemma 5.60.** *Let $G$ be a finite group of order $mn$, where $\gcd(m, n) = 1$. Suppose that $G$ contains a normal subgroup $N$ of order $n$. Then $N$ is the unique subgroup of order $n$ in $G$, and*

$$N = \{x \in G : x^n = 1\}.$$

*Proof.* Exercise. □

**Theorem 5.61.** *Let $G$ be a finite group of order $2n$, where $n$ is odd. Then $G$ contains a unique subgroup $N$ of order $n$. Moreover $N \trianglelefteq G$ and $G \cong N \rtimes_\psi C_2$ for some homomorphism $\psi : C_2 \to \mathrm{Aut}(N)$.*

*Proof.* Consider the left regular representation $\varphi : G \to S_{2n}$ of $G$. Since $\varphi$ is injective, we can identify $G$ with $\varphi(G)$ and assume that $G \leq S_{2n}$. For an element $g \in G$, its orbits on the $2n$ points in $G$ are precisely the right cosets of $\langle g \rangle$ in $G$. Therefore any $g \in G$ is a product of $|G|/|g|$ disjoint cycles of length $|g|$. Consider an element $x \in G$ of order 2, which exists by Cauchy's theorem. Then

$$x = (a_1 a_1')(a_2 a_2') \cdots (a_n a_n')$$

is a product of $n$ transpositions, so $x$ is an odd permutation. Thus $G$ is not contained in $A_{2n}$, which implies that $N = G \cap A_{2n}$ is a normal subgroup of order $n$ in $G$ (Lemma 2.29).

Uniqueness of $N$ follows from Lemma 5.60, and $G \cong N \rtimes_\psi C_2$ since $G$ is the semidirect product of $N$ and $\langle x \rangle \cong C_2$. □

**Theorem 5.62.** *Let $N$ be a finite group of odd order $n$, and let $C_2 = \langle x \rangle$. Then $N \rtimes_\psi C_2 \cong N \rtimes_{\psi'} C_2$ if and only if $\psi(x)$ and $\psi'(x)$ are conjugate in $\mathrm{Aut}(N)$.*

*Proof.* If $\psi(x) = \varphi\psi(x)\varphi^{-1}$ for some $\varphi \in \mathrm{Aut}(N)$, it follows from Lemma 5.43 (ii) that $N \rtimes_\psi C_2 \cong N \rtimes_{\psi'} C_2$.

Conversely, suppose that there exists an isomorphism

$$\pi : N \rtimes_\psi C_2 \to N \rtimes_{\psi'} C_2.$$

Since $N$ is the unique subgroup of order $n$ in both groups, we have $\pi(N) = N$, and thus the restriction of $\pi$ to $N$ provides an automorphism $\varphi : N \to N$.

For the generator $x$ of $C_2$, we have $\pi(x) = n_0 x$ for some $n_0 \in N$. Since $\pi$ is a homomorphism, we get

$$\pi(xnx^{-1}) = \pi(x)\pi(n)\pi(x)^{-1} = n_0 x\varphi(n)x^{-1}n_0^{-1} = n_0\psi'(x)(\varphi(n))n_0^{-1}$$

for all $n \in N$. Since $\pi(xnx^{-1}) = \varphi(\psi(x)(n))$ for all $n \in N$, we conclude that

$$\varphi \circ \psi(x) = \gamma_{n_0} \circ \psi'(x) \circ \varphi,$$

where $\gamma_{n_0}$ is the inner automorphism $n \mapsto n_0 n n_0^{-1}$.

Then $\varphi\psi(x)\varphi^{-1} = \gamma_{n_0}\psi'(x)$, so it will suffice to prove that $\gamma_{n_0}\psi'(x)$ and $\psi'(x)$ are conjugate in $\mathrm{Aut}(N)$. To this end, we note that $\gamma_{n_0}\psi'(x)$ and $\psi'(x)$ both have order 2, so by Theorem 1.71 they generate a subgroup which is dihedral of order $2k$, where $k$ is the order of $\gamma_{n_0}$. Now $k$ is odd since $|N|$ is, so all elements of order 2 are conjugate in $D_{2k}$ (Exercise 5.29), and in particular $\gamma_{n_0}\psi'(x)$ and $\psi'(x)$ are conjugate. □

**Corollary 5.63.** *Let $N$ be a finite group of odd order $n$. Let $t$ be the number of conjugacy classes of elements of order 2 in $\mathrm{Aut}(N)$. Then up to isomorphism, there are $t+1$ semidirect products of the form $N \rtimes_\psi C_2$.*

*Proof.* Follows from Theorem 5.62. (We get one group from the trivial homomorphism $\psi(x) = 1$, which gives the direct product $N \times C_2$. The remaining $t$ groups are given by $\psi : C_2 \to \mathrm{Aut}(N)$ with $\psi(x)$ of order 2.) □

**Example 5.64.** Exercise: As an application of the results of this section, classify the groups of order 30, up to isomorphism. (Similarly, groups of order 66 and 70.)

**Example 5.65.** Suppose that $p > 2$ is a prime. We will classify groups of order $2p^2$. Any group $N$ of order $p^2$ is isomorphic to $C_{p^2}$ or $C_p \times C_p$. We know the following:

- $\mathrm{Aut}(C_{p^2}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times \cong C_{p(p-1)}$, so there is a unique element of order 2 in $\mathrm{Aut}(C_{p^2})$. Thus by Corollary 5.63, there are 2 semidirect products $C_{p^2} \rtimes_\psi C_2$, up to isomorphism.
- $\mathrm{Aut}(C_p \times C_p) \cong \mathrm{GL}_2(p)$, and by results of Section 3.5 there are two conjugacy classes of elements of order 2 in $\mathrm{GL}_2(p)$, with representatives

  $$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

  Therefore by Corollary 5.63, there are 3 semidirect products of the form $(C_p \times C_p) \rtimes_\psi C_2$, up to isomorphism.

By Theorem 5.61, we conclude that there are $2 + 3 = 5$ groups of order $2p^2$, up to isomorphism.

# 6 Sylow theory

In this section, we will prove the fundamental theorems of Sylow on finite groups. Throughout this section, a group $G$ will always be a finite group and $p$ will be a prime.

## 6.1 Double cosets

Let $H$ and $K$ be a subgroups of a group $G$. An $(H, K)$-double coset is a set of the form $HxK$, where $x \in G$.

**Lemma 6.1.** *Let $H, K \leq G$ be finite. Then*

$$|HxK| = \frac{|H||K|}{|x^{-1}Hx \cap K|}$$

*for all $x \in G$.*

*Proof.* Since $|HxK| = |x^{-1}HxK|$, the claim follows from Lemma 1.88 and the fact that $|x^{-1}Hx| = |H|$. □

**Lemma 6.2.** *Let $H, K \leq G$. Then for any two $(H, K)$-double cosets $HxK$ and $HyK$, either $HxK = HyK$ or $HxK \cap HyK = \emptyset$.*

*Proof.* If $HxK \cap HyK$ is nonempty, there exists $h, h' \in H$ and $k, k' \in K$ such that $hxk = h'yk'$. Then $x = h^{-1}h'yk'k^{-1}$, so $HxK = Hh^{-1}h'yk'k^{-1}K = HyK$. □

By Lemma 6.2, for $H, K \leq G$ the $(H, K)$-double cosets partition $G$, i.e. $G$ is a disjoint union

$$G = \bigcup_{x \in G} HxK.$$

Assuming that $G$ is finite, there exist representatives for the double cosets, that is, elements $x_1, \ldots, x_t \in G$ such that

$$G = \bigcup_{i=1}^{t} Hx_iK$$

and $Hx_iK \neq Hx_jK$ for $i \neq j$. Combining this with Lemma 6.1, we get the following result.

**Lemma 6.3.** *Let $G$ be a finite group and $H, K \leq G$. Let $x_1, \ldots, x_t \in G$ be representatives for the $(H, K)$-double cosets. Then*

$$|G| = \sum_{i=1}^{t} \frac{|H||K|}{|x_i^{-1}Hx_i \cap K|}.$$

## 6.2 Sylow theorems

**Theorem 6.4** (Sylow I)**.** *Let $G$ be a finite group and let $p$ be a prime. If $p^\beta$ divides $|G|$, then $G$ contains a subgroup of order $p^\beta$.*

*Proof.* We proceed by induction on the order of $G$, the case where $|G| = 1$ being obvious. Clearly we can assume that $\beta > 0$. The main idea is to use the class equation (Proposition 1.119), which tells us that

$$|G| = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)],$$

where $x_1, \ldots, x_t$ are representatives for the non-central conjugacy classes of $G$.

If $p$ divides $|Z(G)|$, then by Cauchy's theorem $Z(G)$ contains a subgroup $N$ of order $p$. Now $N$ is a normal subgroup of $G$ since it is central, and by induction $G/N$ contains a subgroup $H/N$ of order $p^{\beta-1}$. Then $H$ is a subgroup of $G$ with $|H| = p^\beta$. We may assume then that $p$ does not divide $|Z(G)|$. Since $p$ divides $|G|$, it follows from the class equation that there exists $1 \leq i \leq t$ such that $[G : C_G(x_i)]$ is not divisible by $p$. We have $|G| = [G : C_G(x_i)] \cdot |C_G(x_i)|$, so we conclude that $p^\beta$ must divide $|C_G(x_i)|$. Now $C_G(x_i)$ is a proper subgroup since $x_i$ is not in the center, so by induction $C_G(x_i)$ contains a subgroup of order $p^\beta$. □

Let $p$ be a prime and $G$ a finite group. A *$p$-subgroup* of $G$ is a subgroup $H \leq G$ such that $H$ is a $p$-group. A *Sylow $p$-subgroup* of $G$ is a $p$-subgroup $H \leq G$ with $|H| = p^\alpha$, where $p^\alpha$ is the largest power of $p$ that divides $|G|$. Equivalently, a Sylow $p$-subgroup of $G$ is a $p$-subgroup $H \leq G$ such that $p$ does not divide $[G : H]$.

We will denote the number of Sylow $p$-subgroups in $G$ by $n_p(G)$. Note that $n_p(G) \geq 1$ by Sylow I.

**Lemma 6.5.** *Let $G$ be a finite group and let $P$ be a Sylow $p$-subgroup of $G$. The following statements hold:*

(i) *If $P \trianglelefteq G$, then $P$ contains every $p$-subgroup of $G$.*

(ii) *Let $Q$ be a $p$-subgroup of $G$. Then $Q \cap N_G(P) = Q \cap P$.*

(iii) *$P \trianglelefteq G$ if and only if $n_p(G) = 1$.*

*Proof.* (i) Suppose that $P \trianglelefteq G$. Let $x \in G$ be an element of $p$-power order. The order of $xP$ in $G/P$ must also be a $p$-power. On the other hand, by Lagrange's theorem the order of $xP$ divides $[G : P]$. Since $p$ does

not divide $[G : P]$, it follows that $xP$ is the identity, and thus $x \in P$. So $P$ contains every element of $p$-power order, and therefore it contains every $p$-subgroup of $G$.

(ii) Note that $P$ is a Sylow $p$-subgroup of $N_G(P)$ and $P \trianglelefteq N_G(P)$. So since $Q \cap N_G(P)$ is a $p$-subgroup of $N_G(P)$, we have $Q \cap N_G(P) \leq P$ by (i). Therefore $Q \cap N_G(P) \leq Q \cap P$. The reverse inclusion follows from $P \leq N_G(P)$, so $Q \cap N_G(P) = Q \cap P$.

(iii) Suppose that $P \trianglelefteq G$. If $Q$ is a Sylow $p$-subgroup of $G$, then $Q \leq P$ by (i). Since $|Q| = |P|$ it follows that $Q = P$, and so $n_p(G) = 1$.

For the other direction, suppose that $n_p(G) = 1$. Every conjugate of $P$ is a Sylow $p$-subgroup of $G$, so we must have $g^{-1}Pg = P$ for all $g \in G$. In other words, the subgroup $P$ is a normal subgroup of $G$.

□

**Theorem 6.6.** *Let $p$ be a prime and let $P$ be a Sylow $p$-subgroup of $G$. Let $Q \leq G$ be a $p$-subgroup of $G$. Then there exists $g \in G$ such that $Q \leq g^{-1}Pg$.*

*Proof.* Consider the decomposition of $G$ into a disjoint union of $(P, Q)$-double cosets:

$$G = \bigcup_{i=1}^{t} Px_iQ$$

where $x_1, \ldots, x_t \in G$ and the double cosets $Px_iQ$ are distinct. Then

$$|G| = \sum_{i=1}^{t} |Px_iQ| = \sum_{i=1}^{t} |P|[Q : x_i^{-1}Px_i \cap Q]$$

by Lemma 6.1. Therefore

$$[G : P] = \sum_{i=1}^{t} [Q : x_i^{-1}Px_i \cap Q].$$

Since $[G : P]$ is not divisible by $p$, it follows that for some $1 \leq i \leq t$ we have $[Q : x_i^{-1}Px_i \cap Q]$ not divisible by $p$. Since $Q$ is a $p$-group, this implies $Q = x_i^{-1}Px_i \cap Q$, in other words $Q \leq x_i^{-1}Px_i$. □

**Theorem 6.7** (Sylow II)**.** *Let $p$ be a prime. Any two Sylow $p$-subgroups of $G$ are conjugate.*

*Proof.* Let $P$ and $Q$ be Sylow $p$-subgroups of $G$. By Theorem 6.6, there exists $g \in G$ such that $Q \leq g^{-1}Pg$. Since $|Q| = |P| = |g^{-1}Pg|$, it follows that $Q = g^{-1}Pg$. □

**Theorem 6.8** (Sylow III)**.** *Let $p$ be a prime, and let $p^\alpha$ be the largest power of $p$ dividing $|G|$. Write $|G| = p^\alpha m$. Then the following hold:*

(i) *$n_p(G)$ divides $m$,*

(ii) *$n_p(G) = [G : N_G(P)]$ for any Sylow $p$-subgroup $P \leq G$,*

(iii) *$n_p(G) \equiv 1 \mod p$.*

*Proof.* Let $P \leq G$ be a Sylow $p$-subgroup of $G$. By Sylow II and Lemma 1.137 we have $n_p(G) = [G : N_G(P)]$, which divides

$$m = [G : P] = [G : N_G(P)][N_G(P) : P].$$

Thus (i) and (ii) hold. For (iii), we consider the $(P, N_G(P))$-double coset decomposition of $G$. Let $x_1, \ldots, x_t \in G$ be representatives for the $(P, N_G(P))$-double cosets in $G$ with $x_1 = 1$. Then

$$G = \bigcup_{i=1}^{t} P x_i N_G(P)$$

and $x_2, \ldots, x_t \notin N_G(P)$. Since $Px_1N_G(P) = N_G(P)$, we have

$$\begin{aligned} |G| &= |N_G(P)| + \sum_{i=2}^{t} |Px_iN_G(P)| \\ &= |N_G(P)| + \sum_{i=2}^{t} \frac{|P||N_G(P)|}{|N_G(P) \cap x_i^{-1}Px_i|} \qquad (6.1) \\ &= |N_G(P)| + \sum_{i=2}^{t} |N_G(P)|[P : P \cap x_i^{-1}Px_i] \qquad (6.2) \end{aligned}$$

where (6.1) holds by Lemma 6.1 and (6.2) holds by Lemma 6.5 (ii). Therefore

$$[G : N_G(P)] = 1 + \sum_{i=2}^{t} [P : P \cap x_i^{-1}Px_i].$$

For $2 \leq i \leq t$ we cannot have $P = P \cap x_i^{-1}Px_i$, since this would imply $P = x_i^{-1}Px_i$ and contradict $x_i \notin N_G(P)$. We conclude then that $[P : P \cap x_i^{-1}Px_i]$ is divisible by $p$ for all $2 \leq i \leq t$, and thus $[G : N_G(P)] \equiv 1 \mod p$. By (ii), we have $n_p(G) \equiv 1 \mod p$. □

**Example 6.9.** There are many examples where using Sylow III, we can deduce from the order $|G|$ of a finite group that it has a normal Sylow $p$-subgroup.

(a) Suppose that $|G| = 6 = 2 \cdot 3$. Then $n_3(G)$ divides 2, so $n_3(G) = 1$ or $n_3(G) = 2$. On the other hand $n_3(G) \equiv 1 \mod 3$, so $n_3(G) = 1$. Thus $G$ has a normal subgroup of order 3 (as we have already seen previously, for example in Lemma 5.45).

(b) Suppose that $|G| = pq$, where $p > q$ are primes. By Sylow III $n_p(G)$ divides $q$, so $n_p(G) = 1$ or $q$. Since $p > q$ we have $q \not\equiv 1 \mod p$, so by Sylow III $n_p(G) = 1$. Therefore $G$ has a normal subgroup of order $p$.

Similarly we know that $n_q(G)$ divides $p$, so $n_q(G) = 1$ or $n_q(G) = p$. Since $n_q(G) \equiv 1 \mod q$, if $q \nmid p - 1$, then $n_q(G) = 1$. If $q \mid p - 1$, we have $n_q(G) = p$ when $G = C_p \rtimes_\psi C_q$ is a nontrivial semidirect product.

(c) Suppose that $|G| = 40 = 2^3 \cdot 5$. Then $n_5(G)$ divides $8 = 2^3$, so $n_5(G)$ is equal to 1, 2, 4, or 8. Since $2, 4, 8 \not\equiv 1 \mod 5$, we conclude $n_5(G) = 1$ and so $G$ has a normal subgroup $Q$ of order 5. By Sylow I, there exists a subgroup $P \leq G$ with $|P| = 8 = 2^3$. Then $G$ is the semidirect product of $Q$ and $P$, so

$$G \cong C_5 \rtimes_\psi P$$

for some homomorphism $\psi : P \to \mathrm{Aut}(C_5)$. We know that there are 5 groups of order $|P| = 8$ up to isomorphism. Thus the classification of groups of order 40 is equivalent to classifying the following semidirect products:

- $C_5 \rtimes_\psi C_8$ (3 groups up to isomorphism)
- $C_5 \rtimes_\psi (C_4 \times C_2)$ (4 groups up to isomorphism)
- $C_5 \rtimes_\psi (C_2 \times C_2 \times C_2)$ (2 groups up to isomorphism)
- $C_5 \rtimes_\psi D_8$ (3 groups up to isomorphism)
- $C_5 \rtimes_\psi Q_8$ (2 groups up to isomorphism)

For now we omit the details of how these semidirect products are classified up to isomorphism. However, the conclusion in the end is that there are $3 + 4 + 2 + 3 + 2 = 14$ groups of order 40.

(d) Suppose that $|G| = 42 = 2 \cdot 3 \cdot 7$. Then $n_7(G)$ divides 6, so $n_5(G)$ is equal to 1, 2, 3, or 6. Since $2, 3, 6 \not\equiv 1 \mod 7$, we must have $n_7(G) = 1$ and so $G$ has a normal subgroup of order 7.

(e) Suppose that $|G| = 56 = 2^3 \cdot 7$. Then $n_7(G)$ divides 8, so $n_7(G)$ equals 1, 2, 4, or 8. Since $2, 4 \not\equiv 1 \mod 7$, we have $n_7(G) = 1$ or $n_7(G) = 8$. If $n_7(G) = 1$, then there is a normal subgroup of order 7 in $G$. Suppose that $n_7(G) = 8$. For distinct 7-Sylows $Q, Q'$ we have $Q \cap Q' = \{1\}$ since

they have prime order, so there are a total of $8 \cdot (7-1) = 48 = |G| - 8$ elements of order 7 in $G$. This implies that there can be only one Sylow 2-subgroup, as otherwise we would get too many elements. In that case there is a normal subgroup of order 8.

In conclusion, $G$ will always a have a normal Sylow subgroup (either a 2-Sylow or a 7-Sylow, or both). It follows that either $G \cong P \rtimes_\psi C_7$ or $G \cong C_7 \rtimes_{\psi'} P$, where $|P| = 8$. Classifying these semidirect products up to isomorphism, one finds that there are a total of 13 groups of order 56, up to isomorphism.

