GROUP THEORY IN ALGEBRAIC STRUCTURES

DANIEL MACÍAS CASTILLO

Contents

Preliminary version of 10/2020.

Preface

This is *not* a complete set of notes for Algebraic Structures. Part II of the course, concerning Ring Theory, is not discussed in these notes.

However, these notes do contain all of the relevant material on Group Theory that will be covered in Part I of the course. They may thus be used as a guide and main reference for this part of the course. Some of the specific results, proofs, examples, etc., that appear in these notes may not be explicitly discussed during the lectures, due to obvious time limitations.

At any given moment during the course, I would recommend reading ahead of whichever point the lectures have gotten up to. In this way, the next lectures will become easier to follow, and one may ask any relevant question that may arise through this reading.

I have included many relevant exercises right below most of the results and definitions that occur in the notes. I have also added long lists of exercises at the end of each section.

These lists of exercises do **not**, in any way, intend to replace the official exercise sheets for the course that will be provided. You should give priority to the exercises that appear in the exercise sheets.

However, if you feel that you do not properly understand some part of the course (or even if you just wish to study some part of the course more in depth), then you may certainly use the exercises found in the corresponding parts of these notes to think further about the relevant concepts.

The main reference for the writing of these notes has been the book [2] of Dummit and Foote, which we have occasionally complemented with alternative books such as [1].

Part I: Group Theory

From the moment you started studying and handling sets such as $\mathbb{N} := \{1, 2, 3, \ldots\}$ and $\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, you had encountered a first level of abstraction: the usual jump from considering three oranges, or three pens, to considering the number 3; the agreement that, since *adding* a new orange to an original two oranges results in three oranges, we may write $2 + 1 = 3$.

You may think of group theory, and later also of ring theory, as a second level of abstraction. Consider for example Fermat's Little Theorem, which states that if p is a prime number and a is an integer with $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

Clearly, this result has nothing to do with oranges. The more surprising fact is that this result has nothing to do with integers, or more generally with numbers. Instead, it will be seen to be a direct consequence of Lagrange's Theorem 2.61.

It is therefore interesting to try to consider the sets Lagrange's Theorem applies to, all at once, since we will get information about many different kinds of mathematical objects. This is what we meant by a second level of abstraction: isolating the essential properties of the set $\mathbb{Z}$ and of its natural binary operations, which are really responsible for the truth of the important theorems of arithmetic.

In fact, at some point you may have felt that there was some cheating involved in the first level of abstraction. It is not clear that there is such a thing as zero oranges, or as minus three oranges. The mathematicians of ancient Greece, who are considered responsible for this first jump, did not have a number 0, or any negative numbers. In other words, they could work with $\mathbb{N}$ and with its binary operations $+$ and $\cdot$, but the notion of working with $\mathbb{Z}$ would have seemed nonsensical to them. Why do we want to work with $\mathbb{Z}$ then?

The real reason we need to do this is that the pair $(\mathbb{N}, +)$ does not constitute a group, while the pair $(\mathbb{Z}, +)$ does. In a way, $(\mathbb{Z}, +)$ is the group generated by the set $\mathbb{N}$ with its binary operation $+$. This is what justifies its definition. We can then apply all of the results of group theory to $(\mathbb{Z}, +)$, and from them deduce the corresponding facts about the elements of $\mathbb{N} \subset \mathbb{Z}$.

In a similar way, the triple $(\mathbb{N}, +, \cdot)$ does not constitute a ring, while $(\mathbb{Z}, +, \cdot)$ does.

1. Introduction to group theory and examples

1.1. Definition and first properties.

1.1.1. *Binary operations.* We recall that the cartesian product of two sets S and T is given by

$$S \times T := \{(s,t) : s \in S, t \in T\}.$$

In particular one has $S \times S = \{(s,s') : s, s' \in S\}$.

Definition 1.1. Let S be a set.

(i) A binary operation $\star$ on S is a function

$$\star : S \times S \to S.$$

We often abbreviate $\star((s,s'))$ to $s \star s'$.

(ii) Let T be a subset of S. We say that T is closed under $\star$ if the restriction of $\star$ to

$$T \times T \subseteq S \times S$$

defines a binary operation on T.

In other words, T is closed under $\star$ if $t \star t'$ belongs to T for every t and t' in T.

(iii) The operation $\star$ is associative if

$$s \star (s' \star s'') = (s \star s') \star s''$$

for all $s, s', s'' \in S$.

(iv) The operation $\star$ is commutative if

$$s \star s' = s' \star s \tag{2}$$

for all $s, s' \in S$.

(v) An element s of S is said to 'commute' with an element s' of S (with respect to $\star$) if the equality (2) is valid.

Remark 1.2. It is very easy to prove that, if $\star$ is associative (resp. commutative) as a binary operation on S and $T \subseteq S$, then $\star$ is associative (resp. commutative) as a function on $T \times T \subseteq S \times S$. In particular, if T is closed under $\star$, then $\star$ is associative (resp. commutative) as a binary operation on T.

Examples 1.3.
(i) The sum $+$ and the multiplication $\cdot$ both are binary operations on $\mathbb{Z}$, and both are associative and commutative.

The subset $2\mathbb{Z} := \{2a : a \in \mathbb{Z}\}$ of even integers is closed under $+$ because

$$2a + 2b = 2(a+b),$$

and it is closed under $\cdot$ because

$$(2a) \cdot (2b) = 2(2ab).$$

The subset $2\mathbb{Z} + 1 := \{2a+1 : a \in \mathbb{Z}\}$ is closed under $\cdot$ because

$$(2a+1) \cdot (2b+1) = 2(2ab + a + b) + 1.$$

However, $2\mathbb{Z}+1$ is not closed under $+$ because

$$1+1=2\notin 2\mathbb{Z}+1.$$

(ii) The substraction $-$ is a binary operation on $\mathbb{Z}$, but it is not associative because

$$0-(0-1)=1\neq -1=(0-0)-1,$$

and it is not commutative because

$$1-0=1\neq -1=0-1.$$

Examples 1.4. We fix an integer $n\neq 0$ .For any integer a, we write $[a]_n$ or $\overline{a}^n$ for the class $a+n\mathbb{Z}$ of a modulo n. We often omit n from this notation when it is fixed and clear from context, and simply write $[a]$ or $\overline{a}$. (At some point we will simply drop the bracket and just write a.) We recall that one then has

$$\mathbb{Z}/n\mathbb{Z}=\{[a]:a\in\mathbb{Z}\}.$$

(i) We define a binary operation $+$ on $\mathbb{Z}/n\mathbb{Z}$ by setting

$$[a]+[b]:=[a+b].$$

This is a well-defined function

$$\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$$

because if $[a]=[a']$ and $[b]=[b']$ then $a=a'+na''$ and $b=b'+nb''$ so

$$[a]+[b]=[a+b]=[a'+na''+b'+nb'']=[a'+b'+n(a''+b'')]=[a'+b']=[a']+[b'].$$

(ii) We can define a binary operation $\cdot$ on $\mathbb{Z}/n\mathbb{Z}$ by setting

$$[a]\cdot[b]:=[a\cdot b].$$

This is a well-defined function

$$\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$$

because if $[a]=[a']$ and $[b]=[b']$ then $a=a'+na''$ and $b=b'+nb''$ so

$$[a]\cdot[b]=[a\cdot b]=[(a'+na'')\cdot(b'+nb'')]=[a'\cdot b'+n(a'b''+a''b'+na''b'')]=[a'\cdot b']=[a']\cdot[b'].$$

Exercise 1.5. Prove that the binary operations $+$ and $\cdot$ on $\mathbb{Z}/n\mathbb{Z}$ are both associative and commutative.

1.1.2. *The definition.*

Definition 1.6. A group is a pair $(G,\star)$ comprising a set G and a binary operation $\star$ on G that satisfy the following axioms:

(G1) $\star$ is associative.

(G2) There exists an element e of G, the 'identity element' of G, with the property that

$$g\star e=g=e\star g$$

for every $g\in G$.

(G3) For every element g of G, there exists an associated element g^{-1} of G, the 'inverse element' of g, with the property that

$$g\star g^{-1}=e=g^{-1}\star g.$$

Notation 1.7. We often omit $\star$ when no ambiguity is possible and simply say that the set G is a group.

Definition 1.8.
(i) A group $(G, \star)$ is 'abelian', or commutative, if $\star$ is commutative.
(ii) A group $(G, \star)$ is finite if G is finite.

Examples 1.9.
(i) We know from Example 1.3(ii) that $(\mathbb{Z}, -)$ is not a group, because $-$ is not associative.
(ii) The pair $(\mathbb{Z}, +)$ is an abelian group, with identity element 0 and inverse element $-a$ for each $a \in \mathbb{Z}$. We often abbreviate $(\mathbb{Z}, +)$ to $\mathbb{Z}$.

However, neither of the pairs $(\mathbb{Z}, \cdot)$ or $(\mathbb{Z} \setminus \{0\}, \cdot)$ are groups, because the identity element would have to be 1, but there is no integer a satisfying $2 \cdot a = 1$, so 2 cannot have an associated inverse element.
(iii) Let F be $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. The pair $(F, +)$ is an abelian group, with identity element 0 and inverse element $-q$ for each $q \in F$. We often abbreviate $(F, +)$ to F.

The pair $(F, \cdot)$ is not a group, because the identity element would have to be 1, but there is no q in F satisfying $0 \cdot q = 1$, so 0 cannot have an associated inverse element.

The pair $(F \setminus \{0\}, \cdot)$ is an abelian group, with identity element 1 and inverse element q^{-1} for each $q \in F \setminus \{0\}$. We often abbreviate $(F \setminus \{0\}, \cdot)$ to F^*.
(iv) Any vector space V together with its addition operation $+$ is an abelian group.
(v) Fix an integer $n \neq 0$. The class $[0]$ is the identity element of $(\mathbb{Z}/n\mathbb{Z}, +)$ because

$$[a] + [0] = [a + 0] = [a] = [0 + a] = [0] + [a]$$

and, for any $[a]$ in $\mathbb{Z}/n\mathbb{Z}$, we have the associated inverse element $[-a]$, because

$$[a] + [-a] = [a + (-a)] = [0] = [(-a) + a] = [-a] + [a].$$

We set $0 := [0]$ and $-[a] := [-a]$. We often abbreviate $(\mathbb{Z}/n\mathbb{Z}, +)$ to $\mathbb{Z}/n\mathbb{Z}$. By Exercise 1.5, we know that $\mathbb{Z}/n\mathbb{Z}$ is a finite abelian group.
(vi) Fix an integer $n \neq 0, 1, -1$.

(a) The pair $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is never a group: the identity element would have to be $[1]$, but if $[0] \cdot [a] = [1]$ then $[1] = [0]$, which is always false. So $[0]$ cannot have an inverse element.

(b) The pair $((\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]\}, \cdot)$ is a group if and only if $|n|$ is a prime number (see Exercise 1.10 below).

(c) We may define a subset

$$(\mathbb{Z}/n\mathbb{Z})^\times := \{[a] : \text{ there exists } b \in \mathbb{Z} \text{ such that } [a] \cdot [b] = [1]\}$$

of $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$. We see first that $(\mathbb{Z}/n\mathbb{Z})^\times$ is closed under $\cdot$: indeed, if $[a] \cdot [b] = [1]$ and $[a'] \cdot [b'] = [1]$ then

$$([a] \cdot [a']) \cdot ([b'] \cdot [b]) = (([a] \cdot [a']) \cdot [b']) \cdot [b] = ([a] \cdot ([a'] \cdot [b'])) \cdot [b] = ([a] \cdot [1]) \cdot [b] = [a] \cdot [b] = [1],$$

so $[a] \cdot [a']$ belongs to $(\mathbb{Z}/n\mathbb{Z})^\times$. Here we have used that $\cdot$ is associative, by Exercise 1.5.

The class $[1]$ is the identity element of $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ because

$$[a] \cdot [1] = [a \cdot 1] = [a] = [1 \cdot a] = [1] \cdot [a].$$

Also, by the definition definition of $(\mathbb{Z}/n\mathbb{Z})^\times$, and the fact that $\cdot$ is commutative by Exercise 1.5, we know that every element of $(\mathbb{Z}/n\mathbb{Z})^\times$ has an associated inverse element.

We set $1 := [1]$. We often abbreviate $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ to $(\mathbb{Z}/n\mathbb{Z})^\times$. We note once again that, by Exercise 1.5, we know that $\cdot$ is associative and commutative. Therefore $(\mathbb{Z}/n\mathbb{Z})^\times$ is a finite abelian group.

(vii) Any set with cardinality equal to 1 is clearly a group. We identify all such groups and refer to them as 'the trivial group'. We say that a group is 'non-trivial' if it has cardinality greater than 1.

Exercise 1.10. Fix an integer $n \neq 0, 1, -1$.

(i) Prove that, if p is a prime number, then $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \{[0]\}$.

(ii) Prove that, if an integer $m \neq \pm 1, \pm n$ divides n, then the element $[m]$ of $(\mathbb{Z}/n\mathbb{Z}) \setminus \{[0]\}$ cannot have an associated inverse element with respect to $\cdot$.

(iii) Justify claim (vi)(b) of Examples 1.9.

(iv) Show that $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] : (a, n) = 1\}$.

(v) Use the Euclidean Algorithm to find $[13]_{20}^{-1}$.

1.1.3. *First properties.* You may have noticed that above we have referred to *the* identity element of a group, or *the* inverse element of a given element of a group. We now justify this terminology by proving their uniqueness.

Proposition 1.11. *Let $(G, \star)$ be a group.*

(i) *There is a unique identity element e of G satisfying condition* (G2)*.*

(ii) *If $g \star f = g$ for every $g \in G$ then $f = e$.*

(iii) *If $f \star g = g$ for every $g \in G$ then $f = e$.*

(iv) *If $g_1 \star g_3 = g_2 \star g_3$ then $g_1 = g_2$.*

(v) *If $g_1 \star g_2 = g_1 \star g_3$ then $g_2 = g_3$.*

(vi) *For each $g \in G$, there is a unique inverse element g^{-1} of g satisfying condition* (G3)*.*

(vii) *$(g^{-1})^{-1} = g$ for all $g \in G$.*

(viii) *If $g \star g' = e$ then $g' = g^{-1}$.*

(ix) *If $g' \star g = e$ then $g' = g^{-1}$.*

(x) *$(g \star j)^{-1} = j^{-1} \star g^{-1}$ for all $g, j \in G$.*

(xi) *G is abelian if and only if $(g \star j)^{-1} = g^{-1} \star j^{-1}$ for all $g, j \in G$.*

Proof. If e and e' are identity elements of G then

$$e = e \star e' = e',$$

where the first equality follows from applying (G2) to e' and the second equality from applying (G2) to e. This proves claim (i).

Claim (ii) holds because $f = e \star f = e$.

Claim (iii) holds because $f = f \star e = e$.

Claim (iv) holds because

$$g_1 = g_1 \star e = g_1 \star (g_3 \star g_3^{-1}) = (g_1 \star g_3) \star g_3^{-1} = (g_2 \star g_3) \star g_3^{-1} = g_2 \star (g_3 \star g_3^{-1}) = g_2 \star e = g_2.$$

Claim (v) holds because

$$g_2 = e \star g_2 = (g_1^{-1} \star g_1) \star g_2 = g_1^{-1} \star (g_1 \star g_2) = g_1^{-1} \star (g_1 \star g_3) = (g_1^{-1} \star g_1) \star g_3 = e \star g_3 = g_3.$$

Fix $g \in G$. If $g \star g' = e$ and $g \star g'' = e$ then in particular $g \star g' = g \star g''$. Claim (v) thus implies that $g' = g''$. This proves claim (vi).

The equality in condition (G3) is symmetric, so it states that any element g of G is the inverse $(g^{-1})^{-1}$ of g^{-1}, as required to prove claim (vii).

Claim (viii) holds because if $g \star g' = e = g \star g^{-1}$ then claim (v) implies that $g' = g^{-1}$.

Claim (ix) holds because if $g' \star g = e = g^{-1} \star g$ then claim (iv) implies that $g' = g^{-1}$.

Claim (x) holds follows from applying claim (viii) to the equality

$$(g \star j) \star (j^{-1} \star g^{-1}) = ((g \star j) \star j^{-1}) \star g^{-1} = (g \star (j \star j^{-1})) \star g^{-1} = (g \star e) \star g^{-1} = g \star g^{-1} = e.$$

We finally consider claim (xi). By claim (x), we must prove that G is abelian if and only if $j^{-1} \star g^{-1} = g^{-1} \star j^{-1}$ for all $g, j \in G$. It is clear that if G is abelian, then the latter condition holds.

On the other hand, if $j^{-1} \star g^{-1} = g^{-1} \star j^{-1}$ then

$$g \star j = (g^{-1})^{-1} \star (j^{-1})^{-1} = (j^{-1} \star g^{-1})^{-1} = (g^{-1} \star j^{-1})^{-1} = (j^{-1})^{-1} \star (g^{-1})^{-1} = j \star g,$$

so G is abelian. Here the first and fifth equalities follow from claim (vii) while the second and fourth equalities follow from claim (x).

□

Notation 1.12.
(i) In the sequel, for an abstract group G, we will mostly stop using the very distinctive notation $\star$ for its binary operation and, unless explicitly stated otherwise, this operation will be denoted by $\cdot$. In addition, the identity element of $(G, \cdot)$ will be denoted by 1 instead of by e. In fact, we will often drop the binary operation completely from certain notations, so for instance we will feel justified in simply writing gg' rather that $g \cdot g'$ for the evaluation under $\cdot$ of a pair of elements g, g' of G.

Sometimes, if the group G is abelian and we believe there is a pedagogical advantage to this, we will instead write $+$ for its binary operation. In any such cases, we will always denote by 0 the identity element of $(G, +)$ and write $-g$ for the inverse element of any $g \in G$.
(ii) Now that we are familiar with the associative property of binary operations, we will often stop writing brackets around pairs of elements of a group G whenever no ambiguity is possible. In fact, by an easy induction argument, the associative property of $\cdot$ implies that for any finite family $g_1, g_2, \ldots, g_{n-1}, g_n$ of elements of G, the evaluation

$$g_1 g_2 \cdots g_{n-1} g_n \in G \tag{3}$$

is independent of how the expression is bracketed, and thus we will simply use this unbracketed notation. We will also sometimes write $\prod_{i=1}^{i=n} g_i$ for the expression (3).

In particular, for an element $g \in G$ and a natural number $n \in \mathbb{N}$ we will write g^n for the element $gg \ldots gg$, where g occurs n times. We also set $g^{-n} := (g^{-1})^n$ and $g^0 := 1$.

Example 1.13. It is clear from the associative property that, for any $g_1, g_2, g_3, g_4 \in G$, one has

$$((g_1 g_2) g_3) g_4 = (g_1 g_2)(g_3 g_4) = g_1 (g_2 (g_3 g_4)) = g_1 ((g_2 g_3) g_4) = (g_1 (g_2 g_3)) g_4,$$

so we do not need to distinguish between any of these expressions

Exercise 1.14. Show that $g^{-n} = (g^n)^{-1}$.

1.1.4. *Orders and group tables.* Recalling Fermat's Little Theorem (1), we see that it is a statement concerning an exponent n for which elements all a of $(\mathbb{Z}/p\mathbb{Z})^\times$ satisfy $a^n = 1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Specifically, it states that $n = p - 1$ is such an exponent.

In a general group G and for an arbitrary element g in G, we will be interested in studying the exponents n for which g^n is equal to the identity element of G, or whether such an n exists. It is clear that if $g^n = 1$ and $n \mid m$, then $g^m = (g^n)^{m/n} = 1^{m/n} = 1$. For this reason, in the following definition, we associate to g the smallest such exponent, if one exists.

Definition 1.15.
(i) The 'order' of a finite group G is its cardinality, which we shall always denote by $|G| \in \mathbb{N}$. We thus may say that a finite group 'has finite order'. Otherwise we say that it 'has infinite order'.
(ii) Let g be an element of a group G. Then the 'order of g' is the smallest natural number n with the property that $g^n = 1$, if such a number exists. In particular we then say that g 'has finite order'. If no such number exists, then we say that the order of g is the symbol ∞, and that g 'has infinite order'.

We denote by $\mathrm{o}(g)$ or by $|g|$ the order of g, so that this is an element of $\mathbb{N} \cup \{\infty\}$.

Remark 1.16. Clearly one has $\mathrm{o}(g) = 1$ if and only if $g = 1$.

Exercise 1.17.
(i) Prove that every element of $\mathbb{Z}$, except for the identity 0, has infinite order. Prove that every element of $\mathbb{Q}$, except for the identity 0, has infinite order.
(ii) In $\mathbb{Q}^*$, show that one has

$$\mathrm{o}(q) = \begin{cases} 1, & q = 1, \\ 2, & q = -1, \\ \infty, & q \neq 1, -1. \end{cases}$$

Show that the same equality holds in $\mathbb{R}^*$. Can you find an element $z \neq 1, -1$ of $\mathbb{C}^*$ that has finite order?
(iii) In $\mathbb{Z}/9\mathbb{Z}$, show that

$$\mathrm{o}([0]) = 1, \mathrm{o}([1]) = 9, \mathrm{o}([2]) = 9, \mathrm{o}([3]) = 3, \mathrm{o}([4]) = 9, \mathrm{o}([5]) = 9, \mathrm{o}([6]) = 3, \mathrm{o}([7]) = 9, \mathrm{o}([8]) = 9.$$

(iv) Recall from Exercise 1.10(i) that $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \{[0]\}$ for any prime number p.

(a) In $(\mathbb{Z}/3\mathbb{Z})^\times$, show that $\mathrm{o}([1]) = 1$ and $\mathrm{o}([2]) = 2$.
(b) In $(\mathbb{Z}/5\mathbb{Z})^\times$, show that $\mathrm{o}([1]) = 1, \mathrm{o}([2]) = 4, \mathrm{o}([3]) = 4$ and $\mathrm{o}([4]) = 2$.
(c) In $(\mathbb{Z}/7\mathbb{Z})^\times$ show that $\mathrm{o}([2]]) = 3$ and that $\mathrm{o}([3]) = 6$.

Definition 1.18. Let G be a finite group of order n. Fix a bijection between G and $\{1, \dots, n\}$ and use it to write the elements of G as

$$G = \{g_1, g_2, \dots, g_n\},$$

ensuring that $g_1 = 1$ (the identity element). The 'group table' of G is the $n \times n$-matrix with coefficients in G whose (i, j)-entry is the element $g_i g_j$ of G.

Remark 1.19. The group table of G is symmetric if and only if G is abelian!

Exercise 1.20.
(i) Let $G = \{g_1, g_2\}$ (with $g_1 = 1$) be any group of order 2. Write down the group table of G.
(ii) Let $G = \{g_1, g_2, g_3\}$ (with $g_1 = 1$) be any group of order 3. Write down the group table of G.

1.1.5. *The direct product of two groups.* As we know, to an arbitrary pair of sets S and T one can associate naturally a new set, the cartesian product $S \times T$. It will be very useful to observe that to an arbitrary pair of groups G and J we can also naturally associate a new group, simply by giving the obvious structure to the set $G \times J$ as follows.

Definition 1.21. If $(G, \star_G)$ and $(J, \star_J)$ are groups, we define their 'direct product' to be the pair $(G \times J, \star_{G\times J})$, where $\star_{G\times J}$ is the binary operation

$$(G \times J) \times (G \times J) \to G \times J$$

on $G \times J$ defined by

$$(g, j) \star_{G\times J} (g', j') := (g \star_G g', j \star_J j').$$

Lemma 1.22. *The following claims are valid.*

(i) *The direct product of two groups G and J is a group.*
(ii) *The direct product of G and J is abelian if and only if both G and J are abelian.*
(iii) *The direct product of G and J is finite if and only if both G and J are finite.*

Proof. To prove claim (i) we first note that the binary operation $\star := \star_{G\times J}$ is associative because

$$\begin{aligned}(g, j) \star ((g', j') \star (g'', j'')) =&(g, j) \star (g' \star_G g'', j' \star_J j'')\\ =&(g \star_G (g' \star_G g''), j \star_J (j' \star_J j''))\\ =&((g \star_G g') \star_G g'', (j \star_J j') \star j'')\\ =&(g \star_G g', j \star_J j') \star (g'', j'')\\ =&((g, j) \star (g', j')) \star (g'', j'').\end{aligned}$$

Here the third equality holds because both $\star_G$ and $\star_J$ are associative.

If e_G is the identity of G and e_J is the identity of J then

$$e_{G\times J} := (e_G, e_J) \in G \times J$$

is the identity element because

$$(g, j) \star (e_G, e_J) = (g \star_G e_G, j \star_J e_J) = (g, j)$$

for every $(g, j) \in G \times J$, and because we may apply Proposition 1.11 (ii) to these equalities.

Fix an element (g, j) of $G \times J$. We claim that

$$(g, j)^{-1} := (g^{-1}, j^{-1}) \in G \times J$$

is the inverse of (g, j). Indeed, this follows from applying Proposition 1.11 (viii) to the equality

$$(g, j) \star (g^{-1}, j^{-1}) = (g \star_G g^{-1}, j \star_J j^{-1}) = (e_G, e_J) = e_{G\times J}.$$

This completes the proof of claim (i).

To prove claim (ii) we first assume that both G and J are abelian. Then for any $(g, j), (g', j') \in G \times J$ one has

$$(g, j) \star (g', j') = (g \star_G g', j \star_J j') = (g' \star_G g, j' \star_J j) = (g', j') \star (g, j),$$

so $G \times J$ is abelian.

We now assume that $G \times J$ is abelian. Then for any $g, g' \in G$ one has

$$(g \star_G g', e_J) = (g, e_J) \star (g', e_J) = (g', e_J) \star (g, e_J) = (g' \star_G g, e_J),$$

so we must also have that $g \star_G g' = g' \star_G g$. This proves that G is abelian.

Similarly, for any $j, j' \in J$ one has

$$(e_J, j \star_J j') = (e_G, j) \star (e_G, j') = (e_G, j') \star (e_G, j) = (e_G, j' \star_J j),$$

so we must also have that $j \star_J j' = j' \star_J j$, and thus that J is abelian. This concludes the proof of claim (ii).

Claim (iii) is trivial, since we know that the set $G \times J$ is finite if and only if both of the sets G and J are finite. □

1.2. **Examples.** In this section we give further examples of groups, some of which will play crucial roles in later sections.

1.2.1. *Symmetric groups.* For a non-empty set Ω, a permutation of Ω is a bijective function that has Ω as both its domain and its codomain. We write S_Ω for the set of permutations of Ω.

We define a binary operation $\circ$ on S_Ω through the composition of functions. Explicitly, for a pair (σ, τ) in $S_\Omega \times S_\Omega$, the function

$$\sigma \circ \tau : \Omega \to \Omega$$

is defined by

$$(\sigma \circ \tau)(\omega) := \sigma\big(\tau(\omega)\big)$$

for every $\omega \in \Omega$. It is clear that, since both σ and τ are bijective, the composition $\sigma \circ \tau$ is also bijective, and hence that $\sigma \circ \tau$ is a permutation in S_Ω.

The operation $\circ$ is associative because composition of functions is always associative:

$$(\rho \circ (\sigma \circ \tau))(\omega) = \rho((\sigma \circ \tau)(\omega)) = \rho(\sigma(\tau(\omega))) = (\rho \circ \sigma)(\tau(\omega)) = ((\rho \circ \sigma) \circ \tau)(\omega)$$

for every $\rho, \sigma, \tau \in S_\Omega$ and every $\omega \in \Omega$.

We have the identity permutation, denoted by 1_Ω or id_Ω (or simply 1 or id if Ω is clear from context), and defined by $1_\Omega(\omega) = \omega$ for each $\omega \in \Omega$. Clearly

$$(1_\Omega \circ \sigma)(\omega) = \sigma(\omega) = (\sigma \circ 1_\Omega)(\omega)$$

for any $\sigma \in S_\Omega$.

Since every permutation $\sigma \in S_\Omega$ is by definition bijective, it has a two-sided inverse (bijective) function $\sigma^{-1} : \Omega \to \Omega$ for which

$$\sigma \circ \sigma^{-1} = 1_\Omega = \sigma^{-1} \circ \sigma.$$

This function is thus a permutation σ^{-1} which is the inverse element of σ.

Definition 1.23. For any given non-empty set Ω, the group $(S_\Omega, \circ)$ is called the 'symmetric group on Ω'.

Exercise 1.24. Let Ω be the set $\{1, 2, 3\}$. Decide whether the symmetric group on Ω is or not abelian. (If necessary, write down the group table of S_Ω.)

Definition 1.25. Let n be a natural number and set $\Omega_n := \{1, \ldots, n\}$. We abbreviate S_{Ω_n} to S_n and we also call S_n the 'symmetric group of degree n'.

Lemma 1.26. $|S_n| = n!$.

Proof. A function $\sigma : \Omega_n \to \Omega_n$ is bijective if and only if it is injective because Ω_n is a finite set. So we simply need to count how many injective functions σ exist.

The injective function σ can map 1 to any of the n elements of Ω_n; $\omega(2)$ can then be any element of Ω_n except for $\sigma(1)$, so there are $n-1$ possibilities for $\sigma(2)$; $\omega(3)$ can then be any element of Ω_n except for $\sigma(1)$ and $\sigma(2)$, so there are $n-2$ possibilities for $\sigma(3)$; and so on.

In this way, it is easy to see that there are $n(n-1)(n-2)\ldots 2 \cdot 1 = n!$ possible injective functions from Ω_n into itself. This proves the Lemma. □

Notation 1.27. We introduce two different ways to denote the elements of S_n.

(i) We sometimes denote $\sigma \in S_n$ by

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

(ii) We shall often also use 'cycle decomposition' to denote elements of S_n. Let $m \leq n$ and let $a_1, \ldots, a_m$ be m *distinct* elements of Ω_n. Then the 'm-cycle' $(a_1, \ldots, a_m)$ is the element of S_n defined by

$$a_i \mapsto a_{i+1} \text{ for each } 1 \leq i \leq m-1 \text{ and } a_m \mapsto a_1.$$

We also say that the cycle $(a_1, \ldots, a_m)$ has 'length' m.

An m-cycle $(a_1, \ldots, a_m)$ and an m'-cycle $(b_1, \ldots, b_{m'})$ are said to be 'disjoint' if $a_i \neq b_j$ for every i and j.

It is easy to see that every element of S_n is a composition of disjoint cycles, called its cycle decomposition. See the table on [2, page 30] for the algorithm that gives the cycle decomposition of any element of S_n.

The cycle decomposition is unique up to re-ordering, but please note that

$$(a_1, \ldots, a_m) = (a_m, a_1, \ldots, a_{m-1}) = (a_{m-1}, a_m, a_1, \ldots, a_{m-2}) = \ldots = (a_2, a_3, \ldots, a_m, a_1)$$

and also that, if an m-cycle $\underline{c_m}$ and an m'-cycle $\underline{d_{m'}}$ are disjoint, then

$$\underline{c_m} \circ \underline{d_{m'}} = \underline{d_{m'}} \circ \underline{c_m}. \tag{4}$$

(iii) A cycle of length 2 is also called a 'transposition'. One may also write every element of S_n as a composition of transpositions. Such an expression is **not** unique, but there is a well-defined function $\mathrm{sgn} : S_n \to \{\pm 1\}$, the 'sign of a permutation', where $\mathrm{sgn}(\sigma)$ is given by $(-1)^{t(\sigma)}$ where $t(\sigma)$ is the number of transpositions in *any* expression of σ as a composition of transpositions. In other words, for a given permutation σ, either every such expression has an even number of transpositions, or every such expression has an odd number of transpositions.

We say that σ is even, resp. odd, if $t(\sigma)$ is even, resp. odd, or equivalently, if $\mathrm{sgn}(\sigma) = 1$, resp. $\mathrm{sgn}(\sigma) = -1$.

Example 1.28. Let $\sigma \in S_{13}$ be the permutation

$$\sigma(1) = 12, \sigma(2) = 13, \sigma(3) = 3, \sigma(4) = 1, \sigma(5) = 11, \sigma(6) = 9, \sigma(7) = 5,$$
$$\sigma(8) = 10, \sigma(9) = 6, \sigma(10) = 4, \sigma(11) = 7, \sigma(12) = 8, \sigma(13) = 2.$$

Then the cycle decomposition of σ is

$$\sigma = (1, 12, 8, 10, 4) \circ (2, 13) \circ (3) \circ (5, 11, 7) \circ (6, 9).$$

As discussed in Notation 1.12 that we will usually omit the binary operation (in this case, $\circ$) from the notation. In addition, any 1-cycle is just the identity permutation, so for instance we may remove the 1-cycle $(3) = \mathrm{id}$ from the above expression without changing it. So we will instead write the cycle decomposition of σ as

$$\sigma = (1, 12, 8, 10, 4)(2, 13)(5, 11, 7)(6, 9). \tag{5}$$

Exercise 1.29. Show that the inverse element σ^{-1} of the permutation σ given in (5) is

$$\sigma^{-1} = (1, 4, 10, 8, 12)(2, 13)(5, 7, 11)(6, 9).$$

Exercise 1.30. We know that $|S_3| = 3! = 6$. Show that the cycle decompositions of all elements of S_3 are

$$g_1 = \mathrm{id}, \;\; g_2 = (1, 2), \;\; g_3 = (1, 3), \;\; g_4 = (2, 3), \;\; g_5 = (1, 2, 3), \;\; g_6 = (1, 3, 2).$$

Write down the group table of S_3.