**Lemma 6.10.** *Let $P$ be a Sylow $p$-subgroup of $G$. Let $H$ be a subgroup of $G$ such that $N_G(P) \leq H$. Then $N_G(H) = H$.*

*Proof.* It is clear that $H \leq N_G(H)$. For the converse, let $x \in N_G(H)$. Since $P \leq H$, we have $xPx^{-1} \leq H$. Since $P$ and $xPx^{-1}$ are Sylow $p$-subgroups of $H$, they are conjugate in $H$ (Sylow II), so there exists $h \in H$ such that $hPh^{-1} = xPx^{-1}$. Then $h^{-1}x \in N_G(P)$, so $x \in HN_G(P) = H$. Therefore $N_G(H) \leq H$, and thus $N_G(H) = H$. □

## 6.3 Sylow subgroups of subgroups and quotients

Let $G$ be a finite group and let $p$ be a prime. We will denote the set of Sylow $p$-subgroups of $G$ by $\mathrm{Syl}_p(G)$. That is, if $p^\alpha$ is the largest power of $p$ dividing $G$, we have

$$\mathrm{Syl}_p(G) = \{P \leq G : |P| = p^\alpha\}.$$

Given a subgroup $H \leq G$, or a normal subgroup $N \trianglelefteq G$, what can we say about $\mathrm{Syl}_p(H)$, $\mathrm{Syl}_p(N)$, and $\mathrm{Syl}_p(G/N)$? The next two lemmas provide some answers.

**Lemma 6.11.** *Let $H \leq G$. Then*

$$\mathrm{Syl}_p(H) \subseteq \{P \cap H : P \in \mathrm{Syl}_p(G)\}.$$

*Proof.* Exercise. □

One can find examples where $\mathrm{Syl}_p(H) \subsetneqq \{P \cap H : P \in \mathrm{Syl}_p(G)\}$. (Exercise.)

**Lemma 6.12.** *Let $G$ be a finite group, let $p$ be a prime, and let $N \trianglelefteq G$. Then*

$$\mathrm{Syl}_p(N) = \{P \cap N : P \in \mathrm{Syl}_p(G)\}$$

*and*

$$\mathrm{Syl}_p(G/N) = \{PN/N : P \in \mathrm{Syl}_p(G)\}.$$

*Proof.* Exercise. □

**Lemma 6.13.** *Let $G$ be a finite group, let $p$ be a prime. Then:*

(i) *If $H \leq G$, then $n_p(H) \leq n_p(G)$.*

(ii) *If $N \trianglelefteq G$, then $n_p(N) \mid n_p(G)$.*

(iii) *If $N \trianglelefteq G$, then $n_p(G/N) \mid n_p(G)$*

*Proof.* (i) Follows from Lemma 6.11.

(ii) By Lemma 6.12, every Sylow $p$-subgroup of $N$ has the form $P \cap N$ for some $P \in \mathrm{Syl}_p(G)$. Now

$$(P \cap N)^g = P^g \cap N^g = P^g \cap N$$

for all $g \in G$. Thus $G$ acts by conjugation on the set of Sylow $p$-subgroups of $N$, and this action is transitive since Sylow subgroups are conjugate in $G$ (Sylow II). Thus $n_p(N) = [G : N_G(P \cap N)]$ by the orbit-stabilizer theorem. Now $N_G(P) \leq N_G(P \cap N)$, so

$$n_p(G) = [G : N_G(P \cap N)][N_G(P \cap N) : P \cap N] = n_p(N)[N_G(P \cap N) : P \cap N].$$

Thus $n_p(N) \mid n_p(G)$.

(iii) For $P \in \mathrm{Syl}_p(G)$, we have $PN/N \in \mathrm{Syl}_p(G/N)$. Then $N_{G/N}(PN/N) = N_G(PN)/N$ by Lemma 1.139. Thus

$$n_p(G/N) = [G/N : N_G(PN)/N] = [G : N_G(PN)].$$

On the other hand $N_G(P) \leq N_G(PN)$ (since $(PN)^x = P^x N^x = P^x N$), so

$$\begin{aligned} n_p(G) &= [G : N_G(PN)][N_G(PN) : N_G(P)] \\ &= n_p(G/N)[N_G(PN) : N_G(P)]. \end{aligned}$$

In particular $n_p(G/N) \mid n_p(G)$.

□

We note that tere are examples where $H \leq G$ and $n_p(H) \nmid n_p(G)$. The smallest example occurs for $G = A_5$. There exists a subgroup $H < G$ such that $H \cong S_3$. An exercise shows that $n_2(H) = 3$ and $n_2(G) = 5$, so $n_2(H)$ does not divide $n_2(G)$.

More generally for $N \trianglelefteq G$, we have the following formula:

$$n_p(G) = n_p(N)n_p(G/N)n_p(N_{PN}(P \cap N))$$

We will omit the proof, but this formula is due to Marshall Hall Jr., who studied properties of the numbers $n_p(G)$ in a paper from 1967. Among other things, he proved that there does not exist a finite group $G$ such that $n_3(G) = 22$ (although $22 \equiv 1 \mod 3$).

## 6.4 Number of $p$-subgroups of given order

Let $G$ be a finite group and let $p$ be a prime. Suppose that $p^n$ is the largest power of $p$ that divides $|G|$. By Sylow III, we know that the number of subgroups of order $p^n$ is $\equiv 1 \mod p$. It turns out the same is true for the number of subgroups of order $p^k$, for every $0 \leq k \leq n$. We will prove this in the following.

**Theorem 6.14** (Frobenius, 1895)**.** *Let $G$ be a finite group, and let $p$ be a prime. If $p^k$ divides $|G|$, then the number of subgroups of order $p^k$ in $G$ is $\equiv 1 \mod p$.*

*Proof.* Denote by $r_k$ the number of subgroups of order $p^k$ in $G$. We will proceed by induction on $k$. For $k = 0$ we have $r_0 = 1$, while for $k = 1$ we have $r_1 \equiv 1 \mod p$ by Corollary 1.128. Suppose then that $k \geq 1$ and that $r_k \equiv 1 \mod p$ for all finite groups $G$ with $p^k \mid |G|$. We will show that $r_{k+1} \equiv 1 \mod p$.

To this end, let $P_1, \ldots, P_{r_k}$ be the subgroups of order $p^k$ in $G$. For $1 \leq i \leq r_k$, let $\lambda_i$ be the number of subgroups of order $p^{k+1}$ that contain $P_i$. Note that $\lambda_i$ is the number of subgroups of order $p$ in $N_G(P_i)/P_i$. Indeed, if $P_i \lneqq Q$ and $|Q| = p^{k+1}$, then $P_i \trianglelefteq Q$ by Proposition 1.148. Thus $Q \leq N_G(P_i)$, and $Q/P_i$ is a subgroup of order $p$ in $N_G(P_i)/P_i$. Conversely, if $Q/P_i$ is a subgroup of order $p$ in $N_G(P_i)/P_i$, then $Q$ is a subgroup of order $p^{k+1}$ that contains $P_i$.

Since $P_i$ is contained in some Sylow $p$-subgroup (Theorem 6.6) and since normalizers grow in $p$-groups (Proposition 1.147), the group $N_G(P_i)/P_i$ is divisible by $p$. Thus the number of subgroups of order $p$ in $N_G(P_i)/P_i$ is $\equiv 1 \mod p$ by Corollary 1.128. That is, we have $\lambda_i \equiv 1 \mod p$ for all $1 \leq i \leq r_k$.

Similarly, let $Q_1, \ldots, Q_{r_{k+1}}$ be the subgroups of order $p^{k+1}$ in $G$. For $1 \leq i \leq r_{k+1}$, we denote by $\mu_i$ the number of subgroups of order $p^k$ that are contained in $Q_i$. By induction, we know that $\mu_i \equiv 1 \mod p$ for all $1 \leq i \leq r_{k+1}$.

Then

$$\lambda_1 + \cdots + \lambda_{r_k} = \mu_1 + \cdots + \mu_{r_{k+1}},$$

because both sides of the equation count the number of pairs $(P_i, Q_j)$ with $P_i \leq Q_j$. We have $\lambda_i \equiv 1 \mod p$ and $\mu_j \equiv 1 \mod p$ for all $1 \leq i \leq r_k$ and $1 \leq j \leq r_{k+1}$, so it follows that

$$r_k \equiv r_{k+1} \mod p.$$

We conclude then that $r_{k+1} \equiv 1 \mod p$. □

## 6.5 Nilpotent groups and Sylow subgroups

We have seen previously that a finite abelian group is isomorphic to the direct product of its Sylow subgroups (Lemma 5.22). More generally, this property characterizes finite nilpotent groups.

**Proposition 6.15.** *Let $G$ be a finite group. The following statements are equivalent:*

(i) *$G$ is nilpotent.*

(ii) *Every Sylow subgroup of $G$ is normal.*

(iii) *$G$ is the direct product of its Sylow $p$-subgroups.*

*Proof.* We will prove (i) ⇒ (ii) ⇒ (iii) ⇒ (i).

(i) ⇒ (ii): Suppose that $G$ is nilpotent, and let $P \leq G$ be a Sylow $p$-subgroup of $G$. By Lemma 6.10 we have $N_G(N_G(P)) = N_G(P)$. Therefore $N_G(P)$ cannot be a proper subgroup of $G$, since normalizers grow in nilpotent groups (Proposition 4.43). Thus $N_G(P) = G$, which means that $P \trianglelefteq G$.

(ii) ⇒ (iii): Write the prime factorization of $|G|$ as $|G| = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$. For $1 \leq i \leq t$, let $P_i \leq G$ be a Sylow $p_i$-subgroup of $G$. By assumption $P_i \trianglelefteq G$. Then any product $P_{i_1} \cdots P_{i_t}$ of some $P_i$'s is a subgroup.

Moreover we claim that $|P_{i_1} \cdots P_{i_t}| = |P_{i_1}| \cdots |P_{i_t}|$, and this is easily proven by induction. Indeed, first for $t = 1$ the claim is trivial. For $t > 1$ we have $P_{i_1} \cap (P_{i_2} \cdots P_{i_t}) = \{1\}$, since by induction $P_{i_2} \cdots P_{i_t}$ is a subgroup with order $|P_{i_2}| \cdots |P_{i_t}|$, which is coprime to $|P_{i_1}|$. Thus $|P_{i_1}(P_{i_2} \cdots P_{i_t})| = |P_{i_1}| \cdot |P_{i_2} \cdots P_{i_t}| = |P_{i_1}| \cdot |P_{i_2}| \cdots |P_{i_t}|$ by Lemma 1.88.

It follows then that $P_1 P_2 \cdots P_t$ is a subgroup of order $p_1^{\alpha_1} \cdots p_t^{\alpha_t} = |G|$, so $G = P_1 P_2 \cdots P_t$. For $1 \leq i \leq t$ we have $P_i \cap (P_1 \cdots P_{i-1} P_{i+1} \cdots P_t) = \{1\}$, since $P_1 \cdots P_{i-1} P_{i+1} \cdots P_t$ is a subgroup of order $|P_1| \cdots |P_{i-1}| \cdot |P_{i+1}| \cdots |P_t|$ which is coprime to $|P_i|$. It follows then from Lemma 5.5 that $G$ is the direct product of the subgroups $P_1, \ldots, P_t$.

(iii) $\Rightarrow$ (i): In this case $G$ is isomorphic to $P_1 \times \cdots \times P_t$, where $P_i$ is a finite $p_i$-group for some prime $p_i$. Since finite $p$-groups are nilpotent (Lemma 4.42), and since the direct product of nilpotent groups is nilpotent (Exercise 5.6), we conclude that $G$ is nilpotent. $\square$

For a finite group and a prime $p$, we define

$$O_p(G) := \bigcap_{P \in \mathrm{Syl}_p(G)} P,$$

the intersection of all Sylow $p$-subgroups of $G$. It is clear that $O_p(G) \operatorname{char} G$, and in particular $O_p(G) \trianglelefteq G$. Note also that since Sylow $p$-subgroups are conjugate, for any Sylow $p$-subgroup $P \leq G$ we have $O_p(G) = \cap_{g \in G} P^g$.

**Lemma 6.16.** *Let $G$ be a finite group and let $Q \trianglelefteq G$ be a $p$-group. Then $Q \leq O_p(G)$.*

*Proof.* By Theorem 6.6, there exists Sylow $p$-subgroup $P$ such that $Q \leq P$. Then for $g \in G$ we have $Q = Q^g \leq P^g$, so in fact $Q \leq P^g$ for all $g \in G$. Since Sylow $p$-subgroups are conjugate (Sylow II), we conclude that $Q$ is contained in every Sylow $p$-subgroup of $G$. In other words, $Q \leq O_p(G)$. $\square$

By Lemma 6.16, the subgroup $O_p(G)$ is the largest normal $p$-subgroup of $G$. That is:

- $O_p(G)$ is a $p$-group and $O_p(G) \trianglelefteq G$;
- If $Q$ is a $p$-group and $Q \trianglelefteq G$, then $Q \leq O_p(G)$.

**Lemma 6.17.** *Let $G$ be a finite group and let $p_1, \ldots, p_t$ be the prime divisors of $|G|$. Then $F(G)$ is the direct product of $O_{p_1}(G), \ldots, O_{p_t}(G)$.*

*Proof.* Since $F(G)$ is nilpotent, every Sylow subgroup of $F(G)$ is normal (Proposition 6.15). Let $P_i \trianglelefteq F(G)$ be a Sylow $p_i$-subgroup of $F(G)$. Since $P_i$ is the unique Sylow $p_i$-subgroup of $F(G)$, we have $P_i \operatorname{char} F(G) \trianglelefteq G$ and so $P_i \trianglelefteq G$. Thus $P_i \leq O_{p_i}(G)$. On the other hand $O_{p_i}(G)$ is a nilpotent normal subgroup of $G$, so $O_{p_i}(G) \leq F(G)$. Therefore $O_{p_i}(G) \leq P_i$, since $P_i$ is the unique Sylow $p_i$-subgroup of $G$. Thus $P_i = O_{p_i}(G)$.

We have shown that $O_{p_1}(G), \ldots, O_{p_t}(G)$ are the Sylow subgroups of $F(G)$, so the lemma follows from Proposition 6.15. $\square$

## 6.6 Groups of certain orders are solvable

A classical application of Sylow theorems are proofs of solvability of groups with certain orders. For example, we already now that any finite group of order $p^n$, where $p$ is a prime, must be solvable (Lemma 4.42). Burnside's theorem states that any group of order $p^n q^m$ ($p$, $q$ primes) is solvable. The easiest proof of this fact uses character theory, although later a purely group-theoretical proof was found (Goldschmidt, Bender, Matsuyama). We will give a proof in the special case where $m = 1$.

**Proposition 6.18.** *Let $p$ and $q$ be distinct primes and $n > 0$ an integer. Then any group of order $p^n q$ is solvable.*

*Proof.* Let $G$ be a finite group of order $p^n q$, where $p$ and $q$ are distinct primes and $n > 0$ is an integer. We will first prove that $G$ cannot be simple.

We have $n_p(G) \mid q$, so $n_p(G) = 1$ or $n_p(G) = q$. If $n_p(G) = 1$, then $G$ has a normal Sylow $p$-subgroup. Suppose then that $n_p(G) = q$, in which case $q \equiv 1 \mod p$. Among the $q$ Sylow $p$-subgroups, choose two $P_1$, $P_2$ such that the order of $D = P_1 \cap P_2$ is as large as possible.

We claim that $q$ divides $|N_G(D)|$. If this is not the case, then $N_G(D)$ is a $p$-group, so there exists a Sylow $p$-subgroup $R$ such that $N_G(D) \leq R$. On the other hand $D \lneqq P_1$ and normalizers grow in $p$-groups (Proposition 1.147), so $D \lneqq N_G(D) \cap P_1$. But now $N_G(D) \leq R$, so $D \lneqq R \cap P_1$, which contradicts the assumption that $|D|$ is as large as possible. Thus $q$ divides $|N_G(D)|$.

In particular, there exists a $q$-Sylow subgroup $Q \leq N_G(D)$. Now $Q$ acts on the Sylow $p$-subgroups by conjugation, and this action is faithful and transitive since by $n_p(G) = q$ we have $[G : N_G(P_1)] = q$ and thus $N_G(P_1) = P_1$. In other words, each Sylow $p$-subgroup is equal to $P_1^y$ for some $y \in Q$. On the other hand $D \leq P_1$, so $D = D^y \leq P_1^y$ since $Q \leq N_G(D)$. Therefore $D$ is contained in every Sylow $p$-subgroup of $G$. This implies that

$$D = \bigcap_{P \in \mathrm{Syl}_p(G)} P$$

and in particular $D \trianglelefteq G$.

If $D \neq \{1\}$, then $D$ is a nontrivial proper normal subgroup of $G$, so $G$ is not simple. Suppose then that $D = \{1\}$. Since we have assume that $D$ is the largest possible intersection of two Sylow $p$-subgroups of $G$, in this case $P \cap P' = \{1\}$ for any distinct Sylow $p$-subgroups of $G$. Thus there are a total of $(p^n - 1)q = |G| - q$ non-identity elements in the Sylow $p$-subgroups of $G$, and all of these elements have order divisible by $p$. This leaves space for at most $q$ elements among the Sylow $q$-subgroups of $G$, so there can be at most

one Sylow $q$-subgroup in $G$. Thus $n_q(G) = 1$, in which case $G$ has a normal subgroup of order $q$.

This completes the proof of the fact that $G$ cannot be simple. To prove that $G$ is solvable, we can proceed by induction on $n$. For $n = 1$ we already know that $G$ has a normal Sylow subgroup $N$ (Lemma 5.45). In this case $N$ and $G/N$ are both cyclic, so $G$ is solvable (Lemma 4.23). Suppose that $n > 1$, and let $N$ be a proper non-trivial normal subgroup of $G$. Then $N$ is either a $p$-group, a $q$-group, or a group of order $p^{n'}q$ with $n' < n$, so it is solvable by induction. Similarly $G/N$ is solvable by induction, so $G$ is solvable (Lemma 4.23). □

**Proposition 6.19.** *Let $G$ be a finite group order $p^2q^2$, where $p$ and $q$ are primes. Then $G$ is solvable.*

*Proof.* We already know that groups of order $p$, $q$, $p^2$, $q^2$, $pq$, $p^2q$, and $pq^2$ are solvable (Proposition 6.18, Lemma 4.42). Thus it will suffice to prove that $G$ is not simple.

We can assume that $n_p(G) > 1$, as otherwise $G$ has a normal Sylow $p$-subgroup. Then $n_p(G) = q$ or $n_p(G) = q^2$. In both cases $q^2 \equiv 1 \mod p$, so $p$ divides $q^2 - 1 = (q-1)(q+1)$. Since $p$ is a prime, we conclude that $p \mid q \pm 1$. We can also assume that $n_q(G) > 1$, and then similarly $q \mid p \pm 1$. It is then straightforward to see that we must have $q = p \pm 1$. For example if $p \mid q - 1$ and $q \mid p + 1$, then $p < q \leq p + 1$ which implies $q = p + 1$.

Suppose then without loss of generality that $q = p + 1$. Then either $p$ or $q$ must be even, so $p = 2$ and $q = 3$. In this case $|G| = 36 = 2^2 \cdot 3^2$. Let $P \leq G$ be a 3-Sylow subgroup of $G$. We have $[G : P] = 4$, so the action of left cosets of $P$ gives a homomorphism $\varphi : G \to S_4$ with $\operatorname{Ker}\varphi \leq P$ (Lemma 2.43). Since $S_4$ is not divisible by 9, we conclude that $3 \mid |\operatorname{Ker}\varphi|$, so $\operatorname{Ker}\varphi$ is a non-trivial proper normal subgroup of $G$. □

**Proposition 6.20.** *Let $G$ be a finite group of order $|G| = pqr$, where $p < q < r$ are primes. Then $G$ is solvable.*

*Proof.* We know that groups of order $p$, $q$, $r$, $pq$, $pr$, and $qr$ are solvable, so it will suffice to prove that $G$ is not simple.

To this end, we will prove that $G$ has a normal Sylow subgroup. If this is not the case, then $n_p(G), n_q(G), n_r(G) > 1$. Note that $n_p(G)$ divides $qr$, so $n_p(G) \geq q$. Similarly $n_q(G)$ divides $pr$ and $n_q(G) \equiv 1 \mod p$, so $n_q(G) = r$ or $n_q(G) = pr$; in particular $n_q(G) \geq r$. Finally $n_r(G)$ divides $pq$ and $n_r(G) \equiv 1 \mod r$, so $n_r(G) = pq$. We can now count elements of prime order in $G$:

- $n_p(G) \geq q$, so we have $\geq q(p-1)$ elements of order $p$;

- $n_q(G) \geq r$, so we have $\geq r(q-1)$ elements of order $q$;
- $n_r(G) = pq$, so we have $pq(r-1)$ elements of order $r$;

This gives us at least

$$pq(r-1) + r(q-1) + q(p-1) = pqr + rq - r - q > pqr$$

elements of prime order (since $rq > r+q$), contradicting $|G| = pqr$. Therefore there must be a normal Sylow subgroup. □

## 6.7 Fitting subgroup and normal Sylow subgroups

**Lemma 6.21.** *Let $G$ be a finite solvable group. Then $C_G(F(G)) \leq F(G)$. In other words, we have $C_G(F(G)) = Z(F(G))$.*

*Proof.* Denote $F = F(G)$ and $C = C_G(F)$. Suppose, for the sake of contradiction, that $C \not\leq F$. Consider $CF/F$, the image of $C$ in $G/F$. Then $CF/F$ is a non-trivial group, and it is solvable since $G$ is. Thus there exists $k > 0$ such that $(CF/F)^{(k)} = C^{(k)}F/F$ is nontrivial, but $(CF/F)^{(k+1)} = \{1\}$.

By $F \trianglelefteq G$ we have $C = C_G(F) \trianglelefteq G$. Furthermore $C^{(k)} \operatorname{char} C \trianglelefteq G$, so $C^{(k)} \trianglelefteq G$. Next we will prove that $C^{(k)}$ is nilpotent. To this end, first note that $[C^{(k)}, C^{(k)}] \leq F$ since $(CF/F)^{(k+1)} = C^{(k+1)}F/F$ is trivial. On the other hand $C^{(k)}$ centralizes $F$, so $[C^{(k)}, [C^{(k)}, C^{(k)}]] = \{1\}$ and $C^{(k)}$ is nilpotent of class $\leq 2$.

We have shown that $C^{(k)}$ is a nilpotent normal subgroup of $G$, which implies that $C^{(k)} \leq F$. But this is a contradiction, since $(CF/F)^{(k)} = C^{(k)}F/F$ is nontrivial. Therefore we must have $C \leq F$, which implies $C = Z(F)$. □

Suppose that $G$ is a finite solvable group, so then $C_G(F(G)) = Z(F(G))$ by Lemma 6.21. Since $F(G) \trianglelefteq G$, we have a map $\pi : G \to \operatorname{Aut}(F(G))$, with $\operatorname{Ker} \pi = C_G(F(G)) = Z(F(G))$ (from the conjugation action, see Theorem 5.32). By the first isomorphism theorem, the quotient $G/Z(F(G))$ is isomorphic to a subgroup of $\operatorname{Aut}(F(G))$. Thus $G$ can be seen as a extension of two groups related to $F(G)$:

- There is a normal subgroup $N \trianglelefteq G$, the center of $F(G)$.
- The quotient $G/N$ is isomorphic to a subgroup of $\operatorname{Aut}(F(G))$.

Conceptually, the point of this is that to a large extent the structure of a finite solvable group $G$ is controlled by its Fitting subgroup $F(G)$, since $G$ is an extension of $Z(F(G))$ and a subgroup of $\operatorname{Aut}(F(G))$.

We will mostly apply this in the case where $F(G)$ is abelian: in this case, by Lemma 6.21 the quotient $G/F(G)$ is isomorphic to a subgroup of $\mathrm{Aut}(F(G))$.

**Lemma 6.22.** *Let $G$ be a finite group of order $|G| = p^2q$, where $p$ and $q$ are distinct primes. Then $G$ has a normal Sylow subgroup.*

*Proof.* We know that $G$ is solvable (Proposition 6.18), so $F(G) \neq \{1\}$.

If $q \mid |F(G)|$, then being nilpotent, $F(G)$ has a normal Sylow $q$-subgroup $Q$. Then $Q \operatorname{char} F(G) \trianglelefteq G$ and thus $Q \trianglelefteq G$.

We can assume then that $q \nmid |F(G)|$, so $|F(G)| = p$ or $|F(G)| = p^2$. If $|F(G)| = p$, then $F(G) \cong C_p$ and by Lemma 6.21 the quotient $G/F(G)$ embeds into $\mathrm{Aut}(C_p) \cong C_{p-1}$, which is absurd since $|G/F(G)| = pq > p - 1$. Therefore $|F(G)| = p^2$, in which case $F(G)$ is a normal Sylow $p$-subgroup of $G$. □

**Lemma 6.23.** *Let $G$ be a finite group of order $|G| = p^2q^2$, where $p$ and $q$ are distinct primes. Then $G$ has a normal Sylow subgroup.*

*Proof.* We know that $G$ is solvable (Proposition 6.19), so $F(G) \neq \{1\}$.

If $p^2 \mid |F(G)|$, then as a nilpotent group $F(G)$ has a normal Sylow $p$-subgroup $P$ of order $p^2$. Since $P \operatorname{char} F(G) \trianglelefteq G$, we have $P \trianglelefteq G$. Similarly if $q^2 \mid |F(G)|$, we see that a normal Sylow $q$-subgroup of $F(G)$ is a normal Sylow $q$-subgroup of $G$.

Thus we may assume that $p^2$ and $q^2$ do not divide $|F(G)|$. Since $F(G) \neq \{1\}$, the possibilities are $|F(G)| = p$, $|F(G)| = q$, and $|F(G)| = pq$. In all of these cases $F(G)$ must be cyclic (since it is nilpotent), so by Lemma 6.21 the quotient $G/F(G)$ embeds into $\mathrm{Aut}(F(G))$.

If $|F(G)| = p$, then $G/F(G)$ is a group of order $pq^2$ that embeds into $\mathrm{Aut}(F(G)) \cong \mathrm{Aut}(C_p) \cong C_{p-1}$, which is impossible. For a similar reason $|F(G)| = q$ is impossible.

The only remaining case is $|F(G)| = pq$. In this case $F(G)$ is a nilpotent group of order $pq$, so $F(G) \cong C_p \times C_q$. Then $\mathrm{Aut}(F(G)) \cong \mathrm{Aut}(C_p) \times \mathrm{Aut}(C_q) \cong C_{p-1} \times C_{q-1}$. Now $G/F(G)$ is a group of order $pq$ that embeds into $\mathrm{Aut}(F(G))$, so this is a contradiction since $pq > (p-1)(q-1)$. □

**Lemma 6.24.** *Let $G$ be a finite group of order $|G| = p^3q$, where $p$ and $q$ are distinct primes. Then $G$ has a normal Sylow subgroup, except when $p = 2$, $q = 3$, and $G \cong S_4$.*

*Proof.* We know that $G$ is solvable (Proposition 6.18), so $F(G) \neq \{1\}$.

If $q \mid |F(G)|$, then as a nilpotent group $F(G)$ has a normal Sylow $q$-subgroup $Q$ of order $q$. Since $Q \operatorname{char} F(G) \trianglelefteq G$, we have $Q \trianglelefteq G$. Similarly

if $p^3 \mid |F(G)|$, we see that a normal Sylow $p$-subgroup of $F(G)$ is a normal Sylow $p$-subgroup of $G$.

Therefore we can assume that $q$ and $p^3$ do not divide $|F(G)|$, in which case $|F(G)| = p$ or $|F(G)| = p^2$. In both cases $F(G)$ is abelian, so by Lemma 6.21 the quotient $G/F(G)$ embeds into $\mathrm{Aut}(F(G))$.

If $|F(G)| = p$, then $G/F(G)$ is a group of order $p^2q$ that embeds into $\mathrm{Aut}(F(G)) \cong \mathrm{Aut}(C_p) \cong C_{p-1}$, which is impossible.

Therefore we must have $|F(G)| = p^2$, and in this case $F(G) \cong C_{p^2}$ or $F(G) \cong C_p \times C_p$. Suppose first that $F(G) \cong C_{p^2}$. Then $G/F(G)$ embeds into

$$\mathrm{Aut}(F(G)) \cong \mathrm{Aut}(C_{p^2}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times \cong C_{p(p-1)}.$$

In particular $G/F(G)$ is abelian of order $pq$, so it has a normal subgroup $N/F(G) \trianglelefteq G/F(G)$ of order $p$. Then $N \trianglelefteq G$ is a normal subgroup of order $p^3$, which is not possible when $|F(G)| = p^2$.

Therefore $F(G) \cong C_p \times C_p$. In this case $G/F(G)$ embeds into $\mathrm{Aut}(C_p \times C_p) \cong \mathrm{GL}_2(p)$. We have

$$\begin{aligned} |G/F(G)| &= pq \\ |\,\mathrm{GL}_2(p)| &= (p-1)^2 p(p+1) \end{aligned}$$

so $pq$ divides $(p-1)^2p(p+1)$, which implies $q \mid p \pm 1$. On the other hand, since $G$ does not have a normal Sylow $p$-subgroup, we have $n_p(G) > 1$. By Sylow III this implies $n_p(G) = q$ and $q \equiv 1 \mod p$, so $p \mid q - 1$. Then $p < q \leq p \pm 1$, so it follows that $q = p + 1$. Then either $p$ or $q$ is even, so we must have $p = 2$ and $q = 3$.

Thus we have $|G| = 24 = 2^3 \cdot 3$, with $F(G) \cong C_2 \times C_2$. Since $n_3(G) > 1$, it follows from Sylow III that $n_3(G) = 4$. Then for a 3-Sylow subgroup $Q$, we have $[G : N_G(Q)] = 4$, so $N_G(Q)$ is a group of order 6. We consider the action of $G$ of the Sylow 3-subgroups by conjugation, which gives a homomorphism (Lemma 2.43)

$$\varphi : G \to S_4$$

with

$$\mathrm{Ker}\,\varphi = \bigcap_{g \in G} N_G(Q)^g.$$

Since $K = \mathrm{Ker}\,\varphi$ is a proper subgroup of $N_G(Q)$, it must have order 1, 2, or 3. The order of $K$ cannot be 3, since there is no normal Sylow 3-subgroup in $G$.

We consider the possibility that $|K| = 2$. In this case $G/K$ is a group of order $12 = 2^2 \cdot 3$, so by Lemma 6.22 it has a normal Sylow 2-subgroup or a normal Sylow 3-subgroup. If there exists a normal subgroup $N/K \trianglelefteq G/K$

of order $2^2 = 4$, then $N \trianglelefteq G$ is a normal subgroup of order $2^3$, which is not possible when $F(G) \cong C_2 \times C_2$. The other possibility is that there exists a normal subgroup $N/K \trianglelefteq G/K$ of order 3, in which case $N \trianglelefteq G$ is a normal subgroup of order $2 \cdot 3 = 6$. We know that any group of order 6 has a normal Sylow 3-subgroup, so there exists a unique subgroup $Q \trianglelefteq N$ of order 3. Then $Q \operatorname{char} N \trianglelefteq G$ implies that $Q \trianglelefteq G$, again impossible when $F(G) \cong C_2 \times C_2$.

Thus $|K| = 2$ is not possible, and we must have $|K| = 1$. In other words, the homomorphism $\varphi : G \to S_4$ is injective, and since $|G| = 24 = |S_4|$ it must be an isomorphism. Hence $G \cong S_4$. □

## 6.8 Groups of order $p^2q$ ($p$ and $q$ distinct primes)

Let $p$ and $q$ be distinct primes. We consider the classification of groups of order $p^2q$. As a first step, let $G$ be a finite group of order $|G| = p^2q$, with a Sylow $p$-subgroup $P \leq G$ and a Sylow $q$-subgroup $Q \leq G$. By Lemma 6.22, we know that $G$ has a normal Sylow subgroup, so either $P$ or $Q$ is a normal subgroup. Since $P \cap Q = \{1\}$, we have $|PQ| = |P||Q| = |G|$, so $G = PQ$ and $G$ is a semidirect product of $P$ and $Q$ (or of $Q$ and $P$).

If both $P$ and $Q$ are normal, then $G$ is the direct product of $P$ and $Q$ thus isomorphic to one of the following groups:

$$C_{p^2} \times C_q$$
$$C_p \times C_p \times C_q.$$

It remains to consider the case where $G$ is a nontrivial semidirect product. In this case, we know (Theorem 5.40) that $G$ is isomorphic to a nontrivial semidirect product of one of the following forms:

$$C_{p^2} \rtimes_\psi C_q,$$
$$(C_p \times C_p) \rtimes_\psi C_q,$$
$$C_q \rtimes_\psi C_{p^2},$$
$$C_q \rtimes_\psi (C_p \times C_p).$$

We begin with the following proposition, which is similar to Theorem 5.62.

**Proposition 6.25.** *Let $K = \langle x \rangle$ be a finite cyclic group, and let $H$ be a finite abelian group. Let $\psi, \psi' : K \to \operatorname{Aut}(H)$ be homomorphisms. Suppose that $\gcd(|H|, |K|) = 1$. Then the following statements are equivalent:*

(i) $H \rtimes_\psi K \cong H \rtimes_{\psi'} K$.

(ii) *There exists* $\varphi \in \mathrm{Aut}(K)$ *such that* $\psi(\varphi(x))$ *is conjugate to* $\psi'(x)$ *in* $\mathrm{Aut}(H)$.

*Proof.* (i) $\Rightarrow$ (ii): Suppose that there exists an isomorphism $\sigma : H \rtimes_\psi K \to H \rtimes_{\psi'} K$. Since $\gcd(|H|, |K|) = 1$, by Lemma 5.60 in both groups $H \rtimes_\psi K$ and $H \rtimes_{\psi'} K$ the subgroup $H$ is the unique subgroup of order $|H|$. Therefore $\sigma(H) = H$, so the restriction $\pi = \sigma_{|H} : H \to H$ is an automorphism of $H$.

The image $\sigma(x)$ can be written in the form $hk$ with $h \in H$ and $k \in K$, say $\sigma(x) = h_0 x^d$ with $h_0 \in H$ and $d \in \mathbb{Z}$. We have a surjective homomorphism $\tau : H \rtimes_{\psi'} K \to K$ defined by $hk \mapsto k$ for all $h \in H$ and $k \in K$. Then $\tau\sigma$ must be also surjective, so $\tau\sigma(x) = x^d$ must be a generator of $K$. Therefore $\gcd(d, |K|) = 1$, and the map $\psi_d : K \to K$ defined by $x \mapsto x^d$ is an automorphism of $K$ (Lemma 5.27). Thus $\sigma(x) = h_0\psi_d(x)$.

We now consider the action of $x$ on $H$. Let $h \in H$. Then

$$\sigma(xhx^{-1}) = \sigma(\psi(x)(h)) = (\pi \circ \psi(x))(h).$$

Using the fact that $\sigma$ is a homomorphism and $H$ is abelian, we have

$$\begin{aligned}
\sigma(xhx^{-1}) &= \sigma(x)\sigma(h)\sigma(x)^{-1} && \text{(since } \sigma \text{ is a homomorphism)} \\
&= h_0 x^d \pi(h) x^{-d} h_0^{-1} \\
&= h_0 \cdot \psi'(x^d)(\pi(h)) \cdot h_0^{-1} \\
&= \psi'(x^d)(\pi(h)) && \text{(since } H \text{ is abelian)} \\
&= (\psi'\psi_d(x))(\pi(h)).
\end{aligned}$$

Therefore we conclude that

$$(\pi \circ \psi(x))(h) = (\psi'(\psi_d(x)) \circ \pi)(h)$$

for all $h \in H$. Thus $\pi \circ \psi(x) = \psi'(\psi_d(x)) \circ \pi$, so $\pi\psi(x)\pi^{-1} = \psi'\psi_d(x)$.

Hence $\psi(x)$ and $\psi'\psi_d(x)$ are conjugate in $\mathrm{Aut}(H)$, so (ii) holds with $\varphi = \psi_d^{-1}$.

(ii) $\Rightarrow$ (i): Suppose that there exists $\varphi \in \mathrm{Aut}(K)$ such that $\psi(\varphi(x))$ and $\psi'(x)$ are conjugate in $\mathrm{Aut}(H)$. Then there exists $\pi \in \mathrm{Aut}(H)$ such that $\pi\psi(\varphi(x))\pi^{-1} = \psi'(x)$. For all $k \in \mathbb{Z}$, we have

$$\begin{aligned}
\psi'(x^k) &= \psi'(x)^k \\
&= (\pi\psi(\varphi(x))\pi^{-1})^k \\
&= \pi(\psi(\varphi(x))^k\pi^{-1} \\
&= \pi(\psi(\varphi(x^k))\pi^{-1}
\end{aligned}$$

since $\psi$ and $\varphi$ are homomorphisms. Thus $\pi\psi(\varphi(y))\pi^{-1} = \psi'(y)$ for all $y \in K$, so it follows from Lemma 5.43 (ii) that $H \rtimes_{\psi'} K \cong H \rtimes_{\psi\varphi} K$. By Lemma 5.43 (i) we have $H \rtimes_{\psi\varphi} K \cong H \rtimes_{\psi} K$, so we conclude that $H \rtimes_{\psi} K \cong H \rtimes_{\psi'} K$. □

For the classification of groups of order $p^2q$, we will begin with the cases where the normal Sylow subgroup is cyclic.

**Lemma 6.26.** *Let $p$ and $q$ be distinct primes. Let $N$ be the number of nontrivial semidirect products $C_q \rtimes_\psi (C_p \times C_p)$, up to isomorphism. Then:*

(i) $N = 0$, *if* $p \nmid q - 1$.

(ii) $N = 1$, *if* $p \mid q - 1$.

*Proof.* If $p \nmid q - 1$, then there are no elements of order $p$ in $\mathrm{Aut}(C_q) \cong C_{q-1}$, and thus every homomorphism $\psi : C_p \times C_p \to C_q$ is trivial. This proves (i).

For (ii), suppose that $p \mid q - 1$. Let $\psi, \psi' : C_p \times C_p \to \mathrm{Aut}(C_q)$ be nontrivial homomorphisms. Since $\mathrm{Aut}(C_q) \cong C_{q-1}$ is cyclic, the images $\operatorname{Im}\psi$ and $\operatorname{Im}\psi'$ must be cyclic of order $p$. In fact $\operatorname{Im}\psi = \operatorname{Im}\psi'$, since $C_{q-1}$ has a unique subgroup of order $p$.

By the first isomorphism theorem $\operatorname{Ker}\psi = \langle x \rangle$ and $\operatorname{Ker}\psi' = \langle x' \rangle$ are cyclic of order $p$. Considering $C_p \times C_p$ as a vector space over $\mathbb{F}_p$, we can extend to a basis $\{x, y\}$ of $C_p \times C_p$ by choosing any $y \notin \langle x \rangle$. In this case $\operatorname{Im}\psi = \langle \psi(y) \rangle$.

Since $\operatorname{Im}\psi = \operatorname{Im}\psi'$, we can find $y' \in C_p \times C_p$ such that $\psi'(y') = \psi(y)$. Then $y' \notin \langle x' \rangle$, so $\{x', y'\}$ is another basis of $C_p \times C_p$ as a vector space over $\mathbb{F}_p$.

We can now define a linear map $\varphi : C_p \times C_p \to C_p \times C_p$ by $\varphi(x') = x$ and $\varphi(y') = y$. Since $\varphi$ maps basis to a basis, it is an isomorphism of vector spaces, and thus $\varphi \in \mathrm{Aut}(C_p \times C_p)$. Then we have $\psi\varphi = \psi'$. Indeed,

$$\psi\varphi(x') = \psi(x) = 1 = \psi'(x')$$
$$\psi\varphi(y') = \psi(y) = \psi'(y')$$

and thus $\psi\varphi(g) = \psi'(g)$ for all $g \in C_p \times C_p$, since this holds for $g$ in the basis $\{x', y'\}$.