Exercise 1.31. Show that S_4 is not abelian.

Exercise 1.32. Let $n \geq 3$. A similar argument to the one you just used for S_4 would show that, in fact, S_n is not abelian.

Remark 1.33. We mentioned above that the cycle decomposition of a permutation is unique up to re-ordering but, of course, this is true because we imposed that it is a composition of *disjoint* cycles. There are certainly multiple ways to write a permutation as a product of arbitrary cycles: for instance in S_3 one has

$$(1, 2, 3) = (1, 2)(2, 3).$$

The cycles $(1, 2)$ and $(2, 3)$ are not disjoint, and it is only the left-hand side of this equality that gives the cycle decomposition of the permutation.

We will study symmetric groups in more depth in §4. In particular, see §4.1.1 for some results on the order of permutations.

1.2.2. *Dihedral groups.* In this section we fix $n \geq 3$. Then there is an important construction of certain subsets D_{2n} of S_n that are closed under $\circ$ and for which the pair $(D_{2n}, \circ)$ is also a group (in the terminology of §2.1 below, this means that D_{2n} is a 'subgroup' of S_n). Part of the importance of the group D_{2n} is that it has a geometric interpretation as the 'group of symmetries of the regular n-gon'.

In fact, this last sentence already defines D_{2n}. Fix a labelling of the vertices of the regular n-gon by the numbers in $\Omega_n := \{1, 2, \ldots, n\}$. Then each symmetry s of the regular n-gon *permutes* the vertices and therefore uniquely defines a permutation s of Ω_n, which is the same as saying an element s of S_n. Specifically, if the symmetry s puts vertex i in the place where vertex j was originally, then $s(i) = j$ for the corresponding element s of S_n.

Definition 1.34. We have thus defined a subset

$$D_{2n} := \{ \text{ symmetries of the regular } n - \text{gon } \} \subseteq S_n.$$

We call D_{2n} the 'dihedral group of order $2n$'.

Remark 1.35. One always has $|D_{2n}| = 2n$, so this terminology is consistent. From this fact we also see, because $2n \neq n!$ for all $n \geq 4$, that the inclusion $D_{2n} \subset S_n$ is always strict for such n, meaning that there are permutations in S_n that do not define a symmetry of the regular n-gon. However, $2 \cdot 3 = 3!$ so $D_6 = S_3$.

It is clear from the geometric interpretation that the composition of two symmetries of the regular n-gon is also a symmetry of the regular n-gon, that the identity symmetry is the identity element with respect to composition, and that any symmetry has an inverse element given by the symmetry obtained by reversing the motion. Therefore $(D_{2n}, \circ)$ is indeed a group.

Remark 1.36. Some references denote the dihedral group of order $2n$ by D_n rather than by D_{2n} since, as we already noted, the number of vertices is always half the number of symmetries.

See the explanation in [2, page 24] to justify the fact that $|D_{2n}| = 2n$, or come up with your own geometric explanation.

Notation 1.37. Fix a regular n-gon centered at the origin of the plane and fix a consecutive labelling of the vertices, from 1 to n, in a clockwise manner. Let r denote the clockwise rotation abound the origin through $2\pi/n$. Let s denote the reflexion about the line of symmetry through vertex 1 and the origin. It is then easy to see that:

(i) The elements 1, r, r^2, r^3, $\ldots$, r^{n-1} are all distinct, but $r^n = 1$. In particular, $\mathrm{o}(r) = n$.

(ii) $s \neq 1$ but $s^2 = 1$, so $\mathrm{o}(s) = 2$.

(iii) r^i is never equal to s for any exponent i.

(iv) $s \circ r^i \neq s \circ r^j$ for any $i \neq j$ with $1 \leq i, j \leq n-1$, so

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-2}, r^{n-1}, s, s \circ r, s \circ r^2, \ldots, s \circ r^{n-2}, s \circ r^{n-1}\}. \tag{6}$$

In other words, each element of D_{2n} may be written *uniquely* in the for $s^k r^i$ for some $k \in \{0, 1\}$ and some $i \in \{0, 1, \ldots, n-1\}$.

(v) $r \circ s = s \circ r^{n-1} = s \circ r^{-1}$ and, in particular, since $r \neq r^{-1}$ and using Proposition 1.11(v), we see that the group D_{2n} is never abelian.

(vi) $r^i \circ s = s \circ r^{-i} = s \circ (r^i)^{-1}$ for each $0 \leq i \leq n$.

Exercise 1.38. Prove claims (i)-(vi) in each of the cases $n = 3$ and $n = 4$.

Exercise 1.39. In D_{24}, write the element sr^9sr^6 in the form (6).

Remark 1.40. The rotation r uniquely defines the cycle $r = (1, 2, \ldots, n)$ in S_n. The symmetry s uniquely defines the permutation

$$s = \begin{cases} (2, n)(3, n-1)(4, n-2) \ldots (\frac{n}{2}, \frac{n}{2} + 2), & \text{n is even,} \\ (2, n)(3, n-1)(4, n-2) \ldots (\frac{n+1}{2}, \frac{n+3}{2}), & \text{n is odd,} \end{cases}$$

in S_n.

One can thus fully ignore the geometric interpretation and simply define D_{2n} by these two equalities together with the equality (6).

Exercise 1.41. Ignoring the geometric interpretation, use the previous Remark to write down all the elements of D_8. Then prove that $D_8 \subset S_4$ is closed under $\circ$ and also to verify that every element of D_8 has an inverse element. Write down all the elements of D_{10} too and prove the same things for $D_{10} \subset S_5$.

1.2.3. *General linear groups.* Fix $n \in \mathbb{N}$, let F denote either $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ and write $M_n(F)$ for the set of $n \times n$-matrices with entries in F. We set

$$\mathrm{Gl}_n(F) := \{A \in M_n(F) : \det(A) \neq 0\}.$$

Then, althought $(M_n(F), \cdot)$ is **not** a group (where $\cdot$ is the usual matrix multiplication), precisely because the matrices with trivial determinant do not have an inverse, the pair $(\mathrm{Gl}_n(F), \cdot)$ is a group.

To see this, we recall that $\cdot$ is a binary operation on $M_n(F)$ that is also associative. We must show that $\mathrm{Gl}_n(F)$ is closed under $\cdot$. But if $A, B \in \mathrm{Gl}_n(F)$ then $\det(A \cdot B) = \det(A)\det(B) \neq 0$.

Since the identity matrix $I = I_n$ clearly belongs to $\mathrm{Gl}_n(F)$ and since every element A of $\mathrm{Gl}_n(F)$ has an inverse matrix A^{-1} that must necessarily also belong to $\mathrm{Gl}_n(F)$, it is clear that $(\mathrm{Gl}_n(F), \cdot)$ is a group.

Definition 1.42. The group $\mathrm{Gl}_n(F)$ is called the 'general linear group of degree n'.

Because F is an infinite set, it is very easy to see that $\mathrm{Gl}_n(F)$ is not a finite group. In addition, it is well-known that it is not an abelian group.

Exercise 1.43. Prove that $\mathrm{Gl}_2(F)$ is not abelian.

Remark 1.44. For any prime number p, the set $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ together with the two binary operations $+$ and $\cdot$ is also a 'field', and everything discussed in this section works exactly in the same way for $F = \mathbb{F}_p$. Since $\mathbb{F}_p$ is finite, it is immediately clear that $\mathrm{Gl}_n(\mathbb{F}_p)$ must be a finite group. In fact, one may prove that

$$|\mathrm{Gl}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1}).$$

1.2.4. *The quaternion group of order 8.* The quaternion group of order 8 is

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

with the binary operation $\cdot$ defined by $1x = 1 = x1$ for all $x \in Q_8$, $(-1)(-1) = 1$, $(-1)x = -x = x(-1)$ for all $x \in Q_8$,

$$ii = jj = kk = -1,\ ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ki = j,\ ik = -j.$$

It is quite tedious to verify directly that this binary operation is associative. Once this is achieved, it is clear that Q_8 is a (finite, non-abelian) group of order 8.

1.3. **Homomorphisms.**

1.3.1. *Definition and first properties.*

Definition 1.45. Let $(G, \star_G)$ and $(H, \star_H)$ be groups. Then a function $f : G \to H$ is a 'homomorphism' if

$$f(g_1 \star_G g_2) = f(g_1) \star_H f(g_2) \tag{7}$$

for every $g_1, g_2 \in G$.

Notation 1.46. We also say that such a function f is a 'homomorphism of groups' or a 'group homomorphism'. Following Notation 1.12 we usually just write the displayed condition (7) as $f(g_1g_2) = f(g_1)f(g_2)$, so please always keep in mind that in the left-hand side of this equality we are operating in G, while in the right-hand side we are operating in H.

Exercise 1.47. Prove by induction that if $f : G \to H$ is a homomorphism and $g_1, \ldots, g_n$ are elements of G, then

$$f(\prod_{i=1}^{i=n} g_i) = \prod_{i=1}^{i=n} f(g_i).$$

Lemma 1.48. *If $f : G \to H$ is a homomorphism then $f(e_G) = e_H$ and, for any $g \in G$, $f(g)^{-1} = f(g^{-1})$.*

Proof. For any given $g \in G$ we have $f(g)f(e_G) = f(ge_G) = f(g) = f(g)e_H$ so, by Proposition 1.11 (v), we find $f(e_G) = e_H$.

We now fix $g \in G$ and simply note that $f(g)f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$, so by Proposition 1.11 (viii) we find that $f(g)^{-1} = f(g^{-1})$. □

Exercise 1.49. Show that the function $f : G \to H$ given by $f(g) = e_H$ for every g in G is a homomorphism. This is called the 'trivial' homomorphism from G to H.

1.3.2. *Isomorphisms.*

Definition 1.50. A function $f : G \to H$ is an 'isomorphism' if it is a homomorphism that is also bijective.

Notation 1.51. We sometimes use the notation $f : G \xrightarrow{\sim} H$ or the notation $f : G \cong H$ to indicate that f is an isomorphism. We also say that such a function f is an 'isomorphism of groups' or a 'group isomorphism'.

Definition 1.52. A group G is 'isomorphic' to a group H if there exists an isomorphism $f : G \to H$. In this case we write $G \cong H$.

Lemma 1.53. *The relation $G \cong H$ is an equivalence relation.*

In particular, we may say that G and H are isomorphic, or of the same isomorphism type, or in the same isomorphism class.

Proof. The identity function $\mathrm{id}_G : G \to G$ is clearly an isomorphism, so $G \cong G$.

If $f : G \to H$ is an isomorphism, we claim that the inverse function f^{-1} is a homomorphism. For any $h_1, h_2 \in H$ we have

$$f(f^{-1}(h_1h_2)) = h_1h_2 = f(f^{-1}(h_1))f(f^{-1}(h_2)) = f(f^{-1}(h_1)f^{-1}(h_2)), \tag{8}$$

where the last equality holds because f is a homomorphism.

But, since f is injective, the displayed equality (8) implies that $f^{-1}(h_1h_2) = f^{-1}(h_1)f^{-1}(h_2)$, so we have proved that f^{-1} is a homomorphism. We know that f^{-1} is always bijective. We have therefore proved that if $G \cong H$ then $H \cong G$.

We finally assume to be given isomorphisms of groups $f : G \cong H$ and $f' : H \cong I$. It is clear that $f' \circ f : G \to I$ is bijective, so we must only prove that $f' \circ f$ is a homomorphism to deduce that $f' \circ f : G \cong H$, and thus that $\cong$ is a transitive relation.

The fact that $f' \circ f$ is a homomorphism now follows from the equalities

$$(f' \circ f)(g_1g_2) = f'(f(g_1g_2)) = f'(f(g_1)f(g_2)) = f'(f(g_1))f'(f(g_2)) = (f' \circ f)(g_1)(f' \circ f)(g_2) \tag{9}$$

for any elements $g_1, g_2 \in G$. Here the second equality holds because f is a homomorphism and the second equality holds because f' is a homomorphism. □

Remark 1.54. We note for later use that the argument (9) shows that, for any homomorphisms of groups $f : G \to H$ and $f' : H \to I$, the composition $f' \circ f : G \to I$ is also a homomorphism.

As the use of the term 'isomorphic' suggests, it is generally true that isomorphic groups have the same properties. For example, we have the following.

Lemma 1.55. *If G and H are isomorphic and G is abelian, then so is H.*

Proof. Fix an isomorphism $f : G \to H$ with inverse isomorphism $f^{-1} : H \to G$. Then for any $h_1, h_2 \in H$ one has

$$f^{-1}(h_1)f^{-1}(h_2) = f^{-1}(h_2)f^{-1}(h_1)$$

because G is abelian, and therefore also

$$h_1h_2 = f(f^{-1}(h_1h_2)) = f(f^{-1}(h_1)f^{-1}(h_2)) = f(f^{-1}(h_2)f^{-1}(h_1)) = f(f^{-1}(h_2h_1)) = h_2h_1.$$

□

Remark 1.56. More generally than Lemma 1.55, one also sees directly that if G is an abelian group and $f : G \to H$ is any group homomorphism, then for any elements h_1 and h_2 of $\mathrm{im}(f)$ with $h_1 = f(g_1)$ and $h_2 = f(g_2)$, one has

$$h_1h_2 = f(g_1)f(g_2) = f(g_1g_2) = f(g_2g_1) = f(g_2)f(g_1) = h_2h_1.$$

However, if f is not surjective, this fact does **not** imply that H is abelian.

It is also clear that if G and H are isomorphic and G is finite, then so is H, and moreover that $|G| = |H|$. In addition, we also have the following Lemma and Corollary.

Lemma 1.57. *If $f : G \to H$ is a homomorphism, then for every $g \in G$ one has $\mathrm{o}(f(g)) \leq \mathrm{o}(g)$.*

Proof. Without loss of generality, we may assume that $\mathrm{o}(g) < \infty$. We only need to prove that $f(g)^{\mathrm{o}(g)} = e_H$. But by exercise 1.47 and Lemma 1.48 we find that $f(g)^{\mathrm{o}(g)} = f(g^{\mathrm{o}(g)}) = f(e_G) = e_H$, as required. □

Corollary 1.58. *If $f : G \to H$ is an isomorphism, then for every $g \in G$ one has $\mathrm{o}(f(g)) = \mathrm{o}(g)$.*

Proof. Since both $f : G \to H$ and its inverse $f^{-1} : H \to G$ are homomorphisms (this is shown in the proof of Lemma 1.53), we may apply Lemma 1.57 to both of them to find that

$$\mathrm{o}(g) = \mathrm{o}(f^{-1}(f(g))) \leq \mathrm{o}(f(g)) \leq \mathrm{o}(g).$$

These inequalities must be equalities, thus $\mathrm{o}(g) = \mathrm{o}(f(g))$. □

Exercise 1.59.
(i) Set $\mathbb{R}_{>0} := \{r \in \mathbb{R} : r > 0\}$. Prove that $(\mathbb{R}_{>0}, \cdot)$ is a group. Find an isomorphism $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.
(ii) Decide whether $\mathbb{R}$ and $\mathbb{R}^*$ are or not isomorphic, and whether $\mathbb{R}^*$ and $\mathbb{C}^*$ are or not isomorphic.
(iii) Decide whether $\mathbb{Z}/6\mathbb{Z}$ and S_3 are or not isomorphic.

Exercise 1.60. Let Ω be a finite non-empty set of cardinality n. Prove that $S_\Omega \cong S_n$ by following the following steps.

Fix any bijective function θ from Ω to $\Omega_n := \{1, \ldots, n\}$. Define a function $f_\theta : S_\Omega \to S_n$ by setting

$$f_\theta(\sigma) := \theta \circ \sigma \circ \theta^{-1}$$

for every σ in S_Ω. Then:

(i) Justify that f_θ is well-defined, meaning that $f_\theta(\sigma)$ belongs to S_n.
(ii) Construct a two-sided inverse $S_n \to S_\Omega$ of f_θ to deduce that f_θ is bijective.
(iii) Prove that f_θ is a homomorphism.

1.4. **(More) Exercises.** Don't forget to think about the exercises given throughout the rest of section 1.

Exercise 1.61. Determine which of the following binary operations $\star$ are associative, and also which are commutative:

(i) $a \star b = a + b + ab$ on the set $\mathbb{R}$.
(ii) $a \star b = (a + b)/5$ on the set $\mathbb{Q}$.
(iii) $(a, b) \star (c, d) = (ad + bc, bd)$ on the set $\mathbb{Z} \times \mathbb{Z}$.
(iv) $a \star b = a/b$ on $\mathbb{Q} \setminus \{0\}$.

Exercise 1.62. Determine which of the following sets are groups under the usual addition operation.

(i) The set of rational numbers which, **in lowest terms**, have odd denominator, including $0 \in \mathbb{Q}$.
(ii) The set of rational numbers which, **in lowest terms**, have even denominator, including $0 \in \mathbb{Q}$.
(iii) The set of rational numbers which, **in lowest terms**, have denominator equal to 1 or 2, including $0 \in \mathbb{Q}$.
(iv) The set of rational numbers which, **in lowest terms**, have denominator equal to 1, 2 or 3, including $0 \in \mathbb{Q}$.
(v) The set $\{q \in \mathbb{Q} : |q| < 1\}$.
(vi) The set $\{q \in \mathbb{Q} : |q| \geq 1\} \cup \{0\}$.

Exercise 1.63. We set $G := \{z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{N}\}$.

(i) Prove that G is a group under multiplication.
(ii) Is G closed under addition?

Exercise 1.64. We set $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ and $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.
(i) Prove that both $(\mathbb{Z}[\sqrt{2}], +)$ and $(\mathbb{Q}[\sqrt{2}], +)$ are groups.
(ii) Prove that $(\mathbb{Q}[\sqrt{2}] \setminus \{0\}, \cdot)$ is a group but $(\mathbb{Z}[\sqrt{2}] \setminus \{0\}, \cdot)$ is not a group.

Exercise 1.65. Find the order of each element of $\mathbb{Z}/12\mathbb{Z}$.

Exercise 1.66. In $(\mathbb{Z}/12\mathbb{Z})^\times$, find the order of $[1]$, $[-1]$, $[5]$, $[7]$, $[-7]$, $[13]$.

Exercise 1.67. In $\mathbb{Z}/36\mathbb{Z}$, find the order of $[1]$, $[2]$, $[6]$, $[9]$, $[10]$, $[12]$, $[-1]$, $[-10]$, $[-18]$.

Exercise 1.68. In $(\mathbb{Z}/36\mathbb{Z})^\times$, find the order of $[1]$, $[-1]$, $[5]$, $[13]$, $[-13]$, $[17]$.

In the following exercises, let G be a group.

Exercise 1.69. Prove that $(g_1 g_2 \dots g_{n-1} g_n)^{-1} = g_n^{-1} g_{n-1}^{-1} \dots g_2^{-1} g_1^{-1}$ for any $g_1, \dots, g_n \in G$.

Exercise 1.70. Prove that an element g of G satisfies $g^2 = 1$ if and only if $\mathrm{o}(g) \in \{1, 2\}$.

Exercise 1.71. Prove that if $\mathrm{o}(g) = n \in \mathbb{N}$ then $g^{-1} = g^{n-1}$.

Exercise 1.72. Let x and y be elements of G. Prove that x commutes with y if and only if $y^{-1}xy = x$, if and only if $x^{-1}y^{-1}xy = 1$.

Exercise 1.73. Let g be an element of G and let $a, b \in \mathbb{Z}$. Prove that $g^{a+b} = g^a g^b$ and that $(g^a)^b = g^{ab}$.

Exercise 1.74. Prove that $\mathrm{o}(g) = \mathrm{o}(g^{-1})$ for every $g \in G$.

Exercise 1.75. Assume that G is a finite group and let $g \in G$ be an element of odd order. Prove that there exists $k \in \mathbb{N}$ for which $g = (g^2)^k$.

Exercise 1.76. Prove that $\mathrm{o}(x) = \mathrm{o}(y^{-1}xy)$ for all $x, y \in G$. Deduce that $\mathrm{o}(gh) = \mathrm{o}(hg)$ for all $g, h \in G$.

Exercise 1.77. Prove that if $\mathrm{o}(g) = n \in \mathbb{N}$ and $n = st$ for $s, t \in \mathbb{N}$, then $\mathrm{o}(g^s) = t$.

Exercise 1.78. Prove that if $g^2 = 1$ for every $g \in G$, then G is abelian.

Exercise 1.79. Let G and H be groups and let $g \in G$ and $h \in H$, so that (g, h) is an element of $G \times H$. Prove that $\mathrm{o}((g, h)) = \mathrm{lcm}(\mathrm{o}(g), \mathrm{o}(h))$.

Exercise 1.80. Assume that G is a finite group of even order.
(i) Prove that $\{g \in G : g \neq g^{-1}\}$ has an even number of elements.
(ii) Prove that G has an element of order equal to 2.

Exercise 1.81. Prove that if $\mathrm{o}(g) = n \in \mathbb{N}$ then the elements $1, g, g^2, \dots, g^{n-1}$ are all distinct. Deduce that for any element g of finite order one has $\mathrm{o}(g) \leq |G|$.

Exercise 1.82. Let g be an element of G of finite order n.
(i) Prove that if n is odd then $x^i \neq x^{-i}$ for all $1 \leq i \leq n - 1$.
(ii) Prove that if $n = 2k$ and $1 \leq i \leq n - 1$, then $x^i = x^{-i}$ if and only if $i = k$.

Exercise 1.83. Prove that if g is an element of G of infinite order, then the element g^a for $a \in \mathbb{Z}$ are all distinct.

Exercise 1.84. Prove that if $\mathrm{o}(g) = n \in \mathbb{N}$ then $\{g^a : a \in \mathbb{Z}\} = \{1, g, g^2, \ldots, g^{n-1}\}$.

Exercise 1.85. Let Ω be a non-empty set and let $\mathcal{P}(\Omega)$ be the set of all subsets of Ω. We define a binary operation $\star$ on $\mathcal{P}(\Omega)$ by setting $S \star T := (S \cup T) \setminus (S \cap T)$ for any subsets S and T of Ω. Prove that $(\mathcal{P}(\Omega), \star)$ is an abelian group, and determine the order of each element of $\mathcal{P}(\Omega)$.

Exercise 1.86. Let $\sigma \in S_5$ be the permutation

$$1 \mapsto 3, \quad 2 \mapsto 4, \quad 3 \mapsto 5, \quad 4 \mapsto 2, \quad 5 \mapsto 1,$$

and let $\tau \in S_5$ be the permutation

$$1 \mapsto 5, \quad 2 \mapsto 3, \quad 3 \mapsto 2, \quad 4 \mapsto 4, \quad 5 \mapsto 1.$$

Find the cycle decompositions of each of the following elements of S_5: σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, $\tau^2\sigma$.

Exercise 1.87. Let $\sigma \in S_{15}$ be the permutation

$$\begin{array}{ccccc} 1 \mapsto 13 & 2 \mapsto 2 & 3 \mapsto 15 & 4 \mapsto 14 & 5 \mapsto 10 \\ 6 \mapsto 6 & 7 \mapsto 12 & 8 \mapsto 3 & 9 \mapsto 4 & 10 \mapsto 1 \\ 11 \mapsto 7 & 12 \mapsto 9 & 13 \mapsto 5 & 14 \mapsto 11 & 15 \mapsto 8 \end{array}$$

and let $\tau \in S_{15}$ be the permutation

$$\begin{array}{ccccc} 1 \mapsto 14 & 2 \mapsto 9 & 3 \mapsto 10 & 4 \mapsto 2 & 5 \mapsto 12 \\ 6 \mapsto 6 & 7 \mapsto 5 & 8 \mapsto 11 & 9 \mapsto 15 & 10 \mapsto 3 \\ 11 \mapsto 8 & 12 \mapsto 7 & 13 \mapsto 4 & 14 \mapsto 1 & 15 \mapsto 13. \end{array}$$

Find the cycle decompositions of each of the following elements of S_{15}: σ, τ, σ^2, $\sigma\tau$, $\tau\sigma$, $\tau^2\sigma$.

Exercise 1.88. For each of the permutations whose cycle decomposition was computed in the previous two exercises, determine its order.

Exercise 1.89. Determine the order of each element of S_3 and the order of each element of S_4.

Exercise 1.90. Determine the order of $(1, 12, 8, 10, 4)(2, 13)(5, 11, 7)(6, 9)$ in S_{13}.

Exercise 1.91. Prove that the group $S_{\mathbb{N}}$ is infinite.

Exercise 1.92. Let $\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12) \in S_{12}$. Compute σ^2, σ^3, σ^4 and σ^5. Can you guess a characterisation of the positive integers $n \in \mathbb{N}$ for which σ^n is a 12-cycle?

Exercise 1.93.
(i) If n is odd, prove that the identity is the only element of D_{2n} that commutes with all elements of D_{2n}.
(ii) If n is even, prove that the identity and $r^{n/2}$ are the only elements of D_{2n} that commute with all elements of D_{2n}.

Exercise 1.94. Recall that $\mathbb{F}_2 := \mathbb{Z}/2\mathbb{Z}$ and that

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

Write down all the elements of $\mathrm{Gl}_2(\mathbb{F}_2)$, compute the order of each of them, and determine whether this group is abelian or not.

In the following exercises, F is allowed to denote $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

Exercise 1.95. Prove, by induction on n, that $\mathrm{Gl}_n(F)$ is not abelian.

Exercise 1.96. Let

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in F, a \neq 0, d \neq 0 \right\},$$

$$H := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in F, a \neq 0 \right\}$$

and

$$J := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F \right\}.$$

Prove that all of G, H and J are closed under multiplication of matrices and that all of $(G, \cdot)$, $(H, \cdot)$ and $(J, \cdot)$ are groups. Determine the order of every element of J.

Exercise 1.97. Determine the order of each element of Q_8.

Exercise 1.98. Assume that $G = \{1, a, b, c\}$ is a group of order 4 and that G has no element of order 4. Prove that G is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 1.99. Let $f : G \to H$ be a homomorphism of groups. Show that $f(g^a) = f(g)^a$ for every $g \in G$ and every $a \in \mathbb{Z}$.

Exercise 1.100.
(i) Give an example of two finite, non-trivial groups G and H, of a homomorphism $f : G \to H$, and of an element $g \in G$ for which $\mathrm{o}(f(g)) < \mathrm{o}(g)$.
(ii) Give an example of two non-trivial groups G and H and of a homomorphism $f : G \to H$ with the property that $\mathrm{o}(f(g)) < \mathrm{o}(g)$ for every $g \in G \setminus \{1\}$.

Exercise 1.101. Prove that $\mathbb{Z}$ and $\mathbb{Q}$ are not isomorphic.

Exercise 1.102. Prove that $G \times (H \times J) \cong (G \times H) \times J$ for any groups G, H, J. Prove that $G \times H \cong H \times G$ for any groups G and H.

In the following exercises we write E_8 for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 1.103. Prove that the groups

$$\mathbb{Z}/8\mathbb{Z}, \ \ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \ \ E_8, \ \ D_8 \ \text{ and } \ Q_8$$

are pair-wise non-isomorphic.

Exercise 1.104. Prove that the groups

$$\mathbb{Z}/24\mathbb{Z}, \ \ \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \ \ E_8 \times \mathbb{Z}/3\mathbb{Z}, \ \ D_{24} \ \text{ and } \ S_4$$

are pair-wise non-isomorphic.

Exercise 1.105. Let G be a group. Prove that the (well-defined) function $f : G \to G$ given by $f(g) := g^{-1}$ is a homomorphism if and only if G is abelian.

Exercise 1.106. Let G be a group. Prove that the (well-defined) function $f : G \to G$ given by $f(g) := g^2$ is a homomorphism if and only if G is abelian.

Exercise 1.107. Let G be a group and let $\mathrm{Aut}(G)$ be the set of all isomorphisms $G \xrightarrow{\sim} G$. Prove that composition of functions $\circ$ is a binary operation on $\mathrm{Aut}(G)$ and that $(\mathrm{Aut}(G), \circ)$ is a group (the 'group of automorphisms'of G).

Exercise 1.108. Let A be an abelian group and fix $k \in \mathbb{Z}$.

(i) Prove that the function $f_k : A \to A$ given by $f_k(a) := a^k$ is a homomorphism.
(ii) In the case $k = -1$, prove that f_{-1} is an isomorphism (and thus an 'automorphism' of A).
(iii) In the case $A = \mathbb{Q}$, for which values of k is f_k an automorphism of $\mathbb{Q}$?

Exercise 1.109. Let G be a finite group and assume that there exists an $f \in \mathrm{Aut}(G)$ with the following properties:

(a) $f(g) = g$ if and only if $g = 1$;
(b) $(f \circ f)(g) = g$ for every $g \in G$.

Prove that every element of G is of the form $g^{-1}f(g)$ for some $g \in G$. Then deduce that G is abelian.

Exercise 1.110. Define an injective homomorphism $f : Q_8 \to \mathrm{Gl}_2(\mathbb{C})$ that satisfies

$$f(i) = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \text{ and } f(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

.

2. Subgroups

2.1. **Definition and examples.**

2.1.1. *The definition.* Among the subsets of a group G, we are interested in studying those that are themselves groups *under the same binary operation.* This means that a subgroup H of a group $(G, \star)$ will need to be defined to be a subset H that is closed under $\star$, and so that in addition $(H, \star)$ satisfies the group axioms.

As explained in Remark 1.2, if H is closed under $\star$, then this binary operation on H is automatically associative. We are therefore led to make the following definition:

Definition 2.1. Let $(G, \star)$ be a group and let H be a (non-empty) subset of G. We then say that H is a subgroup of $(G, \star)$ if the following conditions are satisfied:

(S1) H is closed under $\star$.
(S2) The identity element e_G of $(G, \star)$ belongs to H.
(S3) For every $h \in H$, the inverse element h^{-1} of h in G belongs to H.

Exercise 2.2. Prove that, under these conditions, the pair $(H, \star)$ is a group, with identity element $e_H := e_G$, and all elements of which have the same inverse element in H as in G (so the notation h^{-1} is unambiguous). Prove that a subgroup of an abelian group is abelian, and that a subgroup of a finite group is finite.

Notation 2.3. We often omit the binary operation from the notation and simply say that H is a subgroup of G. However, one should not forget that whether a subset H of G is a subgroup or not does depend on which binary operation we are considering G to be equipped with.

We write $(H, \star) \leq (G, \star)$ or, more often, simply $H \leq G$, to indicate that H is a subgroup of G. We say that H is a strict, or proper, subgroup of G if it is a subgroup that is a strict subset of G (obviously, G is always a subgroup of G). We feel free to write $H < G$ if we know that H is a strict subgroup of G, and we write $H \lneq G$ if we want the notation to specify that H is a strict subgroup of G. We write $H \not\leq G$ to indicate that a certain subset H of a group G is not a subgroup of G.

The subset $\{e_G\}$ is always a subgroup of G. We often just write 1 (or 0 if we are using additive notation) to denote this subgroup.

Exercise 2.4. Show that $\leq$ is a transitive relation on the set of subsets of G.

2.1.2. *Alternative definitions.* Although the Definition 2.1 of subgroups is more intuitively clear and leads to an immediate resolution of Exercise 2.2, a closer look at the conditions quickly shows that (S2) is redundant! We obtain the following alternative definition.

Lemma 2.5. *Let $(G, \star)$ be a group and let H be a (non-empty) subset of G. Then H is a subgroup of $(G, \star)$ if and only if conditions* (S1) *and* (S3) *are satisfied.*

Proof. It is trivial that if conditions (S1), (S2) and (S3) are satisfied, then conditions (S1) and (S3) are satisfied. We must therefore only prove the converse by showing that if conditions (S1) and (S3) are satisfied, then so is condition (S2).

Since H is non-empty, we may fix an element h of H. By (S3) we know that the inverse element h^{-1} of h in G also belongs to H. But then, by (S1) we know that $e_G = h \star h^{-1}$ belongs to H, as required. □

We can also try to shorten the definition of a subgroup even further, by synthesizing conditions (S1) and (S3) into a single condition as follows.