Since $\psi\varphi = \psi'$, it follows from Lemma 5.43 (ii) that $C_q \rtimes_\psi (C_p \times C_p) \cong C_q \rtimes_{\psi'} (C_p \times C_p)$. We have shown that there is at most one nontrivial semidirect product $C_q \rtimes (C_p \times C_p)$, up to isomorphism. To finish the proof of (ii), it remains to check that there exists at least one non-trivial homomorphism $\psi : C_p \times C_p \to \mathrm{Aut}(C_q)$. For this, take $\{x, y\}$ a basis of $C_p \times C_p$ and define $\psi(x) = I$ (identity) and $\psi(y) = \sigma$, where $\sigma \in \mathrm{Aut}(C_q)$ is an automorphism of order $p$. (Such an automorphism exists since $p \mid q - 1$ and $\mathrm{Aut}(C_q) \cong C_{q-1}$.) Then $\psi$ defines a non-trivial homomorphism $C_p \times C_p \to \mathrm{Aut}(C_q)$. □

**Remark 6.27.** Alternatively, one can prove Lemma 6.26 by showing that any semidirect product $C_q \rtimes_\psi (C_p \times C_p)$ is isomorphic to $(C_q \rtimes_{\psi'} C_p) \times C_p$ for some homomorphism $\psi' : C_p \to \mathrm{Aut}(C_q)$. Then the result follows from Theorem 5.48.

**Lemma 6.28.** *Let $p$ and $q$ be distinct primes. Let $N$ be the number of nontrivial semidirect products $C_q \rtimes_\psi C_{p^2}$, up to isomorphism. Then:*

(i) $N = 0$, *if* $p \nmid q - 1$.

(ii) $N = 1$, *if* $p \mid q - 1$ *and* $p^2 \nmid q - 1$.

(iii) $N = 2$, *if* $p^2 \mid q - 1$.

*Proof.* Let $C_{p^2} = \langle x \rangle$. Let $\psi, \psi' : C_{p^2} \to \mathrm{Aut}(C_q)$ be homomorphisms. By Proposition 6.25, we know that $C_q \rtimes_\psi C_{p^2} \cong C_q \rtimes_{\psi'} C_{p^2}$ if and only if there exists $\varphi \in \mathrm{Aut}(C_{p^2})$ such that $\psi(\varphi(x))$ and $\psi'(x)$ are conjugate in $\mathrm{Aut}(C_q)$.

On the other hand we know that $\mathrm{Aut}(C_q) \cong (\mathbb{Z}/q\mathbb{Z})^\times \cong C_{q-1}$ is cyclic, so $C_q \rtimes_\psi C_{p^2} \cong C_q \rtimes_{\psi'} C_{p^2}$ if and only if there exists $\varphi \in \mathrm{Aut}(C_{p^2})$ such that $\psi(\varphi(x)) = \psi'(x)$. We will show that this is equivalent to $\langle \psi(x) \rangle = \langle \psi'(x) \rangle$.

To this end, first note that automorphisms $\varphi \in \mathrm{Aut}(C_{p^2})$ are maps defined by $\varphi_d : x \mapsto x^d$, where $\gcd(d, p) = 1$. Thus if $\psi(\varphi_d(x)) = \psi'(x)$, then $\psi(x)^d = \psi'(x)$. Since $\gcd(d, p) = 1$, we have $\langle \psi(x) \rangle = \langle \psi'(x) \rangle$. Conversely, suppose that $\langle \psi(x) \rangle = \langle \psi'(x) \rangle$. The image $\psi(x)$ must have order dividing $p^2$. Thus since $\psi'(x)$ generates $\langle \psi(x) \rangle$, by Lemma 1.46 we have $\psi'(x) = \psi(x)^d = \psi(x^d)$ for some $d \in \mathbb{Z}$ with $\gcd(d, p) = 1$. Therefore $\psi(\varphi_d(x)) = \psi'(x)$.

We have shown that $C_q \rtimes_\psi C_{p^2} \cong C_q \rtimes_{\psi'} C_{p^2}$ if and only if $\langle \psi(x) \rangle = \langle \psi'(x) \rangle$. Since $\mathrm{Aut}(C_q)$ is cyclic $q - 1$, it has a unique subgroup of each order dividing $q - 1$. Thus $\langle \psi(x) \rangle = \langle \psi'(x) \rangle$ if and only if $|\psi(x)| = |\psi'(x)|$. Since $x$ has order $p^2$, the possible orders for $|\psi(x)|$ are 1, $p$, and $p^2$. We can now easily finish the proof:

(i): If $p \nmid q-1$, then there are no elements of order $p$ or $p^2$ in $\mathrm{Aut}(C_q) \cong C_{q-1}$. Thus the only possibility is $\psi(x) = 1$, in which case $\psi$ is trivial.

(ii): If $p \mid q - 1$ and $p^2 \nmid q - 1$, then there is $\sigma \in \mathrm{Aut}(C_q)$ with $|\sigma| = p$, but no element of order $p^2$. We can define a homomorphism $\psi : C_{p^2} \to \mathrm{Aut}(C_q)$ by $\psi(x) = \sigma$, in which case $|\psi(x)| = p$. Thus there is exactly one non-trivial semidirect product.

(iii): If $p^2 \mid q - 1$, there is $\sigma \in \mathrm{Aut}(C_q)$ with $|\sigma| = p^2$. We can define homomorphisms $\psi, \psi' : C_{p^2} \to \mathrm{Aut}(C_q)$ with $\psi(x) = \sigma$ and $\psi'(x) = \sigma^p$.

Then $|\psi(x)| = p^2$ and $|\psi'(x)| = p$. Thus there are exactly two non-trivial semidirect products. □

**Lemma 6.29.** *Let $p$ and $q$ be distinct primes. Let $N$ be the number of nontrivial semidirect products $C_{p^2} \rtimes_\psi C_q$, up to isomorphism. Then:*

(i) $N = 0$, *if* $q \nmid p - 1$.

(ii) $N = 1$, *if* $q \mid p - 1$.

*Proof.* Let $C_q = \langle x \rangle$. Note that $\mathrm{Aut}(C_{p^2}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times \cong C_{p(p-1)}$ for all primes $p$. Thus by applying Proposition 6.25 and arguing exactly as in the proof of Lemma 6.28, we see that $C_{p^2} \rtimes_\psi C_q \cong C_{p^2} \rtimes_{\psi'} C_q$ if and only $|\psi(x)| = |\psi'(x)|$.

Now the order of $|\psi(x)|$ is 1 or $q$, so any two non-trivial semidirect products $C_{p^2} \rtimes_\psi C_q$ must be isomorphic.

If $q \nmid p - 1$, there is no element of order $q$ in $\mathrm{Aut}(C_{p^2}) \cong C_{p(p-1)}$. Thus if $q \nmid p - 1$, any homomorphism $\psi : C_q \to \mathrm{Aut}(C_{p^2})$ is trivial, and so (i) holds.

If $q \mid p - 1$, then there exists an element $\sigma \in \mathrm{Aut}(C_{p^2})$ of order $q$. Then we can define a non-trivial homomorphism $\psi : C_q \to \mathrm{Aut}(C_{p^2})$ by $\psi(x) = \sigma$. Thus (ii) holds in this case. □

With Lemma 6.26, Lemma 6.28, and Lemma 6.29, what remains is to consider semidirect products of the form $(C_p \times C_p) \rtimes_\psi C_q$. Here $\mathrm{Aut}(C_p \times C_p) \cong \mathrm{GL}_2(p)$, and for the classification we will need a few more facts about the structure of $\mathrm{GL}_2(p)$.

**Lemma 6.30.** *Let $p$ be a prime. Then there exists an element of order $p+1$ in $\mathrm{GL}_2(p)$.*

*Proof.* Let $\mathbb{K} = \mathbb{F}_{p^2}$ be a finite field of order $p^2$. As a vector space over $\mathbb{F}_p$, we have $\dim \mathbb{K} = 2$ (see Section 3.1). We know that the multiplicative group of a finite field is cyclic, so $\mathbb{K}^\times \cong C_{p^2-1}$. Now $p+1$ divides $p^2 - 1 = (p-1)(p+1)$, so there exists an element $\varepsilon \in \mathbb{K}^\times$ of order $p + 1$.

Define a map $\varphi : \mathbb{K} \to \mathbb{K}$ by $\varphi(x) = \varepsilon x$ for all $x \in \mathbb{K}$. It is clear that $\varphi$ is an $\mathbb{F}_p$-linear map, and $\varphi$ is a bijection since it has an inverse defined by $x \mapsto \varepsilon^{-1} x$. In other words, we have $\varphi \in \mathrm{GL}(\mathbb{K})$, where again $\mathbb{K}$ is considered as a 2-dimensional vector space over $\mathbb{F}_p$. Since $\varepsilon$ has order $p + 1$ in $\mathbb{K}^\times$, it is easy to see that $|\varphi| = p + 1$.

Thus we have shown that $\mathrm{GL}(\mathbb{K})$ contains an element of order $p + 1$. The lemma follows, since $\mathbb{K}$ has dimension 2 over $\mathbb{F}_p$ and hence $\mathrm{GL}(\mathbb{K}) \cong \mathrm{GL}_2(p)$. □

**Lemma 6.31.** *Let $p$ be a prime, and let $q$ be an odd prime dividing $p+1$. Then Sylow $q$-subgroups of $\mathrm{GL}_2(p)$ are cyclic.*

*Proof.* Note that $|\mathrm{GL}_2(p)| = (p-1)^2p(p+1)$. Let $q^k$ be the largest power of $q$ dividing $|\mathrm{GL}_2(p)|$. We have $\gcd(p-1, p+1) = 2$, so since $q$ is odd and $q \mid p+1$, the largest power of $q$ dividing $|\mathrm{GL}_2(p)|$ is the largest power of $q$ dividing $p+1$. In other words, $q^k$ divides $p+1$.

By Lemma 6.30, there exists $x \in \mathrm{GL}_2(p)$ with $|x| = p+1$. Then $y = x^{(p+1)/q^k}$ has order $|y| = q^k$, so $\langle y \rangle$ is a Sylow $q$-subgroup of $\mathrm{GL}_2(p)$. Since Sylow $q$-subgroups are conjugate, we conclude that every Sylow $q$-subgroup of $\mathrm{GL}_2(p)$ is cyclic. □

**Theorem 6.32.** *Let $p$ and $q$ be distinct primes. Let $N$ be the number of nontrivial semidirect products $(C_p \times C_p) \rtimes_\psi C_q$, up to isomorphism. Then:*

(i) $N = 2$, *if* $q = 2$.

(ii) $N = 1$, *if* $q > 2$ *and* $q \mid p+1$.

(iii) $N = \frac{q+3}{2}$, *if* $q > 2$ *and* $q \mid p-1$.

(iv) $N = 0$, *if* $q > 2$ *and* $q \nmid p \pm 1$.

*Proof.* First we note that if $q = 2$, the result follows from Example 5.65, which shows that there are exactly 2 nontrivial semidirect products of the form $(C_p \times C_p) \rtimes_\psi C_2$, up to isomorphism. We will assume then for the result of the proof that $q > 2$.

Now $\mathrm{Aut}(C_p \times C_p) \cong \mathrm{GL}_2(p)$, and $|\mathrm{GL}_2(p)| = (p-1)^2p(p+1)$. Therefore if $q \nmid p \pm 1$, there is no element of order $q$ in $\mathrm{GL}_2(p)$, and so every homomorphism $\psi : C_q \to \mathrm{Aut}(C_p \times C_p)$ is trivial; as claimed by (iv). Thus we can assume that $q \mid p \pm 1$.

Let $C_q = \langle x \rangle$. We consider the two possibilities in turn.

*Case 1: $q \mid p+1$.*
By Cauchy's theorem there exists an element of order $q$ in $\mathrm{Aut}(C_p \times C_p)$, so there is a nontrivial homomorphism $C_q \to \mathrm{Aut}(C_p \times C_p)$. We will show next that any two nontrivial semidirect products of the form $(C_p \times C_p) \rtimes_\psi C_q$ are isomorphic, as claimed by (ii).

To this end, let $\psi, \psi' : C_q \to \mathrm{Aut}(C_p \times C_p)$ be non-trivial homomorphisms, so $\psi(x)$ and $\psi'(x)$ are automorphisms of order $q$. By Lemma 6.31, the Sylow $q$-subgroups of $\mathrm{Aut}(C_p \times C_p) \cong \mathrm{GL}_2(p)$ are cyclic. In particular each Sylow $q$-subgroup of $\mathrm{GL}_2(p)$ has a unique subgroup of order $q$, so by conjugacy of Sylow $q$-subgroups we conclude that any two subgroups of order $q$ in $\mathrm{GL}_2(p)$

are conjugate (Exercise 6.7). Therefore, there exists $\pi \in \mathrm{Aut}(C_p \times C_p)$ such that $\pi\langle\psi(x)\rangle\pi^{-1} = \langle\psi'(x)\rangle$.

Then $\pi\psi(x)\pi^{-1}$ is a generator for $\langle\psi'(x)\rangle$, so there exists $d \in \mathbb{Z}$ such that $\gcd(d, q) = 1$ and $\psi'(x) = (\pi\psi(x)\pi^{-1})^d = \pi\psi(x^d)\pi^{-1}$. Now $\psi_d : C_q \to C_q$ defined by $x \mapsto x^d$ is an automorphism of $C_q$, and we have shown that $\psi\psi_d(x)$ and $\psi'(x)$ are conjugate in $\mathrm{Aut}(C_p \times C_p)$. It follows therefore from Proposition 6.25 that $(C_p \times C_p) \rtimes_\psi C_q \cong (C_p \times C_p) \rtimes_{\psi'} C_q$.

*Case 2:* $q \mid p - 1$.
First note that in this case we have $p > 2$. We consider $C_p \times C_p$ as a vector space over $\mathbb{F}_p$, and fix a basis $\{v, w\}$ of $C_p \times C_p$. Then we can identify $\mathrm{Aut}(C_p \times C_p) = \mathrm{GL}_2(p)$, with a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

denoting the automorphism

$$v \mapsto v^a w^b$$
$$w \mapsto v^c w^d$$

of $C_p \times C_p$.

Since $q \mid p-1$, there exists an element $\mu \in \mathbb{F}_p^\times$ of order $q$. (In other words, we can find an integer $\mu$ such that $\mu \not\equiv 1 \mod p$ and $\mu^q \equiv 1 \mod p$.) Then $\langle\mu\rangle$ is a subgroup of order $q$ in $\mathbb{F}_p^\times$ and each of its elements is a root of the polynomial $t^q - 1 \in \mathbb{F}_p[t]$. Thus $t^q - 1$ splits into linear factors

$$t^q - 1 = (t - 1)(t - \mu) \cdots (t - \mu^{q-1}).$$

Thus if $g \in \mathrm{GL}_2(p)$ has order $q$, then $g^q - 1 = 0$ and so the minimal polynomial of $g$ divides $t^q - 1$. In this case either $g$ is a scalar matrix of the form $\mu^k I_2$, or it has a minimal polynomial $(t-\mu^i)(t-\mu^j)$ with $\mu^i \neq \mu^j$ (note that $t^q - 1$ has no repeated roots). In any case, it follows that $g$ is conjugate to a diagonal matrix of the form

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$$

with $\alpha^q = \beta^q = 1$. By conjugating $g$ with the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

(which correponds to change of basis from $\{v, w\}$ into $\{w, v\}$), we may assume that $\alpha \neq 1$.

Consider a non-trivial homomorphism $\psi : C_q \to \mathrm{GL}_2(p)$. Then $\psi(x)$ is an element of order $q$ in $\mathrm{GL}_2(p)$. It follows from the discussion in the previous paragraph that there exists a $\pi \in \mathrm{GL}_2(p)$ such that

$$\pi\psi(x)\pi^{-1} = \begin{pmatrix} \mu^a & 0 \\ 0 & \mu^b \end{pmatrix}$$

for some $a, b \in \mathbb{Z}$ with $\mu^a \neq 1$. Now $\mu^a$ has order $q$ in $\mathbb{F}_p^\times$, so it generates $\langle \mu \rangle$ and there exists $d \in \mathbb{Z}$ with $\gcd(d, q) = 1$ such that $\mu^{ad} = \mu$. Then $\varphi : C_q \to C_q$, $x \mapsto x^d$ defines an automorphism of $C_q$, and

$$\pi\psi(\varphi(x))\pi^{-1} = (\pi\psi(x)\pi^{-1})^d = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{bd} \end{pmatrix}.$$

It follows then from Proposition 6.25 that $(C_p \times C_p) \rtimes_\psi C_q \cong (C_p \times C_p) \rtimes_{\psi'} C_q$, where $\psi' : C_q \to \mathrm{GL}_2(p)$ is the homomorphism defined by

$$\psi'(x) = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{bd} \end{pmatrix}.$$

Next, for $0 \leq t \leq q-1$, we define $G_t = (C_p \times C_p) \rtimes_{\psi_t} C_q$, where $\psi_t : C_q \to \mathrm{GL}_2(p)$ is the homomorphism defined by

$$\psi'(x) = \begin{pmatrix} \mu & 0 \\ 0 & \mu^{t} \end{pmatrix}.$$

So far we have proven that any nontrivial semidirect product $(C_p \times C_p) \rtimes_\psi C_q$ is isomorphic to one of the groups

$$G_0, G_1, \ldots, G_{q-1}.$$

Next we will use Proposition 6.25 to determine the isomorphisms between these groups. We will prove the following:

*Claim: $G_t \cong G_s$ if and only if $t = s$, or $ts \equiv 1 \mod q$.*
By Proposition 6.25, we have $G_t \cong G_s$ if and only if there exists $\varphi \in \mathrm{Aut}(C_q)$ such that $\psi_t(\varphi(x))$ and $\psi_s(x)$ are conjugate in $\mathrm{GL}_2(p)$. Any such $\varphi$ is of the form $\varphi = \varphi_d : C_q \to C_q$, $x \mapsto x^d$ for some $d \in \mathbb{Z}$ with $\gcd(d, q) = 1$.

Thus for $0 \leq t, s \leq q-1$, we have $G_t \cong G_s$ if and only if there exists $d \in \mathbb{Z}$ with $\gcd(d, q) = 1$ such that the matrices

$$\begin{pmatrix} \mu^d & 0 \\ 0 & \mu^{td} \end{pmatrix} \text{ and } \begin{pmatrix} \mu & 0 \\ 0 & \mu^{s} \end{pmatrix}$$

are conjugate in $\mathrm{GL}_2(p)$. Two diagonal matrices are conjugate if and only if they have the same diagonal entries, so these two matrices are conjugate if and only if one of the following holds:

- $\mu^d = \mu$ and $\mu^{td} = \mu^s$, in which case $\mu^s = (\mu^d)^t = \mu^t$.
- $\mu^d = \mu^s$ and $\mu^{td} = \mu$, in which case $\mu^{ts} = (\mu^s)^t = (\mu^d)^t = \mu$.

In the first case $\mu^s = \mu^t$ implies $t \equiv s \mod q$, so $t = s$. In the second case $\mu^{ts} = \mu$ implies $ts \equiv 1 \mod q$. The claim follows.

With the claim proven, we can easily see which of the groups

$$G_0, G_1, \ldots, G_{q-1}$$

are isomorphic to each other. Indeed, the groups $G_0$, $G_1$, $G_{q-1}$ are not isomorphic any other $G_i$, while for $1 < i < q-1$ we have $G_i \cong G_{i'}$, where $i'$ is the inverse of $i$ modulo $q$. (Note that 1 and $-1$ are the only elements in $\mathbb{F}_q^\times$ which are equal to their own inverse.) Thus there are a total of

$$3 + \frac{q-3}{2} = \frac{q+3}{2}$$

groups among $G_0, G_1, \ldots, G_{q-1}$, up to isomorphism. □

Let $p$ and $q$ be distinct primes. With Lemma 6.26, Lemma 6.29, Lemma 6.28, and Theorem 6.32, we have completed the classification of groups of order $p^2q$. As a summary, the number of groups of order $p^2q$, up to isomorphism, is given in Table 5.

## 6.9 Transfer

Let $G$ be a finite group. In this section we will discuss the *transfer homomorphism*, which is a certain homomorphism $G \to H/[H,H]$ defined for any subgroup $H \leq G$. For our purposes we will only consider the case where $H$ is abelian, in which case the transfer is a homomorphism $G \to H$. (This will suffice for our purposes, and the more general definition is not much more difficult.)

Let $G$ be a finite group, and let $H \leq G$ be an abelian subgroup. Let $T$ be a *left transversal* for $H$ in $G$, in other words, a set of representatives for the left cosets of $H$ in $G$. Then $|T| = [G : H]$, and

$$\{gH : g \in G\} = \{tH : t \in T\}.$$

We can then define the "dot action" of $G$ on $T$ as follows. For all $g \in G$ and $t \in T$, we have $gtH = t'H$ for a unique $t' \in T$, which we denote by $t' = g \bullet t$. It is straightforward to verify that this defines an action of $G$ on $T$, so the following properties hold:

| | | |
|---|---|---|
| $p \nmid q-1$, $q \nmid p \pm 1$. | $N = 2$ | |
| | Abelian: | $C_{p^2q}$ |
| | | $C_p \times C_{pq}$ |
| | Non-abelian: | None |
| $p > 2$, $q = 2$. | $N = 5$ | |
| | Abelian: | $C_{2p^2}$ |
| | | $C_p \times C_{2p}$ |
| | Non-abelian: | $C_{p^2} \rtimes C_2 \cong D_{2p^2}$ (1 group) |
| | | $(C_p \times C_p) \rtimes C_2$ (2 groups) |
| $p = 2$, $q = 3$. | $N = 5$. | |
| | Abelian: | $C_{12}$ |
| | | $C_2 \times C_6$ |
| | Non-abelian: | $(C_2 \times C_2) \rtimes C_3 \cong A_4$ |
| | | $C_3 \rtimes (C_2 \times C_2) \cong S_3 \times C_2 \cong D_{12}$ |
| | | $C_3 \rtimes C_4$ (1 group) |
| $p^2 \mid q-1$. | $N = 5$ | |
| | Abelian: | $C_{p^2q}$ |
| | | $C_p \times C_{pq}$ |
| | Non-abelian: | $(C_q \rtimes C_p) \times C_p$ (1 group) |
| | | $C_q \rtimes C_{p^2}$ (2 groups) |
| $q > 3$, $p \mid q-1$, $p^2 \nmid q-1$ | $N = 4$ | |
| | Abelian: | $C_{p^2q}$ |
| | | $C_p \times C_{pq}$ |
| | Non-abelian: | $(C_q \rtimes C_p) \times C_p$ (1 group) |
| | | $C_q \rtimes C_{p^2}$ (1 group) |
| $p > 2$, $q > 2$, $q \mid p+1$. | $N = 3$ | |
| | Abelian: | $C_{p^2q}$ |
| | | $C_p \times C_{pq}$ |
| | Non-abelian: | $(C_p \times C_p) \rtimes C_q$ (1 group) |
| $q > 2$, $q \mid p-1$. | $N = \frac{q+9}{2}$ | |
| | Abelian: | $C_{p^2q}$ |
| | | $C_p \times C_{pq}$ |
| | Non-abelian: | $(C_{p^2}) \rtimes C_q$ (1 group) |
| | | $(C_p \times C_p) \rtimes C_q$ ($\frac{q+3}{2}$ groups) |

Table 5: For $p$ and $q$ distinct primes, the number $N$ of groups of order $p^2q$, up to isomorphism.

– $1 \bullet t = t$ for all $t \in T$;

– $(g \bullet h) \bullet t = (gh) \bullet (t)$ for all $t \in T$ and $g, h \in G$;

– For all $g \in G$, the map $t \mapsto g \bullet t$ is a bijection $T \to T$.

(This action is equivalent to action of $G$ on the left cosets of $H$.)

For all $g \in G$ and $t \in T$ we have $gtH = (g \bullet t)H$, so $(g \bullet t)^{-1}gt \in H$. Therefore we can define a map $v_T : G \to H$ by

$$v_T(g) = \prod_{t \in T} (g \bullet t)^{-1} gt$$

for all $g \in G$. We call $v_T$ the *transfer map* from $G$ to $H$. Note that since $H$ is abelian, the product over $T$ is defined uniquely and does not depend on the ordering of $T$.

We will first check that the transfer map does not depend on the choice of $T$, and after that we verify that it is a homomorphism.

**Lemma 6.33.** *Let $H \leq G$ be an abelian subgroup of a finite group $G$. Then $v_T = v_S$ for any left transversals $T, S$ of $H$ in $G$.*

*Proof.* Let $T$ and $S$ be left transversals of $H$ in $G$. We denote the dot action of $G$ on $T$ by $\bullet$ and on $S$ by $\bullet'$. Then $gtH = (g \bullet t)H$ and $gsH = (g \bullet' s)H$ for all $g \in G$, $t \in T$, and $s \in S$.

For each $t \in T$, there exists a unique $s \in S$ such that $sH = tH$. In this case $s = th_t$ for a unique $h_t \in H$, so

$$S = \{th_t : t \in T\}.$$

For all $t \in T$, we have

$$(g \bullet' (th_t))H = gth_tH = gtH = (g \bullet t)H = (g \bullet t)h_{g \bullet t}H.$$

Therefore

$$(g \bullet' (th_t)) = (g \bullet t)h_{g \bullet t}. \tag{6.3}$$

Now we can calculate that

$$\begin{aligned} v_S(g) &= \prod_{s \in S} (g \bullet' s)^{-1} gs \\ &= \prod_{t \in T} (g \bullet' (th_t))^{-1} gth_t \\ &= \prod_{t \in T} ((g \bullet t)h_{g \bullet t})^{-1} gth_t && \text{(by (6.3))} \end{aligned}$$

$$
\begin{aligned}
&= \prod_{t\in T} h_{g\bullet t}^{-1}(g\bullet t)^{-1}gth_t \\
&= \prod_{t\in T} h_{g\bullet t}^{-1}\cdot\prod_{t\in T}(g\bullet t)^{-1}gt\cdot\prod_{t\in T}h_t && \text{(since } H \text{ is abelian)} \\
&= \prod_{t\in T} h_t^{-1}\cdot v_T(g)\cdot\prod_{t\in T}h_t && \text{(since } t\mapsto g\bullet t \text{ is a bijection)} \\
&= v_T(g)
\end{aligned}
$$

for all $g \in G$. Thus $v_S = v_T$. □

Thus for an abelian subgroup $H \leq G$, we can write $v : G \to H$ for the transfer map.

**Lemma 6.34.** *Let $H \leq G$ be an abelian subgroup of a finite group $G$. Then the transfer map $v : G \to H$ is a homomorphism.*

*Proof.* Fix a left transversal $T$ for $H$ in $G$. For all $x, y \in G$, we have

$$
\begin{aligned}
v(xy) &= \prod_{t\in T}((xy)\bullet t)^{-1}xyt \\
&= \prod_{t\in T}(x\bullet(y\bullet t))^{-1}xyt && \text{(since } \bullet \text{ is an action)} \\
&= \prod_{t\in T}(x\bullet(y\bullet t))^{-1}x(y\bullet t)(y\bullet t)^{-1}yt \\
&= \prod_{t\in T}(x\bullet(y\bullet t))^{-1}x(y\bullet t)\cdot\prod_{t\in T}(y\bullet t)^{-1}yt && \text{(since } (g\bullet t)^{-1}gt\in H) \\
&= \prod_{t\in T}(x\bullet t)^{-1}xt\prod_{t\in T}(y\bullet t)^{-1}yt && \text{(since } t\mapsto y\bullet t \text{ is a bijection)} \\
&= v(x)v(y).
\end{aligned}
$$

so $v : G \to H$ is a homomorphism. □

Before applying the transfer homomorphism, we will need one more lemma for calculating the value of $v(g)$ for $g \in G$.

**Lemma 6.35.** *Let $H$ be an abelian subgroup of a finite group $G$, and let $T$ be a left transversal for $H$ in $G$. Let $g \in G$. Let $T_0 \subseteq T$ be representatives for the orbits of $\langle g\rangle$ on $T$ under the dot action, and for $t \in T_0$ denote by $n_t$ the size of the $\langle g\rangle$-orbit*

$$\langle g\rangle\bullet t = \{g^k\bullet t : k\in\mathbb{Z}\}.$$

*Let $v : G \to H$ be the transfer map. Then the following statements hold:*

(i) $\sum_{t\in T_0} n_t = [G : H]$;

(ii) $n_t$ *divides* $|g|$ *for all* $t \in T_0$;

(iii) $t^{-1}g^{n_t}t \in H$ *for all* $t \in T_0$;

(iv) $v(g) = \prod_{t\in T_0} t^{-1}g^{n_t}t$.

*Proof.* Since $T$ is the disjoint union of the $\langle g\rangle$-orbits, (i) follows. Claim (ii) follows since the size of an orbit divides the order of the group, so $n_t$ divides $|\langle g\rangle| = |g|$.

For (iii), let $t \in T_0$. Then the $\langle g\rangle$-orbit of $t$ is

$$\{g^k \bullet t : k \in \mathbb{Z}\} = \{g^k \bullet t : 0 \leq k < n_t\}.$$

For each $t' = g^k \bullet t$ in this orbit, in the product $v(g)$ we have a factor

$$(g \bullet t')^{-1}gt' = (g \bullet (g^k \bullet t))g(g^k \bullet t) = (g^{k+1} \bullet t)^{-1}g(g^k \bullet t).$$

Thus

$$\begin{aligned}\prod_{\substack{t'=g^k\bullet t\\ 0\leq k<n_t}} (g \bullet t')^{-1}gt' &= \prod_{0\leq k<n_t} (g^{k+1} \bullet t)^{-1}g(g^k \bullet t)\\ &= \prod_{0\leq k<n_t} (g^{n_t-k} \bullet t)^{-1}g(g^{n_t-k-1} \bullet t)\\ &= (g^{n_t} \bullet t)^{-1}g^{n_t}(g^0 \bullet t)\\ &= t^{-1}g^{n_t}t,\end{aligned}$$

which proves (iii). Claim (iv) also follows from this calculation, since

$$T = \bigcup_{t\in T_0} \langle g\rangle \bullet t.$$

This completes the proof of the lemma. □

As an example application, we can prove the following.

**Theorem 6.36.** *Let $G$ be a finite group and $[G : Z(G)] = n$. Then the map $g \mapsto g^n$ is a homomorphism $G \to G$.*

*Proof.* We will prove that the map $g \mapsto g^n$ is exactly the transfer map $v : G \to Z(G)$, and thus a homomorphism. To this end, let $T$ be a left transversal for $Z(G)$ in $G$.

Let $g \in G$, and choose $T_0 \subseteq T$ and integers $n_t$ for all $t \in T_0$ with properties as in Lemma 6.35 (i) – (iv). Then $t^{-1}g^{n_t}t \in Z(G)$ and thus $t^{-1}g^{n_t}t = g^{n_t} \in Z(G)$ for all $t \in T_0$. Moreover

$$v(g) = \prod_{t \in T_0} g^{n_t} = g^n,$$

since $\sum_{t \in T_0} n_t = [G : Z(G)] = n$. □

**Theorem 6.37** (Burnside)**.** *Let $G$ be a finite group and $P \leq G$ a Sylow $p$-subgroup of $G$. Suppose that $P \leq Z(N_G(P))$ (in other words, $N_G(P) = C_G(P)$). Then $P$ has a normal complement in $G$: that is, there exists a subgroup $K \trianglelefteq G$ such that $G = KP$, $K \cap P = \{1\}$ and $|K| = [G : P]$.*

*Proof.* Since $P$ is central in $N_G(P)$, in particular it is abelian and we have the transfer homomorphism $v : G \to P$. We will find that $K = \operatorname{Ker} v$ is a normal complement for $P$. To this end, we first prove the following.

*Claim: Let $x, y \in P$. If $x$ and $y$ are conjugate in $G$, then $x = y$.*
Suppose that $x, y \in P$ and $y = gxg^{-1}$ for some $g \in G$. Since $P$ is abelian, we have $P \leq C_G(x)$. Then $gPg^{-1} \leq C_G(gxg^{-1}) = C_G(y)$. But we also have $P \leq C_G(y)$ since $y \in P$, so $P$ and $gPg^{-1}$ are Sylow $p$-subgroups of $C_G(y)$. By Sylow II they are conjugate in $C_G(y)$, so there exists $h \in C_G(y)$ such that $hgPg^{-1}h^{-1} = P$. Then $hg \in N_G(P)$. But $P$ is central in $N_G(P)$, so $hg$ must commute with $x$. Hence

$$x = hgxg^{-1}h^{-1} = hyh^{-1} = y,$$

where the last equality holds since $h \in C_G(y)$.

We will use the claim to evaluate the transfer $v : G \to P$ on elements of $P$. Let $T \subseteq G$ be a left transversal for $P$ in $G$. Consider $g \in P$, and let $T_0 \subseteq T$ and $n_t$ be as in Lemma 6.35. Then $\sum_{t \in T_0} n_t = [G : P]$, and

$$v(g) = \prod_{t \in T_0} t^{-1}g^{n_t}t,$$

where $t^{-1}g^{n_t}t \in P$ for all $t \in T_0$. We have $g^{n_t} \in P$ and $t^{-1}g^{n_t}t \in P$ elements of $P$ which are conjugate in $G$, so by the claim above $g^{n_t} = t^{-1}g^{n_t}t$. Therefore

$$v(g) = \prod_{t \in T_0} g^{n_t} = g^{[G:P]}$$

for all $g \in P$.

This proves that $P \cap \operatorname{Ker} v = \{1\}$, since $\gcd(|P|, [G : P]) = 1$ for a Sylow $p$-subgroup $P$. Hence $v$ restricted to $P$ is injective, which shows that $v$ must be a surjective homomorphism. By the first isomorphism theorem $K = \operatorname{Ker} v$ has order $[G : P]$, and the theorem follows. □

## 6.10 Groups of squarefree order

An integer $n > 1$ is said to be *squarefree* if it is not divisible by the square of any prime. In this case $n = p_1 p_2 \cdots p_t$ for some distinct primes $p_1$, ..., $p_t$. In this section, we will give a complete classification of all groups of squarefree order.

For $n$ squarefree, we will see that the number of groups of order $n$ is

$$\operatorname{gnu}(n) = \sum_{\substack{m|n \\ n/m|\phi(m)}} \prod_{\substack{p|\frac{n}{m} \\ p \text{ prime}}} \frac{p^{f(p,m)} - 1}{p - 1},$$

where:

- $\phi$ is the Euler totient function,
- $f(p, m)$ is the number of prime divisors $q$ of $m$ such that $q \equiv 1 \mod m$.

This result was originally proven by Hölder (1895).

**Lemma 6.38.** *Let $G$ be a group of order $|G| = p_1 p_2 \cdots p_t$, where $p_1 < p_2 < \cdots < p_t$ are primes. Then the following are equivalent:*

(i) *$G$ is nilpotent.*

(ii) *$G$ is abelian.*

(iii) *$G$ is cyclic.*

*Proof.* (i) ⇒ (ii): If $G$ is nilpotent, it is isomorphic to the direct product of its Sylow subgroups. In this case the Sylow subgroups of $G$ are cyclic, so $G$ is abelian.
(ii) ⇒ (iii): Follows from the fact that $C_m \times C_n \cong C_{mn}$ if $\gcd(m, n) = 1$. (Lemma 5.18.)
(iii) ⇒ (i): This is clear. □

**Theorem 6.39.** *Let $G$ be group of order $|G| = p_1 p_2 \cdots p_t$, where $p_1 < p_2 < \cdots < p_t$ are primes. Then for all $1 \leq i \leq t$, there exists a normal subgroup $N \trianglelefteq G$ such that $|N| = p_i p_{i+1} \cdots p_t$. (In particular, $G$ has a normal Sylow $p_t$-subgroup.)*

*Proof.* If $t = 1$ the claim is trivial, so we assume that $t > 1$ and proceed by induction on $t$.

Let $P \leq G$ be a Sylow $p_1$-subgroup of $G$. Recall that $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$. On the other hand $p_1$ is the smallest prime divisor of $|G|$, so the order of $\mathrm{Aut}(P) \cong C_{p_1-1}$ is coprime to $|G|$, and thus $N_G(P)/C_G(P)$ is trivial. In other words $N_G(P) = C_G(P)$, so $P \leq Z(N_G(P))$. By Burnside's normal complement theorem (Theorem 6.37), there exists a normal subgroup $K \trianglelefteq G$ with $|K| = [G : P] = p_2 \cdots p_t$.

With this we can complete the proof. For $i = 1$ we can choose $N = G$. For $2 \leq i \leq t$, by induction there exists a normal subgroup $N \trianglelefteq K$ such that $|N| = p_i p_{i+1} \cdots p_t$. Since $\gcd(|N|, [K : N]) = 1$, it follows from Lemma 5.60 that $N$ is the unique subgroup of its order in $K$. Thus $N \operatorname{char} K \trianglelefteq G$, which gives $N \trianglelefteq G$ and completes the proof. □

**Theorem 6.40.** *Let $G$ be group of order $|G| = p_1 p_2 \cdots p_t$, where $p_1 < p_2 < \cdots < p_t$ are primes. Then $G$ is solvable.*

*Proof.* For $t = 1$ the claim is trivial, so assume that $t > 1$ and proceed by induction on $t$. By Theorem 6.39, there exists a normal subgroup $N \trianglelefteq G$ with $|N| = p_2 \cdots p_t$. By induction $N$ is solvable, and $G/N$ is solvable since it is cyclic; thus $G$ is solvable (Lemma 4.23). □

**Theorem 6.41.** *Let $G$ be a group of order $|G| = p_1 p_2 \cdots p_t$, where $p_1 < p_2 < \cdots < p_t$ are primes. Then the Fitting subgroup $F(G)$ has a cyclic complement $K$ in $G$. That is, there exists a cyclic subgroup $K \leq G$ such that $K \cap F(G) = \{1\}$ and $G = F(G)K$.*

*Proof.* From Theorem 6.40 we know that $G$ is solvable. Thus by Lemma 6.21 we have $C_G(F(G)) = F(G)$, and so $G/F(G)$ embeds into $\mathrm{Aut}(F(G))$. Since $F(G)$ is nilpotent, by Lemma 6.38 we have $F(G) \cong C_d$ for some $d \mid n$. Thus $G/F(G)$ embeds into $\mathrm{Aut}(C_d) \cong (\mathbb{Z}/d\mathbb{Z})^\times$, so in particular $G/F(G)$ is abelian.

Hence $G/F(G)$ is cyclic of order $n/d$ by Lemma 6.38. It is generated by a coset $gF(G)$ for some $g \in G$, in which case $g$ must have order divisible by $n/d$. Then $g' = g^k$ for $k = |g|d/n$ is an element of order $n/d$ in $G$. Let $K = \langle g' \rangle$. Then $K$ is a cyclic subgroup of order $n/d = [G : F(G)]$. We have $K \cap F(G) = \{1\}$ since $\gcd(d, n/d) = 1$. Then $G = F(G)K$ since

$$|F(G)K| = \frac{|F(G)| \cdot |K|}{|F(G) \cap K|} = |F(G)| \cdot |K| = |G|.$$

This completes the proof of the theorem. □

With Theorem 6.41, we have essentially described the structure of a group $G$ with squarefree order $|G|$. Indeed, by Theorem 6.41 we know that $G \cong F(G) \rtimes_\psi K$, where $F(G)$ and $K$ are both cyclic. Moreover, since $C_G(F(G)) = F(G)$ by the solvability of $G$, the homomorphism $\psi : K \to \mathrm{Aut}(F(G))$ must be injective. This means that there is an element of order $[G : F(G)]$ in $\mathrm{Aut}(F(G))$.

With this in mind, we can now construct all groups of squarefree order. Let $n > 1$ be a squarefree integer. Let $m \mid n$, and write $C_m = \langle y \rangle$ and $C_{n/m} = \langle x \rangle$. Let $\sigma \in \mathrm{Aut}(C_m)$ be an automorphism of order $n/m$ (if one exists). Then we define

$$G_{m,\sigma} = C_m \rtimes_\psi C_{n/m},$$

where $\psi : C_{n/m} \to \mathrm{Aut}(C_m)$ is the homomorphism defined by $\psi(x) = \sigma$.