Lemma 2.6. *Let $(G, \star)$ be a group and let H be a (non-empty) subset of G. Then H is a subgroup of $(G, \star)$ if and only if the following condition holds:*

(S') *For all x and y in H, the element $x \star y^{-1}$ belongs to H.*

Proof. We use Lemma 2.5, so we only need to show that conditions (S1) and (S3) hold if and only if condition (S$'$) holds.

Fix x and y in H. If condition (S3) holds then y^{-1} belongs to H and if condition (S1) also holds we thus get that $x \star y^{-1}$ belongs to H. So condition (S$'$).

To prove the converse we assume that (S$'$) holds. Since H is non-empty, we may fix an element z of H. Then $e_G = z \star z^{-1}$ belongs to H by (S$'$) applied with $x = z$ and $y = z$.

Let now h be an arbitrary element of H. Then $h^{-1} = e_G \star h^{-1}$ belongs to H, by (S$'$) applied with $x = e_G$ and $y = h$. So condition (S3) holds.

Finally, to deduce that (S1) holds we fix any elements h and j of H. Then, since we have already proved that (S3) holds, we know that j^{-1} belongs to H. But then $h \star j = h \star (j^{-1})^{-1}$ belongs to H, by (S$'$) applied to $x = h$ and $y = j^{-1}$. This proves that condition (S1) holds and thus completes the proof.

□

In the case of finite subsets H, checking the subgroup conditions becomes essentially trivial.

Lemma 2.7. *Let $(G, \star)$ be a group and let H be a (non-empty) finite subset of G. Then H is a subgroup of $(G, \star)$ if and only if it is closed under $\star$.*

Proof. We assume that H is closed under $\star$ and, by Lemma 2.5, only need to prove that condition (S3) is valid.

We fix an element h of H. We must prove that h^{-1} belongs to H. Now, because H is closed under $\star$, all of the elements of the sequence

$$h, h^2, h^3, h^4, \dots \tag{10}$$

belong to H. Since H is finite, we must have $h^n = h^m$ for some natural number n and m with $n \neq m$. Without loss of generality, we have $n < m$. We set $r := m - n \in \mathbb{N}$. Then

$$h \star h^{r-1} = h^r = h^{m-n} = h^m \star h^{-n} = h^m \star (h^n)^{-1} = h^n \star (h^n)^{-1} = e_G.$$

Therefore $h^{-1} = h^{r-1}$ which, as an element of the sequence (10), belongs to H. This proves that condition (S3) holds, as required. □

2.1.3. *Intersections and examples.*

Exercise 2.8. Let $\{H_i : i \in I\}$ be a (non-empty) set of subgroups of a group G. Prove that the subset $\bigcap_{i \in I} H_i$ of G is a subgroup.

Exercise 2.9. Let H and K be subgroups of G. Prove that $H \cap K \leq H$ (hence also $H \cap K \leq K$).

Example 2.10. We will determine all the subgroups of each of the groups $G := \mathbb{Z}/4\mathbb{Z}$ and $J := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Obviously 0 and G are subgroups of G while 0 and J are subgroups of J.

If $H \neq G$ is a subgroup of G, it can not contain [1], because then $[2] = [1] + [1]$, and hence also $[3] = [1] + [2]$, would have to belong to H, and this would contradict $H \neq G$. It also can not contain [3], because then $[2] = [3] + [3]$, and hence also $[1] = [3] + [2]$, would have to belong to H. So the only non-trivial possibility for H is $H := \{[0], [2]\}$. This set is indeed a subgroup of G, as $[2] + [2] = [0]$ and $-[2] = [2]$. So there exist three subgroups of G:

$$0, H := \{[0], [2]\} \text{ and } G.$$

If $H \neq J$, we claim that it can not contain three distinct elements. That is, we claim that $|H| \neq 3$, so $|H| \leq 2$. To prove this, we note that $([0], [1]) + ([1], [0]) = ([1], [1])$, that $([0], [1]) + ([1], [1]) = ([1], [0])$ and that $([1], [0]) + ([1], [1]) = ([0], [1])$. So, if H contained $([0], [0])$ and then also two of the elements $([0], [1])$, $([1], [0])$ and $([1], [1])$, it would have to contain the third one, contradicting $H \neq J$.

So the only non-trivial possibilities for H are the subsets of cardinality 2 containing the identity, namely $H_1 := \{([0], [0]), ([0], [1])\}$, $H_2 := \{([0], [0]), ([1], [0])\}$ and $H_3 := \{([0], [0]), ([1], [1])\}$. It is easy to verify that H_1, H_2 and H_3 are subgroups of J. So there exist five subgroups of J:

$$0, H_1, H_2, H_3 \text{ and } J.$$

Exercise 2.11. Determine which of the given subsets of a given group is a subgroup:

(i) The subset $\mathbb{N}$ of the group $\mathbb{Z}$.
(ii) The subset $\mathbb{Z}$ of the group $\mathbb{Q}$.
(iii) The subset $\mathbb{Q}$ of $\mathbb{R}$.
(iv) The subset $(2\mathbb{Z} + 1) \cup \{0\}$ of $\mathbb{Z}$.
(v) The subset $2\mathbb{Z}$ of $\mathbb{Z}$.
(vi) The subset $n\mathbb{Z} := \{nz : z \in \mathbb{Z}\}$ of $\mathbb{Z}$, for $n \geq 3$.
(vii) The subset $\mathbb{Z} \setminus \{0\}$ of $\mathbb{Q}^*$.
(viii) The subset $\mathbb{Q}^*$ of $\mathbb{R}^*$.
(ix) The subset $\{\pm 1\}$ of $\mathbb{Q}^*$.
(x) The subset $\{x + x\mathbf{i} : x \in \mathbb{R}\}$ of $\mathbb{C}$.
(xi) The subset $\{x \in \mathbb{R} : x^2 \in \mathbb{Q}\}$ of $\mathbb{R}$.
(xii) The subset $\{z \in \mathbb{C} : |z| = 1\}$ of $\mathbb{C}^*$.
(xiii) The subset of rational numbers which (in lowest terms) have even denominator, of the group $\mathbb{Q}$.
(xiv) The subset of rational numbers which (in lowest terms) have odd denominator, of the group $\mathbb{Q}$.
(xv) The subset $\{x \in \mathbb{R}^* : x^2 \in \mathbb{Q}\}$ of $\mathbb{R}^*$.
(xvi) The subset of 2-cycles in S_3.
(xvii) The subset of 2-cycles in S_n, for $n \geq 4$.
(xviii) The subset $S(\omega) := \{\sigma \in S_\Omega : \sigma(\omega) = \omega\}$ of S_Ω, for a fixed non-empty set Ω and a fixed element ω of Ω.
(xix) The subset $\{1, r, r^2, \ldots, r^{n-1}\}$ of D_{2n}.

(xx) The subset $\{1, r^2, s, sr^2\}$ of D_8.
(xxi) The subset $\{1, r^2, sr, sr^3\}$ of D_8.
(xxii) The subsets G, H and J of $\mathrm{Gl}_2(F)$ that are defined in Exercise 1.96.

2.1.4. *The kernel and the image of a homomorphism.* We now see how every homomorphism of groups $f : G \to J$ has some important associated subgroups of G and of J.

Definition 2.12. Let $f : G \to J$ be a homomorphism of groups. We define a subset

$$\ker(f) := \{g \in G : f(g) = e_J\} \subseteq G$$

of G and a subset

$$\mathrm{im}(f) := f(G) = \{f(g) : g \in G\} \subseteq J$$

of J. These are the 'kernel' and the 'image' of f, respectively.

Proposition 2.13. *Let $f : G \to J$ be a homomorphism. Then:*

(i) $\mathrm{im}(f)$ *is a subgroup of J.*
(ii) $\ker(f)$ *is a subgroup of G.*
(iii) *The function f is injective if and only if* $\ker(f) = 1$.
(iv) *The homomorphism f is an isomorphism if and only if one has both* $\ker(f) = 1$ *and* $\mathrm{im}(f) = J$.

Proof. We often use Lemma 1.48 which states that $f(1) = 1$ and also that $f(g)^{-1} = f(g^{-1})$ for every $g \in G$.

The set $\mathrm{im}(f)$ is non-empty because and contains $1 = f(1)$. One has $f(g_1)f(g_2) = f(g_1g_2) \in \mathrm{im}(f)$, so $\mathrm{im}(f)$ is a closed subset of J. In addition, for any $g \in G$ one has $f(g)^{-1} = f(g^{-1}) \in \mathrm{im}(f)$, so $\mathrm{im}(f)$ contains the inverse of any of its elements. This proves claim (i).

The set $\ker(f)$ is non-empty and contains 1. Now, if $f(g_1) = 1$ and $f(g_2) = 1$ then $f(g_1g_2) = f(g_1)f(g_2) = 1 \cdot 1 = 1$, so g_1g_2 belongs to $\ker(f)$. This shows that $\ker(f)$ is a closed subset of G. In addition, if $f(g) = 1$ then $f(g^{-1}) = f(g)^{-1} = 1^{-1} = 1$, so g^{-1} belongs to $\ker(f)$. This shows that $\ker(f)$ contains the inverse of any of its elements. This proves claim (ii).

We now consider claim (iii). It is clear that if f is injective then $\ker(f) = 1$, as it contains 1 but could not contain more than one element. To prove the converse we assume that $\ker(f) = 1$, and then also that $f(g_1) = f(g_2)$. But then

$$f(g_1g_2^{-1}) = f(g_1)f(g_2^{-1}) = f(g_1)f(g_2)^{-1} = f(g_2)f(g_2)^{-1} = 1,$$

so $g_1g_2^{-1} \in \ker(f) = 1$. It follows that $g_1g_2^{-1} = 1$ and then that $g_1 = g_2$. This proves that f would be injective, as required.

Claim (iv) follows immediately from claim (iii). □

Remark 2.14. Since 1 always belongs to $\ker(f)$ by Lemma 1.48, in the setting of claim (iii) it is enough to verify that $f(g) \neq 1$ for every $g \neq 1$ in order to conclude that f is injective.

Notation 2.15. If $f : G \to J$ is a homomorphism of groups and H is a subgroup of G that is clear from context, we will sometimes abbreviate the restriction $f\mid_H$ of f to H to the notation f^*.

Lemma 2.16. *Let $f : G \to J$ be a homomorphism and let H be a subgroup of G. Let also K be a subgroup of J which satisfies* $\mathrm{im}(f) \subseteq K$*. Then:*

(i) $f^* : H \to J$ *is a group homomorphism.*
(ii) $f : G \to K$ *is a group homomorphism.*
(iii) $\ker(f^*) = \ker(f) \cap H$*, so in particular* $\ker(f^*)$ *is a subgroup of* $\ker(f)$*.*
(iv) $\mathrm{im}(f^*)$ *is a subgroup of* $\mathrm{im}(f)$*.*

Proof. Claim (i) is clear, as $f^*(hh') = f(h)f(h') = f(h)f(h') = f^*(h)f^*(h)$ for any $h, h' \in H$. Claim (ii) is also obvious.

If x belongs to $\ker(f^*)$ then x belongs to H and $f(x) = f^*(x) = 1$, so h belongs to $\ker(f)$. This shows that $\ker(f^*) \subseteq \ker(f) \cap H$.

If h belongs to $\ker(f) \cap H$ then $f^*(h) = f(h) = 1$, so h belongs to $\ker(f^*)$. We conclude that $\ker(f^*) = \ker(f) \cap H$.

Now the proved equality implies, by Exercise 2.9, that $\ker(f^*)$ is a subgroup of $\ker(f)$.

Clearly
$$\mathrm{im}(f^*) = f^*(H) = f(H) \subseteq f(G) = \mathrm{im}(f).$$
We know from Proposition 2.13(i) that $\mathrm{im}(f)$ is a subgroup of J. Thus we can apply claim (ii) to $f^* : H \to J$, and with $K = \mathrm{im}(f)$, to deduce that
$$f^* : H \to \mathrm{im}(f)$$
is a group homomorphism. By applying Proposition 2.13(i) again to this displayed homomorphism, we find that $\mathrm{im}(f^*)$ is a subgroup of $\mathrm{im}(f)$. □

2.2. **Cyclic groups and cyclic subgroups.**

2.2.1. *The subgroup generated by a subset of a group.* You have surely encountered in Linear Algebra the notion of the subspace generated by a subset of a vector space. You may recall that if S is a subset of a vector space V (over a field F), then $\langle S\rangle$ is the smallest, or more accurately the unique minimal, subspace of V which contains S. You may also recall that $\langle S\rangle$ can be explicitly computed as the linear span $\{f_1s_1 + \ldots + f_ns_n : n \in \mathbb{N}, s_i \in S, f_i \in F\}$ of S. In other words, by allowing any combination of the structural operations of V to be applied to elements of S.

We will now formalise the analogous notion in the theory of groups.

Definition 2.17. Let G be a group and let S be any subset of G. Then the 'subgroup of G generated by S' is
$$\langle S\rangle := \bigcap_{S\subseteq H\leq G} H.$$
Here the intersection runs over all subgroups of G which contain S. Clearly, $S \subseteq \langle S\rangle \subseteq G$. By Exercise 2.8, we know that $\langle S\rangle$ is a subgroup of G.

Exercise 2.18. Prove that, if S is a subgroup of G, then $\langle S\rangle = S$.

It should be clear that the above definition of $\langle S\rangle$ formalises the intuitive idea of smallest subgroup of G which contains S: $\langle S\rangle$ is the unique minimal element of the set $\{H \leq G : S \subseteq H\}$, ordered by inclusion.

However, we will now give alternative constructions $\langle S\rangle$ which will be more useful when trying to explicitly determine this subgroup in any given example.

In order to do this, for a subset S of a group G, we set

$$\begin{aligned}\overline{S} &:= \{s_1^{\alpha_1}s_2^{\alpha_2}\dots s_n^{\alpha_n} : n\in\mathbb{N}, \alpha_i\in\mathbb{Z}, s_i\in S\},\\ \widehat{S} &:= \{s_1^{\alpha_1}s_2^{\alpha_2}\dots s_n^{\alpha_n} : n\in\mathbb{N}, \alpha_i\in\mathbb{Z}, s_i\in S, s_i\neq s_{i+1}\},\\ \widetilde{S} &:= \{s_1^{\gamma_1}s_2^{\gamma_2}\dots s_n^{\gamma_n} : n\in\mathbb{N}, \gamma_i\in\{\pm1\}, s_i\in S\}.\end{aligned}$$

If S is the empty set, we take the convetion of letting any of these sets be the trivial subgroup $\{1\}$ of G.

Proposition 2.19. *Let G be a group and let S be any subset of G. Then*

$$\langle S\rangle = \overline{S} = \widehat{S} = \widetilde{S}.$$

Proof. Because $s^\alpha s^{\alpha'} = s^{\alpha+\alpha'}$ for any $s\in S$ and any $\alpha,\alpha'\in\mathbb{Z}$, it is clear that $\overline{S} = \widehat{S}$.

Because s^α may be expressed as $s^\gamma\dots s^\gamma$, with $\gamma = 1$ if α is a positive integer or with $\gamma = -1$ if α is a negative integer, it is clear that $\overline{S} = \widetilde{S}$.

It is therefore enough to prove that $\langle S\rangle = \widetilde{S}$ and, to do this, we must first prove that $\widetilde{S}$ is a subgroup of G. Let $x = s_1^{\gamma_1}s_2^{\gamma_2}\dots s_{n-1}^{\gamma_{n-1}}s_n^{\gamma_n}$ and $y = t_1^{\delta_1}t_2^{\delta_2}\dots t_{m-1}^{\delta_{m-1}}t_m^{\delta_m}$ be elements of $\overline{S}$. Then

$$y^{-1} = t_m^{-\delta_m}t_{m-1}^{-\delta_{m-1}}\dots t_2^{-\delta_2}t_1^{-\delta_1}$$

by Exercise 1.69 so

$$xy^{-1} = s_1^{\gamma_1}s_2^{\gamma_2}\dots s_{n-1}^{\gamma_{n-1}}s_n^{\gamma_n}t_m^{-\delta_m}t_{m-1}^{-\delta_{m-1}}\dots t_2^{-\delta_2}t_1^{-\delta_1}.$$

Clearly xy^{-1} is an element of $\widetilde{S}$, so $\widetilde{S}$ is a subgroup of G, by Lemma 2.6.

To prove that $\widetilde{S} = \langle S\rangle$ we first observe that any element $s = s^1$ of S belongs to $\widetilde{S}$, so $\widetilde{S}$ is a subgroup of G which contains S. From the definition of $\langle S\rangle$ we immediately get that $\langle S\rangle \subseteq \widetilde{S}$.

To prove the converse inclusion, it is enough to note that, since $\langle S\rangle$ is a subgroup of G that contains S, it must contain every expression of the form $s_1^{\gamma_1}s_2^{\gamma_2}\dots s_n^{\gamma_n}$. It is then clear that $\widetilde{S}\subseteq\langle S\rangle$ so we finally deduce that $\widetilde{S} = \langle S\rangle$, as required. □

Notation 2.20. Given the claim of Proposition 2.19, we abandon the notations $\overline{S}$, $\widehat{S}$ and $\widetilde{S}$ and only use $\langle S\rangle$ in the sequel. For a finite set $\{s_1,\dots,s_k\}$, we abbreviate $\langle\{s_1,\dots,s_k\}\rangle$ to $\langle s_1,\dots,s_k\rangle$. Given sets S and T we sometimes write $\langle S,T\rangle$ in place of $\langle S\cup T\rangle$.

Example 2.21. In the group $\mathbb{Z}$ we have $\langle 1\rangle = \mathbb{Z}$. We also have $\langle -1\rangle = \mathbb{Z}$. In fact, one has $\langle S\rangle = \mathbb{Z}$ for any subset S of $\mathbb{Z}$ that contains either 1 or -1. For example, $\langle\mathbb{N}\rangle = \mathbb{Z}$. However, $\langle 2\rangle = 2\mathbb{Z} \lneq \mathbb{Z}$.

Example 2.22. We use the notation of Example 2.10.

We first consider the group $G := \mathbb{Z}/4\mathbb{Z}$ and the subgroup $H := \{[0],[2]\}$ of G. Then we have

$$\langle[2]\rangle = H$$

and also

$$\langle[1]\rangle = \langle[3]\rangle = \langle[1],[2]\rangle = \langle[1],[3]\rangle = \langle[2],[3]\rangle = \langle[1],[2],[3]\rangle = G.$$

We now consider the group $J := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the three non-trivial subgroups H_1, H_2, H_3 of J that are defined in Example 2.10. Then we have

$$\langle([0],[1])\rangle = H_1, \quad \langle([1],[0])\rangle = H_2, \quad \langle([1],[1])\rangle = H_3$$

and also

$$\langle([0],[1]),([1],[0])\rangle = \langle([0],[1]),([1],[1])\rangle = \langle([1],[0]),([1],[1])\rangle = \langle([0],[1]),([1],[0]),([1],[1])\rangle = J.$$

Example 2.23. The description (6) shows that, in D_{2n}, the subgroup $\langle r, s\rangle$ is equal to D_{2n}. If we also put $a = s$ and $b = rs$, then clearly $\langle a, b\rangle \subseteq \langle r, s\rangle$. But since $r = ba$, we also have $\langle r, s\rangle \subseteq \langle a, b\rangle$, so $\langle a, b\rangle = D_{2n}$. Note however that the element sr of D_{2n} is **not** of the form $a^\alpha b^\beta$ for any $\alpha, \beta \in \mathbb{Z}$. This illustrates the fact that, in the alternative descriptions of $\langle S\rangle$ given in Proposition 2.19, we always allow elements to be repeated in the relevant expressions. One does have $sr = aba$.

Exercise 2.24. In $G = \mathrm{Gl}_2(\mathbb{R})$ we set

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad B := \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}.$$

Find $\mathrm{o}(A)$ and $\mathrm{o}(B)$, and prove that the subgroup $\langle A, B\rangle$ of G is infinite.

2.2.2. *Definition and first properties.* Cyclic groups form a very special class of groups, which have particularly simple properties. These are the groups that can be generated by a single element (or, strictly speaking, by a set with a single element).

Definition 2.25.
(i) A group G is cyclic if there exists an element g in G with the property that $\langle g\rangle = G$.
(ii) Any element g which satisfies $\langle g\rangle = G$ in a cyclic group G is called a generator of G. We also say that g generates G.
(iii) Let G be any group. Then H is called a cyclic subgroup of G if it is both a subgroup of G and a cyclic group.

Lemma 2.26. *A group G is cyclic if and only if there exists an element g in G with the property that $\{g^a : a \in \mathbb{Z}\} = G$.*

Proof. Proposition 2.19 states that $\langle g\rangle = \widehat{\{g\}} = \{g^a : a \in \mathbb{Z}\}$, and the lemma then becomes immediate from the definition of a cyclic group. □

Corollary 2.27. *Every cyclic group is abelian.*

Proof. Let G be a cyclic group and let g be a generator of G. Then for any $x, y \in G$, Lemma 2.26 implies that $x = g^a$ and $y = g^b$ for some $a, b \in \mathbb{Z}$, and we find that

$$xy = g^a g^b = g^{a+b} = g^{b+a} = g^b g^a = yx,$$

as required. Here the second and fourth equalities hold by Exercise 1.73. □

Exercise 2.28. Let G be a cyclic group and let g be a generator of G. Prove that g^{-1} is a generator of G.

Example 2.29. Clearly $\mathbb{Z}$ is a cyclic group generated by 1. It is also generated by -1. However, there are no other generators of $\mathbb{Z}$: one has $\langle b\rangle = \{a \cdot b : a \in \mathbb{Z}\} = b\mathbb{Z} = |b|\mathbb{Z}$, which is strictly contained in $\mathbb{Z}$ if $b \neq 1, -1$.

Example 2.30. We use the notation of Examples 2.10 and 2.22. The group $G = \mathbb{Z}/4\mathbb{Z}$ is cyclic, and both $[1]$ and $[3]$ are generators of G. The element $[2]$ is not a generator of G, but the subgroup $H := \{[0],[2]\}$ of G is also cyclic, and $[2]$ is a generator of H.

The group $J := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not cyclic. However, all three of the subgroups H_1, H_2 and H_3 of J are cyclic, with the respective generators given in Example 2.22. But this fact also implies that no element of J generates all of J, which is how we deduce that J is not a cyclic group.

Exercise 2.31. Prove that the group $\mathbb{Z}/n\mathbb{Z}$ is always cyclic. Find all generators of the cyclic group $\mathbb{Z}/6\mathbb{Z}$.

Exercise 2.32. In the group $G := (\mathbb{Z}/5\mathbb{Z})^\times = \{[1],[2],[3],[4]\}$, prove that

$$\langle[1]\rangle = \{[1]\}, \quad \langle[2]\rangle = G, \quad \langle[3]\rangle = G, \quad \langle[4]\rangle = \{[1],[4]\}.$$

Exercise 2.33. In D_8, prove that $r^{105} = r$ and that $r^{-42} = r^2$. Is the group D_8 cyclic?

2.2.3. *Order of cyclic groups.* Before stating our first result relating cyclic group orders to element orders, we require the following auxiliary results which are very important in their own right.

Lemma 2.34. *Let G be a group and let h be an element of G.*

(i) *If h has finite order n, then the elements $1, h, h^2, h^3, \dots, h^{n-1}$ of G are distinct.*

(ii) *If h has infinite order, then $h^a \neq h^b$ for any integers a, b with $a \neq b$.*

Proof. We argue by contradiction. To prove claim (i), suppose that $h^a = h^b$ with $a, b \in \{0,1,2,3,\dots,n-1\}$ and with $a \neq b$. Without loss of generality, assume that $a < b$. Then

$$h^{b-a} = h^b h^{-a} = h^b (h^a)^{-1} = h^b (h^b)^{-1} = 1. \tag{11}$$

But $1 \leq b - a \leq n-1$, which contradicts the fact that n is the order of h.

To prove claim (ii), suppose that $h^a = h^b$ with $a, b \in \mathbb{Z}$ and with $a \neq b$. Without loss of generality, assume that $a < b$. Then the same equality (11) shows that $h^{b-a} = 1$ with $1 \leq b - a$, which contradicts the fact that h has infinite order. □

Proposition 2.35. *Let G be a group and let h be an element of G. If $h^a = 1 = h^b$ with $a, b \in \mathbb{Z}$, then $h^d = 1$ for $d = (a, b)$. In particular, if $h^c = 1$ for some $c \in \mathbb{Z}$, then $\mathrm{o}(h)$ divides c.*

Proof. By the Euclidean Algorithm, there are r and s in $\mathbb{Z}$ for which $d = ar + bs$. It follows that

$$h^d = h^{ar+bs} = h^{ar}h^{bs} = (h^a)^r (h^b)^s = 1^r 1^s = 1,$$

as required.

To prove the second claim let $h^c = 1$. If $c = 0$ then clearly $\mathrm{o}(h)$ divides c. We assume that $c \neq 0$. Then h must have finite order, and we set $n := \mathrm{o}(h) \in \mathbb{N}$. Let $d := (c, n)$, so we know that $h^d = 1$. Since n is the order of h, we cannot have $d \leq n$. But $1 \leq d \leq n$, so we find that $d = n$. In particular, $\mathrm{o}(h) = n = d = (d, c)$ divides c, as required. □

We may now directly relate the order of an element with the order of the group it generates. Please note that this result fully justifies the use of the term 'order' in Definition 1.15 (ii).

Proposition 2.36. *Let G be a group and let h be an element of G. Set $H := \langle h\rangle$. Then h has finite order if and only if H is finite, and there is an equality $\mathrm{o}(h) = |H|$. In addition:*

(i) *If H has order $n \in \mathbb{N}$, then $h^n = 1$ and $1, h, h^2, h^3, \dots, h^{n-1}$ are all the distinct elements of H.*

(ii) *If H is infinite then $h^m \neq 1$ for each $m \in \mathbb{Z}$, $m \neq 0$, and $h^a \neq h^b$ if $a \neq b$.*

Proof. We first assume that h has finite order $n \in \mathbb{N}$. By Lemma 2.34 (i), the elements $1, h, h^2, h^3, \dots, h^{n-1}$ are all distinct. We must prove that H has no other elements, to deduce that $|H| = n$. By Proposition 2.19, it is enough to show that h^a belongs to $\{1, h, h^2, h^3, \dots, h^{n-1}\}$ for every $a \in \mathbb{Z}$.

To do this we use the Division Algorithm to write $a = nq + k$ with $0 \leq k \leq n - 1$. Then

$$h^a = h^{nq+k} = h^{nq}h^k = (h^n)^q h^k = 1^q h^k = 1h^k = h^k,$$

as required.

Finally, we now assume that h has infinite order. Then Lemma 2.34 proves tat H is infinite and also all of the additional claims.

It is furthermore now clear that h has finite order if and only if H is finite. □

The next result shows that, in fact, the structure of a cyclic group is completely determined by its order.

Theorem 2.37. *Any two cyclic groups of the same order are isomorphic. Moreover, if G and J are two cyclic groups of the same order, then for any generators x of G and y of J, the function*

$$f_{x,y} : G \to J$$

defined by setting $f_{x,y}(x^a) := y^a$ for each $a \in \mathbb{Z}$, is a well-defined isomorphism.

Proof. We fix x and y. If G and J are both infinite, then x has infinite order by Proposition 2.36, and hence $f_{x,y}$ is well-defined by Lemma 2.34 (ii).

If both G and J are finite of order $n \in \mathbb{N}$, to prove that $f_{x,y}$ is well-defined, we fix $a, b \in \mathbb{Z}$ with $x^a = x^b$, and we must prove that $y^a = y^b$.

Since $x^{a-b} = 1$ by the same argument as in (11), Proposition 2.35 then implies that n divides $a - b$. But if $a - b = nq$ then $y^a = y^{nq+b} = (y^n)^q y^b = 1^q y^b = y^b$, as required.

We have proved that $f_{x,y}$ is well-defined in either case. Now if $g_1 = x^a$ and $g_2 = x^b$ are any elements of G, then

$$f_{x,y}(g_1g_2) = f_{x,y}(x^a x^b) = f_{x,y}(x^{a+b}) = y^{a+b} = y^a y^b = f_{x,y}(x^a)f_{x,y}(x^b) = f_{x,y}(g_1)f_{x,y}(g_2),$$

so $f_{x,y}$ is a homomorphism.

It is finally very easy to deduce from Proposition 2.36 that $f_{x,y}$ is both surjective and injective, hence also an isomorphism. □

Corollary 2.38. *The following claims are valid.*

(i) *If G is a cyclic group of infinite order, then $\mathbb{Z} \cong G$.*

(ii) *If G is a finite cyclic group of order n, then $\mathbb{Z}/n\mathbb{Z} \cong G$.*

Proof. This result is immediate upon combining Theorem 2.37 with Example 2.29 and Exercise 2.31. □

Notation 2.39. We denote by C_n the isomorphism class of $\mathbb{Z}/n\mathbb{Z}$. By abuse of notation, when we do not need to distinguish between isomorphic groups, we sometimes refer to C_n as 'the cyclic group of order n'. However, when we use C_n to denote a group, we always use multiplicative notation!

Proposition 2.40. *Let G be a group, let g be an element of G and let k be a non-zero integer.*

(i) *If g has infinite order then g^k has infinite order.*

(ii) *If g has finite order then*

$$\mathrm{o}(g^k) = \frac{\mathrm{o}(g)}{(\mathrm{o}(g), k)}.$$

Proof. To prove claim (i) we argue by contradiction. Suppose that g has infinite order but $\mathrm{o}(g^k) = m \in \mathbb{N}$. Then

$$g^{km} = (g^k)^m = 1$$

and also

$$g^{-km} = (g^{km})^{-1} = 1^{-1} = 1.$$

One of km or $-km$ must be positive,so the corresponding displayed equality contradicts the fact thet g has infinite order.

To prove claim (ii) we set $y := g^k$, $n := \mathrm{o}(g)$ and $d := (n, k)$, so we must prove that $\mathrm{o}(y) = n/d$.

Let $k = da$ and $n = db$ for integers a, b with $b > 0$. We must prove $\mathrm{o}(y) = b$. We note for later use that

$$(a, b) = 1 \tag{12}$$

by definition.

We first compute that

$$y^b = g^{kb} = g^{dab} = (g^{db})^a = (g^n)^a = 1^a = 1,$$

so Proposition 2.35 implies that $\mathrm{o}(y)$ divides b. It will be enough to prove that b divides $\mathrm{o}(y)$.

But

$$g^{k\mathrm{o}(y)} = (g^k)^{\mathrm{o}(y)} = y^{\mathrm{o}(y)} = 1,$$

so Proposition 2.35 also implies that n divides $k\mathrm{o}(y)$, which means that db divides $da\mathrm{o}(y)$, which means that b divides $a\mathrm{o}(y)$. But this last fact combines with (12) to imply that b divides $\mathrm{o}(y)$, as required to complete the proof. □

Corollary 2.41. *Let G be a finite cyclic group and let g be a generator of G. Then g^k is a generator of G if and only if $(k, \mathrm{o}(g)) = 1$.*

Proof. Proposition 2.36 states $|G| = \mathrm{o}(g)$ and also that the subgroup $H_k := \langle g^k \rangle$ of G has order $|H_k| = \mathrm{o}(g^k)$.

Since $|H_k| \leq |G|$, we see that g^k is a generator of G if and only if $\mathrm{o}(g^k) = \mathrm{o}(g)$. By Proposition 2.40, this last condition holds if and only if $(k, \mathrm{o}(g)) = 1$, as required. □

Exercise 2.42. Determine the set of generators of the cyclic group $\mathbb{Z}/12\mathbb{Z}$.

Exercise 2.43. Let G be an infinite cyclic group and let g be a generator of G. Prove that the set of generators of G is equal to $\{g, g^{-1}\}$.

2.2.4. *Subgroups of cyclic groups.* The following result gives a complete description of the subgroups of a cyclic group.

Theorem 2.44. *Let G be a cyclic group.*

(i) *All subgroups of G are cyclic. Moreover, if $H \neq \{1\}$ is a subgroup of G, g is a generator of G and d is the smallest natural number for which g^d belongs to H, then g^d is a generator of H.*
(ii) *If G is finite, then for every natural number d that divides $|G|$, there is a unique subgroup of G of order d. Moreover, there is a bijection between the set of subgroups of G and the set of natural numbers that divide $|G|$ (so there are no additional subgroups of G).*
(iii) *If G is infinite, then every nontrivial subgroup of G is infinite, and there is a bijection between the set of nontrivial subgroups of G and the set $\mathbb{N}$.*

Remark 2.45. Fix a generator g of G. Then in the setting of claim (ii) and for each natural number d that divides $|G|$, the element $g^{|G|/d}$ is a generator of the subgroup of G that has order d (you may use claim (i) to prove this).

Proof. Since $\{1\} = \langle 1 \rangle$ is always a cyclic group, to prove claim (i) it is enough to consider a nontrivial subgroup H of G. We also fix a generator g of G. Then any non-trivial element h of H is of the form g^a for some $a \neq 0$, and $h^{-1} = g^{-a}$ must also belong to H. Since $H \neq \{1\}$, the set

$$\mathcal{P} := \{b \in \mathbb{N} : g^b \in H\}$$

is therefore non-empty. As in the statement of claim (i) we may then set

$$d := \min(\mathcal{P}).$$

We must prove that g^d generates H.

Since g^d belongs to H, we know that $\langle g^d \rangle$ is contained in H. To prove the converse inclusion, let h be an element of H. Then $h = g^a$ for some integer a, and by the Division Algorithm we may write $a = qd + r$ for $0 \leq r \leq d - 1$. Then

$$g^r = g^{a-qd} = g^a (g^d)^{-q} = h(g^d)^{-q}$$

belongs to H, because both h and g^d belong to H.

By the minimality of d, this means that $r = 0$. But then $a = qd$ so $h = g^a = (g^d)^q$ belongs to $\langle g^d \rangle$. We have proved the reverse inclusion, so $H = \langle g^d \rangle$ is cyclic. This completes the proof of claim (i).

To prove claim (ii) we assume that G is finite with $n := |G|$, we fix a generator g of G and a natural number d that divides n. We set $k := n/d$. Then Proposition 2.40(ii) implies that $\mathrm{o}(g^k) = n/(n, n/d) = n/(n/d) = d$ so Proposition 2.36 implies that $H_d := \langle g^k \rangle$ has order d.

We must show that H_d is the unique subgroup of G of order d. Let K be such a group. By claim (i) we know that $K = \langle g^b \rangle$ where b is the smallest natural number for which g^b

belongs to K. By Proposition 2.40(ii) we also know that

$$\frac{n}{k} = d = |K| = |\langle g^b \rangle| = \mathrm{o}(g^b) = \frac{n}{(n,b)},$$

so $k = (n, b)$. Therefore k divides b, say $b = kq$, so $g^b = (g^k)^q$ belongs to $\langle g^k \rangle = H_d$ and therefore

$$K = \langle g^b \rangle \subseteq H_d.$$

Since K and H_k have the same order, they must be equal. This proves the uniqueness of H_d.

To prove the final assertion of claim (ii), we must show that the order of every subgroup of G must divide $|G|$. Let J be a subgroup of G. By claim (i) we know that $J = \langle g^m \rangle$ for some integer m. But then

$$|J| = \mathrm{o}(g^m) = \frac{\mathrm{o}(g)}{(\mathrm{o}(g), m)} = \frac{|G|}{(|G|, m)},$$

which divides $|G|$ as required. Here we have used Proposition 2.40(ii) and Proposition 2.36.

The proof of claim (iii) is similar, and we leave it as an exercise for an interested reader. □

Exercise 2.46. In $G = \mathbb{Z}/12\mathbb{Z}$, show that $[1], [5], [7]$ and $[11]$ are all generators of G. Find the set of generators of the subgroup of G of order 6, the set of generators of the subgroup of G of order 4, the set of generators of the subgroup of G of order 3 and the set of generators of the subgroup of G of order 2.

2.3. **Lagrange's Theorem.** You may have noticed that in the examples of a finite group G we have encountered so far, each element we have considered has order dividing $|G|$. And, more generally, that each subgroup we have considered also has order dividing $|G|$. In this section we will formalise this intuition thanks to Lagrange's Theorem.

2.3.1. *The cosets of a subgroup.*

Definition 2.47. Let G be a group and let H be a subgroup of G. For any element g of G, the set

$$gH := \{gh : h \in H\}$$

is called a left coset of H in G. For any element g of G, the set

$$Hg := \{hg : h \in H\}$$

is called a right coset of H in G.

Notation 2.48. If $G = (G, +)$ is a group for which we use additive notation, then we shall often write $g + H$ for the left coset gH and $H + g$ for right coset Hg.

Example 2.49. We consider the group $G = \mathbb{Z}$ together with the subgroup $H = 5\mathbb{Z}$. Then we have

$$\begin{aligned} &0 + 5\mathbb{Z} = 5\mathbb{Z} = \{5a : a \in \mathbb{Z}\} = 5\mathbb{Z} + 0, \\ &1 + 5\mathbb{Z} = \{1 + 5a : a \in \mathbb{Z}\} = 5\mathbb{Z} + 1, \qquad 2 + 5\mathbb{Z} = \{2 + 5a : a \in \mathbb{Z}\} = 5\mathbb{Z} + 2, \\ &3 + 5\mathbb{Z} = \{3 + 5a : a \in \mathbb{Z}\} = 5\mathbb{Z} + 3, \qquad 4 + 5\mathbb{Z} = \{4 + 5a : a \in \mathbb{Z}\} = 5\mathbb{Z} + 4. \end{aligned}$$

It is also easy to see that, for any $0 \leq r \leq 4$ and any $q \in \mathbb{Z}$, one has

$$(5q + r) + 5\mathbb{Z} = r + 5\mathbb{Z} = 5\mathbb{Z} + r = 5\mathbb{Z} + (5q + r).$$

Exercise 2.50. We consider the group $G = D_6$ together with the subgroups $H = \{1, r, r^2\}$ and $H' = \{1, s\}$. Verify that we have the following equalities:

(i) $1H = rH = r^2H = H = Hr^2 = Hr = H1$.
(ii) $sH = (sr)H = (sr^2)H = \{s, sr, sr^2\} = H(sr^2) = H(sr) = Hs$.
(iii) $1H' = sH' = H' = H's = H'1$.
(iv) $rH' = (sr^2)H' = \{r, sr^2\}$.
(v) $r^2H' = (sr)H' = \{r^2, sr\}$.
(vi) $H'r = H'(sr) = \{r, sr\}$.
(vii) $H'r^2 = H'(sr^2) = \{r^2, sr^2\}$.

Remark 2.51. Please note from the above exercise that, for instance, $rH' \neq H'r$. However, as we will see shortly, not only do both left and right cosets have the same cardinality as the subgroup they are associated to, but also they each define partitions of the group G. But these may be two different partitions!

Exercise 2.52. Construct a surjective homomorphism $D_6 \to \mathbb{Z}/2\mathbb{Z}$. Convince yourself that there does not exist a surjective homomorphism $D_6 \to \mathbb{Z}/3\mathbb{Z}$.

Lemma 2.53. *The sets H, g_1H and Hg_2 have the same cardinality, for any elements g_1, g_2 of G.*

Proof. If we fix $g_1 \in G$, then the function $f_{g_1} : H \to g_1H$, defined by setting $f_{g_1}(h) := g_1 \cdot h$ for each $h \in H$, is a well defined bijection. Indeed, it is clearly surjective, and also injective by the cancellation property Proposition 1.11. Alternatively, it admits an inverse function defined by left-multiplication by g_1^{-1}.

This shows that H has the same cardinality as g_1H for any $g_1 \in G$. The proof that H has the same cardinality as Hg_2 for any $g_2 \in G$ is identical. □

Definition 2.54. Let G be a group and let H be a subgroup of G. We define a binary relation on G by saying that an element x of G is 'congruent modulo H' (or 'related modulo H') to an element y of G, if the element $y^{-1}x$ belongs to H.

If x is congruent modulo H to y then we write

$$x \equiv y \pmod{H}$$

or simply $x \equiv y \ (H)$ or even $x \equiv_H y$.

Proposition 2.55. *Let G be a group and let H be a subgroup of G. Then the relation of Definition 2.54 is an equivalence relation and, for any $g \in G$, the equivalence class $[g]_H$ of g under this relation is equal to gH.*

Proof. The relation is reflexive because $x^{-1}x = 1$ belongs to H, since it is a subgroup, for any $x \in G$.

Assume that $x \equiv y \ (H)$, so $y^{-1}x$ belongs to H. Since H is a subgroup, we then know that $(y^{-1}x)^{-1}$ belongs to H. But $(y^{-1}x)^{-1} = x^{-1}y$ (by Proposition 1.11), so $y \equiv x \ (H)$. The relation is thus symmetric.

Assume that $x \equiv y \ (H)$, so $y^{-1}x$ belongs to H, and also that $y \equiv z \ (H)$, so $z^{-1}y$ belongs to H. Since H is a subgroup we get that $(z^{-1}y)(y^{-1}x)$ belongs to H, and this element is clearly equal to $z^{-1}x$. Therefore $x \equiv z \ (H)$, so the relation is transitive.

Let now g be any element of G. The equivalence class $[g]_H$ of g is by definition

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

But $g^{-1}x$ belongs to H if and only if x belongs to gH, so we find that $[g]_H = gH$, as required. □

Corollary 2.56. *Let G be a group and let H be a subgroup of G. Then the set of left cosets of H in G is a partition of G.*

Furthermore, $xH = yH$ if and only if $x \equiv y \ (H)$.

Remark 2.57. We deduce that $gH = H$ if and only if g belongs to H.

Exercise 2.58. It is clear from Example 2.49 that for integers x and y, one has $x \equiv y \pmod{5\mathbb{Z}}$ if and only if $x \equiv y \pmod 5$. Show that, for any natural number n, one has $x \equiv y \pmod{n\mathbb{Z}}$ if and only if $x \equiv y \pmod n$.

Remark 2.59. One can define a *different* equivalence relation than the one in Definition 2.54 that has the property that, for any element g of G, the equivalence class of g is equal to Hg. We emphasize again that, in general, this relation would be different and hence would give a different partition of G. However one again has $Hg = H$ if and only if g belongs to H.

Exercise 2.60. Can you give an explicit definition of an equivalence relation that has the property described in Remark 2.59?

2.3.2. *Lagrange, Euler, Fermat, Cauchy.* We may now easily prove Lagrange's Theorem by using the properties of left cosets (an analogous argument may also be developed through the use of right cosets).

Theorem 2.61. *Let G be a finite group and let H be a subgroup of G. Then the order of H divides the order of G. In addition, the number of left cosets of H in G is equal to $|G|/|H|$.*

Proof. By Corollary 2.56 we know that the set of left cosets of H in G is a partition of the finite group G. Explicitly, this means that there is a natural number m, the number of left cosets of H in G, and elements $g_1, \dots, g_m$ of G, with the properties that

$$G = \bigcup_{1 \le i \le m} g_i H$$

and that $(g_j H) \cap (g_k H) = \emptyset$ whenever $j \neq k$.

We only need to show that $|G| = m|H|$ in order to complete the proof. We know from the above description of G that $|G| = \sum_{1 \le i \le m} |g_i H|$ (here we have used the fact that the given cosets are disjoint). But Lemma 2.53 states that $|g_i H| = |H|$ for each i, so we conclude that $|G| = \sum_{1 \le i \le m} |H| = m|H|$, as required. □

Example 2.62. You checked in Exercise 2.50 that in $G = D_6$, a group of order 6, the subgroup $H = \{1, r, r^2\}$ has 2 left cosets, namely H itself and $\{s, sr, sr^2\}$. You also checked that the subgroup $H' = \{1, s\}$ has 3 left cosets, namely H', $\{r, sr^2\}$ and $\{r^2, sr\}$.

Definition 2.63. Let G be a group and let H be a subgroup of G. The number of left cosets of H in G is called the 'index' of H in G and is denoted by $[G : H]$ (or sometimes $|G : H|$ or $(G : H)$). We say that this index is finite or infinite depending on whether this number is finite or not.

Remark 2.64. It is easy to see, by using Lemma 2.53 and Remark 2.59, that the index of H in G is equal to the number of right cosets of H in G.

Remark 2.65. Lagrange's Theorem implies that if G is a finite group, then any subgroup H of G has finite index in G equal to $|G|/|H|$. However if G is an infinite group, then there exist subgroups of G that have finite index and subgroups of G that have infinite index. For instance, the subgroup $H = G$ of G always has finite index equal to 1 in G, while the subgroup $H = \{1\}$ has infinite index in G.

Exercise 2.66. How many subgroups of $\mathbb{Z}$ have infinite index? And, for each natural number n, how many subgroups of $\mathbb{Z}$ have finite index equal to n?

Corollary 2.67. *Let G be a finite group. Then for every $g \in G$, the order $\mathrm{o}(g)$ of g divides $|G|$. In particular, $g^{|G|} = 1$.*

Proof. By Proposition 2.36 we know that $\mathrm{o}(g) = |\langle g \rangle|$, so Lagrange's Theorem implies that $\mathrm{o}(g)$ divides $|G|$. The equality $g^{|G|} = 1$ is an immediate consequence. □

Exercise 2.68.
(i) Prove Euler's Theorem, stating that if n is a natural number and a is an integer coprime to n, then

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where φ denotes Euler's function.
(ii) Prove Fermat's Little Theorem, stating that if p is a prime number and a is an integer with $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Corollary 2.69. *Let G be a finite group whose order is a prime number. Then G is cyclic. In particular if $|G| = p$ is prime then G has isomorphism class C_p.*

Proof. Let g be any element of G that is different from 1 (if $G = \{1\}$ then $|G|$ is not prime). Then $\mathrm{o}(g) > 1$. By Corollary 2.67, $\mathrm{o}(g)$ divides $|G|$, which is prime, so in fact $\mathrm{o}(g) = |G|$.

By Proposition 2.36 we therefore know that the subgroup $\langle g \rangle$ of G has order equal to $|G|$. Therefore we must have $\langle g \rangle = G$, which means that G is cyclic.

The final assertion is immediate from Corollary 2.38 (ii), which allowed us to introduce C_p in Notation 2.39. □

Remark 2.70. The full converse to Lagrange's Theorem is **not** true. There exist finite groups G and natural numbers n dividing $|G|$ with the property that G has no subgroup of order n. We will see explicit examples in the next section. There are, however, some partial converses to Lagrange's Theorem, that we will prove below. For instance:

(i) If G is a finite abelian group and n divides $|G|$ then G has a subgroup of order n.
(ii) If G is a finite group and p is a prime divisor of $|G|$, then G has a subgroup of order p (which is necessarily cyclic by Corollary 2.69). This result is known as Cauchy's Theorem.

2.4. **(More) Exercises.** Don't forget to think about the exercises given throughout the rest of section 2.

Exercise 2.71. Give an example of a group $(G, \star)$ and of a subset H of G that is closed under $\star$ but is not a subgroup of G

Exercise 2.72. Let G be a group of finite order $n \geq 2$. Prove that G can not have a subgroup of order $n-1$.

Exercise 2.73. Let A be an abelian group and set $A_{\text{tor}} := \{a \in A : \text{o}(a) < \infty\}$. Prove that A_{tor} is a subgroup of A. This subgroup is called the 'torsion subgroup' of A.

Exercise 2.74. Let A be an abelian group and $n \in \mathbb{N}$. Show that $\{a \in A : \text{o}(a) \mid n\}$ is a subgroup of A.

Exercise 2.75. Find a group G for which the subset $\{g \in G : \text{o}(g) < \infty\}$ is not a subgroup of G.

Exercise 2.76. Fix $n \geq 2$ and set $A := \mathbb{Z} \times (\mathbb{Z}/n\mathbb{Z})$.

(i) Find all the elements of A_{tor}.
(ii) Show that the subset $\{a \in A : \text{o}(a) = \infty\} \cup \{(0, [0])\}$ is not a subgroup of A

Exercise 2.77. Let H and K be subgroups of G. Prove that $H \cup K$ is a subgroup of G if and only if either $H \cup K = H$ or $H \cup K = K$.

Exercise 2.78. We define a subset

$$\text{Sl}_n(F) := \{A \in \text{Gl}_n(F) : \det(A) = 1\}$$

of $\text{Gl}_n(F)$, called the 'special linear group'. Prove that it is a subgroup. Is $\text{Sl}_n(F)$ the kernel of any homomorphism $\text{Gl}_n(F) \to \text{Gl}_m(F)$ for some m?

Exercise 2.79. Let G and J be groups. Prove that the subsets $H_G := \{(g, 1) : g \in G\}$ and $H_J := \{(1, j) : j \in J\}$ are subgroups of $G \times J$. Define a homomorphism $f_J : G \times J \to J$ for which $\ker(f_J) = H_G$ and a homomorphism $f_G : G \times J \to G$ for which $\ker(f_G) = H_J$.

Exercise 2.80. Let G be a group. Prove that the subset $\{(g, g) : g \in G\}$ is a subgroup of $G \times G$.

Exercise 2.81.
(i) Show that if H_1 is a subgroup of a group G_1 and H_2 is a subgroup of a group G_2 then $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$.
(ii) Find groups G_1 and G_2 and a subgroup H of $G_1 \times G_2$ that is **not** equal to $H_1 \times H_2$ for any subgroups H_1 of G_1 and H_2 of G_2.

Exercise 2.82. Let A be an abelian group and $n \in \mathbb{Z}$. Prove that the subsets $\{a^n : a \in A\}$ and $\{a \in A : a^n = 1\}$ are subgroups of A.

Exercise 2.83. Show that $\{x \in D_{2n} : x^2 = 1\}$ is not a subgroup of D_{2n}.

Exercise 2.84. Let H be a subgroup of $\mathbb{Q}$ with the property that $1/h$ belongs to H for every non-zero element of H. Prove that either $H = 0$ or $H = \mathbb{Q}$.

Exercise 2.85.
(i) Find all subgroups of $\mathbb{Z}/48\mathbb{Z}$, giving a generator for each. Give also all the containments between these subgroups.
(ii) Find all generators of $\mathbb{Z}/48\mathbb{Z}$.
(iii) Show that, for each $x \in \mathbb{Z}/48\mathbb{Z}$, there is a unique homomorphism

$$f_x : \mathbb{Z}/48\mathbb{Z} \to \mathbb{Z}/48\mathbb{Z}$$

that satisfies $f_x([1]) = x$.
(iv) Determine all elements x of $\mathbb{Z}/48\mathbb{Z}$ for which f_x is an isomorphism.

Exercise 2.86. Find all generators of $\mathbb{Z}/202\mathbb{Z}$.

Exercise 2.87. Find the number of generators of $\mathbb{Z}/49000\mathbb{Z}$.

Exercise 2.88. What is the order of $[30]$ in $\mathbb{Z}/54\mathbb{Z}$? Write down all the elements of the subgroup $\langle[30]\rangle$ of $\mathbb{Z}/54\mathbb{Z}$, and determine the order of each of these elements.

Exercise 2.89. Find all cyclic subgroups of D_8. Find a *proper* subgroup of D_8 that is not cyclic.

Exercise 2.90. Prove that the following groups are *not* cyclic: $C_2 \times C_2$, $C_2 \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Q} \times \mathbb{Q}$.

Exercise 2.91. Prove that $C_2 \times \mathbb{Z}$ is not isomorphic to $\mathbb{Z}$ and that $C_2 \times \mathbb{Q}$ is not isomorphic to $\mathbb{Q}$.

Exercise 2.92. Let $\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12) \in S_{12}$. Find σ^a for each of $a = 13, 65, 626, 1195, -6, -81, -570, -1211$.

Exercise 2.93.
(i) Prove that if elements x and y of a group G commute, then $\mathrm{o}(xy)$ divides $\mathrm{lcm}(\mathrm{o}(x), \mathrm{o}(y))$.
(ii) Find a group G and elements x and y of G so that $\mathrm{o}(xy)$ does not divide $\mathrm{lcm}(\mathrm{o}(x), \mathrm{o}(y))$.
(iii) Find a group G and commuting elements x and y of G so that $\mathrm{o}(xy)$ does not equal $\mathrm{lcm}(\mathrm{o}(x), \mathrm{o}(y))$.

Exercise 2.94. Let G be a group and let g be an element of G of finite order. Let n be any positive multiple of $\mathrm{o}(g)$. Prove that there is a unique homomorphism $f : \mathbb{Z}/n\mathbb{Z} \to G$ with the property that $f([1]) = g$.

Exercise 2.95. Let G be any group and let g be any element of G. Prove that there is a unique homomorphism $f : \mathbb{Z} \to G$ with the property that $f(1) = g$.

Exercise 2.96. Let p be a prime and $n \in \mathbb{N}$. Let G be a group and let g be an element of G for which $g^{p^n} = 1$. Prove that $\mathrm{o}(g) = p^m$ for some $0 \le m \le n$.

Exercise 2.97. Let p be an *odd* prime and let $n \in \mathbb{N}$. Use the Binomial Theorem to show that

$$(1 + p)^{p^{n-1}} \equiv 1 \pmod{p^n}$$

but

$$(1 + p)^{p^{n-2}} \not\equiv 1 \pmod{p^n}.$$

What is the order of $[1 + p]$ in the group $(\mathbb{Z}/p^n\mathbb{Z})^\times$?

Exercise 2.98. What is the order of $[5]$ in $(\mathbb{Z}/2^n\mathbb{Z})^\times$, for $n \geq 3$?

Exercise 2.99. Show that if $n \geq 3$ then the group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is *not* cyclic.

Exercise 2.100. Let G be a finite group and let k be an integer coprime to $|G|$. Prove that the function $G \to G$ given by $g \mapsto g^k$ for each $g \in G$ is surjective. (Careful: this function is in general **not** a homomorphism.)

Exercise 2.101. For each $a \in \mathbb{Z}$ we define a function

$$\sigma_a : C_n \to C_n$$

by setting $\sigma_a(x) := x^a$ for each $x \in C_n$. (Recall that we always use multiplicative notation in 'the group' C_n.)

(i) Prove that σ_a is a homomorphism.
(ii) Prove that σ_a is an isomorphism if and only if $(a, n) = 1$.
(iii) Prove that $\sigma_a = \sigma_b$ if and only if $a \equiv b \pmod{n}$.
(iv) Prove that every automorphism of C_n is equal to σ_a for some $a \in \mathbb{Z}$ (coprime to n, by (ii)).
(v) Prove that $\sigma_a \circ \sigma_b = \sigma_{ab}$.
(vi) Prove that there is an isomorphism

$$f : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(C_n)$$

given by $f([a]) := \sigma_a$.
(vii) Prove that $\mathrm{Aut}(C_n)$ is abelian of order equal to $\varphi(n)$.

Exercise 2.102. Prove that if $S \subseteq S'$ are subsets of a group G then $\langle S \rangle \subseteq \langle S' \rangle$. Give an example of such a group G and such sets S and S' for which $S \neq S'$ but $\langle S \rangle = \langle S' \rangle$.

Exercise 2.103. Show that if $x, y \in S_3$ have $x \neq y$ and $\mathrm{o}(x) = 2 = \mathrm{o}(y)$ then $\langle x, y \rangle = S_3$.

Exercise 2.104. Prove that the subgroup $\langle (1,2); (1,2)(3,4) \rangle$ of S_4 is isomorphic to $C_2 \times C_2$.

Exercise 2.105. Prove that the subgroup $\langle (1,2); (1,3)(2,4) \rangle$ of S_4 is isomorphic to D_8.

Exercise 2.106. Prove that the subgroup $\langle (1,2,3,4); (1,2,4,3) \rangle$ is equal to S_4.

Exercise 2.107. Prove that the subset $\{-1\} \cup \{1/p : p \in \mathbb{N} \text{ is prime}\}$ generates $\mathbb{Q}^*$.

Exercise 2.108. A group G is called 'finitely generated' if there is a finite subset S of G such that $\langle S \rangle = G$.

(i) Prove that every finite group G is finitely generated.
(ii) Prove that $\mathbb{Z}$ is finitely generated.
(iii) Prove that $\mathbb{Q}$ and $\mathbb{Q}^*$ are **not** finitely generated.
(iv) Let H be a subgroup of $\mathbb{Q}$ that is finitely generated. Prove that H is cyclic.
(v) Find a **proper** subgroup of $\mathbb{Q}$ that is not cyclic.

Exercise 2.109. Let p be a prime and set

$$G := \{z \in \mathbb{C} : z^{p^n} = 1 \text{ for some } n \in \mathbb{N}\}.$$

For each $k \in \mathbb{N}$ set

$$H_k := \{z \in \mathbb{C} : z^{p^k} = 1\}.$$

(i) Prove that H_k is a finite subgroup of G and that $H_k \subseteq H_l$ if and only if $k \leq l$.
(ii) Prove that H_k is a cyclic group.
(iii) Prove that every proper subgroup of G is equal to H_k for some k.
(iv) Prove that G is **not** finitely generated.

Exercise 2.110. Let p be a prime and let G be a group of order $2p$. Show that every proper subgroup of G is cyclic.

Exercise 2.111. Let G be a group and let g be an element of G of finite order $\mathrm{o}(g) = n$. Let $d \in \mathbb{N}$ be a divisor of n. Prove that G has an element of order d.

Exercise 2.112. Find subgroups H and K of D_8 with the property that the subset

$$HK := \{hk : h \in H, k \in K\}$$

is **not** a subgroup of G.

Exercise 2.113. Let p be a prime and $n \in \mathbb{N}$. Let H and K be subgroups of C_{p^n}. Show that either $H \subseteq K$ or $K \subseteq H$ (or both).

Exercise 2.114. Let n be a natural number for which $2^n + 1$ is a prime number.
(i) Determine the order of $[2]$ in $(\mathbb{Z}/(2^n + 1)\mathbb{Z})^\times$.
(ii) Deduce that n is a power of 2.

Exercise 2.115.
(i) Find all the subgroups of D_{16} that are contained in $\langle sr^2, r^4 \rangle$.
(ii) Find all the subgroups of D_{16} that are contained in $\langle sr^7, r^4 \rangle$.
(iii) Find all the subgroups of D_{16} that contain $\langle r^4 \rangle$.
(iv) Find all the subgroups of D_{16} that contain $\langle s \rangle$.

Exercise 2.116. Show that if H and K are finite subgroups of a group G that have coprime orders, then $H \cap K = \{1\}$.

3. Isomorphism theorems

3.1. **Normal subgroups and quotient groups.** The subgroups of a group G give us information about the structure of G. Recall that a subgroup of G may be thought of as an injective homomorphism $H \hookrightarrow G$ of groups. It is natural to wonder whether we can carry out an analogous study of surjective homomorphisms $G \twoheadrightarrow J$ of groups.

In addition, we know from Definition 2.54 and Proposition 2.55 that each subgroup H fo G defines an equivalence relation $\equiv_H$ on G. In fact, as outlined in Remak 2.59 and Exercise 2.60, H defines *two* natural equivalence relations on G, which are in general different but may coincide for some examples (see also Example 2.49, Exercise 2.50, Remark 2.51 and Exercise 2.52).

We know that there is a surjective 'projection' function π_H from G to the set of equivalence classes $G/\equiv_H$. So the natural question at this point is: **does the binary operation on G induce a well-defined binary operation on the set $G/\equiv_H$?**

If this question had an affirmative answer, then $G/\equiv_H$ would be a group, whose identity element would be H, and π_H would be a surjective homomorphism of groups, whose kernel would be H.

To say that 'the binary operation on G induces a binary operation on the set $G/\equiv_H$' would mean that, for any two elements C_1, C_2 of $G/\equiv_H$, choosing any 'representatives' $g_1, g_2 \in G$ with $C_1 = g_1H$ and $C_2 = g_2H$ and then setting

$$C_1 \star C_2 := (g_1 \star g_2)H,$$

would give a *well-defined* function

$$\big((G/\equiv_H) \times (G/\equiv_H)\big) \to G/\equiv_H .$$

The answer to the question is **not** affirmative in general. Consider, as in Exercise 2.50, the group $G = D_6$ and subgroup $H' = \{1, s\}$. We have

$$(D_6/\equiv_{H'}) = \{H', \{r, sr^2\}, \{r^2, sr\}\}$$

with $1H' = sH' = H'$, $rH' = (sr^2)H' = \{r, sr^2\}$ and $r^2H' = (sr)H' = \{r^2, sr\}$. Then, at the same time,

$$H' \star \{r, sr^2\} = (1H') \star (rH') = (1r)H' = rH' = \{r, sr^2\}$$

and

$$H' \star \{r, sr^2\} = (sH') \star (rH') = (sr)H' = \{r^2, sr\}.$$

Clearly, this is not a well-defined function, as $\{r, sr^2\} \neq \{r^2, sr\}$.

Even if the answer to the question is not affirmative in general, it may be affirmative for some examples. For instance, let $f : G \to J$ be a homomorphism of groups. Recall from Definition 2.12 and Proposition 2.13 (ii) that the kernel $K := \ker(f)$ of f is a subgroup of G. We will prove below that the binary operation on G does induce a binary operation on the set $G/\equiv_K$.

In fact, we will prove that the following three conditions on a subgroup H of a group G are equivalent:

(i) The two natural equivalence relations on G defined by H coincide.
(ii) The binary operation on G induces a well-defined binary operation on $G/\equiv_H$.
(iii) H is the kernel of some homomorphism, that has domain G.

We will say that H is a 'normal subgroup of G' if it satisfies either of these three equivalent conditions. In that case, the resulting set $G/\equiv_H$ will indeed be a group, which we shall denote simply by G/H and call the 'quotient group' of G over H.

3.1.1. *The fibres of a homomorphism.*

Definition 3.1. Let $f : G \to J$ be a homomorphism of groups. For each $y \in J$, the set

$$f^{-1}(y) := f^{-1}(\{y\}) = \{x \in G : f(x) = y\}$$

is called the 'fibre' of f at y.

Remarks 3.2.
(i) We have $\ker(f) = f^{-1}(1)$, so the kernel of f is a distinguished fibre of f.
(ii) Clearly $f^{-1}(y)$ is non-empty if and only if y belongs to $\mathrm{im}(f)$. In particular the set of non-empty fibres of f is

$$\{f^{-1}(y) : y \in J\} = \{f^{-1}(y) : y \in \mathrm{im}(f)\} = \{f^{-1}(f(x)) : x \in G\}. \tag{13}$$

Example 3.3. Fix a natural number n and consider the map

$$f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

given by $f(a) := [a]$ for each $a \in \mathbb{Z}$. Clearly f is a surjective homomorphism with kernel

$$\ker(f) = n\mathbb{Z}. \tag{14}$$

For each $b \in \mathbb{Z}$ we have

$$f^{-1}([b]) = \{a \in \mathbb{Z} : [a] = [b]\} = \{a \in \mathbb{Z} : a \equiv b \ \ (n\mathbb{Z})\} = b + n\mathbb{Z} = b + \ker(f).$$

Thus the fibres of f are

$$\ker(f) = f^{-1}([0]),\ \ 1+\ker(f) = f^{-1}([1]),\ \ 2+\ker(f) = f^{-1}([2]), \ldots, (n-1)+\ker(f) = f^{-1}([n-1]).$$

Keeping (14) in mind, it is now very easy to see that the set of fibres of f coincides with the set $\mathbb{Z}/\equiv_{\ker(f)}$ of left cosets of $\ker(f)$ in $\mathbb{Z}$.

In this special case, the addition in $\mathbb{Z}$ induces a well-defined binary operation on $\mathbb{Z}/\equiv_{\ker(f)}$. Indeed, if $C_1 = a_1 + \ker(f) = b_1 + \ker(f)$ and $C_2 = a_2 + \ker(f) = b_2 + \ker(f)$ then $\{a_1 + nx : x \in \mathbb{Z}\} = \{b_1 + nx : x \in \mathbb{Z}\}$ and $\{a_2 + nx : x \in \mathbb{Z}\} = \{b_2 + nx : x \in \mathbb{Z}\}$ and therefore

$$\begin{aligned}(a_1 + a_2) + \ker(f) = \{a_1 + a_2 + nx : x \in \mathbb{Z}\} &= \{a_1 + b_2 + nx : x \in \mathbb{Z}\}\\ &= \{b_1 + b_2 + nx : x \in \mathbb{Z}\} = (b_1 + b_2) + \ker(f).\end{aligned}$$

This proves that the addition $C_1 + C_2$ is well-defined for any C_1, C_2 in $\mathbb{Z}/\equiv_{\ker(f)}$, as it does not depend on the choice of representatives.

It is very easy to see that $(\mathbb{Z}/\equiv_{\ker(f)}, +)$ is a group. If $C_i = a_i + \ker(f)$ for $i = 1, 2, 3$ then

$$\begin{aligned}(C_1 + C_2) + C_3 &= ((a_1 + a_2) + \ker(f)) + C_3 = ((a_1 + a_2) + a_3) + \ker(f)\\ &= (a_1 + (a_2 + a_3)) + \ker(f) = C_1 + ((a_2 + a_3) + \ker(f)) = C_1 + (C_2 + C_3),\end{aligned}$$

which shows that $+$ is associative. The element $\ker(f)$ of $\mathbb{Z}/\equiv_{\ker(f)}$ is the identity element, since for any $C = a + \ker(f)$ we have

$$\begin{aligned} C + \ker(f) &= (a + \ker(f)) + (0 + \ker(f)) = (a + 0) + \ker(f) = a + \ker(f) = C \\ &= a + \ker(f) = (0 + a) + \ker(f) = (0 + \ker(f)) + (a + \ker(f)) = \ker(f) + C. \end{aligned}$$

For any element $C = a + \ker(f)$, the inverse element is $-C := (-a) + \ker(f)$, since

$$\begin{aligned} C + (-C) &= (a + \ker(f)) + ((-a) + \ker(f)) = (a - a) + \ker(f) = \ker(f) \\ &= (-a + a) + \ker(f) = ((-a) + \ker(f)) + (a + \ker(f)) = (-C) + C. \end{aligned}$$

The reader should at this point have the intuition that the group $(\mathbb{Z}/\equiv_{\ker(f)}, +)$ has 'the same structure' as the group $(\mathbb{Z}/n\mathbb{Z}, +)$. To formalise this intuition, simply note that f induces the group *isomorphism*

$$\overline{f} : \mathbb{Z}/\equiv_{\ker(f)} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z},$$

given by

$$\overline{f}(a + \ker(f)) := f(a) + \ker(f) = f(a) + n\mathbb{Z} = [a]_n.$$

This example justifies the notation $\mathbb{Z}/n\mathbb{Z}$!