**Theorem 6.42.** *Let $n > 1$ be squarefree and let $G$ be a group of order $n$. Then there exists $m \mid n$ and an automorphism $\sigma \in \mathrm{Aut}(C_m)$ such that $G \cong G_{m,\sigma}$.*

*Proof.* Let $m$ be the order of $F(G)$. We have $F(G) \cong C_m$ since $F(G)$ is nilpotent (Lemma 6.38). By Theorem 6.41, there exists a cyclic subgroup $K = \langle x \rangle$ of order $n/m$ such that $G = F(G)K$ and $F(G) \cap K = \{1\}$.

Since $G$ is solvable, we have $F(G) = C_G(F(G))$. Thus the homomorphism $\psi : K \to \mathrm{Aut}(F(G))$ defined by $\psi(k)(h) = khk^{-1}$ for all $k \in K$ and $h \in F(G)$ is injective. In particular $\psi(x) = \sigma$ is an element of order $n/m$ in $\mathrm{Aut}(F(G))$. By Theorem 5.40 we have

$$G \cong F(G) \rtimes_\psi K$$

and it is clear that $F(G) \rtimes_\psi K \cong G_{m,\sigma}$. □

**Lemma 6.43.** *Let $n > 1$ be squarefree, let $m \mid n$ and let $\sigma \in \mathrm{Aut}(C_m)$ be an automorphism of order $n/m$. Then $F(G_{m,\sigma}) = C_m$.*

*Proof.* We have $G_{m,\sigma} = H \rtimes_\psi K$, where $H \cong C_m$ and $K \cong C_{n/m}$. We will prove that $F(G_{m,\sigma}) = H$. Since $H \trianglelefteq G_{m,\sigma}$, we have $H \leq F(G_{m,\sigma})$.

For the other inclusion, first we note that

$$F(G_{m,\sigma}) = H(F(G_{m,\sigma}) \cap K)$$

since $G_{m,\sigma} = HK$ and $H \leq F(G_{m,\sigma})$. Furthermore since $F(G_{m,\sigma})$ is nilpotent of squarefree order, it is cyclic by Lemma 6.38. In particular $F(G_{m,\sigma})$ centralizes $H$. Since the homomorphism $\psi : K \to \mathrm{Aut}(H)$ is injective, no non-identity element of $K$ centralizes $H$, and thus $F(G_{m,\sigma}) \cap K = \{1\}$. We conclude then that $F(G_{m,\sigma}) = H$. □

**Theorem 6.44.** *Let $n > 1$ be squarefree. Let $m, m' \mid n$ and let $\sigma, \sigma' \in \mathrm{Aut}(C_m)$ be automorphisms of orders $n/m$ and $n/m'$, respectively. Then $G_{m,\sigma} \cong G_{m',\sigma'}$ if and only if $m = m'$ and $\langle \sigma \rangle = \langle \sigma' \rangle$.*

*Proof.* Suppose that $G_{m,\sigma} \cong G_{m',\sigma'}$. Then $F(G_{m,\sigma}) \cong F(G_{m',\sigma'})$, so by Lemma 6.43 we have $m = m'$. Let $C_{n/m} = \langle x \rangle$. Since $\mathrm{Aut}(C_m)$ is abelian, by Proposition 6.25 there exists $d \in \mathbb{Z}$ with $\gcd(d, n/m) = 1$ such that $\sigma^d = \sigma'$. Since $|\sigma| = |\sigma'| = n/m$, it follows that $\langle \sigma \rangle = \langle \sigma' \rangle$.

Conversely, suppose that $m = m'$ and $\langle \sigma \rangle = \langle \sigma' \rangle$. Then there exists $d \in \mathbb{Z}$ with $\gcd(d, n/m) = 1$ such that $\sigma^d = \sigma'$. It follows then from Proposition 6.25 that $G_{m,\sigma} \cong G_{m,\sigma'}$, as claimed by the theorem. □

Let $n > 1$ be squarefree. From Theorem 6.42 we know that any group $G$ of order $n$ is isomorphic to $G_{m,\sigma}$ for some $m \mid n$ and some automorphism $\sigma \in \mathrm{Aut}(C_m)$ of order $n/m$. Furthermore, from Theorem 6.44 we know precisely when two groups $G_{m,\sigma}$, $G_{m',\sigma'}$ are isomorphic: we have $G_{m,\sigma} \cong G_{m',\sigma'}$ if and only if $m = m'$ and $\sigma$, $\sigma'$ generate the same cyclic subgroup of $\mathrm{Aut}(C_m)$. With this we can conclude the following.

**Theorem 6.45.** *Let $n > 1$ be squarefree and $m \mid n$. Let $g_m$ be the number of groups $G$ of order $n$ with $|F(G)| = m$, up to isomorphism. Then $g_m$ is the number of subgroups of order $n/m$ in $\mathrm{Aut}(C_m)$, which is given by*

$$g_m = \prod_{\substack{p \mid \frac{n}{m} \\ p \text{ prime}}} \frac{p^{f(p,m)} - 1}{p - 1}.$$

*Here $f(p, m)$ denotes the number of prime divisors $q$ of $m$ such that $q \equiv 1 \bmod p$.*

*Proof.* It follows from Theorem 6.42, Lemma 6.43, and Theorem 6.44 that $g_m$ is the number of subgroups of order $n/m$ in $\mathrm{Aut}(C_m)$.

To prove the formula for $g_m$, write $n/m = p_1 \cdots p_t$ with $p_i$ distinct primes, and $m = q_1 \cdots q_s$ with $q_i$ distinct primes. For $1 \leq i \leq t$, let $d_i$ be the number of subgroups of order $p_i$ in $\mathrm{Aut}(C_m)$. Then we have

$$g_m = \prod_{1 \leq i \leq t} d_i.$$

(Indeed, since $\mathrm{Aut}(C_m)$ is abelian, any subgroup of order $n/m$ in $\mathrm{Aut}(C_m)$ is a direct product of unique subgroups $P_1, \ldots, P_t$ with $|P_i| = p_i$.)

It remains to verify that the number $d = d_i$ of subgroups of order $p = p_i$ in $\mathrm{Aut}(C_m)$ is equal to

$$\frac{p^{f(p,m)} - 1}{p - 1}.$$

For this, note that

$$\begin{aligned}\mathrm{Aut}(C_m) &\cong \mathrm{Aut}(C_{q_1}) \times \mathrm{Aut}(C_{q_2}) \times \cdots \times \mathrm{Aut}(C_{q_s}) \\ &\cong C_{q_1-1} \times C_{q_2-1} \times \cdots \times C_{q_s-1}.\end{aligned}$$

As a cyclic group, each $C_{q_i-1}$ either has no elements of order $p$, or a unique subgroup of order $p$. Therefore in $\mathrm{Aut}(C_m)$ there is a subgroup $X$ isomorphic to $C_p^{f(p,m)}$, and furthermore $X$ contains every subgroup of $\mathrm{Aut}(C_m)$ with order $p$.

The value of $d$ is thus given by the number of subgroups of order $p$ in $C_p^{f(p,m)}$. Any non-identity element of $C_p^{f(p,m)}$ has order $p$, and the subgroup generated by it contains $p-1$ elements of order $p$. Combining this with the fact that distinct subgroups of order $p$ have no elements of order $p$ in common, we conclude that the number of subgroups of order $p$ in $C_p^{f(p,m)}$ is equal to

$$\frac{p^{f(p,m)}-1}{p-1}.$$

This completes the proof of the theorem. □

Note that $\mathrm{Aut}(C_m) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ has order $\phi(m)$, so $\mathrm{Aut}(C_m)$ contains an element of order $n/m$ only if $n/m$ divides $\phi(m)$. Thus we have the following formula for the number of groups of squarefree order $n$.

$$\mathrm{gnu}(n) = \sum_{\substack{m|n \\ n/m|\phi(m)}} \prod_{\substack{p|\frac{n}{m} \\ p \text{ prime}}} \frac{p^{f(p,m)}-1}{p-1},$$

where $f(p,m)$ is defined as above.

# Exercises

In each exercise, $G$ is a group. We recall notation from the lecture notes:

- $|S|$ = cardinality of a set $S$.
- $|x|$ = order of an element $x \in G$.
- $o_d(G)$ = the number of elements of order $d$ in $G$.
- For $S \subseteq G$ and $g \in G$, we denote $S^g := g^{-1}Sg$.
- For $S, T \subseteq G$, we denote $ST = \{st : s \in S, t \in T\}$.
- $\mathbb{R}_{>0} = \{x \in \mathbb{R} : x > 0\}$.
- Similarly $\mathbb{Z}_{\geq 0} = \{0, 1, 2, 3, \ldots\}$, etc.
- $\mathrm{gnu}(n)$ = number of finite groups of order $n$, up to isomorphism.
- $\nu_p(n)$ = the largest integer $\alpha \geq 0$ such that $p^\alpha \mid n$ (for $p$ prime and $n \neq 0$).
- $\mathbb{F}_p$ is the field $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ of integers modulo $p$ (for $p$ prime).
- $k(G)$ = number of conjugacy classes in $G$.

## Section 1

**1.1** Let $n > 0$ be an integer. Prove that $1 \leq \mathrm{gnu}(n) < \infty$. Why $\mathrm{gnu}(0) = 0$?

**1.2** Examples of non-abelian groups:

(a) Let $\Omega$ be a set with $|\Omega| \geq 3$. Show that $\mathrm{Sym}(\Omega)$ is not abelian.

(b) Let $\mathbb{F}$ be a field and let $n \geq 2$ be an integer. Show that $\mathrm{GL}_n(\mathbb{F})$ is not abelian.

**1.3** Let $G = \mathrm{GL}_2(\mathbb{Q})$. Define $x, y \in G$ by $x = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ and $y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Show that $|x| = 2$, $|y| = 2$, and $|xy| = \infty$.

**1.4** Let $G$ be a group.

(a) Suppose that $x^2 = 1$ for all $x \in G$. Prove that $G$ is abelian.

(b) Suppose that $(xy)^2 = x^2y^2$ for all $x \in G$. Prove that $G$ is abelian.

(c) Suppose that $G$ is abelian. Prove that $(xy)^n = x^n y^n$ for all $n \in \mathbb{Z}$.

**1.5** Suppose that $\Omega$ and $\Omega'$ are sets such that $|\Omega| = |\Omega'|$. (In other words, suppose that there exists a bijection $\Omega \to \Omega'$.) Prove that $\mathrm{Sym}(\Omega) \cong \mathrm{Sym}(\Omega')$.

**1.6** Let $G$ and $H$ be groups, and let $\varphi : G \to H$ be an isomorphism.

(a) Prove that the inverse map $\varphi^{-1} : H \to G$ is an isomorphism.

(b) Let $\varphi' : G \to H$ be an isomorphism. Prove that $\varphi' = \varphi\psi$ for a unique automorphism $\psi : G \to G$.

(c) Prove that $G$ is abelian if and only if $H$ is abelian.

(d) Prove that $G$ is cyclic if and only if $H$ is cyclic.

(e) Prove that $|x| = |\varphi(x)|$ for all $x \in G$.

(f) For $d > 0$, let $o_d(G)$ be the cardinality of the set $\{x \in G : |x| = d\}$. Prove that $o_d(G) = o_d(H)$ for all $d > 0$.

**1.7** Prove the following statements.

(a) $(\mathbb{Q}, +) \ncong (\mathbb{R}, +)$.

(b) $(\mathbb{Q}, +) \ncong (\mathbb{Z}, +)$.

(c) $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$. (Hint: Use the fact that $e^{x+y} = e^x e^y$.)

(d) $(\mathbb{Q}, +) \ncong (\mathbb{Q}_{>0}, \cdot)$.

**1.8** Let $H \lneqq G$. Prove that $G$ is generated by $G \setminus H = \{x \in G : x \notin H\}$.

**1.9** Let $G = (\mathbb{Z}, +)$.

(a) Prove that $G = \langle 2, 3\rangle$. Find a generator for the subgroup $\langle 4, 6, 12\rangle$ of $G$.

(b) For $a, b \in \mathbb{Z}$, what are the generators of $\langle a, b\rangle$?

(c) Find a generator for $\langle 2\rangle \cap \langle 3\rangle$ and $\langle 14\rangle \cap \langle 12\rangle$.

(d) For $a, b \in \mathbb{Z}$, what are the generators of $\langle a\rangle \cap \langle b\rangle$?

**1.10** Let $p$ be a prime number and $G$ a finite group. Let $x \in G$ and $k \in \mathbb{Z}_{\geq 0}$. Suppose that $x^{p^k}$ has order divisible by $p$. Prove that $|x| = p^k |x^{p^k}|$.

**1.11** Let $x \in G$ have order $mn$, where $\gcd(m, n) = 1$. Prove that there exist unique elements $y, z \in G$ such that $x = yz = zy$ and $|y| = m$, $|z| = n$. (Hint: Use Bézout's lemma.)

**1.12** Let $G = \langle g \rangle$ be a cyclic group.

(a) Suppose that $|G| = 174$. Describe all subgroups of $G$.

(b) Suppose that $|G| = p^2$, where $p$ is a prime. Describe all subgroups of $G$.

(c) Suppose that $|G| = pq$, where $p$ and $q$ are distinct primes. Describe all subgroups of $G$.

(d) Suppose that $|G| = p^k$, where $p$ is a prime and $k \geq 1$. Describe all subgroups of $G$.

**1.13** Let $G$ be a group.

(a) Suppose that the number of subgroups of $G$ is finite. Prove that $G$ is finite.

(b) Suppose $G \neq \{1\}$ and that $G$ has only two subgroups, $\{1\}$ and $G$. What can you say about the structure of $G$?

(c) Let $G$ be a group and suppose that $G$ has exactly three subgroups, $\{1\}$, $H$, and $G$. What can you say about the structure of $G$?

(d) Let $G$ be a group and suppose that for any $H \leq G$, either $H = \{1\}$ or $H \cong G$. What can you say about the structure of $G$?

**1.14** Let $G = (\mathbb{Q}, +)$.

(a) The following subgroup
$$\langle \frac{2}{3}, \frac{12}{7} \rangle$$
of $(\mathbb{Q}, +)$ is cyclic. Which elements generate it?

(b) Show that every finitely generated subgroup of $G$ is cyclic.

(c) Let $H$ and $K$ be nontrivial subgroups of $G$. Show that $H \cap K$ is nontrivial.

(d) Let $H$ be the set of rational numbers of the form
$$\frac{a}{2^k},$$
where $a \in \mathbb{Z}$ and $k \geq 0$. Prove that $H$ is a subgroup of $(\mathbb{Q}, +)$ and that $H$ is not cyclic.

(e) Let $H$ be the set of all rational numbers with finite decimal expansion (for example $1/8 = 0.125 \in H$, but $1/3 = 0.333\ldots \notin H$). Prove that $H$ is a subgroup of $(\mathbb{Q}, +)$. Is $H$ cyclic?

**1.15** Let $z$ be an odd integer and $k > 0$.

(a) For $z \equiv 1 \mod 4$, prove that $\nu_2(z^{2^k} - 1) = \nu_2(z - 1) + k$.

(b) For $z \equiv 3 \mod 4$, prove that $\nu_2(z^{2^k} - 1) = \nu_2(z + 1) + k$.

(c) For $n \geq 3$, prove that $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is not cyclic.

(d) For $n \geq 2$, prove that $\overline{5}$ has order $2^{n-2}$ in $(\mathbb{Z}/2^n\mathbb{Z})^\times$. What are the orders of $\overline{3}$ and $\overline{7}$?

**1.16** Let $G$ be a group. For $m \in \mathbb{Z}$, we define $G(m) = \{x \in G : x^m = 1\}$.

(a) Let $G$ be an abelian group. Show that $G(m) \leq G$ for all $m \in \mathbb{Z}$.

(b) Suppose that $G = \langle g \rangle$ is cyclic of finite order $n$. Let $m \geq 0$ be an integer. Find a generator for $G(m)$. What is the order of $G(m)$?

(c) What does $G(m)$ look like when $G$ is infinite cyclic?

(d) For $G = S_3$, calculate $G(m)$ for $m = 1, 2, 3, 4, 5, 6$. Which ones are subgroups?

**1.17** Let $S \subseteq G$ and let $\varphi : G \to H$ be a homomorphism. Prove that $\langle \varphi(S) \rangle = \varphi(\langle S \rangle)$.

**1.18** (See Lemma 1.70.) Let $G = \langle x, y \rangle$ and $H = \langle z, w \rangle$ be groups such that the following hold:

- $|x| = 2$, $xyx^{-1} = y^{-1}$, and $x \notin \langle y \rangle$;
- $|z| = 2$, $zwz^{-1} = w^{-1}$, and $z \notin \langle w \rangle$.

Suppose that $|y| = |w|$. Prove that the map $\varphi : G \to H$ defined by $\varphi(x^i y^j) = z^i w^j$ for all $i, j \in \mathbb{Z}$ is a well-defined isomorphism.

**1.19** (See Section 1.7.) Construction of dihedral groups:

(a) Let $n \geq 3$. Define $x, y \in S_n$ as $x : \{1, \ldots, n\} \to \{1, \ldots, n\}$, $x(i) = n + 1 - i$ for all $1 \leq i \leq n$, and $y = (1\ 2\ \cdots\ n)$. Prove that $\langle x, y \rangle$ is dihedral of order $2n$.

(b) Consider $x, y \in \mathrm{Sym}(\mathbb{Z})$, where the bijections $x, y : \mathbb{Z} \to \mathbb{Z}$ are defined by

$$x(i) = -i \text{ for all } i \in \mathbb{Z},$$
$$y(i) = i + 1 \text{ for all } i \in \mathbb{Z}.$$

Prove that $\langle x, y \rangle$ is an infinite dihedral group.

**1.20** Let $G = \langle x, y \rangle$ be dihedral, where $|x| = 2$, $xyx^{-1} = y^{-1}$, and $x \notin \langle y \rangle$. Prove that every element of $G \setminus \langle y \rangle$ has order 2.

**1.21** Prove that every proper subgroup of $Q_8$ is cyclic. What are the subgroups of $Q_8$?

**1.22** Let $H$ and $K$ be subgroups of a group $G$. Show that $HK$ is a subgroup if and only if $HK = KH$. Find an example where $HK$ is not a subgroup of $G$.

**1.23** (Basic observations about normal subgroups.)

(a) Let $H$ be a subgroup of $G$ such that $[G : H] = 2$. Prove that $H \trianglelefteq G$.

(b) Let $G = Q_8$. Show that every subgroup of $G$ is normal.

(c) Let $G = D_8$. Find subgroups $H \trianglelefteq K \trianglelefteq G$ such that $H \not\trianglelefteq G$.

**1.24** Let $G$ be a group.

(a) Let $H \leq G$. Suppose that $G = HH^g$ for some $g \in G$. Prove that $G = H$.

(b) Let $H, K \leq G$ and suppose that $G = HK$. Prove that $G = H^x K^y$ for all $x, y \in G$.

**1.25** Let $G = \mathrm{Sym}(\mathbb{Z})$, the group formed by bijections $\mathbb{Z} \to \mathbb{Z}$.

(a) Show that $H = \{\sigma \in G : \sigma(x) = x \text{ for all } x \leq 0\}$ is a subgroup of $G$.

(b) For $g \in G$, show that $H^g = \{\sigma \in G : \sigma(x) = x \text{ for all } x \in g^{-1}(\mathbb{Z}_{\leq 0})\}$.

(c) Find an element $g \in G$ such that $H^g \subset H$ and $H^g \neq H$.

**1.26** Let $G = \mathrm{GL}_2(\mathbb{R})$.

(a) Show that

$$H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{Z} \right\}$$

is a subgroup of $G$.

(b) Consider a diagonal matrix $g = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ with $\alpha, \beta \in \mathbb{R} \setminus \{0\}$. Describe $H^g$. For which values of $\alpha$ and $\beta$ does $H^g \subseteq H$ hold? What about $H^g = H$? Find $\alpha$ and $\beta$ such that $H^g \subset H$, but $H^g \neq H$.

**1.27** Suppose that $G$ is abelian. Prove that $G$ is simple if and only if $G$ is cyclic of prime order.

**1.28** A proper subgroup $M < G$ is said to be *maximal*, if $M \leq H \leq G$ implies $H = M$ or $H = G$.

(a) Let $M < G$ be a maximal subgroup. If $M$ is a normal subgroup, prove that $G/M$ is cyclic of prime order.