We will show that some of the arguments in Example 3.3 extend to a more general setting. For now, we begin by proving that, whenever a subgroup is the kernel of a homomorphism, the left and right cosets associated to this subgroup coincide.

Proposition 3.4. *Let $f : G \to J$ be a homomorphism of groups.*

(i) *Let g be any element of G. Then*

$$g\ker(f) = f^{-1}(f(g)) = \ker(f)g.$$

(ii) *Let g and h be elements of G. Then the following conditions are equivalent:*
   (a) *h belongs to $g\ker(f)$.*
   (b) *$h\ker(f) = g\ker(f)$.*
   (c) *$f(h) = f(g)$.*
   (d) *$\ker(f)h = \ker(f)g$.*
   (e) *h belongs to $\ker(f)g$.*

Proof. To prove claim (i) we fix $g \in G$ and we only prove the first equality, $g\ker(f) = f^{-1}(f(g))$. We leave the second equality, which is very similar, as an exercise.

Let k belong to $\ker(f)$. We first claim that gk belongs to $f^{-1}(f(g))$. To se this we must prove that $f(gk) = f(g)$. But this equality is valid because

$$f(gk) = f(g)f(k) = f(g)1 = f(g).$$

We have proved that $g\ker(f) \subseteq f^{-1}(f(g))$.

To prove the converse, let x be any element of G with $f(x) = f(g)$. We must prove that x belongs to $g\ker(f)$. But

$$x = g(g^{-1}x) \tag{15}$$

where $g^{-1}x$ belongs to $\ker(f)$, because

$$f(g^{-1}x) = f(g^{-1})f(x) = f(g)^{-1}f(x) = f(g)^{-1}f(g) = 1.$$

Here the second equality uses Lemma 1.48. So (15) shows that x belongs to $g\ker(f)$. This completes the proof of the equality $g\ker(f) = f^{-1}(f(g))$.

We now prove claim (ii) by using claim (i). The element h belongs to $g\ker(f)$ if and only if it belongs to $f^{-1}(f(g))$, which happens if and only if $f(h) = f(g)$. This shows that (a) is equivalent to (c).

If (c) is valid then

$$h\ker(f) = f^{-1}(f(h)) = f^{-1}(f(g)) = g\ker(f),$$

so (b) is valid.

Similarly if (b) is valid then one easily shows that $f^{-1}(f(h)) = f^{-1}(f(g))$. This equality imples that $f(h)$ must be equal to $f(g)$, so (c) must be valid.

Finally it is clear from claim (i) that (a) is equivalent to (e) and that (b) is equivalent to (d), so all claims must be equivalent. □

Corollary 3.5. *Let $f : G \to J$ be a homomorphism of groups. Then the set of non-empty fibres of f coincides with the set of left cosets of $\ker(f)$ in G.*

Proof. From (13) we know that the set of non-empty fibres of f is $\{f^{-1}(f(g)) : g \in G\}$, which is then equal to the set $\{g\ker(f) : g \in G\}$ of left cosets of $\ker(f)$ in G by Proposition 3.4. □

Remark 3.6. Clearly another application of Proposition 3.4 also shows that the set of non-empty fibres of f coincides with the set of right cosets of $\ker(f)$ in G.

Definition 3.7. Let $f : G \to J$ be a homomorphism of groups. We write $G/\ker(f)$ for the set of left cosets of $\ker(f)$ in G.

Corollary 3.8. *Let $f : G \to J$ be a homomorphism of groups. The binary operation on G induces a well-defined binary operation on $G/\ker(f)$, which makes $G/\ker(f)$ into a group. The identity element of $G/\ker(f)$ is $\ker(f)$ and the inverse of each coset $g\ker(f)$ is $g^{-1}\ker(f)$.*

Moreover, f induces a well-defined isomorphism of groups

$$\overline{f} : G/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$$

given by

$$\overline{f}(g\ker(f)) := f(g)$$

for each $g \in G$.

Proof. We fix elements C_1 and C_2 of $G/\ker(f)$ and elements a_1, b_1, a_2, b_2 of G for which

$$C_1 = a_1\ker(f) = b_1\ker(f), \quad C_2 = a_2\ker(f) = b_2\ker(f).$$

From Proposition 3.4 we get that $f(a_1) = f(b_1)$ and that $f(a_2) = f(b_2)$.

To prove that the binary operation on G induces a well-defined binary operation on $G/\ker(f)$ it is enough to show that $(a_1a_2)\ker(f)$ is equal to $(b_1b_2)\ker(f)$. But this is true because

$$\begin{aligned}(a_1a_2)\ker(f) = f^{-1}(f(a_1a_2)) &= f^{-1}(f(a_1)f(a_2))\\ &= f^{-1}(f(b_1)f(b_2)) = f^{-1}(f(b_1b_2)) = (b_1b_2)\ker(f).\end{aligned}$$

Here the first and last equality are also given by Proposition 3.4.

The induced operation is associative because if $C_i = a_i \ker(f)$ for $i = 1, 2, 3$ then

$$\begin{aligned}(C_1C_2)C_3 = ((a_1a_2)\ker(f))C_3 &= ((a_1a_2)a_3)\ker(f)\\ &= (a_1(a_2a_3))\ker(f) = C_1((a_2a_3)\ker(f)) = C_1(C_2C_3).\end{aligned}$$

For any $C = g\ker(f)$ we have

$$\begin{aligned}C\ker(f) = (g\ker(f))(1\ker(f)) &= (g1)\ker(f) = g\ker(f) = C\\ &= g\ker(f) = (1g)\ker(f) = (1\ker(f))(g\ker(f)) = \ker(f)C\end{aligned}$$

and also

$$\begin{aligned}(g\ker(f))(g^{-1}\ker(f)) &= (gg^{-1})\ker(f) = 1\ker(f) = \ker(f)\\ &= 1\ker(f) = (g^{-1}g)\ker(f) = (g^{-1}\ker(f))(g\ker(f)).\end{aligned}$$

These equalitites combine to imply that $\ker(f)$ is the identity element for the induced binary operation and that $C^{-1} = g^{-1}\ker(f)$. This proves that $G/\ker(f)$ is a group.

We now show that $\overline{f}$ is a well-defined function. If $g\ker(f) = h\ker(f)$ then by Proposition 3.4 we have $f(g) = f(h)$, so $\overline{f}(g\ker(f)) = \overline{f}(h\ker(f))$ is well-defined.

We observe that $\overline{f}$ is a homomorphism of groups because

$$\overline{f}((g_1\ker(f))(g_2\ker(f))) = \overline{f}((g_1g_2)\ker(f)) = f(g_1g_2) = f(g_1)f(g_2) = \overline{f}(g_1\ker(f))\overline{f}(g_2\ker(f)).$$

It is immediately clear that $\overline{f}$ is a surjective function onto $\mathrm{im}(f)$, since for any $g \in G$, $f(g)$ is the image under $\overline{f}$ of $g\ker(f)$.

To conclude that $\overline{f}$ is an isomorphism it is enough to prove that it is injective, so by Proposition 2.13(iii) it is enough to verify that $\ker(\overline{f}) = \{\ker(f)\}$. Therefore (keeping in mind Remark 2.14) we must only prove that if $g\ker(f) \neq \ker(f)$ then

$$\overline{f}(g\ker(f)) = f(g) \neq 1.$$

We assume that $g\ker(f) \neq \ker(f)$ and argue by contradiction. If $f(g) = 1$ then the equivalence of (c) and (b) in Proposition 3.4 (ii) would imply that $g\ker(f) = \ker(f)$, a contradiction. So we must have $f(g) \neq 1$. This shows that $\ker(f)$ is the only element of $\ker(\overline{f})$, so f is injective and thus an isomorphism. □

Remark 3.9. Let $f : G \to J$ be a homomorphism of groups. By Proposition 3.4 and Corollaries 3.5 and 3.8, we find that the the binary operation of G induces a binary operation on the set of non-empty fibres of f which makes it into a group (with identity $\ker(f)$). Moreover, there is an isomorphism $\overline{f}$ from this group to $\mathrm{im}(f)$ which, if $f^{-1}(y)$ is a non-empty fibre of f, is given by $\overline{f}(f^{-1}(y)) = y$.

Remark 3.10. It is straightforward to give another yet description of $\overline{f}$ in terms of right cosets of $\ker(f)$ in G.

Notation 3.11. We often abbreviate the coset $g\ker(f)$ in $G/\ker(f)$ to $[g]$ or to $\overline{g}$ when f is clear from context.

Examples 3.12. (i) In Example 3.3 we were able to show that $\mathbb{Z}/\ker(f)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for the given homomorphism $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ because we implicitly used that f is surjective, so $\mathrm{im}(f) = \mathbb{Z}/n\mathbb{Z}$. As we mentioned, since $\ker(f) = n\mathbb{Z}$, this example justifies the use of the notation $\mathbb{Z}/n\mathbb{Z}$.
(ii) If $f : G \to J$ is an isomorphism then $\ker(f) = \{1\}$ and we have the composite isomorphism

$$G/\{1\} \xrightarrow{\overline{f}} J \xrightarrow{f^{-1}} G,$$

which is explicitly computed as

$$f^{-1}(\overline{f}(g\{1\})) = f^{-1}(f(g)) = g.$$

Of course, even without using Corollary 3.8 it is easy to see that the map $G/\{1\} \to G$ which maps $g\{1\}$ to g is an isomorphism.
(iii) For the trivial homomorphism $f : G \to J$, which maps every $g \in G$ to 1 in J, we have $\ker(f) = G$ and the isomorphism

$$G/G \cong \{1\}.$$

(iv) Consider $\mathbb{R}^2$ and $\mathbb{R}$ as groups under addition (this is automatic since they are vector spaces) and the (surjective) function

$$f : \mathbb{R}^2 \to \mathbb{R}$$

given by $f((x, y)) := x$. This is a group homomorphism (check this fact!). Clearly

$$\ker(f) = \{(x, y) : x = 0\},$$

which geometrically corresponds to the y-axis. Note that the fibre above each $x_0 \in \mathbb{R}$ is simply the vertical line

$$f^{-1}(x_0) = \{(x_0, y) : y \in \mathbb{R}\}$$

through $(x_0, 0)$, which gives a geometrical interpretation of the left coset $(x_0, 0) + \ker(f)$. The group operation on $\mathbb{R}^2/\ker(f)$ induced by the addition on $\mathbb{R}^2$ simply takes any vertical lines $f^{-1}(x_1)$ and $f^{-1}(x_2)$, for any x_1 and x_2, and gives back the line $f^{-1}(x_1 + x_2)$.

Exercise 3.13. We define a function

$$f : Q_8 \to (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$$

by setting

$$f(\pm 1) = ([0], [0]), \;\; f(\pm i) = ([0], [1]), \;\; f(\pm j) = ([1], [0]), \;\; f(\pm k) = ([1], [1]).$$

Show that f is a group homomorphism and write down the group table of $Q_8/\ker(f)$.

3.1.2. *Normal subgroups.*

Proposition 3.14. *Let G be a group and let H be a subgroup of G. Then the following conditions are equivalent.*

(i) *The binary operation on G induces a well-defined binary operation on the set of left cosets of H in G.*
(ii) *The element ghg^{-1} belongs to H for every $g \in G$ and every $h \in H$.*
(iii) *We have an equality of sets $gH = Hg$ for every $g \in G$.*

Proof. We first prove that the conditions (i) and (ii) are equivalent.

We first assume that (i) holds and we fix $g \in G$ and $h \in H$. We must prove that ghg^{-1} belongs to H.

We recall from Remark 2.57 that $hH = H = 1H$. By condition (i) we know that $(gh)H = (g1)H = gH$ and then, using condition (i) again, also that $(ghg^{-1})H = (gg^{-1})H = 1H = H$. Remark 2.57 now implies that $ghg^{-1}1 = ghg^{-1}$ must belong to H, as required.

Conversely, we assume that condition (ii) holds. We let $C_1 = g_1H = g_1'H$ and $C_2 = g_2H = g_2'H$. We know from Corollary 2.56 that

$$h_1 := (g_1')^{-1}g_1 \text{ and } h_2 := (g_2')^{-1}g_2$$

are both elements of H and then from condition (ii) (applied with $h = h_1$ and $g = (g_2')^{-1}$) that

$$h_3 := (g_2')^{-1}h_1g_2'$$

also belongs to H.

We must prove that $(g_1g_2)H = (g_1'g_2')H$. Again by Corollary 2.56, since the set of left cosets of H in G is a partition of G, it will be enough to prove that these two sets have a common element. Clearly g_1g_2 belongs to $(g_1g_2)H$, so it is enough to prove that g_1g_2 also belongs to $(g_1'g_2')H$. This required containment is true because

$$g_1g_2 = g_1'(g_1')^{-1}g_1g_2'(g_2')^{-1}g_2 = g_1'h_1g_2'h_2 = g_1'g_2'((g_2')^{-1}h_1g_2')h_2 = g_1'g_2'h_3h_1.$$

We next prove that conditions (ii) and (iii) are equivalent.

We first assume that (ii) holds and we fix $g \in G$. Then

$$gH = \{gh : h \in H\} = \{(ghg^{-1})g : h \in H\} \subseteq Hg$$

and, similarly,

$$Hg = \{hg : h \in H\} = \{g(g^{-1}hg) : h \in H\} \subseteq gH.$$

Thus gH and Hg must be equal, as required.

Conversely, we assume that condition (iii) holds and we fix $g \in G$ and $h \in H$. Then $gh = h'g$ for some h' in H and therefore $ghg^{-1} = h'gg^{-1} = h' \in H$, as required. □

Definition 3.15.
(i) Let G be a group and let H be a subgroup of G. We say that 'H is normal in G' if ghg^{-1} belongs to H for every $g \in G$ and every $h \in H$.
(ii) Let G be a group and let H be a subset of G. We say that 'H is a normal subgroup of G' to indicate that H is a subgroup of G that is normal in G.

Notation 3.16. Let G be a group. The notation $H \trianglelefteq G$ means that H is a normal subgroup of G.

Definition 3.17. Let G be a group and let H be a subset of G. For any element g of G, the set

$$gHg^{-1} := \{ghg^{-1} : h \in H\}$$

is called the 'conjugate of H by g'. Each individual element of the form ghg^{-1} is called the 'conjugate of h by g'. We also say that 'g normalises H' if the set gHg^{-1} is equal to H.

Exercise 3.18. Let G be a group and let H be a subgroup of G.

(i) For any $g \in G$, prove that the conjugate gHg^{-1} of H by g is a subgroup of G.

(ii) For any $g \in G$, prove that the function
$$f_g : H \to gHg^{-1},$$
given by $f_g(h) := ghg^{-1}$ for each $h \in H$, is a homomorphism.

(iii) Prove that each homomorphism f_g in claim (ii) is actually an isomorphism.

(iv) Prove that H is normal in G if and only if every element g of G normalises H.

Remark 3.19. Let G be a group, let H be a subgroup of G and let g_0 be an element of G. It is not true that $g_0Hg_0^{-1} \subseteq H$ if and only if $g_0Hg_0^{-1} = H$. However, it is true that $gHg^{-1} \subseteq H$ for every $g \in G$ if and only if $gHg^{-1} = H$ for every $g \in G$.

Corollary 3.20. *Let G be a group and let H be a subgroup of G. If H is normal in G, then the set of left cosets of H in G is a group under the binary operation induced from the binary operation on G. The identity element of this group is H and, for any $g \in G$, one has $(gH)^{-1} = g^{-1}H$.*

Proof. By Proposition 3.14 we know that the binary operation on the set of left cosets of H in G is well-defined. Associativity of this operation follows easily from associativity of the original operation, as
$$\begin{aligned}((g_1H)(g_2H))g_3H &= ((g_1g_2)H)g_3H = ((g_1g_2)g_3)H \\ &= (g_1(g_2g_3))H = g_1H((g_2g_3)H)) = g_1H((g_2H)(g_3H))\end{aligned}$$
for any $g_1, g_2, g_3 \in G$.

The fact that H is the identity element of this group follows easily from the equality $H = 1H$, and then the equality $(gH)^{-1} = g^{-1}H$ also becomes very easy to verify. □

Definition 3.21. Let G be a group and let H be a normal subgroup of G. We write G/H for the set of left cosets of H in G, always considered as a group with the binary operation induced by that of G. We call G/H the 'quotient group of G over H'. We also write π_H for the function $G \to G/H$ defined by
$$\pi_H(g) := gH$$
and call it the 'projection map' of G onto G/H.

Exercise 3.22. Let G be a group and let H be a normal subgroup of G. Prove that $\pi_H : G \to G/H$ is a group homomorphism, that it is surjective, and that $\ker(\pi_H) = H$.

Proposition 3.23. *Let G be a group and let H be a subgroup of G. Then H is normal in G if and only if H is the kernel of a group homomorphism that has G as its domain.*

Proof. We know from Corollary 3.8 that if $H = \ker(f)$ for some group homomorphism $f : G \to J$, then the binary operation on G induces a well-defined binary operation on the set of left cosets of H in G. By Proposition 3.14 it would then follow that H is normal in G.

Conversely, assume that H is normal in G. Then from Exercise 3.22 we know that H is the kernel of the homomorphism of groups $\pi_H : G \to G/H$. □

Exercise 3.24. Let G be a group and let H be a normal subgroup of G. Verify that $(gH)^a = g^aH$ in G/H, for every $a \in \mathbb{Z}$.

Proposition 3.25. *Let G be an abelian group. Then every subgroup of G is normal in G.*

Proof. Let H be any subgroup of G. Let g be any element of G and let h be any element of H. Then $ghg^{-1} = hgg^{-1} = h$ belongs to H, so H is normal in G. □

Remark 3.26. In general, an abelian subgroup H of a group G is **not** normal in G. For instance, in the list (16) below, the subgroups H', H'' and H''' of $G = D_6$ are all abelian, but they are not normal in G.

Remark 3.27. A subgroup H of a group G can be normal in G even if there are elements h of H and g of G for which $ghg^{-1} \neq h$. For instance, in $G = D_6$ we know from Exercise 2.50 that $H = \{1, r, r^2\}$ is normal in G, but

$$srs = r^2 \neq r \text{ and } sr^2s = r \neq r^2.$$

Of course, the key point is that we still have the equality of sets

$$sHs = \{1, r^2, r\} = H,$$

so that s normalises H.

Examples 3.28.
(i) The subgroups $\{1\}$ and G of G are both normal in G, and there are canonical isomorphisms $G/\{1\} \cong G$ and $G/G \cong \{1\}$. See also Examples 3.12 (ii) and (iii).
(ii) All the subgroups of $G = D_6$ are

$$G,\ H = \{1, r, r^2\},\ H' = \{1, s\},\ H'' = \{1, sr\},\ H''' = \{1, sr^2\} \text{ and } \{1\}. \tag{16}$$

We know that both $\{1\}$ and G are normal in G and we know from Exercise 2.50 that H is normal in G but that H' is not normal in G, as

$$rH' = \{r, sr^2\} \neq \{r, sr\} = H'r.$$

In a similar way one can show that H'' and H''' are not normal in G.
(iii) By Proposition 3.25, all subgroups of $\mathbb{Z}$ are normal. All the possible quotients of $\mathbb{Z}$ are $\{0\} = \mathbb{Z}/\mathbb{Z}$, $\mathbb{Z} = \mathbb{Z}/\{0\}$ and the finite cyclic groups $\mathbb{Z}/n\mathbb{Z}$ for each natural number $n \neq 1$ (as $1\mathbb{Z} = \mathbb{Z}$). Using Theorem 2.44, this description extends to any infinite cyclic group $G = \langle g \rangle$. Explicitly, any non-trivial subgroup of G is of the form $H_n = \langle g^n \rangle$ for $n \in \mathbb{N}$, which is necessarily normal in G, and one then has

$$G/H_n = \{H_n, gH_n, g^2H_n, \ldots, g^{n-1}H\}.$$

By Exercise 3.24, this quotient group is a cyclic group $G/H_n = \langle gH_n \rangle$, that therefore has isomorphism class C_n.
(iv) By Proposition 3.25, all subgroups of C_n are normal. Let $C_n = \langle g \rangle$. Using Theorem 2.44 and Remark 2.45, any non-trivial subgroup of C_n is of the form $H_d = \langle g^d \rangle$ for natural numbers d which divide n. One then has $|H_d| = \mathrm{o}(g^d) = n/d$ and

$$C_n/H_d = \{H_d, gH_d, g^2H_d, \ldots, g^{d-1}H_d\}.$$

By Exercise 3.24, this quotient group is a cyclic group $C_n/H_d = \langle gH_d \rangle$, that therefore has isomorphism class C_d. In particular

$$|C_n/H_d| = d = n/(n/d) = |C_n|/|H_d|.$$

Remark 3.29. From Examples 3.28 (iii) and (iv) we conclude that every quotient group of a cyclic group is again a cyclic group. Moreover, if $G = \langle g \rangle$ and H is a subgroup of G then $G/H = \langle gH \rangle$.

Exercise 3.30. Use Exercise 3.13 to show that the subgroup $\langle -1 \rangle$ is normal in Q_8. Which other group is $Q_8/\langle -1 \rangle$ isomorphic to?

Lemma 3.31. *Let G be a group and let H be a subgroup of G whose index $[G : H]$ in G is equal to 2. Then H is normal in G and G/H has isomorphism class C_2.*

Proof. We use Corollary 2.56, Remark 2.57 and Remark 2.59, which tell us that the set of left cosets of H in G is a partition of G, that the set of right cosets of H in G is also a partition of G, that $gH = H$ if and only if g belongs to H and that $Hg = H$ if and only if g belongs to H.

Now since $[G : H] = 2$, the set of left cosets of H in G must be $\{H, G \setminus H\}$. From Remark 2.64 we also know that the set of right cosets of H in G must be $\{H, G \setminus H\}$.

To conclude that H is normal in G we use Proposition 3.14. For each g in G, either g belongs to H, in which case $gH = H = Hg$, or g belongs to $G \setminus H$, in which case gH must be equal to $G \setminus H$ and Hg must be equal to $G \setminus H$, so that we again get $gH = Hg$. This concludes the proof of the fact that H is normal in G.

Now $G/H = \{H, G \setminus H\}$ is a group (of order 2) that is clearly cyclic, with generator $G \setminus H$, and thus has isomorphism class C_2. □

Lemma 3.32. *Let G be a group. Let m be a natural number. Assume that G has a unique subgroup H_m that has order m. Then H_m is normal in G.*

Proof. By Exercise 3.18 (i) and (iii), we know that for any $g \in G$, the conjugate gH_mg^{-1} of H_m by g is a subgroup of G with the property that $H_m \cong gH_mg^{-1}$. Therefore $|gH_mg^{-1}| = |H_m| = m$ and so, by uniqueness, we must have $gH_mg^{-1} = H$.

We have proved that every element g of G normalises H_m, so Exercise 3.18 (iv) implies that H_m is normal in G. □

Remark 3.33. Please think about the fact that being a normal subgroup of a group depends on both the subgroup and the group, not only on the subgroup. For instance, one can have a group G, a subgroup $H \leq G$ of G and a normal subgroup $N \trianglelefteq H$ of H. In this situation, N is a subgroup of G, but N may not be normal in G.

Moreover, the property of being a normal subgroup is not even transitive. Even if $H \trianglelefteq G$ and $N \trianglelefteq H$, the subgroup N may not be normal in G.

To see a counterexample to the possible transitivity of this property, we consider the group $G = D_8$, the subgroup

$$H := \langle s, r^2 \rangle = \{1, s, r^2, sr^2\}$$

and the subgroup

$$N := \langle s \rangle = \{1, s\}.$$

Then H has index $[G : H] = |G|/|H| = 8/4 = 2$ in G and N has index $[H : N] = |H|/|N| = 4/2 = 2$ in H, so Lemma 3.31 implies that H is normal in G and that N is normal in H.

However, N in not normal in G. To see this we simply note that $rsr^{-1} = sr^2$ does not belong to N.

Example 3.34. In $G = S_4$, for each $i \in \{1, 2, 3, 4\}$, we consider the subset

$$H_i := \{\sigma \in S_4 : \sigma(i) = i\}.$$

It is easy to see that H_i is a subgroup of S_4: the identity permutation clearly belongs to H_i, the inverse function of any element of H_i clearly must belong to H_i, and the composition of two elements of H_i clearly must belong to H_i. However, H_i is not normal in S_4.

We show that H_1 is not normal in S_4. One can write down identical arguments for $i = 2, 3, 4$.

We fix any element τ of S_4. Then every element σ of τH_1 must satisfy $\sigma(1) = \tau(1)$. Conversely, if σ is any element of S_4 that satisfies $\sigma(1) = \tau(1)$ then

$$(\tau^{-1}\sigma)(1) = \tau^{-1}(\tau(1)) = 1$$

so $\tau^{-1}\sigma$ belongs to H_1. We conclude that

$$\tau H_1 = \{\sigma \in S_4 : \sigma(1) = \tau(1)\}.$$

Similarly, any element σ of $H_1\tau$ must satisfy $\sigma(\tau^{-1}(1)) = 1$. Conversely, if σ is any element of S_4 that satisfies $\sigma(\tau^{-1}(1)) = 1$ then

$$(\sigma\tau^{-1})(1) = 1$$

so $\sigma\tau^{-1}$ belongs to H_1. We conclude that

$$H_1\tau = \{\sigma \in S_4 : \sigma(\tau^{-1}(1)) = 1\}.$$

To finally conclude that H_1 is not normal in S_4 it is enough to find an element τ of S_4 for which $\tau H_1 \neq H_1\tau$. Take, for example, $\tau = (1, 2)$. Then

$$\tau H_1 = \{\sigma \in S_4 : \sigma(1) = 2\}$$

while

$$H_1\tau = \{\sigma \in S_4 : \sigma(2) = 1\}.$$

The element $(1, 2, 3)$ of S_4 then belongs to τH_1 but not to $H_1\tau$, so that these sets cannot be equal, as required.

The following Exercise uses Lemma 3.31 to show that a full converse to Lagrange's Theorem would not be true, by constructing a group of order 12 that has no subgroups of order 6.

Exercise 3.35. We fix a group $C_2 = \{e, f\}$ of order 2 with identity e. We define an associated function

$$\mathrm{sgn} : S_4 \to C_2$$

by setting $\mathrm{sgn}(\sigma) = e$ if σ is an even permutation and $\mathrm{sgn}(\sigma) = f$ if σ is an odd permutation.

(i) Prove that sgn is a group homomorphism, and thus that

$$A_4 := \ker(\mathrm{sgn})$$

is a group.

(ii) Write down the cycle decomposition of each element of A_4 and the order of each of them. In particular, you should find that $|A_4| = 12$. Deduce that, if H is any subgroup of A_4 of order 6, then H would be normal in A_4 and A_4/H would have isomorphism class C_2.

(iii) Show that, if H is any subgroup of A_4 of order 6, then σ^2 would belong to H for every $\sigma \in A_4$.

(iv) Prove that A_4 cannot have a subgroup of order 6.

3.1.3. *Centralisers and Normalisers.* Throughout §3.1.2 we have seen numerous characterisations of the property of a subgroup being normal in a group. In this section we introduce some additional constructions that are helpful when analising this condition and will also be of interest in the sequel.

Definition 3.36. Let G be a group and let S be a non-empty subset of G.

(i) We call
$$C_G(S) := \{g \in G : gsg^{-1} = s \text{ for all } s \in S\}$$
the 'centraliser' of S in G.

(ii) We call
$$Z(G) := C_G(G)$$
the 'centre' of G.

(iii) We call
$$N_G(S) := \{g \in G : gSg^{-1} = S\}$$
the 'normaliser' of S in G.

Exercise 3.37. Prove that $C_G(S)$ is a subgroup of $N_G(S)$ and that $N_G(S)$ is a subgroup of G. In this way we thus also find that $C_G(S)$ is a subgroup of G and in particular that $Z(G)$ is a subgroup of G.

Exercise 3.38. Show that, if G is abelian, then $C_G(S) = N_G(S) = G$ for any non-empty subset S of G. In particular, we get $Z(G) = G$ in this case.

Exercise 3.39. Show that $C_{Q_8}(\{i\}) = \{\pm 1, \pm i\}$ and that $N_{Q_8}(\langle i \rangle) = Q_8$. Determine $Z(Q_8)$.

Exercise 3.40. Consider the subset $S = \{1, (1,2)\}$ of S_3. Show that $C_{S_3}(S) = N_{S_3}(S) = S$ and that $Z(S_3) = \{1\}$.

The normaliser of a subgroup measures how close it is to being normal, as evidenced by the following criterion.

Proposition 3.41. *Let G be a group and let H be a subgroup of G. Then H is normal in G if and only if $N_G(H) = G$.*

Proof. Clearly $N_G(H) = G$ if and only if every element g of G normalises H, so the result follows from Exercise 3.18 (iv). □

The centre of a group provides a natural source of normal subgroups of said group.

Lemma 3.42. *If G is a group and H is a subgroup of $Z(G)$ then H is normal in G. In particular, $Z(G)$ is a normal subgroup of G.*

Proof. Let $h \in H$ and $g \in G$. Then $g^{-1}hg = g^{-1}h(g^{-1})^{-1} = h$ since h belongs to $Z(G)$, and therefore $ghg^{-1} = g(g^{-1}hg)g^{-1} = h$ belongs to H. □

Notation 3.43. We sometimes abbreviate $C_G(\{s\})$ to $C_G(s)$.

3.2. **The theorems.**

3.2.1. *The first isomorphism theorem.* We have essentially already proved the first isomorphism theorem, sometimes also known as the fundamental theorem of homomorphisms.

Theorem 3.44. *If* $f : G \to J$ *is a homomorphism of groups, then* $\ker(f)$ *is a normal subgroup of* G *and there is a canonical isomorphism*

$$\overline{f} : G/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$$

given by

$$\overline{f}(g \ker(f)) := f(g)$$

for each $g \in G$.

In particular, the index $[G : \ker(f)]$ *is equal to the order of* $\mathrm{im}(f)$ *(whether finite or infinite).*

Proof. We know from Proposition 3.23 that $\ker(f)$ is a normal subgroup of G. The remaining claims were proved in Corollary 3.8. □

Exercise 3.45. Give an alternative description of the isomorphism class of $\mathrm{Gl}_2(\mathbb{R})/\mathrm{Sl}_2(\mathbb{R})$, with $\mathrm{Sl}_2(\mathbb{R})$ as defined in Exercise 2.78.

The following general fact, which we leave as an exercise for the reader, is very useful in many settings.

Remark 3.46. Let G be a group, let H be a normal subgroup of G and let $f : G \to J$ be a group homomorphism. Then f induces a well-defined function $\overline{f} : G/H \to J$ through the formula $\overline{f}(gH) = f(g)$ if and only H is contained in $\ker(f)$.

If H is indeed contained in $\ker(f)$ then $\overline{f}$ is a group homomorphism with $\mathrm{im}(\overline{f}) = \mathrm{im}(f)$ and with $\ker(\overline{f}) = \ker(f)/H$.

3.2.2. *The second isomorphism theorem.* Before we can state the next isomorphism theorem we must introduce some additional notation and preliminary results.

Definition 3.47. Let G be a group and let H and K be subgroups of G. We define a set

$$HK := \{hk : h \in H, k \in K\}.$$

Notation 3.48. In an abelian group G, if we wish to use additive notation, we will sometimes write $H + K = \{h + k : h \in H, k \in K\}$ instead of HK.

Proposition 3.49. *If* H *and* K *are both finite subgroups of* G *then the cardinality of* HK *is* $\frac{|H||K|}{|H\cap K|}$.

Proof. The set HK is the union of cosets

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

We know that the left cosets of K in G form a partition from Corollary 2.56 and also that each such coset hK has $|K|$ elements by Lemma 2.53. It is therefore enough to show that there are $\frac{|H|}{|H\cap K|}$ distinct cosets of the form hK, $h \in H$.

To do this we note that, given $h_1, h_2 \in H$, one has $h_1K = h_2K$ if and only if $h_2^{-1}h_1$ belongs to K, which happens if and only if $h_2^{-1}h_1$ belongs to $H \cap K$, which happens if and only if $h_1(H \cap K) = h_2(H \cap K)$. Therefore the number of distinct cosets of the form hK, $h \in H$, is the same as the number of distinct cosets of the form $h(H \cap K)$, $h \in H$. By Lagrange's Theorem 2.61 we know that this last number is equal to $\frac{|H|}{|H\cap K|}$, as required. □

Remark 3.50. Note that HK is not necessarily a subgroup of G! For example, in $G = S_3$, with $H = \langle(1, 2)\rangle = \{1,(1, 2)\}$ and $K = \langle(2, 3)\rangle = \{1,(2, 3)\}$ we have $|H| = |K| = 2$ and $|H \cap K| = 1$ so Proposition 3.49 implies that HK has 4 elements. Since S_3 has order 6 and 4 does not divide 6, Lagrange's Theorem 2.61 implies that HK cannot be a subgroup of S_3.

Proposition 3.51. *Let G be a group and let H and K be subgroups of G. Then HK is a subgroup of G if and only if $HK = KH$.*

Proof. We assume first that $HK = KH$. We will prove that HK is then a subgroup of G by applying the criterion of Lemma 2.6. We thus fix $x, y \in HK$. We must prove that xy^{-1} belongs to HK.

We write $x = h_1k_1$ and $y = h_2k_2$ with each h_i in H and each k_i in K. Then $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1}$.

Now, since $HK = KH$ we have $(k_1k_2^{-1})h_2^{-1} = h'k'$ for some $h' \in H$ and $k' \in K$. We finally find that $xy^{-1} = (h_1h')k'$, which belongs to HK, as required.

Conversely we now assume that HK is a subgroup of G. Clearly both H and K are subsets (and in fact, subgroups) of the group HK. Therefore kh belongs to HK for any $h \in H$ and $k \in K$. This shows that $KH \subseteq HK$.

To find the converse inclusion and thus the required equality we fix $h \in H$ and $k \in K$. Since HK is a group, the inverse $(hk)^{-1}$ of hk belongs to HK and may be written as $h'k'$ with $h' \in H$ and $k' \in K$. Therefore

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

This shows that hk must belong to KH. We conclude that $HK \subseteq KH$ and thus that $HK = KH$, as required. □

Remark 3.52. The equality of sets $HK = KH$ does not imply that all elements of H commute with all elements of K. For example in $G = D_{2n}$ with $H = \langle r\rangle$ and $K = \langle s\rangle$, although one has $rs = sr^{-1}$ so r and s do not commute, it is also easy to deduce from this equality that $HK = KH = G$.

Corollary 3.53. *If H and K are subgroups of G for which H is contained in $N_G(K)$, the set HK is a subgroup of G.*

In particular, given a normal subgroup K of G, the subset HK is a subgroup of G for every subgroup H of G.

Proof. We assume that H is contained in $N_G(K)$ and we will show that $HK = KH$, so our first claim will follow from Proposition 3.51.

For any $h \in H$ and $k \in K$, our assumption means that hkh^{-1} belongs to K. Therefore $hk = (hkh^{-1})h$ belongs to KH, which shows that $HK \subseteq KH$.

Similarly $kh = h(h^{-1}kh)$ with $h^{-1}kh$ in K by assumption, which shows that $KH \subseteq HK$.

The final claim is valid because, by Proposition 3.41, a normal subgroup K of G always satisfies $N_G(K) = G$. □

Corollary 3.54. *Let H and K be normal subgroups of G. Then HK is a normal subgroup of G.*

Proof. From Corollary 3.53 we know that HK is a subgroup of G. Let $g \in G$, $h \in H$ and $k \in K$. Then

$$ghkg^{-1} = (ghg^{-1})(gkg^{-1})$$

where ghg^{-1} belongs to H and gkg^{-1} belongs to K. □

Exercise 3.55. In $G = S_4$ we consider the subgroups $H = D_8$ and $K = \langle(1, 2, 3)\rangle$. Use Proposition 3.49, together with Lagrange's Theorem 2.61, to prove that $S_4 = HK$.

We finally get to the second isomorphism theorem (sometimes known as the 'diamond isomorphism theorem', see [2, Thm. 18, p. 97]).

Theorem 3.56. *Let G be a group and let H and K be subgroups of G for which H is contained in $N_G(K)$. Then $HK \leq G$, $K \trianglelefteq HK$, $(H \cap K) \trianglelefteq H$ and there is a canonical isomorphism*

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

which maps an element $h(H \cap K)$ to hK.

Proof. By Corollary 3.53 we know that $HK \leq G$.

Since H is contained in $N_G(K)$ and K is always also contained in $N_G(K)$, we know that HK must be contained in $N_G(K)$. Every element of the group HK therefore normalises K (by definition of the normaliser $N_G(K)$), so K must be normal in HK by Exercise 3.18 (iv).

We now show the remaining claims by applying the First Isomorphism Theorem 3.44. It is enough to construct a surjective group homomorphism

$$f : H \to (HK)/K$$

with $\ker(f) = (H \cap K)$ which corresponds with the given explicit description.

To do this we set $f(h) := hK$ for each $h \in H$. Clearly f is a group homomorphism, as for $h, h' \in H$ one has

$$f(h)f(h') = (hK)(h'K) = (hh')K = f(hh')$$

by definition of the binary operation on the quotient group $(HK)/K$. (Alternatively, f is a homomorphism because it is just the restriction of the natural projection $HK \to (HK)/K$ to H.)

The map f is surjective because for any $h \in H$ and any $k \in K$, the coset

$$(hk)K = (hK)(kK) = (hK)K = hK$$

is the image of h under f (in the second equality we have used Remark 2.57).

We finally claim that $\ker(f) = (H \cap K)$. Again by Remark 2.57, an element h of H belongs to $\ker(f)$ if and only if it belongs to K, which happens if and only if it belongs to $H \cap K$. This completes the proof. □

Exercise 3.57. In the setting of Theorem 3.56, prove directly that $H \cap K$ is a normal subgroup of H, without applying the First Isomorphism Theorem 3.44.

3.2.3. *The third isomorphism theorem.* The third isomorphism theorem considers the structure of quotient groups of quotient groups.

Theorem 3.58. *Let G be a group and let H and K be normal subgroups of G with $H \subseteq K$. Then H is a normal subgroup of K, K/H is a normal subgroup of G/H and there is a canonical isomorphism*

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

which maps an element $(gH)(K/H)$ to gK.

Proof. We know that H is normal in K because it is normal in G (and by definition of being normal in a group).

We will prove the remaining claims by applying the First Isomorphism Theorem 3.44. We define a function

$$f : G/H \to G/K$$

by setting $f(gH) := gK$ for each $g \in G$. This function is well-defined because if $g_1H = g_2H$ then

$$g_2^{-1}g_1 \in H \subseteq K$$

so $g_1K = g_2K$.

The function f is clearly a group homomorphism and it is clearly surjective. To complete the proof it is now enough to show that $\ker(f) = K/H$. This equality is indeed valid, since

$$\ker(f) = \{gH \in G/H : gK = K\} = \{gH \in G/H : g \in K\} = K/H.$$

□

Exercise 3.59. In the setting of Theorem 3.58, prove directly that K/H is a normal subgroup of G/H, without applying the First Isomorphism Theorem 3.44.

3.2.4. *The fourth isomorphism theorem.* We finally get to the fourth isomorphism theorem (sometimes known as the 'lattice isomorphism theorem', see [2, Thm. 20, p. 98,99], and sometimes included within the First Isomorphism Theorem 3.44, see [1]). We leave the proof of this result as an exercise for the reader.

Theorem 3.60. *Let G be a group and let H be a normal subgroup of G. We consider the sets*

$$S_G^H := \{J \leq G : H \subseteq J\}, \qquad S_{G/H} := \{L \leq G/H\}.$$

Then the function $\overline{\cdot} : S_G^H \to S_{G/H}$ given by $\overline{J} := J/H$ is a bijection that has the following properties for any $J_1, J_2 \in S_G^H$.

(i) *$J_1 \subseteq J_2$ if and only if $\overline{J_1} \subseteq \overline{J_2}$.*
(ii) *If $J_1 \subseteq J_2$ then $[J_2 : J_1] = [\overline{J_2} : \overline{J_1}]$.*
(iii) *$\overline{\langle J_1, J_2 \rangle} = \langle \overline{J_1}, \overline{J_2} \rangle$.*

(iv) $\overline{J_1 \cap J_2} = \overline{J_1} \cap \overline{J_2}$.

(v) *J_1 is normal in G if and only if $\overline{J_1}$ is normal in $\overline{G} = G/H$.*

Exercise 3.61. Prove Theorem 3.60.

Example 3.62. For $G = Q_8$ and $H = \langle -1 \rangle = \{1, -1\}$, it is easy to prove that G/H is equal to $\{1H, iH, jH, kH\}$ and also isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. From Example 2.10 we then know that G/H has 5 distinct subgroups, and this includes G/H itself, the identity subgroup, and 3 distinct subgroups of order 2. From Theorem 3.60 we know that the only subgroups of $G = Q_8$ that contain -1 are G, H, $\langle i \rangle$, $\langle j \rangle$ and $\langle k \rangle$.

Exercise 3.63. Find all subgroups of D_8 that contain r^2.

3.3. **Simple groups and solvable groups.** Before we discuss simple or solvable groups, we prove a useful result that will be further generalised in §4.

3.3.1. *Cauchy's Theorem for abelian groups.* We already mentioned Cauchy's Theorem in Remark 2.70(ii): if G is a finite group and p is a prime divisor of $|G|$ then G has an element of order p. For now, we restrict ourselves to prove this result for *abelian* groups G, a case in which the proof becomes completely elementary.

Theorem 3.64. *If G is a finite abelian group and p is a prime divisor of $|G|$ then G has an element of order p.*

Proof. We prove the result by induction on $|G|$. If $|G| = 1$ then the result is trivial. We henceforth assume that $G \neq \{1\}$. We assume that the result is valid for every finite abelian group that has order strictly smaller than $|G|$ and divisible by p; this will be our inductive hypothesis.

We fix an element $x \neq 1$ of G. If $|G| = p$ then, by Lagrange's Theorem, we would have $\mathrm{o}(x) = p$, which would complete the proof. We henceforth assume that $|G| \neq p$ and thus that $|G| > p$.

If p divides $\mathrm{o}(x)$, say $\mathrm{o}(x) = pn$ for some $n \in \mathbb{N}$, then by Proposition 2.40(ii) we would have $\mathrm{o}(x^n) = p$, which would complete the proof. We henceforth assume that p does not divide $\mathrm{o}(x)$.

We set $H := \langle x \rangle$, so $p \nmid |H|$. Since G is abelian, H is normal in G. The quotient group G/H is finite and abelian. By Lagrange's Theorem, we have

$$|G/H| = |G|/|H|$$

and, since $H \neq \{1\}$, G/H has order strictly smaller that $|G|$. Since p does not divide $|H|$ it must divide $|G/H|$.

By the inductive hypothesis, G/H contains an element $\overline{y} = yH$, for some $y \in G$, that has order p. The element yH cannot be the identity, so y cannot belong to H, but $y^pH = (yH)^p = H$, so y^p must belong to H. The subgroup $\langle y^p \rangle$ must be contained in H but the subgroup $\langle y \rangle$ cannot be contained in H, so in particular $\langle y^p \rangle \neq \langle y \rangle$. The inclusion $\langle y^p \rangle \subset \langle y \rangle$ of finite groups must therefore be strict.

It then follows that $\mathrm{o}(y^p) < \mathrm{o}(y)$. By Proposition 2.40(ii) p must therefore divide $\mathrm{o}(y)$. Just as above, using once again Proposition 2.40(ii), a power of y then must have order equal to p. Specifically, $\mathrm{o}(y^m) = p$ where $\mathrm{o}(y) = pm$. □

3.3.2. *Simple groups and composition series.* Often one studies a group G through the use of inductive arguments, by identifying a (non-trivial, proper) normal subgroup H of G, studying first the groups H and G/H, which may have smaller order than G, and trying to piece together the conclusions to obtain similar conclusions about G. We will see various examples of this method of reasoning in the sequel. We just saw one in Theorem 3.64.

The following class of groups, despite what their name might suggest, make it particularly complicated to try to argue in such a manner.

Definition 3.65. A (non-trivial) group G is called 'simple' if it has no normal subgroups, other than $\{1\}$ and G itself.

Exercise 3.66. Show that if a finite group has prime order then it is simple.

Exercise 3.67. Show that if an abelian group is simple then it has isomorphism class C_p for some prime number p. (Hint: treat the infinite and finite cases separately, use Theorem 3.64 in the latter case.)

Remark 3.68. There are, however, non-abelian simple groups (both finite and infinite). The finite simple groups have been fully classified. We will discuss a specific family of such groups, the 'alternating groups', in §4 (you already encountered an alternating group, namely A_4, in Exercise 3.35). However, all such examples will be groups of even order: a celebrated theorem of Feit and Thompson states that every finite simple group of odd order has isomorphism class C_p for some prime number p (hence is, in particular, abelian).

Definition 3.69. In a group G, a finite sequence of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$

is called a 'composition series' if N_{i+1}/N_i is a simple group for every $0 \leq i \leq k-1$. In that case, the quotient groups N_{i+1}/N_i are called 'composition factors' of G.

Remark 3.70. The given definition of a composition series does **not** require that each subgroup N_i is normal in G. It requires N_i only to be normal in N_{i+1}. For example, in D_8 we have the following two composition series:

$$\{1\} \trianglelefteq \langle s\rangle \trianglelefteq \langle s, r^2\rangle \trianglelefteq D_8 \quad \text{and} \quad \{1\} \trianglelefteq \langle r^2\rangle \trianglelefteq \langle r\rangle \trianglelefteq D_8. \tag{17}$$

In both of these sequences, each subgroup N_i has index 2 in N_{i+1}, so N_i is indeed normal in N_{i+1} by Lemma 3.31, and the quotient N_{i+1}/N_i is simple simply because it has order 2. However $\langle s\rangle$ is not normal in D_8.

Remark 3.71. The Jordan-Hölder Theorem states that every finite group has a composition series, which is moreover unique, in a very strong sense. In particular, the natural number k is uniquely defined, so it is no coincidence that $k = 3$ in both of the composition series occurring in (17). See [2, Thm. 22, p. 103] for a precise statement of the Theorem.

Exercise 3.72. Find three composition series for Q_8 and seven composition series for D_8.

3.3.3. *Solvable groups.* We now introduce a class of groups that is of great in importance in Galois theory.

Definition 3.73. A group G is 'solvable' if there exists a finite sequence of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$

such that N_{i+1}/N_i is abelian for every $0 \leq i \leq k-1$.

Another example of how to piece together information about a normal subgroup and the associated quotient into information about the actual group is given by the following useful result.

Lemma 3.74. *Let G be a group and let H be a normal subgroup of G. If both H and G/H are solvable groups then G is a solvable group.*

Proof. We set $\overline{G} := G/H$ and we fix sequences

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = H$$

and

$$H = \overline{M_0} \trianglelefteq \overline{M_1} \trianglelefteq \overline{M_2} \trianglelefteq \ldots \trianglelefteq \overline{M_{l-1}} \trianglelefteq \overline{M_l} = \overline{G}$$

such that N_{i+1}/N_i is abelian for every $0 \leq i \leq k-1$ and such that $\overline{M_{i+1}}/\overline{M_i}$ is abelian for every $0 \leq i \leq l-1$.

By the Fourth Isomorphism Theorem 3.60 there are subgroups M_i of G that contain H for which $M_i/H = \overline{M_i}$ and $M_i \trianglelefteq M_{i+1}$ for every $0 \leq i \leq l-1$. By the Third Isomorphism Theorem 3.58 we then also get that each quotient

$$M_{i+1}/M_i \cong (M_{i+1}/H)/(M_i/H) = \overline{M_{i+1}}/\overline{M_i}$$

is abelian.

The sequence of subgroups

$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = H = M_0 \trianglelefteq M_1 \trianglelefteq M_2 \trianglelefteq \ldots \trianglelefteq M_{l-1} \trianglelefteq M_l = G$$

finally shows that G is solvable. □

3.4. **(More) Exercises.** Don't forget to think about the exercises given throughout the rest of section 3.

Exercise 3.75. Let A be an abelian group and let B be a subgroup of A. Show that A/B is abelian.

Exercise 3.76. Let G be a group and let H be a normal subgroup of G.

(i) Let g be an element of G for which g^n belongs to H for some natural number n. Prove that the order of gH in G/H is the minimum of $\{n \in \mathbb{N} : g^n \in H\}$.

(ii) Let g be an element of G for which $g^n \notin H$ for each $n \in \mathbb{N}$. Prove that gH has infinite order in G/H.

(iii) Give an example of G, H and g with $\mathrm{o}(gH) < \mathrm{o}(g) < \infty$.

Exercise 3.77. Let $f : \mathbb{R}^* \to \mathbb{R}^*$ be given by $f(x) := |x|$ (the absolute value of x). Show that f is a homomorphism and determine the image, the kernel, and all the fibres of f.

Exercise 3.78. Let $f : \mathbb{C}^* \to \mathbb{R}^*$ be given by $f(x + yi) := x^2 + y^2$. Show that f is a homomorphism and determine the image, the kernel, and all the fibres of f.

Exercise 3.79. Let $f : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ be given by $f([a]_8) := [a]_4$. Show that f is a well-defined homomorphism and determine the image, the kernel, and all the fibres of f.

Exercise 3.80. Let $f : \mathbb{Z}/24\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$ be given by $f([a]_{24}) := [a]_{12}$. Show that f is a well-defined homomorphism and that $\ker(f)$ is isomorphic to $12\mathbb{Z}/24\mathbb{Z}$ and also has isomorphism class C_2.

Exercise 3.81. Show that

$$\big(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}\big)/\langle([2],[2])\rangle$$

is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 3.82. Let F be $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. Let G be the subgroup of $\mathrm{Gl}_2(F)$ comprising upper triangular matrices (with non-trivial determinant). Let $f : G \to F^* \times F^*$ be the function given by

$$f\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = (a, d).$$

Show that f is a surjective homomorphism and determine its fibres. Prove that $\ker(f)$ is isomorphic to F.

Exercise 3.83. Let S^1 be the unit circle in the complex plane (the multiplicative group of complex numbers with absolute value equal to 1) and let $f : \mathbb{R} \to S^1$ be the function given by $f(x) := e^{2\pi i x}$. Show that f is a surjective homomorphism and determine the fibres of $1, -1, i$ and $e^{4\pi i/3}$. Repeat the same exercise for the function $f : \mathbb{R} \to S^1$ given by $f(x) := e^{4\pi i x}$.

Exercise 3.84.
(i) Show that every coset of $\mathbb{Z}$ in $\mathbb{Q}$ contains exactly one rational number q for which $0 \le q < 1$.
(ii) Show that every element of the quotient group $\mathbb{Q}/\mathbb{Z}$ has finite order, but also that there exist elements of arbitrarily large order.
(iii) Show that the function $f : \mathbb{Q}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ given by $f(q + \mathbb{Z}) = q + \mathbb{Z}$ is a well-defined injective homomorphism.
(iv) Show that $\mathrm{im}(f) = (\mathbb{R}/\mathbb{Z})_{\mathrm{tor}}$, in the notation of Exercise 2.73.
(v) Show that $\mathbb{Q}/\mathbb{Z}$ is isomorphic to $\mu := \{z \in \mathbb{C} : z^n = 1 \text{ for some } n \in \mathbb{N}\}$.

Exercise 3.85. Let G be a group, let S be a generating set for G and let H be a normal subgroup of G. Prove that $\{sH : s \in S\}$ is a generating set for G/H.

Exercise 3.86. Show that $D_{16}/Z(D_{16})$ is isomorphic to D_8. Show that

$$(D_{16}/Z(D_{16}))\,/Z\,(D_{16}/Z(D_{16}))$$

is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Show that $H := \langle sZ(D_{16}), r^2 Z(D_{16})\rangle$ is a normal subgroup of $D_{16}/Z(D_{16})$ and determine the isomorphism class of

$$\big(D_{16}/Z(D_{16})\big)/H.$$

Exercise 3.87.
(i) Prove that the intersection of two normal subgroups of a group is a normal subgroup.

(ii) Prove that the intersection of an arbitrary non-empty collection of normal subgroups of a group is a normal subgroup.
(iii) Prove that if $N \trianglelefteq G$ and $H \leq G$ then $N \cap H \trianglelefteq H$.

Exercise 3.88. Prove that a subgroup H of a group G is normal in G if and only if $gHg^{-1} \subseteq H$ for every $g \in G$.

Exercise 3.89. Set

$$H := \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{Z} \right\}.$$

Show that H is a subgroup of $\mathrm{Gl}_2(\mathbb{Q})$. Show that

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} H \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} \subseteq H.$$

Show that $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ does **not** normalise H.

Exercise 3.90. Let G be a group.

(i) Let S be a subset of G. Prove that $\langle S \rangle$ is normal in G if and only if

$$gSg^{-1} \subseteq \langle S \rangle$$

for every $g \in G$.

(ii) Given $x \in G$, show that $\langle x \rangle$ is normal in G if and only if for each $g \in G$, one has $gxg^{-1} = x^a$ for some $a \in \mathbb{Z}$.

(iii) Let n be a natural number and set

$$S_n := \{g \in G : \mathrm{o}(g) = n\}.$$

Prove that $H_n := \langle S_n \rangle$ is normal in G.

Exercise 3.91. Let G be a group and let H be a finite subgroup of G.

(i) Show that an element g of G normalises H if and only if

$$gHg^{-1} \subseteq H.$$

(ii) Let S be a generating set for H. Show that an element g of G normalises H if and only if

$$gSg^{-1} \subseteq H.$$

(iii) Let T be a generating set for G. Prove that H is normal in G if and only if

$$tSt^{-1} \subseteq H$$

for every t in T.

Exercise 3.92. Let G be a group. Show that g^a belongs to $C_G(\{g\})$ and to $N_G(\{g\})$ for any $g \in G$ and any $a \in \mathbb{Z}$.

Exercise 3.93. Consider the subset $S = \{1, r, r^2, r^3\}$ of D_8. Show that $C_{D_8}(S) = S$, that $N_{D_8}(S) = D_8$ and that $Z(D_8) = \{1, r^2\}$. Show that $D_8/Z(D_8)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 3.94. For $n \geq 3$, show that $Z(D_{2n}) = \{1\}$ if n is odd and that $Z(D_{2n}) = \{1, r^{n/2}\}$ if n is even.

Exercise 3.95. Let G be a group. Show that $C_G(Z(G)) = N_G(Z(G)) = G$.

Exercise 3.96. Let H be a subgroup of a group G. Show that H is a subgroup of $N_G(H)$. Prove that H is a subgroup of $C_G(H)$ if and only if H is abelian.

Exercise 3.97. Show that $C_G(\langle g \rangle) = C_G(\{g\})$ for any $g \in G$.

Exercise 3.98. Let $H \leq G$ and let $N \trianglelefteq H$. Prove that $H \leq N_G(N)$. Deduce that $N_G(N)$ is the largest subgroup of G in which N is normal.

Exercise 3.99. Prove that every subgroup of Q_8 is normal in Q_8 and determine the isomorphism class of each quotient of Q_8.

Exercise 3.100. Find all normal subgroups of D_8.

Exercise 3.101. Let $n \geq 3$ be a natural number and let k be a natural number dividing n. Prove that $\langle r^k \rangle$ is normal in D_{2n} and that $D_{2n}/\langle r^k \rangle$ is isomorphic to D_{2k}.

Exercise 3.102. Let G be a group. Prove that if $G/Z(G)$ is cyclic then G is abelian.

Exercise 3.103. Let G and J be groups. Prove that

$$H_J := \{(g, 1) : g \in G\}$$

is a normal subgroup of $G \times J$ and that

$$(G \times J)/H_J \cong J.$$

Exercise 3.104. Let A be an abelian group and set

$$D := \{(a, a) : a \in A\}.$$

Prove that D is a normal subgroup of $A \times A$ and that

$$(A \times A)/D \cong A.$$

Exercise 3.105. Prove that $\{(a, a) : a \in S_3\}$ is not normal in $S_3 \times S_3$.

Exercise 3.106. Let G be a group.

(i) Let H be a normal subgroup of G. Prove that, given x and y in G, the elements xH and yH of G/H commute if and only if the 'commutator element'

$$[x, y] := x^{-1}y^{-1}xy$$

of x and y belongs to H.

(ii) Prove that the 'commutator subgroup' of G, defined as

$$G' := \langle \{[x, y] : x, y \in G\} \rangle,$$

is normal in G, and also that the quotient group G/G' is abelian.

Exercise 3.107. Let H and K be normal subgroups of a group G for which $H \cap K = \{1\}$. Prove that any element of H commutes with any element of K.

Exercise 3.108.
(i) Find a group G with a normal subgroup H of G for which both H and G/H are abelian but G is not.
(i) Find a group G with a normal subgroup H of G for which both H and G/H are cyclic but G is not.

Exercise 3.109. Let $f : G_1 \to G_2$ be a group homomorphism.

(i) Show that for any subgroup H_2 of G_2, the pre-image $f^{-1}(H_2)$ is a subgroup of G_1.
(ii) Show that if in addition H_2 is normal in G_2 then $f^{-1}(H_2)$ is normal in G_1.
(iii) Show that if f is surjective and H_1 is a normal subgroup of G_1 then $f(H_1)$ is a normal subgroup of G_2. (We already knew, from Proposition 2.13, that the image of any subgroup of G_1 under any homomorphism $G_1 \to G_2$ is always a subgroup of G_2.)
(iv) Show that if H_1 is any subgroup of G_1 that contains $\ker(f)$ then $f^{-1}(f(H_1)) = H_1$.

Exercise 3.110. Let $H \leq K \leq G$. Prove that $[G : H] = [G : K][K : H]$.

Exercise 3.111. Prove that S_4 does not have any normal subgroups of order 8 or of order 3.

Exercise 3.112. Let G be a finite group, let H be a subgroup of G and let K be a normal subgroup of G. Prove that if $|H|$ and $[G : K]$ are coprime then H is contained in K.

Exercise 3.113. Prove that if K is a normal subgroup of a finite group G and $|K|$ is coprime to $[G : K]$, then K is the unique subgroup of G of order $|K|$.

Exercise 3.114. Let G be a group. Let A be an abelian subgroup that is normal in G and let B be any subgroup of G. Prove that $A \cap B$ is normal in AB.

Exercise 3.115. Let G be a group and let H be a normal subgroup of G whose index $[G : H] = p$ in G is a prime number. Prove that any subgroup K of G is either contained in H or satisfies both $G = HK$ and $[K : (K \cap H)] = p$.

Exercise 3.116. Let G_1 and G_2 be groups and let H_1 and H_2 be normal subgroups of G_1 and of G_2 respectively. Prove that $H_1 \times H_2$ is normal in $G_1 \times G_2$ and that

$$(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2).$$

Exercise 3.117. Let G be a group and let H and K be normal subgroups of G with the property that $G = HK$. Prove that

$$G/(H \cap K) \cong (G/H) \times (G/K).$$

Exercise 3.118. Let p be a prime number and write

$$\mu_{p^\infty} := \{z \in \mathbb{C} : z^{p^n} = 1 \text{ for some } n \in \mathbb{N}\}$$

for the group of p-power roots of unity. Prove that μ_{p^∞} is isomorphic to a quotient of μ_{p^∞} by a non-trivial subgroup of μ_{p^∞}.

Exercise 3.119. Use Cauchy's Theorem 3.64 to prove that a finite abelian group has a subgroup of order d for every positive divisor d of $|G|$.

Exercise 3.120. Prove that subgroups and quotient groups of a solvable group are solvable.

Exercise 3.121. Let G be a finite group. Prove that the following conditions are equivalent for G:

(i) G is solvable.

(ii) There exists a finite sequence of subgroups
$$1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \ldots \trianglelefteq N_{k-1} \trianglelefteq N_k = G$$
such that N_{i+1}/N_i is cyclic for every $0 \leq i \leq k-1$.

(iii) All composition factors of G are of prime order.

Exercise 3.122. Prove, without using the Feit-Thompson Theorem, that the following conditions are equivalent:

(i) Every finite group of odd order is solvable.

(ii) The only simple groups of odd order are those of prime order.

4. Group actions and Sylow's Theorem

4.1. **Symmetric and Alternating groups.** In this section we fix $n \geq 3$ and we continue the study of the symmetric groups S_n that we briefly started in §1.2.1, and we introduce another important class of groups, the alternating groups A_n, which in particular serve as our basic example of non-abelian simple groups.

Before proceeding we recall that for any non-empty set Ω we have defined the symmetric group S_Ω on Ω as the group of permutations of Ω. The following useful terminology will be consistent with the new terminology that we will introduce in §4.2 below.

Definition 4.1. A group G is called a 'permutation group' if it is a subgroup of a symmetric group S_Ω for some non-empty set Ω.

4.1.1. *Orders of permutations.* Before introducing any new contents we briefly study the order of a permutation.

Lemma 4.2. *An m-cycle in S_n (for any $m \leq n$) has order equal to m.*

Proof. Clearly an m-cycle $c = (a_1, \ldots, a_m)$ satisfies $c^m = 1$. For $k < m$ however, $c^k(a_1) = a_{k+1} \neq a_1$ so $c^k \neq 1$, which completes the proof. □

We already noted in (4) the very useful fact that disjoint cycles commute. Let us record this fact formally for later use.

Lemma 4.3. *Disjoint cycles commute.*

Proof. Assuming the cycles $\sigma = (a_1, \ldots, a_m)$ and $\tau = (b_1, \ldots, b_{m'})$ in S_n to be disjoint, the function $\sigma \circ \tau$ maps a_i to $\sigma(a_i)$, maps b_j to $\tau(b_j)$, and fixes any number in $\{1, \ldots, n\} \setminus \{a_1, \ldots, a_m, b_1, \ldots, b_{m'}\}$. The same description holds for the function $\tau \circ \sigma$, so they are equal. □

Exercise 4.4. Find a 10-cycle σ in S_{10} for which $\sigma^k = (1,2)(3,4)(5,6)(7,8)(9,10)$ for some $k \in \mathbb{N}$.

Exercise 4.5. Show that an element of S_n has order equal to 2 if and only if its cycle decomposition is a product of 2-cycles.

Lemma 4.6. *Let p be a prime number. An element of S_n has order equal to p if and only if its cycle decomposition is a product of p-cycles.*

Proof. We first recall that a non-trivial element g of a group has order p if and only if $g^p = 1$.

Now, if σ has cycle decomposition $\sigma_1 \ldots \sigma_m$ then, because disjoint cycles commute by Lemma 4.3, the cycle decomposition of σ^k is $\sigma_1^k \ldots \sigma_m^k$ for each $k \in \mathbb{N}$.

The element σ has order p if and only the cycle decomposition of σ^p is the identity, and by the above discussion, this happens if and only if $\sigma_i^p = 1$ for each i, which happens if and only if each σ_i has order p. By Lemma 4.2 this happens if and only each σ_i is a p-cycle, as required. □

Exercise 4.7. Find a counterexample to Lemma 4.6 for an integer p that is not prime.

Exercise 4.8. Assume that an element σ of S_n has cycle decomposition $\tau_1 \dots \tau_t$. Prove that $\mathrm{o}(\sigma) = \mathrm{lcm}(\mathrm{length}(\tau_1), \dots, \mathrm{length}(\tau_t))$.

Exercise 4.9.
(i) Find all numbers m for which S_5 contains an element of order m.
(ii) Find all numbers m for which S_7 contains an element of order m.

4.1.2. *Signs of permutations and Alternating Groups.* We already mentioned the following useful in Notation 1.27 (iii) terminology.

Definition 4.10. A 2-cycle in S_n is also called a transposition.

Lemma 4.11. *Every element of S_n is a product of transpositions. More precisely, $S_n = \langle T \rangle$ where $T := \{(i, j) : 1 \leq i < j \leq n\} \subset S_n$.*

Proof. Any cycle has an equality of the form

$$(a_1, a_2, \dots, a_m) = (a_1, a_m)(a_1, a_{m-1})(a_1, a_{m-2}) \dots (a_1, a_2). \tag{18}$$

Since any permutation is a product of cycles, it is also a product of transpositions. □

Remark 4.12. Although clearly every element of S_n can be expressed as a product of transpositions, such decompositions are not unique. For instance in S_3 one has

$$(1, 2, 3) = (1, 2)(2, 3) = (1, 3)(1, 2) = (1, 2)(1, 3)(1, 2)(1, 3).$$

In fact there is an infinite number of ways to write this permutation as a number of transpositions. However, it is impossible to write $(1, 2, 3)$ as a product of an odd number of transpositions!