(b) Show that there are no maximal subgroups in $(\mathbb{Q}, +)$.

**1.29** (Conjugacy classes for some examples.)

(a) Determine the conjugacy classes of $G = Q_8$.

(b) Determine the conjugacy classes of $G = D_2$, $G = D_4$, $G = D_6$.

(c) Determine the conjugacy classes of $G = D_{2n}$ for $n \geq 4$ even. (You should find $k(G) = (n+6)/2$ classes.)

(d) Determine the conjugacy classes of $G = D_{2n}$ for $n \geq 5$ odd. (You should find $k(G) = (n+3)/2$ classes.)

(e) Determine the conjugacy classes of $G = D_\infty$. (There are an infinite number of conjugacy classes.)

**1.30** Let $n \geq 3$. Show that $Z(S_n) = \{1\}$.

**1.31** Prove that if $G/Z(G)$ is cyclic, then $G$ is abelian.

**1.32** Prove that if $N \trianglelefteq G$ and $|N| = 2$, then $N \leq Z(G)$.

**1.33** (See Theorem 1.124.) Let $p$ be a prime number. Suppose that $G$ contains a subgroup $U$ of order $p$. For $x \in G$, define $[x] = xU$ if $x \in C_G(U)$, and $[x] = \{uxu^{-1} : u \in U\}$ if $x \notin C_G(U)$.

(a) Show that for all $x, y \in G$, either $[x] = [y]$ or $[x] \cap [y] = \emptyset$.

(b) Show that $[x]$ contains exactly $p$ elements for all $x \in G$.

(c) Suppose that $x \in G$ is such that $x^p = 1$. Show that $y^p = 1$ for all $y \in [x]$.

(d) Prove that if $G$ has only finitely many elements of order $p$, then $o_p(G) \equiv -1 \mod p$.

**1.34** Let $G$ be a finite group.

(a) Prove that $k(G) = 2$ if and only if $G \cong C_2$.

(b) Prove that $k(G) = 3$ if and only if $G \cong C_3$ or $G \cong S_3$. (Hint: Use the class equation.)

**1.35** Let $G$ be a group and $N \trianglelefteq G$. Let $N \leq H \leq G$. Then $N_{G/N}(H/N) = N_G(H)/N$.

**1.36** Let $p$ be a prime. Let $G$ be a non-abelian $p$-group of order $p^3$. Prove that $k(G) = p^2 + p - 1$.

**1.37** Consider the *Heisenberg group*

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

(a) Show that $H_p$ is a non-abelian subgroup of $\mathrm{GL}_3(p)$ such that $|H_p| = p^3$.

(b) Determine $Z(H_p)$.

(c) If $p > 2$, prove that $x^p = 1$ for all $x \in H_p$.

(d) By part (a), the group $H_2$ is a non-abelian group of order 8. Is $H_2 \cong Q_8$ or $H_2 \cong D_8$?

**1.38** Let $G$ be a group.

(a) Prove that $C_G(g^x) = C_G(g)^x$ for all $g, x \in G$.

(b) Suppose that $G$ is finite. Prove that the number of pairs $(x, y) \in G \times G$ such that $xy = yx$ is equal to $k(G)|G|$. Conclude that the probability that two randomly chosen elements of $G$ commute is equal to $k(G)/|G|$.

## Section 2

**2.1** Let $\sigma = (i_1 \ \cdots \ i_k)$ and $\tau = (j_1 \ \cdots \ j_\ell)$ be cycles in $S_n$. If $\sigma$ and $\tau$ are disjoint, then $\sigma\tau = \tau\sigma$.

**2.2** (Generators for $S_n$.)

(a) Show that $S_n$ is generated by (1 2), (1 3), ..., (1 $n$).

(b) Show that $S_n$ is generated by (1 2), (2 3), ..., ($n-1$ $n$).

(c) Show that $S_n = \langle (1\ 2), (1\ 2\ \cdots\ n) \rangle$.

**2.3** Let $\sigma \in S_n$ be a $k$-cycle.

(a) Prove that $|\sigma| = k$.

(b) Let $d \mid k$. Prove that $\sigma^d$ is a product of $d$ pairwise disjoint cycles of length $k/d$.

**2.4** Denote the maximal order of an element of $S_n$ by $g(n)$. Below is a list of small values:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $g(n)$ | 1 | 2 | 3 | 4 | 6 | 6 | 12 | 15 | 20 | 30 | 30 | 60 | 60 | 84 |

Using the values of $g(n)$ given above, find an element of largest order in $S_n$ for $1 \leq n \leq 14$.

**2.5** Let $\sigma, \tau \in S_n$. Consider the set $Y$ of pairs $\{i, j\}$ such that $\{\tau(i), \tau(j)\} \in I(\sigma)$. Prove that $|Y| = |I(\sigma)|$.

**2.6** Let $\sigma = (i\ j) \in S_n$ with $1 \leq i < j \leq n$. Calculate $|I(\sigma)|$, the number of inversions of $\sigma$.

**2.7** Let $n \geq 3$. Prove that $A_n$ has no subgroup of index 2.

**2.8** Let $n \geq 4$. Prove that $C_{S_n}(A_n) = \{1\}$. Conclude that $Z(A_n) = \{1\}$.

**2.9** Let $n \geq 2$ and $G \leq S_n$. Then either $G \leq A_n$, or $G \cap A_n$ is a normal subgroup of index 2 in $G$.

**2.10** Find representatives for the conjugacy classes of $S_5$, and the size of each conjugacy class.

**2.11** Let $G = S_4$.

(a) Prove that $N = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ is a normal subgroup of $G$.

(b) Find all the normal subgroups of $G$. (Hint: A normal subgroup is the union of conjugacy classes.)

**2.12** Suppose that $n \geq 5$ and $N \trianglelefteq S_n$. Prove that $N = \{1\}$, $N = A_n$, or $N = S_n$.

**2.13** Prove that (1 2 3) and (1 3 2) are not conjugate in $A_4$. Find all the conjugacy classes in $A_4$.

**2.14** Let $\sigma \in S_n$ be an $n$-cycle. Prove that $C_{S_n}(\sigma) = \langle \sigma \rangle$.

**2.15** Let $O = \mathrm{orb}_\sigma(i)$ be an orbit of $\sigma \in S_n$. Prove that if $g \in C_{S_n}(\sigma)$, then $g(O)$ is an orbit of $\sigma$. Prove then that $C_{S_n}(\sigma)$ acts on the orbits of $\sigma$.

**2.16** Let $n \geq 3$.

(a) Let $\sigma \in A_n$. Suppose that in the cycle decomposition of $\sigma$, there is a cycle of even length. Prove that $C_{S_n}(\sigma) \not\leq A_n$.

(b) Let $\sigma \in A_n$. Suppose that in the cycle decomposition of $\sigma$, there are two cycles with equal length. Prove that $C_{S_n}(\sigma) \not\leq A_n$. (Hint: If the length is even, use the previous part. If the length is odd, use an odd permutation that swaps the two orbits corresponding to the cycles.)

(c) Prove that for $\sigma \in A_n$, the conjugacy class $\sigma^{S_n}$ splits in $A_n$ if and only if the cycle decomposition of $\sigma$ consists of disjoint cycles with distinct odd lengths. (Hint: For one direction, use the other parts of this exercise. For the other direction, use exercises 2.14 and 2.15.)

**2.17** Let $G$ be a group and $H \leq G$. Consider the action of $G$ on the set

$$X = \{gH : g \in G\}$$

of left cosets of $H$ in $G$. Prove that $G$ acts transitively on $X$, and that $\mathrm{stab}_G(xH) = xHx^{-1}$ for all $x \in G$.

**2.18** Let $G = \mathrm{GL}_2(\mathbb{F})$, where $\mathbb{F}$ is a field. Let $V = \mathbb{F}^2$, with standard basis $e_1$, $e_2$ of column vectors. Describe $\mathrm{stab}_G(e_1)$ and $\mathrm{stab}_G(e_2)$. Prove that for all $v \in \mathbb{F}^2 \setminus \{0\}$, the stabilizer $\mathrm{stab}_G(v)$ is conjugate in $G$ to $\mathrm{stab}_G(e_1)$.

**2.19** Consider the normal subgroup $N = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ of $G = S_4$.

(a) Show that $G$ acts on $N \setminus \{1\}$ by conjugation.

(b) Prove that the homomorphism $\varphi : G \to S_3$ corresponding to this action is surjective with $\operatorname{Ker} \varphi = N$.

(c) Prove that $G/N \cong S_3$.

**2.20** Let $G \leq S_n$ such that $G \cong Q_8$. Prove that $n \geq 8$.

**2.21** Let $G$ be a finite group and $H < G$ a proper subgroup. Let $[G : H] = r > 1$.

(a) Prove that for all $x \in G$, there exists $0 < k \leq r$ such that $x^k \in H$.

(b) Prove that if $G$ is simple, then $|G|$ divides $r!$.

**2.22** Let $n \geq 5$. Let $H$ be a proper subgroup of $A_n$. Prove that $[A_n : H] \geq n$.

**2.23** Let $G$ be a finite group and let $p$ be the smallest prime divisor of $|G|$. Suppose that there is a subgroup $H < G$ such that $[G : H] = p$. Prove that $H \trianglelefteq G$.

**2.24** (On inclusions between symmetric and alternating groups.)

(a) Let $n \geq 1$. Prove that $S_n$ is isomorphic to a subgroup of $S_{n+1}$.

(b) Let $n \geq 1$. Prove that $A_n$ is isomorphic to a subgroup of $A_{n+1}$.

(c) Let $n \geq 3$. Prove that $S_n$ is isomorphic to a subgroup of $A_{n+2}$.

(d) Prove that $S_3$ is not isomorphic to a subgroup of $A_4$.

(e) Let $n \geq 4$. Prove that $S_n$ is not isomorphic to a subgroup of $A_{n+1}$.

## Section 3

**3.1** Let $n \geq 1$. Prove the following:

(a) $Z(\mathrm{GL}_n(q)) = \{\lambda I_n : \lambda \in \mathbb{F}_q^\times\}$, the subgroup of scalar matrices in $\mathrm{GL}_n(q)$.

(b) $Z(\mathrm{SL}_n(q)) = \{\lambda I_n : \lambda \in \mathbb{F}_q^\times, \lambda^n = 1\}$, the subgroup of scalar matrices in $\mathrm{SL}_n(q)$.

(*Hint:* For $1 \leq i, j \leq n$; let $E_{i,j}$ be the $(n \times n)$ matrix with 1 as the $(i, j)$ entry (row $i$, column $j$) and zeroes elsewhere. For all $1 \leq i, j \leq n$ with $i \neq j$, we have $I_n + E_{i,j} \in \mathrm{SL}_n(q)$. Thus if a matrix commutes with every element of $\mathrm{SL}_n(q)$, it will commute with $E_{i,j}$ for all $i \neq j$. Use this fact to show that if a matrix commutes with every element of $\mathrm{SL}_n(q)$, it must be a scalar matrix.)

**3.2** Let $p(t) \in \mathbb{F}[t]$ be a polynomial of degree 2 or degree 3. Prove that $p(t)$ is an irreducible over $\mathbb{F}$ if and only if $p(t)$ has no root in $\mathbb{F}$. Find an example of a polynomial $p(t) \in \mathbb{F}[t]$ of degree 4 such that $p(t)$ has no roots, but $p(t)$ is not irreducible.

**3.3** Let $q$ be a prime power. Prove that the number of irreducible polynomials in $\mathbb{F}_q[t]$ of the form $t^2 + \beta t + \alpha$ is equal to $q(q-1)/2$. (Hint: count the number of reducible polynomials.)

**3.4** Determine the irreducible monic polynomials of degree 2 in $\mathbb{F}_2[t]$ and $\mathbb{F}_3[t]$.

**3.5** Let $q$ be a prime power. Prove that the number of irreducible polynomials in $\mathbb{F}_q[t]$ of the form $t^2+\beta t+1$ is equal to $(q-1)/2$ if $q$ is odd, and $q/2$ if $q$ is even.

**3.6** Let $G=\mathrm{GL}_2(q)$ and $g=\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}\in G$, where $\alpha,\beta\in\mathbb{F}_q^\times$ and $\alpha\neq\beta$. Describe $C_G(g)$ and calculate $|C_G(g)|$.

**3.7** Let $G=\mathrm{GL}_2(q)$ and $g=\begin{pmatrix}\alpha & 1\\ 0 & \alpha\end{pmatrix}\in G$, where $\alpha\in\mathbb{F}_q^\times$. Describe $C_G(g)$ and calculate $|C_G(g)|$.

**3.8** Suppose that $t^2+\beta t+\alpha\in\mathbb{F}_q[t]$ be an irreducible polynomial over $\mathbb{F}_q$. Let $G=\mathrm{GL}_2(q)$ and $g=\begin{pmatrix}0 & -\alpha\\ 1 & -\beta\end{pmatrix}\in G$.

(a) Show that

$$C_G(g)=\{\lambda I_2+\mu g:\lambda,\mu\in\mathbb{F}_q \text{ and } (\lambda,\mu)\neq(0,0)\}$$

and conclude that $|C_G(g)|=(q-1)(q+1)$.

(b) Prove that $C=\{\lambda I_2+\mu g:\lambda,\mu\in\mathbb{F}_q\}$ equipped with matrix multiplication and addition is a field with $q^2$ elements.

**3.9** Let $p(t)\in\mathbb{F}[t]$ and write $p(t)=t^n+c_{n-1}t^{n-1}+\cdots+c_1t+c_0$, where $c_i\in\mathbb{F}$. Define

$$A=\begin{pmatrix}0 & 0 & \cdots & 0 & -c_0\\ 1 & 0 & \cdots & 0 & -c_1\\ 0 & 1 & \cdots & 0 & -c_2\\ \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 1 & -c_{n-1}\end{pmatrix}.$$

(a) Prove that the characteristic polynomial of $A$ is equal to $p(t)$.

(b) Prove that the minimal polynomial of $A$ is equal to $p(t)$. (Hint: Let $e_1,\ldots,e_n$ be the standard basis of column vectors. Show first that for any polynomial $q(t)$ of degree $<n$, we have $q(A)e_1\neq 0$.)

**3.10** Describe representatives for the conjugacy classes in $\mathrm{GL}_2(3)$, and determine the size of each conjugacy class. (There are a total of 8 conjugacy classes.)

**3.11** Describe representatives for the conjugacy classes of elements of order 3 in $\mathrm{GL}_2(7)$. (There are 5 conjugacy classes of elements of order 3 in $\mathrm{GL}_2(7)$.)

**3.12** Describe representatives for the conjugacy classes of elements of order 3 in $\mathrm{GL}_2(5)$.

**3.13** We have $|\mathrm{GL}_3(7)| = 2^6 \cdot 3^4 \cdot 7^3 \cdot 19$, so by Cauchy's theorem $\mathrm{GL}_3(7)$ contains elements of order 19. Find representatives for conjugacy classes of elements of order 19 in $\mathrm{GL}_3(7)$. (There are 6 classes. Use the factorization $t^{19} - 1 = (t-1)(t^3 + 2t - 1)(t^3 + 3t^2 + 3t - 1)(t^3 + 4t^2 + t - 1)(t^3 + 4t^2 + 4t - 1)(t^3 + 5t^2 - 1)(t^3 + 6t^2 + 3t - 1)$ in $\mathbb{F}_7[t]$, which you do not need to verify.)

**3.14** Let $\mathbb{F}$ be a field of characteristic $\neq 2$. Let $A \in \mathrm{SL}_2(\mathbb{F})$ be such that $A$ has order 2. Then $A = -I_2$.

**3.15** Let $m, n > 1$ be integers.

(a) Find elements $x, y \in \mathrm{PSL}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})/\{\pm I_2\}$ such that $|x| = m$, $|y| = n$, and $|xy| = \infty$. (Hint: Imitate the proof of Theorem 3.22, using primitive roots of unity in $\mathbb{C}$.)

(b) Find $x, y \in \mathrm{PSL}_2(\mathbb{C})$ such that $|x| = m$, $|y| = \infty$, $|xy| = n$.

**3.16** Let $m > 1$ be an integer.

(a) Find matrices $x, y \in \mathrm{GL}_2(\mathbb{C})$ such that $|x| = m$, $|y| = \infty$, and $|xy| = \infty$.

(b) Find matrices $x, y \in \mathrm{GL}_2(\mathbb{C})$ such that $|x| = \infty$, $|y| = \infty$, and $|xy| = m$.

**3.17** Let $\mathbb{F}$ be a field. Prove that $\mathrm{GL}_2(\mathbb{F})$ is generated by the set of transvections, together with matrices of the form $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$, where $\lambda \in \mathbb{F}^\times$.

**3.18** Let $A \in \mathrm{GL}_n(\mathbb{F})$, and let $V = \mathbb{F}^n$. Suppose that every $v \in V \setminus \{0\}$ is an eigenvector of $A$. Prove that $A$ must be a scalar matrix.

**3.19** Prove that $\mathrm{PGL}_2(3) \cong S_4$ and $\mathrm{PSL}_2(3) \cong A_4$. (Hint: Consider the action of $\mathrm{GL}_2(3)$ on the set of 1-dimensional subspaces of $\mathbb{F}_3^2$.)

## Section 4

**4.1** Let $G$ be a group and $x, y, z \in G$. Prove the following identities:

(a) $[x, y]^{-1} = [y, x]$.

(b) $xy = yx[x, y]$.

(c) $[xy, z] = [x, z]^y[y, z]$.

(d) $[x, yz] = [x, z][x, y]^z$.

(e) $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ for any homomorphism $\varphi : G \to H$.

**4.2** Let $x, y \in G$.

(a) Suppose that $x$ commutes with $[x, y]$. Prove that $[x^n, y] = [x, y]^n$ for all $n \in \mathbb{Z}_{\geq 0}$.

(b) Suppose that both $x$ and $y$ commute with $[x, y]$. Prove that $(xy)^n = x^n y^n [y, x]^{\frac{n(n-1)}{2}}$ for all $n \in \mathbb{Z}_{\geq 0}$.

**4.3** Let $G = Q_8$. Determine $[G, G]$.

**4.4** Let $G = D_{2n}$. Determine $[G, G]$.

**4.5** Let $p$ be a prime and let $G$ be a non-abelian $p$-group of order $p^3$. Show that $[G, G]$ has order $p$ and $[G, G] = Z(G)$.

**4.6** Let $G = S_n$, where $n \geq 3$. Prove that $[G, G] = A_n$.

**4.7** Let $S$ be a subset of $G$.

(a) Let $\phi : G \to H$ be a homomorphism. Prove that $\langle \phi(S) \rangle = \phi(\langle S \rangle)$.

(b) Let $g \in G$. Prove that $\langle S \rangle^g = \langle S^g \rangle$.

(c) Prove that $C_G(\langle S \rangle) = C_G(S)$.

**4.8** Let $G$ be a group and suppose that $G = \langle S \rangle$ for some $S \subseteq G$.

(a) Prove the following:

$$[G, G] = \langle [x, y]^g : x, y \in S \text{ and } g \in G \rangle.$$

(b) Find an example where $[G, G]$ is larger than $\langle [x, y] : x, y \in S \rangle$. (Hint: $S_n = \langle (1\ 2),\ (1\ 2\ \cdots\ n) \rangle$.)

**4.9** Let $G$ be a group and $H, K \leq G$. Prove that $[H, K] \trianglelefteq \langle H, K \rangle$. (Hint: Use Exercise 4.1 (c).)

**4.10** Let $G$ be a group and $H, K \trianglelefteq G$. Prove that $[H, K] \leq H \cap K$.

**4.11** (Examples of solvable groups.)

(a) Prove that all dihedral groups are solvable (including the infinite dihedral group $D_\infty$).

(b) Let $p$ be a prime. Prove that any finite $p$-group is solvable.

(c) Prove that $Q_8$ is solvable.

(d) Prove that $S_3$ is solvable.

**4.12** Let $G$ be a group and let $H, K \leq G$ be solvable subgroups such that $H \trianglelefteq G$. Prove that $HK$ is solvable.