Exercise 4.13. In S_{13}, write $(1, 12, 8, 10, 4)(2, 13)(5, 11, 7)(6, 9)$ as a product of transpositions.

Exercise 4.14. Show that S_n is not abelian.

We now formally introduce the notion of the sign of a permutation.

Definition 4.15. Consider the polynomial

$$\Delta = \Delta(x_1, \dots, x_n) := \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

in n variables. For each σ in S_n we then define a polynomial

$$\sigma(\Delta) := \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

We then define the sign of σ to be

$$\mathrm{sgn}(\sigma) := \begin{cases} +1, & \text{if } \sigma(\Delta) = \Delta, \\ -1, & \text{if } \sigma(\Delta) = -\Delta. \end{cases} \tag{19}$$

We say that σ is even if $\mathrm{sgn}(\sigma) = 1$ and that σ is odd if $\mathrm{sgn}(\sigma) = -1$.

Lemma 4.16. *The equality (19) defines a function on all of S_n, called the sign function.*

Proof. Fix $\sigma \in S_n$. Fix k and l with $1 \leq k < l \leq n$. Recall that σ is a bijection from $\{1, \dots, n\}$ to itself, and write σ^{-1} for its inverse. If $\sigma^{-1}(k) < \sigma^{-1}(l)$ then $\sigma(\Delta)$ has a factor $x_k - x_l$, but cannot have a factor $x_l - x_k$. If on the other hand $\sigma^{-1}(k) > \sigma^{-1}(l)$ then $\sigma(\Delta)$ has a factor $x_l - x_k$, but cannot have a factor $x_k - x_l$.

Write $t(\sigma)$ for the cardinality of the set $\{(k, l) : 1 \leq k < l \leq n, \sigma^{-1}(k) > \sigma^{-1}(l)\}$. Then $\sigma(\Delta)$ is the product $\prod_{1 \leq k < l \leq n} \pm(x_k - x_l)$, in which the minus sign occurs exactly $t(\sigma)$ times. Therefore

$$\sigma(\Delta) = (-1)^{t(\sigma)} \prod_{1 \leq k < l \leq n} (x_k - x_l) = (-1)^{t(\sigma)} \Delta \in \{\pm\Delta\}. \tag{20}$$

This shows that sgn does assign a value to σ, as required. □

Remark 4.17. In the sequel we will use the notation $t(\sigma)$ for the cardinality of the set $\{(i, j) : 1 \leq i < j \leq n, \sigma^{-1}(i) > \sigma^{-1}(j)\}$, so that (20) shows that $\operatorname{sgn}(\sigma) = (-1)^{t(\sigma)}$.

Exercise 4.18. In S_4 we consider $\sigma = (1, 2, 3, 4)$ and $\tau = (4, 2, 3)$. Compute $\operatorname{sgn}(\tau), \operatorname{sgn}(\sigma)$ and $\operatorname{sgn}(\tau\sigma)$.

In the next result we interpret $\{\pm 1\}$ as a group under the usual multiplication (which gives it isomorphism class C_2 as it has order 2).

Proposition 4.19. *The function* $\operatorname{sgn} : S_n \to \{\pm 1\}$ *is a surjective group homomorphism, and all transpositions are odd.*

Proof. By Remark 4.17, to verify that sgn is a homomorphism it is enough to prove that

$$t(\sigma) + t(\sigma') \equiv t(\sigma\sigma') \pmod 2 \tag{21}$$

for any $\sigma, \sigma' \in S_n$, since then $\operatorname{sgn}(\sigma)\operatorname{sgn}(\sigma') = (-1)^{t(\sigma)+t(\sigma')} = (-1)^{t(\sigma\sigma')} = \operatorname{sgn}(\sigma\sigma')$.

To prove the required congruence relation we recall that $(\sigma\sigma')^{-1} = (\sigma')^{-1}\sigma^{-1}$. Using this equality, a case by case analysis of the possible parities of $t(\sigma)$ and $t(\sigma')$ easily shows the required congruence (21).

From the fact that sgn is a homomorphism it follows that $\operatorname{sgn}(1) = 1$, so if we can prove that all transpositions are odd, then in particular sgn is surjective.

We first compute $\operatorname{sgn}((1, 2))$. It is clear that $\{(i, j) : 1 \leq i < j \leq n, (1, 2)(i) > (1, 2)(j)\} = \{(1, 2)\}$ so $t((1, 2)) = 1$ and $\operatorname{sgn}((1, 2)) = -1$.

Let (k, l) be any transposition in S_n. Then

$$(k, l) = (1, k)(2, l)(1, 2)(1, k)(2, l)$$

and, since sgn is a homomorphism, we get that

$$\begin{aligned} \operatorname{sgn}((k, l)) =& \operatorname{sgn}(((1, k)(2, l))(1, 2)((1, k)(2, l))) \\ =& \operatorname{sgn}((1, k)(2, l)) \operatorname{sgn}((1, 2)) \operatorname{sgn}((1, k)(2, l)) \\ =& (-1) \operatorname{sgn}((1, k)(2, l))^2 \\ =& -1, \end{aligned}$$

as required. □

Corollary 4.20. *For a given element σ of S_n, the parity of the number of transpositions in every expression of σ as a product of transpositions is the same. In particular, σ is even if this parity is even and σ is odd if this parity is odd.*

Proof. By Proposition 4.19 we know that $\mathrm{sgn}(\sigma) = (-1)^k$ whenever σ can be expressed as a product of k transpositions. Therefore the parity of k cannot depend on the choice of such an expression, and corresponds to whether σ is even or odd. □

Corollary 4.21. *An m-cycle is even if m is odd and odd if m is even.*

Proof. This follows upon combining Proposition 4.19 with (18), as they imply that

$$\mathrm{sgn}((a_1, \dots, a_m)) = (-1)^{m-1}.$$

□

Corollary 4.22. *A permutation is odd if and only if the number of cycles of even length in its cycle decomposition is odd.*

Proof. This follows immediately upon combining Proposition 4.19 and Corollary 4.21. □

Example 4.23. In S_{18}, the permutation

$$(1, 2, 3, 4, 5, 6)(7, 8, 9)(10, 11)(12, 13, 14, 15)(16, 17, 18)$$

is odd, but the permutation

$$(1, 2, 3, 4, 5, 6)(7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18)$$

is even.

Definition 4.24. The 'alternating group of degree n' is

$$A_n := \ker\left(\mathrm{sgn} : S_n \to \{\pm 1\}\right),$$

which is the (normal) subgroup of S_n comprising even permutations.

Lemma 4.25. $|A_n| = n!/2$.

Proof. By the First Isomorphism Theorem 3.44, we know that A_n is normal in S_n and we have an isomorphism $S_n/A_n \cong \mathrm{im}(\mathrm{sgn}) = \{\pm 1\}$, which implies that $2 = |S_n/A_n| = |S_n|/|A_n|$. We already know that $|S_n| = n!$ by Lemma 1.26, which completes the proof. □

Exercise 4.26. Prove that A_3 has isomorphism class C_3.

Exercise 4.27. Prove that A_4 is not abelian.

4.2. **Group actions.**

4.2.1. *Definitions, examples and general properties.*

Definition 4.28. Let G be a group and let A be a non-empty set. A 'group action' of G on A is a function

$$\cdot : G \times A \to A$$

which, abbreviating $\cdot(g, a)$ to $g \cdot a$, satisfies the following properties:

(A1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$,$a \in A$.

(A2) $1 \cdot a = a$ for every $a \in A$.

We say that 'G acts on A via $\cdot$', or simply that 'G acts on A' when the action is clear from the context.

Notation 4.29. The expression $g \cdot a$ is often further abbreviated to ga.

Remark 4.30. To be more precise, we should have defined the function $\cdot$ to be a 'left group action' or a 'group action from the left', as there exists an analogous notion of a right group action, which we will not use here.

Recall that S_A is the set of permutations of a set A.

Definition 4.31. The 'permutation representation' associated to a group action of G on A is the function

$$\rho : G \to S_A$$

which, after abbreviating $\rho(g)$ to ρ_g, is defined by

$$\rho_g(a) := g \cdot a \tag{22}$$

for each $g \in G$ and each $a \in A$.

For this definition to make sense we must immediately verify that each function ρ_g is indeed a permutation of A!

Lemma 4.32. *Let G act on A. Then for every $g \in G$, the function $\rho_g : A \to A$ defined by (22) belongs to S_A.*

Proof. It is enough to show that ρ_g has a double-sided inverse, which will be $\rho_{g^{-1}}$.

For any $a \in A$ we have

$$(\rho_{g^{-1}} \circ \rho_g)(a) = \rho_{g^{-1}}(\rho_g(a)) = \rho_{g^{-1}}(g \cdot a) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1 \cdot a = a.$$

This proves that $\rho_{g^{-1}} \circ \rho_g = \mathrm{id}_A$. The same argument shows that $\rho_g \circ \rho_{g^{-1}} = \rho_{(g^{-1})^{-1}} \circ \rho_{g^{-1}} = \mathrm{id}_A$, so $\rho_{g^{-1}}$ is indeed a double-sided inverse of ρ_g. □

The permutation representation ρ is in fact a group homomorphism.

Lemma 4.33. *Let G act on A. Then the function $\rho : G \to S_A$ is a group homomorphism.*

Proof. For every $g_1, g_2 \in G$ and $a \in A$ we have

$$\begin{aligned}(\rho(g_1g_2))(a) &= \rho_{g_1g_2}(a) = (g_1g_2) \cdot a = g_1 \cdot (g_2 \cdot a)\\ &= g_1 \cdot \rho_{g_2}(a) = \rho_{g_1}(\rho_{g_2}(a)) = (\rho_{g_1} \circ \rho_{g_2})(a) = (\rho(g_1) \circ \rho(g_2))(a).\end{aligned}$$

This means that $\rho(g_1g_2) = \rho(g_1) \circ \rho(g_2)$, as required. □

Exercise 4.34. Let G be a group and let A be a non-empty set. Let $f : G \to S_A$ be a group homomorphism. Prove that the function $G \times A \to A$ given by

$$g \cdot a := (f(g))(a) \tag{23}$$

is a group action of G on A. Conclude that the set of group actions of G on A and the set of group homomorphisms $G \to S_A$ are in bijective correspondence.

Definition 4.35. Given a group G, and following Exercise 4.34, we define a 'permutation representation of G' to be a homomorphism $f : G \to S_A$ for any non-empty set A. We shall say that the action (23) of G on A 'induces' the associated permutation representation f.

Examples 4.36.
(i) The 'trivial action' of G on A is $g \cdot a = a$ for every $g \in G$ and $a \in A$. The associated permutation representation is the trivial homomorphism $G \to S_A$ which maps every $g \in G$ to 1_A.
(ii) Let F be either $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ (or any field) and let V be a vector space over F. Then the multiplicative group F^* acts on V via scalar multiplication. In particular, in this way, F^* acts on F.
(iii) For any non-empty set A, the group $G = S_A$ acts on A via evaluation, $g \cdot a = g(a)$. The associated permutation representation is the identity homomorphism $S_A \to S_A$.
(iv) The group $G = D_{2n}$ also acts on $A = \{1, \dots, n\}$ via evaluation. The associated permutation representation is the inclusion $D_{2n} \subseteq S_n$. This action has a natural geometric interpretation, by identifying the set A with the set of vertices of a regular n-gon: evaluation of an element of $G = D_{2n}$ then simply means applying the corresponding symmetry to the n-gon.
(v) Any group G acts on the set $A = G$ via left multiplication, $g \cdot g' = gg'$. This action is called the (left) regular action of G on itself.

Definition 4.37. The subgroup $\{g \in G : g \cdot a = a \text{ for all } a \in A\}$ of G is the 'kernel of the action of G on A'.

Exercise 4.38. Prove that the kernel of the action of G on A is equal to the kernel of the associated permutation representation ρ. Determine the kernel of each action described in Examples 4.36.

Exercise 4.39. Let G be a group and consider the set $A = G$.

(i) Find an example of group G for which the formula $g \cdot a = ag$ does not define an action of G on itself.
(ii) Show that the formula $g \cdot a = ag^{-1}$ does define an action of G on itself. Describe the associated permutation representation.
(iii) Show that the formula $g \cdot a = gag^{-1}$ does define an action of G on itself, called the 'conjugation action'. Describe the associated permutation representation and the kernel of the action.
(iv) Given an action of G on A and a subgroup H of G, show that H acts on A via the restriction of the original action, with associated permutation representation of H given by the restriction of the permutation representation of G.
(v) In particular, any subgroup H of G acts on $A = G$ via left multiplication, $h \cdot a = ha$, and via conjugation, $h \cdot a = hah^{-1}$. Describe the associated permutation representations.

Definition 4.40. Let G act on A. For each $a \in A$, the 'stabiliser' of a in G is the set

$$G_a := \{g \in G : g \cdot a = a\}.$$

Lemma 4.41. *For any $a \in A$, the subset G_a is a subgroup of G.*

Proof. By the axiom $(A2)$ we know that 1 belongs to G_a.

If g, h belong to G_a then

$$(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a,$$

so gh belongs to G_a.

Finally, if g belongs to G_a then

$$a = 1 \cdot a = (g^{-1}g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a,$$

so g^{-1} also belongs to G_a. □

Example 4.42. In Example 3.34 we showed that the subgroup $\{\sigma \in S_4 : \sigma(1) = 1\}$ is not normal in S_4. This subgroup is the stabiliser G_1 of $1 \in A$ of the action via evaluation of $G = S_4$ on the set $A = \{1, 2, 3, 4\}$, as described in Examples 4.36 (iii).

More generally, one can prove that for the action via evaluation of $G = S_n$ on the set $A = \{1, \dots, n\}$ and for any $i \in A$, the stabiliser

$$G_i = \{\sigma \in S_n : \sigma(i) = i\}$$

of i is not normal in $G = S_n$. In fact, one can show that $N_G(G_i) = G_i$ so, in some sense, G_i is as far from being normal in S_n as possible.

Exercise 4.43. Prove that for the action via evaluation of $G = S_n$ on the set $A = \{1, \dots, n\}$ and for any $i \in A$, the stabiliser G_i of i is not normal in $G = S_n$. Prove also that G_i is isomorphic to S_{n-1}.

Exercise 4.44. For the action via evaluation of $G = D_8$ on the set $A = \{1, 2, 3, 4\}$, find the stabiliser of every element of A.

Proposition 4.45. *Let G act on A. Then the binary relation on A defined by $a \sim b$ if $a = g \cdot b$ for some $g \in G$ is an equivalence relation. In addition for each $a \in A$, the cardinality of the equivalence class $[a]$ of a under $\sim$ is $[G : G_a]$.*

Proof. The relation $\sim$ is reflexive because $a = 1 \cdot a$ by $(A2)$.

If $a \sim b$ with $a = g \cdot b$ then

$$b = 1 \cdot b = (g^{-1}g) \cdot b = g^{-1} \cdot (g \cdot b) = g^{-1} \cdot a,$$

so $b \sim a$. The relation is thus symmetric.

If $a \sim b$ and $b \sim c$ with $a = g \cdot b$ and $b = h \cdot c$ then $a = g \cdot (h \cdot c) = (gh) \cdot c$ so $a \sim c$. The relation is thus transitive and therefore an equivalence relation, as required.

We now compute the cardinality of $[a] = \{g \cdot a : g \in G\}$. It is enough to construct a bijection from $[a]$ to the set of left cosets of G_a in G.

We first claim that mapping $g \cdot a$ to gG_a for any $g \in G$ gives a well-defined injection. Indeed, for elements g, h of G, one has $g \cdot a = h \cdot a$ if and only if the element $h^{-1} \cdot (g \cdot a) = (h^{-1}g) \cdot a$ is equal to a, if and only if $h^{-1}g$ belongs to G_a, if and only if $gG_a = hG_a$.

Knowing that $(g \cdot a) \mapsto gG_a$ is a well-defined map, it is also clearly surjective, thus gives a bijection between $[a]$ and the set of left cosets of G_a in G. This proves that the cardinality of $[a]$ is $[G : G_a]$. □

Definition 4.46.
(i) For each $a \in A$, the equivalence class $[a] = \{g \cdot a : g \in G\}$ is called to 'orbit' of a in G. We sometimes denote it by $\mathcal{O}_a^G$ or simply by $\mathcal{O}_a$ when G is clear from context.
(ii) The action of G on A is called 'transitive' if for every pair a, b in A there exists a $g \in G$ with $a = g \cdot b$.
(iii) For any subgroup H of S_n, the 'orbits of H' will be the orbits of the elements of $A = \{1, \ldots, n\}$ in H under the evaluation action of H (obtained as the restriction of the evaluation action of S_n). For any $\sigma \in S_n$, the 'orbits of σ' will be the orbits of $\langle\sigma\rangle$.

Exercise 4.47. Show that the action of G is transitive if and only if $\mathcal{O}_a = \mathcal{O}_b$ for every $a, b \in A$, and that the action of G is transitive if and only if $\mathcal{O}_a^G = A$ for every $a \in A$.

Exercise 4.48. Prove that the evaluation action of $G = S_n$ on $A = \{1, \ldots, n\}$ is transitive.

Remark 4.49. Recall from Exercise 4.39 that if G acts on A then any subgroup H of G acts on A via the restriction of the original action. However, even if the original action of G is transitive, the action of H need not be transitive.

For instance we consider the evaluation action of $G = S_4$ on $A = \{1, 2, 3, 4\}$ and we set $H := \langle(1, 2), (3, 4)\rangle$. We know from Exercise 4.48 that the action of G is transitive. However, for the action of H we have the orbit

$$\mathcal{O}_1^H = \{h(1) : h \in H\} = \{1, 2\}$$

of $1 \in A$ and the orbit

$$\mathcal{O}_3^H = \{h(3) : h \in H\} = \{3, 4\}$$

of $3 \in A$, so there is more than one orbit for this action and it is not transitive.

Exercise 4.50. Find all the orbits of the action of the cyclic subgroup $H = \langle(1, 2)(3, 4, 5)\rangle$ of $G = S_5$ on $A = \{1, 2, 3, 4, 5\}$.

4.2.2. *Cycle decompositions.* In §1.2.1 we already explained that every element of S_n has a cycle decomposition, and that this decomposition is unique, up to re-ordering of the (disjoint) cycles (we know disjoint cycles commute by Lemma 4.3), and obviously also up to choosing which number to write first within each individual cycle (since $(a_1, \ldots, a_m) = (a_i, a_{i+1}, \ldots, a_m, a_1, \ldots, a_{i-1})$). See also [2, p. 30] for an algorithm that leads to the cycle decomposition of any permutation.

In this section we use the theory of group actions to give an alternative justification of the existence and uniqueness of cycle decompositions.

Fix $\sigma \in S_n$ and set $H := \langle\sigma\rangle$ and $A := \{1, \ldots, n\}$. By Proposition 4.45 we know that the set $\{\mathcal{O}_a^H : a \in A\}$ is a partition of A.

We fix $a \in A$ and write H_a for the stabiliser of a in H. From the proof of Proposition 4.45 we also know that there is a (well-defined) bijection between $\mathcal{O}_a^H$ and the set of left cosets of H_a in H, given by

$$\sigma^i(a) \mapsto \sigma^i H_a.$$

Since H_a is cyclic it is abelian, so H_a is normal in H, and the given bijection is between $\mathcal{O}_a^H$ and H/H_a. Moreover H/H_a is a cyclic group of order $d := [H : H_a] = |H/H_a| = |\mathcal{O}_a^H|$. We conclude that

$$\mathcal{O}_a^H = \{a, \sigma(a), \sigma^2(a), \ldots, \sigma^{d-1}(a)\}.$$

The above argument shows that σ cycles the elements of any given orbit $\mathcal{O}^H$. Put another way, given an orbit $\mathcal{O}^H$ of cardinality $d_{\mathcal{O}^H}$, σ acts on its elements as a $d_{\mathcal{O}^H}$-cycle.

Since the set of orbits $\mathcal{O}^H$ is a partition of A, we obtain a decomposition of σ into disjoint cycles by simply composing the $d_{\mathcal{O}^H}$-cycles corresponding to each different orbit $\mathcal{O}^H$.

Now, these orbits are uniquely determined by σ, although of course we may compose their associated cycles in whichever order we wish (again, disjoint cycles commute by Lemma 4.3).

Within each orbit $\mathcal{O}^H$ we may begin with any element $a \in \mathcal{O}^H$ as a representative. Choosing some $\sigma^i(a) \in \mathcal{O}^H_a$ as the initial representative of the orbit $\mathcal{O}^H_a = \mathcal{O}^H_{\sigma^i(a)}$ instead of a, we simply end up re-ordering the elements of $\mathcal{O}^H_a$ as

$$\sigma^i(a), \sigma^{i+1}(a), \dots, \sigma^{d-1}(a), a, \sigma(a), \dots, \sigma^{i-1}(a).$$

This change in the corresponding cycle simply amounts to writing a different number in first place.

4.2.3. *Left multiplication action and Cayley's Theorem.* We recall that any group G acts on itself (the set $A = G$) via left multiplication, meaning that

$$g \cdot a := ga$$

for any $g, a \in G$. This action is sometimes called the '(left) regular action' of G. We write ρ for the associated permutation representation, which is sometimes called the '(left) regular representation' of G.

If G is a finite group then any choice of bijection α between G and $\{1, \dots, |G|\}$ induces an isomorphism $\alpha^* : S_G \cong S_{|G|}$, given by

$$(\alpha^*(\sigma))(i) = (\alpha \circ \sigma \circ \alpha^{-1})(i)$$

for every $\sigma \in S_G$ and every $i \in \{1, \dots, |G|\}$. In this way we may then identify the permutation representation ρ with a homomorphism $G \to S_{|G|}$, and often omit the choice of α from the notation.

Example 4.51. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and set $\alpha((0,0)) = 1$, $\alpha((0,1)) = 2$, $\alpha((1,0)) = 3$ and $\alpha((1,1)) = 4$. We identify ρ with a homomorphism $G \to S_4$. Obviously $\rho(0,0) = 1$. We compute the remaining values of ρ.

We have

$$\begin{aligned}
\rho((0,1))(1) &= \rho((0,1))(0,0) = (0,1) + (0,0) = (0,1) = 2,\\
\rho((0,1))(2) &= \rho((0,1))(0,1) = (0,1) + (0,1) = (0,0) = 1,\\
\rho((0,1))(3) &= \rho((0,1))(1,0) = (0,1) + (1,0) = (1,1) = 4,\\
\rho((0,1))(4) &= \rho((0,1))(1,1) = (0,1) + (1,1) = (1,0) = 3,\\
\rho((1,0))(1) &= \rho((1,0))(0,0) = (1,0) + (0,0) = (1,0) = 3,\\
\rho((1,0))(2) &= \rho((1,0))(0,1) = (1,0) + (0,1) = (1,1) = 4,\\
\rho((1,0))(3) &= \rho((1,0))(1,0) = (1,0) + (1,0) = (0,0) = 1,\\
\rho((1,0))(4) &= \rho((1,0))(1,1) = (1,0) + (1,1) = (0,1) = 2,\\
\rho((1,1))(1) &= \rho((1,1))(0,0) = (1,1) + (0,0) = (1,1) = 4,\\
\rho((1,1))(2) &= \rho((1,1))(0,1) = (1,1) + (0,1) = (1,0) = 3,\\
\rho((1,1))(3) &= \rho((1,1))(1,0) = (1,1) + (1,0) = (0,1) = 2,
\end{aligned}$$

$$\rho((1,1))(4) = \rho((1,1))(1,1) = (1,1) + (1,1) = (0,0) = 1.$$

So we find

$$\rho((0,1)) = (1,2)(3,4), \quad \rho((1,0)) = (1,3)(2,4) \text{ and } \rho((1,1)) = (1,4)(2,3).$$

Please observe that this action is transitive and also that the stabiliser of each element of G is $\{1\}$, and therefore the kernel of the action and of the associated representation is also trivial.

Proposition 4.52. The (left) regular action of any group G is transitive, the stabiliser of each element of G is trivial and the kernel of this action, or equivalently of the (left) regular representation, is also trivial.

Proof. For any $a, b \in G$ we have $a = (ab^{-1})b$, so the action is transitive.

For any a in G, the stabiliser $G_a = \{g \in G : ga = a\}$ is trivial by the usual cancellation property.

Finally, the kernel of the action is clearly equal to $\bigcap_{a \in G} G_a$, which is trivial since each G_a is. □

We may now easily deduce Cayley's Theorem from Proposition 4.52.

Theorem 4.53. *Every group is isomorphic to a permutation group. In particular, if G is a finite group then G is isomorphic to a subgroup of $S_{|G|}$.*

Proof. It is enough to prove that any group G is isomorphic to a subgroup of S_G. The final claim would then also follow because if G is finite then S_G is isomorphic to $S_{|G|}$.

Now the (left) regular representation

$$\rho : G \to S_G$$

is injective by Proposition 4.52, so it defines an isomorphism from G to $\mathrm{im}(\rho)$. This completes the proof. □

Remark 4.54. Of course, Cayley's Theorem does **not** state that G is isomorphic to S_G, which would be a blatantly false statement. For instance, in Example 4.51 we showed that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is isomorphic to the subgroup

$$\{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

of S_4. It certainly cannot, however, be isomorphic to S_4.

Exercise 4.55. Let G be a group and let H be a subgroup of G. Write A for the set of left cosets of H in G.

(i) Prove that G acts via left multiplication on the set A,

$$g \cdot (g'H) := (gg')H.$$

(ii) Prove that this action is transitive.
(iii) Prove that the stabiliser of $H \in A$ is $H \subseteq G$.
(iv) Prove that the kernel of the action is $\bigcap_{g \in G} gHg^{-1}$.
(v) Prove that the kernel of the action is the largest normal subgroup of G contained in H.

We use Exercise 4.55 to prove a generalisation of Lemma 3.31.

Lemma 4.56. *Let G be a finite group. Let p be the smallest prime divisor of $|G|$. Then any subgroup of G of index p is normal in G.*

Proof. Let H be a subgroup of G of index p. Let K be the kernel of the action of G on the set A of left cosets of H in G. By assumption, A has cardinality p. By Exercise 4.55 (v), K is contained in H, and we set $k := [H : K]$. It will be enough to prove that $k = 1$, since then $H = K$ is normal in G.

We first note that the permutation representation $\rho : G \to S_A \cong S_p$ induces, by the First Isomorphism Theorem 3.44, an isomorphism

$$G/K \cong \mathrm{im}(\rho).$$

Since

$$|G/K| = [G : K] = [G : H][H : K] = pk,$$

the subgroup $\mathrm{im}(\rho)$ of S_p has order pk. By Lagrange's Theorem 2.61 we get that pk divides $p!$.

It follows that k divides $p!/p = (p-1)!$. Since all prime divisors of $(p-1)!$ are smaller than p, all prime divisors of k are smaller than p.

On the other hand, if ℓ is a prime divisor of k then ℓ also divides

$$[G : H]k|K| = [G : H][H : K][K : \{1\}] = |G|,$$

which would contradict the minimality of p. Therefore k has no prime divisors, or equivalently $k = 1$, as required. □

Remark 4.57. In the setting of Lemma 4.56, there might not be any subgroups of G of index p. For example, A_4 has order 12 but no subgroups of index 2. In such cases, the Lemma does not say anything.

4.2.4. *Conjugation action and the class equation.* We recall that any group G also acts on itself (the set $A = G$) via conjugation, meaning that

$$g \cdot a := gag^{-1}$$

for any $g, a \in G$. Indeed, one has both

$$g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2ag_2^{-1}) = g_1g_2ag_2^{-1}g_1^{-1} = (g_1g_2)a(g_1g_2)^{-1} = (g_1g_2) \cdot a$$

and also $1 \cdot a = 1a1^{-1} = 1a1 = a$.

Definition 4.58. The orbits of G under the conjugation action are called the 'conjugacy classes' of G. (Two elements a and b of G are conjugate if and only if they belong to the same conjugacy class.)

Examples 4.59. (i) If G is abelian then the conjugation action of G coincides with the trivial action of G on G, as $g \cdot a = gag^{-1} = a$ for every g and a.
(ii) If G is non-trivial then the conjugation action of G is never transitive: the conjugacy class $\mathcal{O}_1$ of 1 is

$$\mathcal{O}_1 = \{g \cdot 1 : g \in G\} = \{g1g^{-1} : g \in G\} = \{1\},$$

so it cannot be equal to G.

(iii) We compute all conjugacy classes in S_3. We have $\mathcal{O}_1 = \{1\}$. We have $1 \cdot (1,2) = (1,2) = (1,2) \cdot (1,2)$, $(1,3) \cdot (1,2) = (2,3) = (1,2,3) \cdot (1,2)$, $(2,3) \cdot (1,2) = (1,3) = (1,3,2) \cdot (1,2)$, so we get

$$\mathcal{O}_{(1,2)} = \{(1,2),(1,3),(2,3)\}.$$

We know $(1,2,3)$ belongs to $\mathcal{O}_{(1,2,3)}$ so it is enough to determine whether $(1,3,2)$ belongs to this same conjugacy class or not. One finds that $(1,2) \cdot (1,3,2) = (1,2,3)$ so we only get a a third conjugacy class

$$\mathcal{O}_{(1,2,3)} = \{(1,2,3),(1,3,2)\}.$$

Exercise 4.60. Prove that an element a of G belongs to $Z(G)$ if and only if its conjugacy class $\mathcal{O}_a$ is equal to $\{a\}$, if and only if the conjugacy class of a is a singleton. Deduce that the conjugation action of G restricts to define a conjugation action of G on the set $G \setminus Z(G)$.

Proposition 4.61. *The conjugacy class of any element g of G has cardinality $[G : C_G(g)]$.*

Proof. By Proposition 4.45 we know that the conjugacy class of g has cardinality $[G : G_g]$, where G_g denotes the stabiliser of g under the conjugation action. But clearly $G_g = C_G(g)$. □

Exercise 4.62. Let G be a group. We write $A(G)$ for the set of subsets of G. We define a 'conjugation action of G on $A(G)$' by setting

$$g \cdot S := gSg^{-1} \tag{24}$$

for any $g \in G$ and any $S \in A(G)$. Two subsets of G are conjugate if and only if they belong to the same orbit under this action.

(i) Verify that (24) does indeed define an action of G on $A(G)$.
(ii) Prove that the number of conjugates of a subset S of G is $[G : N_G(S)]$.

We now apply Proposition 4.61 to obtain the 'Class Equation'. Before stating this result, we recall from Exercise 4.60 that any element a of $Z(G)$ has conjugacy class $\{a\}$, and thus that the conjugation action of G restricts to define a conjugation action of G on the set $G \setminus Z(G)$.

Theorem 4.63. *Let G be a finite group and let $g_1, \dots, g_r$ be a set of representatives of the distinct conjugacy classes of $G \setminus Z(G)$. Then*

$$|G| = |Z(G)| + \sum_{i=1}^{i=r} [G : C_G(g_i)]. \tag{25}$$

Proof. Let $Z(G) = \{z_1, z_2, \dots, z_m\}$. Let $\mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_r$ be the distinct conjugacy classes of $G \setminus Z(G)$, each with representative g_i for $1 \leq i \leq r$ (meaning that $\mathcal{K}_i = \mathcal{O}_{g_i}$ is the conjugacy class of g_i). Then the full set of conjugacy classes of G is

$$\{z_1\}, \{z_2\}, \dots, \{z_m\}, \mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_r,$$

which is a partition of G (by Proposition 4.45). Therefore

$$|G| = (\sum_{i=1}^{i=m} 1) + (\sum_{i=1}^{i=r} |\mathcal{K}_i|) = |Z(G)| + \sum_{i=1}^{i=r} [G : C_G(g_i)],$$

where we have used that the cardinality of $\mathcal{K}_i$ is $[G : C_G(g_i)]$ by Proposition 4.61. □

Examples 4.64. (i) If G is abelian then $Z(G) = G$ and therefore the Class Equation is the trivial statement $|G| = |G|$.
(ii) In any group G and for any $g \in G$ we have $\langle g \rangle \leq C_G(g)$, and for any $g \in G \setminus Z(G)$ we have $C_G(g) \neq G$. This observation helps compute conjugacy classes. For instance in $G = Q_8$ we have $Z(Q_8) = \{\pm 1\}$. We have $i \notin Z(Q_8)$, so $C_{Q_8}(i) \neq Q_8$, and also $\langle i \rangle \leq C_{Q_8}(i) \leq Q_8$ with $[Q_8 : \langle i \rangle] = 2$. Therefore $C_{Q_8}(i) = \langle i \rangle$ and the conjugacy class of i has cardinality 2, meaning it is $\{\pm i\}$ (since $-i = kik^{-1}$) and contains no other elements. Similarly one computes that the conjugacy class of j is $\{\pm j\}$ and the conjugacy class of k is $\{\pm k\}$.
(iii) In $G = D_8$ we have $Z(D_8) = \{1, r^2\}$. We have $\langle r \rangle \leq C_{D_8}(r) \leq D_8$ with $[D_8 : \langle r \rangle] = 2$ so $C_{D_8}(r) = \langle r \rangle$ and the conjugacy class of r has cardinality 2, meaning it is $\{r, r^3\}$ (since $r^3 = srs$) and contains no other elements. For the element s of D_8 we could a priori either have $C_{D_8}(s) = \langle s \rangle = \{1, s\}$ or $|C_{D_8}(s)| = 4$, but clearly r^2 belongs to $C_{D_8}(s)$, so it must be the latter situation. Thus $[D_8 : C_{D_8}(s)] = 2$ and the conjugacy class of s is $\{s, sr^2\}$ (since $sr^2 = rsr^{-1}$). There are two remaining elements in D_8, namely sr and sr^3, and they must form the final conjugacy class $\{sr, sr^3\}$ together, as neither of them is in $Z(D_8)$ and thus neither of them can form a conjugacy class as a singleton.