**4.13** Let $\mathbb{F}$ be a field such that $|\mathbb{F}| \geq 3$. Prove that $[\mathrm{GL}_2(\mathbb{F}), \mathrm{GL}_2(\mathbb{F})] = \mathrm{SL}_2(\mathbb{F})$.

**4.14** We have $\mathrm{GL}_2(2) = \mathrm{SL}_2(2)$. Determine $[\mathrm{GL}_2(2), \mathrm{GL}_2(2)]$.

**4.15** Let $G = C_{p^k}$, where $p$ is a prime. Show that $G$ has only one composition series.

**4.16** Let $G = C_{pq}$, where $p$ and $q$ are distinct primes. How many composition series does $G$ have?

**4.17** Show that $\mathbb{Z}$ does not admit a composition series.

**4.18** (Dedekind's rule) Let $G$ be a group. Let $A, B, C \leq G$ be such that $B \leq A$. Prove that $A \cap BC = B(A \cap C)$.

**4.19** Let $G$ be a non-trivial group.

(a) Let $G$ be a finite abelian group. Prove that $G$ has a composition series where each quotient is cyclic of prime order.

(b) Suppose that $G$ is abelian. Prove that $G$ has a composition series if and only if $G$ is finite.

(c) Suppose that $G$ is solvable. Prove that $G$ has a composition series if and only if $G$ is finite.

**4.20** Let $G$ be a finite group. Prove that $|x^G| \leq |[G, G]|$ for all $x \in G$.

**4.21** Let $\mathbb{F}$ be a field, and let $B$ be the set of upper triangular matrices in $\mathrm{GL}_2(\mathbb{F})$:

$$B = \left\{ \begin{pmatrix} \lambda & \zeta \\ 0 & \mu \end{pmatrix} : \lambda, \mu \in \mathbb{F}^\times, \zeta \in \mathbb{F} \right\}.$$

(a) Prove that $B \leq \mathrm{GL}_2(\mathbb{F})$.

(b) Suppose that $|\mathbb{F}| > 2$. Prove that $[B, B] = U$, where

$$U = \left\{ \begin{pmatrix} 1 & \zeta \\ 0 & 1 \end{pmatrix} : \zeta \in \mathbb{F} \right\}.$$

What happens when $|\mathbb{F}| = 2$?

(c) Suppose that $|\mathbb{F}| > 2$. Prove that $B$ is solvable but not nilpotent.

**4.22** Let $G$ be a nilpotent group and let $N \trianglelefteq G$ such that $N \neq \{1\}$. Prove that $[N, G] \lneqq N$.

**4.23** Let $G$ be a nilpotent group and $H$ be a proper subgroup of $G$. Then $H \lneqq N_G(H)$. (Hint: Show that there exists $k \geq 1$ such that $\gamma_k(G) \not\leq H$ and $\gamma_{k+1}(G) \leq H$.)

**4.24** Let $G$ be a group.

(a) Prove that $Z^k(G) \operatorname{char} G$ for all $k \geq 0$.

(b) Suppose that $\gamma_{c+1}(G) = \{1\}$ for some $c \geq 1$. Prove that $\gamma_{c-i+1}(G) \leq Z^i(G)$ for all $1 \leq i \leq c$. (In particular $Z^c(G) = G$.)

(c) Suppose that $Z^c(G) = G$ for some $c \geq 1$. Prove that $\gamma_{c-i+1}(G) \leq Z^i(G)$ for all $1 \leq i \leq c$. (In particular $\gamma_{c+1}(G) = \{1\}$.)

**4.25** Let $G$ be a group.

(a) (Hall–Witt identity) Let $x, y, z \in G$. Prove the following identity:

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1$$

(b) (Three subgroups lemma) Let $H, K, L \leq G$. Suppose that two of the following higher commutator subgroups are trivial:

$$[H, K, L], [K, L, H], [L, H, K].$$

Prove that $[H, K, L] = [K, L, H] = [L, H, K] = \{1\}$.

(c) Let $N$ be a normal subgroup. Suppose that two of the following higher commutor subgroups are contained in $N$:

$$[H, K, L], [K, L, H], [L, H, K].$$

Prove that all three of them are contained in $N$.

(d) Let $i, j \geq 1$. Prove that $[\gamma_i(G), \gamma_j(G)] \leq \gamma_{i+j}(G)$. (Hint: Proceed by induction on $i$, and use (c).)

(e) Prove that $G^{(k)} \leq \gamma_{2^k}(G)$ for all $k \geq 0$.

**4.26** Let $G$ be a group and $k \geq 2$. Prove that

$$\gamma_k(G) = \langle [x_1, x_2, \ldots, x_k] : x_1, x_2, \ldots, x_k \in G \rangle.$$

**4.27** Let $G = S_3$.

(a) Find elements $x, y, z \in G$ such that $[[x, y], z] \neq [x, [y, z]]$.

(b) Find subgroups $H, K, L \leq G$ such that $[[H, K], L] \neq [H, [K, L]]$.

**4.28** Let $G$ be a group and $H, K, L \trianglelefteq G$. Prove that $[HK, L] = [H, L][K, L]$ and $[H, KL] = [H, K][H, L]$.

**4.29** Let $G$ be a finite group.

(a) Prove that $F(G)\operatorname{char} G$.

(b) Prove that if $K \trianglelefteq G$, then $F(K) \leq F(G)$.

(c) Find an example where $K \leq G$ and $F(K) \not\leq F(G)$.

(d) Suppose that $G$ is solvable and $G \neq \{1\}$. Prove that $F(G) \neq \{1\}$.

## Section 5

**5.1** Let $G_1, \ldots, G_n$ be groups. Let $\widehat{G_i} := \{1\} \times \cdots \times \{1\} \times G_i \times \{1\} \times \cdots \times \{1\}$. Then $G_i \trianglelefteq G_1 \times \cdots \times G_n$ and

$$(G_1 \times \cdots \times G_n)/\widehat{G_i} \cong G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n.$$

**5.2** Let $G$ be a group and let $H, K \trianglelefteq G$. Suppose that $H \cap K = \{1\}$. Then $hk = kh$ for all $h \in H$ and $k \in K$.

**5.3** Let $H$ and $K$ be groups. Then for any $A \leq H$ and $B \leq K$, the product $A \times B$ is a subgroup of $H \times K$.

**5.4** Let $H$ and $K$ be finite groups.

(a) Suppose that $\gcd(|H|, |K|) = 1$. Prove that if $N \leq H \times K$, then $N = A \times B$ for some $A \leq H$ and $B \leq K$.

(b) Suppose that $H \neq \{1\}$. Prove that $H \times H$ has a subgroup which is not of the form $A \times B$.

**5.5** Let $G = H \times K$. Define the projection maps $\pi_H : G \to H$ and $\pi_K : G \to K$ by $\pi_H(h, k) = h$ and $\pi_K(h, k) = k$ for all $h \in H$ and $k \in K$.

(a) Prove that $\pi_H$ and $\pi_K$ are surjective homomorphisms.

(b) Prove that $\operatorname{Ker} \pi_H \cong K$ and $\operatorname{Ker} \pi_K \cong H$.

(c) For any subgroup $X \leq G$, prove that $X \leq \pi_H(X) \times \pi_K(X)$. Find an example where $X \neq \pi_H(X) \times \pi_K(X)$.

(d) Generalize (a) and (b) for $G = H_1 \times H_2 \times \cdots \times H_k$, where $H_1$, $H_2$, …, $H_k$ are groups and $k \geq 2$.

**5.6** Let $G$ and $H$ be groups. Prove the following statements:

(a) $(G \times H)^{(k)} = G^{(k)} \times H^{(k)}$ for all $k \geq 0$.

(b) $\gamma_k(G \times H) = \gamma_k(G) \times \gamma_k(H)$ for all $k \geq 1$.

(c) $Z^k(G \times H) = Z^k(G) \times Z^k(H)$ for all $k \geq 0$.

(d) The direct product $G \times H$ is abelian if and only if $G$ and $H$ are abelian.

(e) The direct product $G \times H$ is solvable if and only if $G$ and $H$ are solvable.

(f) The direct product $G \times H$ is nilpotent if and only if $G$ and $H$ are nilpotent.

**5.7** Let $G$ and $H$ be finite groups. Prove that $F(G \times H) = F(G) \times F(H)$.

**5.8** Prove that $(\mathbb{Q}, +)$ is not isomorphic to a direct product of cyclic groups.

**5.9** Let $G = \langle x_1, \ldots, x_k \rangle$ be a finitely generated abelian group. Prove that any subgroup $H \leq G$ is generated by $\leq k$ elements. (Hint: Proceed by induction and consider $H \cap \langle x_2, \ldots, x_k \rangle$.)

**5.10** Let $G$ be an abelian group. Let $\operatorname{tor}(G) = \{g \in G : |g| < \infty\}$, the set of elements of finite order in $G$.

(a) Prove that $\operatorname{tor}(G)$ is a subgroup of $G$.

(b) Prove that $G/\operatorname{tor}(G)$ has no non-trivial element of finite order.

(c) Let $G$ and $H$ be abelian groups. If $G \cong H$, prove that $\operatorname{tor}(G) \cong \operatorname{tor}(H)$ and $G/\operatorname{tor}(G) \cong H/\operatorname{tor}(H)$.

(d) Suppose that $G = C_{n_1} \times \cdots \times C_{n_k} \times \mathbb{Z}^r$, where $k \geq 0$, $n_1, \ldots, n_k > 1$, and $r \geq 0$. Prove that

$$\begin{aligned} \operatorname{tor}(G) &\cong C_{n_1} \times \cdots \times C_{n_k}, \\ G/\operatorname{tor}(G) &\cong \mathbb{Z}^r. \end{aligned}$$

(e) Find a non-abelian group $X$ such that $\operatorname{tor}(X)$ is not a subgroup of $X$.

**5.11** Let $(G, +)$ be an abelian group.

(a) Prove that for all $n > 0$, the set $nG = \{ng : g \in G\}$ is a subgroup of $G$.

(b) If $G$ and $H$ are abelian groups such that $G \cong H$, prove that $nG \cong nH$ and $G/nG \cong H/nH$.

(c) Let $r, s \geq 0$. Prove that $\mathbb{Z}^r \cong \mathbb{Z}^s$ if and only if $r = s$. (Hint: use part (b).)

**5.12** Let $(G, +)$ be an abelian group. Recall from Exercise 1.16 that for all $m \in \mathbb{Z}$, the set $G(m) = \{g \in G : mg = 0\}$ is a subgroup of $G$.

(a) Let $(G_1, +)$, ..., $(G_t, +)$ be abelian groups and $G = G_1 \times \cdots \times G_t$. Prove that $G(m) = G_1(m) \times \cdots \times G_t(m)$ for all $m \in \mathbb{Z}$.

(b) If $m \mid n$, prove that $G(m) \leq G(n)$.

(c) Let $G$ be cyclic of order $n$. Prove that $G/G(d) \cong C_{n/d}$.

(d) Let $G$ be cyclic of order $n$ and let $d \mid d' \mid n$. Prove that $G(d)/G(d') \cong C_{d/d'}$.

**5.13** Let $G$ the following subgroup of $\mathrm{GL}_2(\mathbb{Q})$:

$$G = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Let $U$ be the following subgroup of $\mathrm{GL}_2(\mathbb{Q})$:

$$U = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} : x \in \mathbb{Q} \right\}.$$

Prove that $H = G \cap U$ is not finitely generated. (This example shows that a subgroup of a finitely generated group is not necessarily finitely generated.)

**5.14** Let $n > 0$ be an integer and write the prime factorization of $n$ as $n = p_1^{k_1} \cdots p_t^{k_t}$, where $p_i$ are distinct primes and $k_i > 0$ for all $1 \leq i \leq t$. Prove that up to isomorphism, the number of finite abelian groups of order $n$ is $p(k_1) \cdots p(k_t)$, where $p(k)$ denotes the number of *partitions* of an integer $k > 0$. (For example $p(4) = 5$, since the partitions of 4 are 4, $1 + 3$, $2 + 2$, $1 + 1 + 2$, and $1 + 1 + 1 + 1$. Other values: $p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, $p(5) = 6$, $p(6) = 11$.)

**5.15** Let $G$ be a finite abelian $p$-group, say $G \cong C_{p^{\alpha_1}} \times \cdots \times C_{p^{\alpha_t}}$ with $\alpha_1 \geq \cdots \geq \alpha_t > 0$.

(a) Prove that for $H \leq G$, we have $H \cong C_{p^{\beta_1}} \times \cdots \times C_{p^{\beta_t}}$ for some $\beta_1 \geq \cdots \geq \beta_t \geq 0$.

(b) Prove that in (a), we have $\beta_i \leq \alpha_i$ for all $1 \leq i \leq t$.

(c) Prove that for $G/H$, we have $G/H \cong C_{p^{\gamma_1}} \times \cdots \times C_{p^{\gamma_t}}$ for some $\gamma_1 \geq \cdots \geq \gamma_t \geq 0$.

(d) Prove that in (c), we have $\gamma_i \leq \alpha_i$ for all $1 \leq i \leq t$.

**5.16** Let $G$ be a finite abelian group and let $H \leq G$ be a subgroup. Prove that there exists $K \leq G$ such that $K \cong G/H$. (Hint: Use exercise 5.15).

**5.17** Let $G = Q_8$.

(a) Prove that $G/Z(G) \cong C_2 \times C_2$.

(b) Prove that $G$ has no subgroup isomorphic to $C_2 \times C_2$.

**5.18** Prove that there does not exist a group $G$ with $G/Z(G) \cong Q_8$. (Hint: $Q_8$ has a subgroup of order 2, which is contained in every nontrivial subgroup of $Q_8$.)

**5.19** Let $G$ and $H$ be groups. Prove that if $G \cong H$, then $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$. Find an example where $\mathrm{Aut}(G) \cong \mathrm{Aut}(H)$, but $G \ncong H$.

**5.20** Prove that $\mathrm{Aut}(C_2 \times C_2) \cong S_3$.

**5.21** Let $G$ and $H$ be finite groups.

(a) Suppose that $\gcd(|G|, |H|) = 1$. Prove that $\mathrm{Aut}(G \times H) \cong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

(b) Prove that $\mathrm{Aut}(G) \times \mathrm{Aut}(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(G \times H)$.

(c) Find an example where $\mathrm{Aut}(G \times H) \ncong \mathrm{Aut}(G) \times \mathrm{Aut}(H)$.

**5.22** Prove that $\mathrm{Aut}(S_4) \cong S_4$.

**5.23** Let $p$ be a prime and let $G$ be a finite group. Prove that $G$ is an elementary abelian $p$-group if and only if $G$ is abelian and $x^p = 1$ for all $x \in G$.

**5.24** Let $(G, +)$ be an abelian group. Suppose that there exists a prime $p$ such that $pg = 0$ for all $g \in G$.

(a) For $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$, define $\overline{x} \cdot g = xg$ for all $g \in G$. Prove that this makes $G$ into a vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

(b) Let $V$ be a vector space over $\mathbb{F}_p$. Show that for $(G, +) = (V, +)$, we have $pg = 0$ for all $g \in G$.

(c) Let $\varphi : G \to G$ be map. Show that $\varphi$ is a homomorphism if and only if $\varphi$ is a $\mathbb{F}_p$-linear map.

**5.25** When is the order of $\mathrm{Inn}(G)$ a prime number?

**5.26** Let $H$ and $K$ be groups, and let $G = H \rtimes_\psi K$ be an external semidirect product, where $\psi : K \to \mathrm{Aut}(H)$ is a homomorphism. Let $\widehat{H}$ and $\widehat{K}$ be as in Theorem 5.36. Prove that the following statements are equivalent:

(i) $G = H \times K$.

(ii) $\psi : K \to \mathrm{Aut}(H)$ is trivial.

(iii) $\widehat{K}$ is a normal subgroup of $G$.

**5.27** Let $H$ and $K$ be groups.

(a) Suppose that $H \cong H'$ and $K \cong K'$. Prove that any external semidirect product $H \rtimes_\psi K$ is isomorphic to $H' \rtimes_{\psi'} K'$ for some homomorphism $\psi' : K' \to \mathrm{Aut}(H')$.

(b) Let $\psi, \psi' : K \to \mathrm{Aut}(H)$ be homomorphisms. Suppose that $\psi' = \psi\varphi$ for some $\varphi \in \mathrm{Aut}(K)$. Prove that $H \rtimes_\psi K \cong H \rtimes_{\psi'} K$.

(c) Let $\psi, \psi' : K \to \mathrm{Aut}(H)$ be homomorphisms. Suppose that there exists $\phi \in \mathrm{Aut}(H)$ such that $\psi'(x) = \phi\psi(x)\phi^{-1}$ for all $x \in K$. Prove that $H \rtimes_\psi K \cong H \rtimes_{\psi'} K$.

**5.28** Let $G$ be a finite group of order $mn$, where $\gcd(m, n) = 1$. Suppose that $G$ contains a normal subgroup $N$ of order $n$. Then $N$ is the unique subgroup of order $n$ in $G$, and

$$N = \{x \in G : x^n = 1\}.$$

**5.29** Let $G = D_{2n}$ (dihedral group), where $n > 0$ is odd. Prove that all elements of order 2 are conjugate in $G$.

**5.30** Classify groups of order 30 up to isomorphism.

## Section 6

**6.1** Let $G$ be a finite group and let $p$ be a prime. We denote the set of Sylow $p$-subgroups of $G$ by $\mathrm{Syl}_p(G)$.

(a) Let $H \leq G$. Prove that

$$\mathrm{Syl}_p(H) \subseteq \{P \cap H : P \in \mathrm{Syl}_p(G)\}.$$

(b) Find an example of a group $G$ and $H \leq G$ such that

$$\mathrm{Syl}_p(H) \subsetneqq \{P \cap H : P \in \mathrm{Syl}_p(G)\}.$$

**6.2** Let $G$ be a finite group and let $p$ be a prime.

(a) Let $N \trianglelefteq G$. Prove that

$$\mathrm{Syl}_p(N) = \{P \cap N : P \in \mathrm{Syl}_p(G)\}.$$

(b) Let $N \trianglelefteq G$. Prove that

$$\mathrm{Syl}_p(G/N) = \{PN/N : P \in \mathrm{Syl}_p(G)\}.$$

**6.3** Let $G$ be a group of order $|G| = 20 = 2^2 \cdot 5$.

(a) Show that $G$ is isomorphic to some semidirect product $C_5 \rtimes_\psi P$, where $|P| = 2^2$.

(b) Classify semidirect products $C_5 \rtimes_\psi C_4$, up to isomorphism. (There are 3 in total.)

(c) Classify semidirect products $C_5 \rtimes_\psi (C_2 \times C_2)$, up to isomorphism. (There are 2 in total.)

**6.4** (Examples of $H \leq G$ such that $n_p(H) \nmid n_p(G)$.)

(a) Let $G = S_5$ and $H = S_4$. Show that $n_3(H) = 4$ and $n_3(G) = 10$.

(b) Let $G = A_5$. Show that there is a subgroup $H < G$ such that $H \cong S_3$. Prove that $n_2(H) = 3$ and $n_2(G) = 5$.

**6.5** Let $G$ and $H$ be finite groups. Prove that $n_p(G \times H) = n_p(G)n_p(H)$.

**6.6** Let $p$ and $q$ be distinct primes. Classify semidirect products of the form $C_q \rtimes_\psi (C_p \times C_p \times \cdots \times C_p)$, up to isomorphism.

**6.7** Let $G$ be a finite group and let $p$ be a prime.

(a) Suppose that a Sylow $p$-subgroup of $G$ is cyclic. Prove that if $p^k \mid |G|$, then any two subgroups of order $p^k$ are conjugate in $G$.

(b) Find an example where $p^k \mid |G|$, and $G$ contains two subgroups of order $p^k$ which are not conjugate in $G$.

**6.8** Let $G$ be a finite abelian group and $H \leq G$. Prove that for the transfer map $v : G \to H$, we have $v(g) = g^{[G:H]}$ for all $g \in G$.

**6.9** Let $G$ be a group of squarefree order $|G|$. Prove that for all $d \mid n$, there exists a subgroup of order $d$ in $G$.