We now give some important applications of the Class Equation.

Theorem 4.65. *Let G be a group whose order is a power of a prime number. Then $Z(G) \neq \{1\}$.*

Proof. Let $|G| = p^n$ for some $n \in \mathbb{N}$. For any $g \in G \setminus Z(G)$ we know $C_G(g) \neq G$, and since $[G : C_G(g)]$ divides $|G|$ it must be a power of p. Now in the Class Equation (25) p divides both $|G|$ and $\sum_{i=1}^{i=r} [G : C_G(g_i)]$ so it must also divide $|Z(G)|$, which is thus greater that 1. □

Corollary 4.66. *If p is a prime and G is a group of order p^2, then G is abelian and its isomorphism class is either C_{p^2} or $C_p \times C_p$.*

Proof. Since $Z(G) \neq \{1\}$ by Theorem 4.65, the quotient $G/Z(G)$ can only have order 1 or p, and is therefore cyclic either way. By Exercise 3.102 we then know that G is abelian.

If G has an element of order p^2 then G is cyclic and hence has isomorphism class C_{p^2}. Otherwise, every $x \neq 1$ in G must have order p. We assume that this is the case.

Fix any $x \neq 1$ and then fix any y in $G \setminus \langle x \rangle$. Both x and y have order p. We have $\langle x \rangle \subsetneq \langle x, y \rangle \leq G$ (with the first inclusion strict by the choice of y) so $|\langle x, y \rangle|$ divides p^2 and is greater than $|\langle x \rangle| = p$. Thus $|\langle x, y \rangle| = p^2$ and $G = \langle x, y \rangle$.

The group $\langle x \rangle \times \langle y \rangle$ has isomorphism class $C_p \times C_p$ because both x and y have order p. It is therefore enought to verify that the function

$$f : \langle x \rangle \times \langle y \rangle \to \langle x, y \rangle = G$$

given by $f((x^a, y^b)) := x^a y^b$ is an isomorphism (for $0 \leq a, b \leq p-1$). Since we already know that G is abelian, we get

$$\begin{aligned} f((x^a, y^b)(x^c, y^d)) = f((x^{a+c}, y^{b+d})) = x^{a+c} y^{b+d} \\ = x^a (x^c y^b) y^d = x^a y^b x^c y^d = f((x^a, y^b)) f((x^c, y^d)), \end{aligned}$$

so f is a homomorphism.

Now f is surjective, by Proposition 2.19 combined with the fact that G is abelian. But a surjective function between two sets of cardinality p^2 must necessarily be bijective, so f is an isomorphism, as required. □

4.2.5. *Conjugacy classes in S_n.*

Lemma 4.67. *Let σ and τ be elements of S_n and let*

$$(a^1_1, a^1_2, \ldots, a^1_{k_1})(a^2_1, a^2_2, \ldots, a^2_{k_2}) \ldots (a^r_1, a^r_2, \ldots, a^r_{k_r})$$

be the cycle decomposition of σ. Then $\tau\sigma\tau^{-1}$ has cycle decomposition

$$(\tau(a^1_1), \tau(a^1_2), \ldots, \tau(a^1_{k_1}))(\tau(a^2_1), \tau(a^2_2), \ldots, \tau(a^2_{k_2})) \ldots (\tau(a^r_1), \tau(a^r_2), \ldots, \tau(a^r_{k_r})).$$

Proof. Given $1 \leq i, j \leq n$ we have $\sigma(i) = j$ if and only if

$$(\tau\sigma\tau^{-1})(\tau(i)) = \tau(\sigma(i)) = \tau(j).$$

Thus the ordered pair i, j appears in the cycle decomposition of σ if and only if the ordered pair $\tau(i), \tau(j)$ appears in the cycle decomposition of $\tau\sigma\tau^{-1}$. This completes the proof. □

Example 4.68. If in S_9 we have $\sigma = (1, 2)(3, 4, 5)(6, 7, 8, 9)$ and $\tau = (1, 3, 5, 7)(2, 4, 6, 8)$ then

$$\tau\sigma\tau^{-1} = (3, 4)(5, 6, 7)(8, 1, 2, 9).$$

Definition 4.69.
(i) If $\sigma \in S_n$ is the product of disjoint cycles of lengths $k_1, k_2, \ldots, k_r$ with $k_1 \leq k_2 \leq \ldots \leq k_r$, including the 1-cycles, then the sequence $k_1, k_2, \ldots, k_r$ is called the 'cycle type' of σ.
(ii) Given a natural number n, a 'partition of n' is any non-decreasing sequence of natural numbers whose sum is equal to n.

Remark 4.70. By definition the cycle type of an element of S_n is a partition of n.

Examples 4.71.
(i) The cycle type of an m-cycle in S_n is $1, 1, \ldots, 1, m$, where 1 occurs $n - m$ times in the sequence.
(ii) The cycle type of $\tau = (1, 3, 5, 7)(2, 4, 6, 8) \in S_9$ is $1, 4, 4$.

Proposition 4.72. *Two elements of S_n are conjugate if and only if they have the same cycle type. The number of conjugacy classes in S_n equals the number of partitions of n.*

Proof. From Lemma 4.67 it is clear that conjugate premutations have the same cycle type. Conversely, if

$$\sigma = (a^1_1, a^1_2, \ldots, a^1_{k_1})(a^2_1, a^2_2, \ldots, a^2_{k_2}) \ldots (a^r_1, a^r_2, \ldots, a^r_{k_r})$$

and

$$\sigma' = (b^1_1, b^1_2, \ldots, b^1_{k_1})(b^2_1, b^2_2, \ldots, b^2_{k_2}) \ldots (b^r_1, b^r_2, \ldots, b^r_{k_r})$$

both have cycle type $k_1, k_2, \ldots, k_r$ then the map $\tau(a^j_i) := b^j_i$ defines a permutation τ in S_n, and Lemma 4.67 implies that $\sigma' = \tau\sigma\tau^{-1}$.

The second claim follows immediately from the first, as certainly any partiton of n may be achieved as the cycle type of a permutation of S_n. □

Examples 4.73.
(i) If in S_9 we have

$$\sigma = (2,4,7,6)(3,5)(8,9) = (1)(3,5)(8,9)(2,4,7,6)$$

and

$$\sigma' = (1,8)(2,6,9,5)(4,7) = (3)(1,8)(4,7)(2,6,9,5)$$

then $\sigma' = \tau_1\sigma\tau_1^{-1}$ for $\tau_1 = (1,3)(4,6,5,8)(7,9)$.

Please note that we may also write σ' in alternative ways, for instance

$$\sigma' = (3)(4,7)(8,1)(5,2,6,9) = (3)(8,1)(4,7)(5,2,6,9).$$

Thus we also have $\sigma' = \tau_2\sigma\tau_2^{-1}$ and $\sigma' = \tau_3\sigma\tau_3$ for $\tau_2 = (1,3,4,2,5,7,6,9)$ and $\tau_3 = (1,3,8,4,2,5)(6,9,7)$.
(ii) For $n = 5$, the partitions of 5 are

$$\{1,1,1,1,1\},\ \{1,1,1,2\},\ \{1,1,3\},\ \{1,4\},\ \{5\},\ \{1,2,2\},\ \{2,3\}.$$

A set of representatives of all the conjugacy classes of S_5 is therefore given by

$$1,\ (1,2),\ (1,2,3),\ (1,2,3,4),\ (1,2,3,4,5),\ (1,2)(3,4),\ (1,2)(3,4,5).$$

Exercise 4.74. Fix an m-cycle σ in S_n, with $m \leq n$. Write H_σ for the subgroup of S_n which fixes all of the m integers that occur in the cycle σ.

(i) Determine the number of conjugates of σ.
(ii) Determine the order of $C_{S_n}(\sigma)$.
(iii) Prove that $C_{S_n}(\sigma) = \{\sigma^i\tau : 0 \leq i \leq m-1, \tau \in H_\sigma\}$.

We will now apply some of the above results to prove that A_5 is a simple group. This will be our main example of a non-abelian simple group. Before proceeding we need a final general result that will be used in the proof.

Lemma 4.75. *Let G be a group. If H is a normal subgroup of G and $\mathcal{K}$ is a conjugacy class of G then either $\mathcal{K} \subseteq H$ or $\mathcal{K} \cap H = \emptyset$. In particular, every normal subgroup of G is a union of conjugacy classes.*

Proof. If x belongs to $\mathcal{K} \cap H$ then every conjugate gxg^{-1} of x belongs to gHg^{-1}, for every $g \in G$. Since H is normal in G, every conjugate of x belongs to H, meaning that the conjugacy class $\mathcal{K}$ of x is contained in H. □

Theorem 4.76. *A_5 is a simple group.*

Proof. We recall that $|A_5| = 60$. We claim that A_5 has five conjugacy classes, of cardinalities $1, 15, 20, 12$ and 12. We note that two elements of A_5 that have different cycle type are not conjugate in S_5, and therefore cannot be conjugate in A_5 either.

There are twenty 3-cycles in S_5, and all of them obviously belong to A_5. We claim that they are all conjugate in A_5. By Exercise 4.74(iii) we have

$$\begin{aligned} C_{S_5}((1,2,3)) &= \{(1,2,3)^i\tau : i \in \{0,1,2\}, \tau \in \{1,(4,5)\}\} \\ &= \{1,(1,2,3),(1,3,2),(4,5),(1,2,3)(4,5),(1,3,2)(4,5)\} \end{aligned}$$

and therefore

$$C_{A_5}((1,2,3)) = \{1, (1,2,3), (1,3,2)\}.$$

By Proposition 4.61, the conjugacy class of $(1,2,3)$ in A_5 has cardinality $60/3 = 20$, so all twenty 3-cycles are conjugate in A_5.

There are twenty-four 5-cycles in S_5, and all of them obviously belong to A_5. We claim that they comprise two different conjugacy classes in A_5, both of them of cardinality 12. By Exercise 4.74(iii) we have $C_{S_5}((1,2,3,4,5)) = \langle(1,2,3,4,5)\rangle$ and therefore $C_{A_5}((1,2,3,4,5)) = \langle(1,2,3,4,5)\rangle$ has order 5. By Proposition 4.61, the conjugacy class of $(1,2,3,4,5)$ in A_5 has cardinality $60/5 = 12$.

There is therefore some 5-cycle σ that is not conjugate to $(1,2,3,4,5)$ in A_5 (in fact, the method of proof of Proposition 4.72 shows that any element of S_5 conjugating $(1,2,3,4,5)$ into $(1,3,5,2,4)$ must be an odd permutation, and therefore that these two 5-cycles cannot be conjugate in A_5, so one may take $\sigma = (1,3,5,2,4)$). By exactly the same argument as above we get $C_{S_5}(\sigma) = \langle\sigma\rangle$ and $C_{A_5}(\sigma) = \langle\sigma\rangle$ and so the conjugacy class of σ in A_5 has cardinality $60/5 = 12$. We conclude that the twenty-four 5-cycles comprise two different conjugacy classes in A_5, both of them of cardinality 12, as claimed.

There are fifteen remaining non-trivial elements of A_5. We easily find that these must be

$$\begin{aligned}
&(1,2)(3,4), (1,2)(3,5), (1,2)(4,5), (1,3)(2,4), (1,3)(2,5), (1,3)(4,5),\\
&(1,4)(2,3), (1,4)(2,5), (1,4)(3,5), (1,5)(2,3), (1,5)(2,4), (1,5)(3,4),\\
&(2,3)(4,5), (2,4)(3,5), (2,5)(3,4), \qquad (26)
\end{aligned}$$

so they all have cycle type $2,2$. We claim that they are all conjugate in A_5.

By Exercise 4.77 below we know that $C_{A_5}((1,2)(3,4))$ has order 4 so indeed, by Proposition 4.61, the conjugacy class of $(1,2)(3,4)$ in A_5 has cardinality $60/4 = 15$, so all remaining non-trivial elements are conjugate in A_5.

Having computed the cardinalities of all conjugacy classes in A_5, let H be a normal subgroup of G. Then on the one hand the order of H is a divisor of 60 by Lagrange's Theorem, so it must be one of

$$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.$$

On the other hand by Lemma 4.75 we know that H must be a union of conjugacy classes, including the conjugacy class $\{1\}$, so the possibilities for its order are

$$1, 13, 16, 21, 25, 28, 33, 36, 40, 45, 48, 60.$$

The only numbers occurring in both lists are 1 and 60 so either $H = \{1\}$ or $H = A_5$. This proves that A_5 is simple. □

Exercise 4.77. Verify that no 5-cycle can belong to $C_{A_5}((1,2)(3,4))$, that no 3-cycle can belong to $C_{A_5}((1,2)(3,4))$, and finally use the list (26) to verify that

$$C_{A_5}((1,2)(3,4)) = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Remark 4.78. In fact A_n is simple for all $n \geq 5$. See [2, §4.6] for a proof of this fact.

4.3. **Sylow's Theorem.**

4.3.1. *The result.* In this section we prove a partial converse to Lagrange's Theorem 2.61 that is a very important result of group theory in its own right.

Definition 4.79. Let p be a prime number.

(i) A group of order p^α, for a natural number α, is called a 'p-group'. A 'p-subgroup' of a group is a subgroup of said group that is also a p-group.
(ii) If G is a finite group of order $p^\alpha m$ for $\alpha \geq 0, m \geq 1$ and with $p \nmid m$, then any subgroup of G of order p^α is called a 'Sylow p-subgroup' of G.
(iii) Let G be a finite group. The set of Sylow p-subgroups of G will be denoted by $\mathrm{Syl}_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$, or just by n_p when G is clear from context.

Clearly any conjugate of a Sylow p-subgroup of G is also a Sylow p-subgroup (see Exercise 3.18).

We may now state Sylow's Theorem.

Theorem 4.80. *Let G be a finite group and let p be a prime. Then:*

(i) *G has Sylow p-subgroups.*
(ii) *If P is a Sylow p-subgroup of G and Q is any p-subgroup of G then*

$$Q \subseteq gPg^{-1}$$

for some $g \in G$. In particular, any two Sylow p-subgroups of G are conjugate in G.
(iii) *We have*

$$n_p(G) \equiv 1 \quad (\textit{mod } p)$$

and also

$$n_p(G) = [G : N_G(P)] \tag{27}$$

for any Sylow p-subgroup P of G.

Remark 4.81. Let G be a group of order $p^\alpha m$ with $p \nmid m$. Let P be a Sylow p-subgroup of G. Since $P \leq N_G(P)$, the equality (27) implies that $n_p(G)$ divides m.

Before proving Sylow's Theorem we require the following auxiliary lemma.

Lemma 4.82. *Let P be a Sylow p-subgroup of G and let Q be any p-subgroup of p. Then $Q \cap N_G(P) = Q \cap P$.*

Proof. We set $H := Q \cap N_G(P)$. Since $P \subseteq N_G(P)$ it is clear that $Q \cap P \subseteq H$, and we must prove the reverse inclusion. It is clearly enough to prove that $H \subseteq P$.

To prove that $H \subseteq P$ we will simply prove that PH is a p-subgroup of G. If we can do this, we would have $P \subseteq PH$ with P a p-subgroup of G of the largest possible order, and thus we would have $P = PH$. But if $P = PH$ then $H \subseteq P$, as required.

Since H is contained in $N_G(P)$, we know from Corollary 3.53 that PH is a subgroup of G. By Proposition 3.49 we also have

$$|PH| = \frac{|P||H|}{|P \cap H|}.$$

Recalling that H is a subgroup of the p-group Q, we see that all the factors in the right-hand side of the above expression are powers of p. We conclude that PH is indeed a p-subgroup of G, as required to complete the proof. □

We finally provide the proof of Sylow's Theorem 4.80.

Proof. Write $|G| = p^\alpha m$ with $\alpha \geq 0, m \geq 1$ and $p \nmid m$.

We first prove claim (i) of Theorem 4.80 by induction on $|G|$. If $|G| = 1$ then there is nothing to prove. We now assume any group of order less than $p^\alpha m$ has Sylow p-subgroups.

We first assume that p divides $|Z(G)|$. By Cauchy's Theorem 3.64 for abelian groups, the abelian group $Z(G)$ has a subgroup N that has order p. Since N is contained in $Z(G)$ it is also normal in G. Then $\overline{G} := G/N$ has order $p^{\alpha-1}m < p^\alpha m$. By the inductive hypothesis, $\overline{G}$ has a subgroup L of order $p^{\alpha-1}$.

By the Fourth Isomorphism Theorem 3.60, there is a subgroup P of G that contains N and has the property that $P/N = L$. But then $|P| = |P/N| \cdot |N| = p^{\alpha-1} \cdot p = p^\alpha$. Thus P is a Sylow p-subgroup of G.

We now assume that p does not divide $|Z(G)|$. If $\alpha = 0$ then the result is trivial, so we assume $\alpha \geq 1$. Let $g_1, \ldots, g_r$ be a set of representatives of the distinct conjugacy classes of $G \setminus Z(G)$. By the Class Equation (25), if p divides each $[G : C_G(g_i)]$ for each i then p would divide $|Z(G)|$. Hence for some j we have that p does not divide $[G : C_G(g_j)]$. We fix such a j.

Since p does not divide $[G : C_G(g_j)]$ and

$$p^\alpha m = |C_G(g_j)|[G : C_G(g_j)]$$

we must have $|C_G(g_j)| = p^\alpha k$ for some k (with $p \nmid k$). Since $g_j \notin Z(G)$ we know that $C_G(g_j)$ must be a proper subgroup of G, so also $|C_G(g_j)| < |G|$. By the inductive hypothesis $C_G(g_j)$ has a subgroup P of order p^α, which is of course also a subgroup of G. This completes the proof of claim (i).

In order to prove claims (ii) and (iii) we first use claim (i) to fix a Sylow p-subgroup P of G. We write

$$\mathcal{S}(P) := \{gPg^{-1} : g \in G\}$$

for the set of conjugates of P. By Exercise 3.18, each element P' of $\mathcal{S}(P)$ is a Sylow p-subgroup of G. By definition G acts on $\mathcal{S}(P)$ by conjugation. Of course, any subgroup of G also acts on $\mathcal{S}(P)$ by conjugation.

Let Q be any subgroup of G. By Proposition 4.45 the orbits $\mathcal{O}^Q_{P'}$, as P' ranges through $\mathcal{S}(P)$, of the action of Q on $\mathcal{S}(P)$ form a partition of $\mathcal{S}(P)$. We may thus fix such orbits $\mathcal{O}^Q_{P_1}, \ldots, \mathcal{O}^Q_{P_{s_Q}}$ with the property that $\mathcal{S}(P)$ is the disjoint union

$$\mathcal{S}(P) = \mathcal{O}^Q_{P_1} \cup \ldots \cup \mathcal{O}^Q_{P_{s_Q}},$$

so that

$$|\mathcal{S}(P)| = \sum_{i=1}^{i=s_Q} |\mathcal{O}^Q_{P_i}|. \tag{28}$$

We always choose and order such orbits so that $P_1 = P$.

We claim that for any p-subgroup Q of G, any choice $P_1, \ldots, P_{s_Q}$ as above and any $1 \leq i \leq s_Q$ one has

$$|\mathcal{O}^Q_{P_i}| = [Q : (P_i \cap Q)]. \tag{29}$$

Indeed, by Proposition 4.45 we have $|\mathcal{O}^Q_{P_i}| = [Q : Q_{P_i}]$ where Q_{P_i} is the stabiliser of P_i in Q, which is equal to $Q \cap N_G(P_i)$ and, by Lemma 4.82, $Q \cap N_G(P_i) = Q \cap P_i$. These facts together combine to prove (29).

We next claim that

$$|\mathcal{S}(P)| \equiv 1 \pmod p. \tag{30}$$

We prove this fact by applying (28) and (29) to the p-subgroup $Q = P$ of G. For $P_1 = P$ we get $|\mathcal{O}^P_P| = 1$. For all $2 \leq i \leq s_P$ we have $P_i \neq P$ so $P_i \cap P$ is stricly contained in P. From (29) we get that

$$|\mathcal{O}^P_{P_i}| = [P : (P_i \cap P)]$$

is greater than 1. It is also a power of p, since P is a p-group. Therefore p divides $|\mathcal{O}^P_{P_i}|$ for every $2 \leq i \leq s_P$ and (28) implies that

$$|\mathcal{S}(P)| \equiv 1 + \sum_{i=2}^{i=s_P} 0 = 1 \pmod p,$$

as required to prove (30).

We finally proceed to prove claims (ii) and (iii) of Theorem 4.80. Let Q be any p-subgroup of G. We prove that Q must be contained in some conjugate of P by applying (28) and (29) to the p-subgroup Q. We argue by contradiction.

Suppose that Q is not contained in any conjugate of P. Then $P_i \cap Q$ would be strictly contained in Q for every $1 \leq i \leq s_Q$. From (29) we would get that

$$|\mathcal{O}^Q_{P_i}| = [Q : (P_i \cap Q)]$$

is greater than 1. It is also a power of p, since Q is a p-group. Therefore p would divide $|\mathcal{O}^Q_{P_i}|$ for every $1 \leq i \leq s_Q$, and (28) would then imply that $|\mathcal{S}(P)|$ is divisible by p, contradicting (30). We have proved that Q must be contained in some conjugate of P.

The final statement in claim (ii) now follows immediately, since any conjugate of P also has order p^α by Exercise 3.18.

To prove claim (iii) we first note that claim (ii) implies that $\mathrm{Syl}_p(G) = \mathcal{S}(P)$. In particular

$$n_p(G) = |\mathcal{S}(P)| \equiv 1 \pmod p$$

by (30), as required.

We finally note that

$$n_p(G) = |\mathcal{S}(P)| = |\mathcal{O}^G_P| = [G : G_P] = [G : N_G(P)],$$

where the third equality is by Proposition 4.45, with G_P the stabiliser of P under the conjugation action of G, which is just $N_G(P)$. □

Remark 4.83. Note that Theorem 4.80 combines with Exercise 3.18 to imply that, for a given prime p and finite group G, any two Sylow p-subgroups of G are isomorphic.

Corollary 4.84. *Let G be a finite group and let p be a prime. Let P be a sylow p-subgroup of G. Then the following conditions are equivalent.*

(i) *P is the unique Sylow p-subgroup of G (so $n_p(G) = 1$).*
(ii) *P is normal in G.*
(iii) *For any set S of elements of G of p-power order, the subgroup $\langle S\rangle$ of G is a p-subgroup.*

Proof. Condition (i) is equivalent to condition (ii) because a subgroup P is normal in G if and only if it is equal to all of its conjugates (so the required equivalency then follows from Sylow's Theorem 4.80).

We now show that conditions (i) and (ii) imply condition (iii). Assume that P is the unique Sylow p-subgroup of G (and is normal) and fix a set S as in condition (iii). For each $x \in S$ the cyclic subgroup $\langle x\rangle$ of G is a p-subgroup and thus Sylow's Theorem 4.80 (ii) (with $Q = \langle x\rangle$) implies that there is $g \in G$ for which x belongs to gPg^{-1}. But we know that $gPg^{-1} = P$. This argument proves that $S \subseteq P$ which implies that $\langle S\rangle \subseteq P$, which implies that $\langle S\rangle$ is a p-subgroup of G.

Conversely, assume that condition (iii) holds. We will prove that condition (i) must also hold. Let S be the union of all Sylow p-subgroups of G. If there were any other Sylow p-subgroup of G other than P, then S would not be contained in P: indeed, all Sylow p-subgroups have the same order so they cannot be included in each other, and there would be some element of S not in P. It is thus enough to show that $S \subseteq P$.

But P is a subgroup of $\langle S\rangle$, where $\langle S\rangle$ is a p-subgroup of G by condition (iii), and P has maximal order. We therefore get $P = \langle S\rangle$ or equivalently, $S \subseteq P$, as required. □

Examples 4.85. (i) If p does not divide the order of G, then the (unique) Sylow p-subgroup of G is the trivial subgroup and Sylow's Theorem becomes trivial for G and p.
(ii) If G is a p-group then the (unique) Sylow p-subgroup of G is G and Sylow's Theorem is also trivial for G and p.
(iii) The group S_3 has three Sylow 2-subgroups:

$$\{1,(1,2)\}, \quad \{1,(1,3)\}, \quad \{1,(2,3)\}.$$

Note that $3 \equiv 1 \pmod 2$. However the group S_3 has a unique Sylow 3-subgroup $A_3 = \{1,(1,2,3),(1,3,2)\}$, which of course is normal in S_3.
(iv) The group A_4 has a unique Sylow 2-subgroup

$$\{1,(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}.$$

It has, however, four Sylow 3-subgroups

$$\{1,(1,2,3),(1,3,2)\}, \ \{1,(1,2,4),(1,4,2)\}, \ \{1,(1,3,4),(1,4,3)\}, \ \{1,(2,3,4),(2,4,3)\}.$$

Note that $4 \equiv 1 \pmod 3$.
(v) The group S_4 has $n_2(S_4) = 3$ and $n_3(S_4) = 4$.

Exercise 4.86. Find all Sylow 2-subgroups and all Sylow 3-subgroups of S_4.

Exercise 4.87. Let A be a finite abelian group. For each prime p set

$$A_p := \{a \in A : \mathrm{o}(a) = p^k, k \geq 0\}.$$

Prove that A_p is a subgroup of A and moreover, prove that A_p is the unique Sylow p-subgroup of A.

4.3.2. *Some applications of Sylow's Theorem.* We already discussed Cauchy's Theorem in Remarks 2.70(ii) and we then proved it for abelian groups in Theorem 3.64. Sylow's Theorem now puts us in a position to prove the general case:

Theorem 4.88. *Let G be a finite group and let p be a prime number dividing $|G|$. Then G has an element of order p.*

Exercise 4.89. Use Sylow's Theorem 4.80 and Cauchy's Theorem for abelian groups 3.64 to prove Cauchy's Theorem 4.88.

Remark 4.90. Note that we never used the general version of Cauchy's Theorem when proving Sylow's Theorem, but only the version for abelian groups, so our line of reasoning is not circular.

Example 4.91. Let G be a group of order pq, for distinct prime numbers p and q. Without loss of generality we assume that $p < q$. We fix P in $\mathrm{Syl}_p(G)$ and Q in $\mathrm{Syl}_q(G)$. We will prove the following claims:

(i) Q is normal in G.
(ii) If $p \nmid q-1$ then P is normal in G.
(iii) If P is normal in G then G is cyclic.

Claim (i) holds because $n_q = 1 + kq$ for some $k \geq 0$ by Theorem 4.80(iii) while also n_q divides p by Remark 4.81. Since $p < q$ we must have $n_q = 1$, so Q is normal in G by Corollary 4.84.

Similarly n_p divides q by Remark 4.81, so we always have $n_p \in \{1, q\}$, with P normal in G if and only if $n_p = 1$ (see Corollary 4.84). Since $n_p = 1 + pl$ for some $l \geq 0$, in the setting of claim (ii) we cannot have $n_p = q$. This proves claim (ii).

We now prove claim (iii). Assume that P is normal in G, so $N_G(P) = G$. Both P and Q are cyclic groups (as they have prime order). Let $P = \langle x \rangle$ and $Q = \langle y \rangle$.

We write $\mathrm{Aut}(P)$ for the set of automorphisms of P, meaning isomorphisms with P as both the domain and the codomain. Then $\mathrm{Aut}(P)$ is a group under composition (see Exercise 1.107).

We have a well-defined conjugation action of $N_G(P)$ on P: given $x \in N_G(P)$ and $\pi \in P$, the element $x \cdot \pi := x\pi x^{-1}$ of G in fact belongs to P, and it is easy to see that this action satisfies the axioms (A1) and (A2). Now the permutation representation associated to this action is not only a homomorphism $N_G(P) \to S_P$ but in fact, recalling that $\mathrm{Aut}(P)$ is a subgroup of S_P, is a well-defined homomorphism

$$\rho : N_G(P) \to \mathrm{Aut}(P).$$

This is because $\rho_x : P \to P$ satisfies

$$\rho_x(\pi_1\pi_2) = x\pi_1\pi_2x^{-1} = x\pi_1x^{-1}x\pi_2x^{-1} = \rho_x(\pi_1)\rho_x(\pi_2)$$

and is thus a homomorphism for each $x \in N_G(P)$. We clearly have $\ker(\rho) = C_G(P)$.

Recall (from [2, Prop. 16, §4.4, p. 135] or from Exercise 2.101) that $\mathrm{Aut}(P)$ is a group of order $p-1$. But the First Isomorphism Theorem then implies that

$$G/C_G(P) = N_G(P)/C_G(P) = N_G(P)/\ker(\rho) \cong \mathrm{im}(\rho) \leq \mathrm{Aut}(P).$$

Since neither p nor q can divide $p-1$, we must have $\operatorname{im}(\rho) = 1$ and therefore also $G = C_G(P)$.

Therefore y belongs to $C_G(P)$ and hence x commutes with y. This implies that the element xy has order pq. The subgroup $\langle xy \rangle$ of G then has order $pq = |G|$ so it is equal to G, meaning that G is cyclic, as required.

Exercise 4.92.
(i) Find a Sylow 7-subgroup Q of S_7.
(ii) Find a subgroup P of $N_{S_7}(Q)$ of order 3.
(iii) Prove that PQ is a non-abelian group of order 21.

Remark 4.93. Let G be a group of order 30. If G has a subgroup of order 15 then it is necessarily both normal (by Lemma 3.31) and cyclic, by Example 4.91.

In fact, one can apply Sylow's Theorem to also prove that G does necessarily have a subgroup of order 15. See [2, p. 143,144] for this argument.

Example 4.94. Let G be a group of order 12. We will show that either G has a normal Sylow 3-subgroup or $G \cong A_4$.

Suppose $n_3 \neq 1$ and fix a Sylow 3-subgroup P of G. Since $n_3 \mid 4$ and $n_3 \equiv 1 \pmod 3$, we must have $n_3 = 4$. Since distinct Sylow 3-subgroups intersect in the identity and each contains two elements of order 3, G must contain 8 elements of order 3. Since $[G : N_G(P)] = n_3 = 4$ we must have $N_G(P) = P$.

Now G acts by conjugation on its set of Sylow 3-subgroups, so this action affords a permutation representation
$$\rho : G \to S_4.$$
The kernel K of this action is the subgroup of G which normalises all Sylow 3-subgroups of G. In particular $K \subseteq N_G(P) = P$. Since P is not normal in G by assumption we must have $K = 1$, so
$$G \cong \operatorname{im}(\rho) \subseteq S_4.$$
Since G contains 8 elements of order 3 and there are precisely 8 elements of order 3 in S_4, all of them contained in A_4, the order of $\operatorname{im}(\rho) \cap A_4$ is at least 8. Since both $\operatorname{im}(\rho)$ and A_4 have order 12 it follows that $\operatorname{im}(\rho) = A_4$, and thus $G \cong A_4$.

Example 4.95. Let G be a group of order p^2q, for distinct primes p and q. We show that G has either a normal Sylow p-subgroup or a normal Sylow q-subgroup. Fix P in $\operatorname{Syl}_p(G)$ and Q in $\operatorname{Syl}_q(G)$.

Assume first that $p > q$. Since $n_p \mid q$ and $n_p \equiv 1 \pmod p$ we must have $n_p = 1$, so P is normal in G.

Assume now that $p < q$. If $n_q = 1$ then Q is normal in G. Otherwise $n_q = 1 + tq$ for some $t \in \mathbb{N}$. Now n_q divides p^2 but $n_q > q > p$, so necessarily $n_q = p^2$. Thus
$$tq = p^2 - 1 = (p-1)(p+1).$$
Since q is prime it divides either $p-1$ or $p+1$. Since $q > p$ the former is impossible and the latter forces $q = p+1$, which can only happen for $p = 2$ and $q = 3$ and $|G| = 12$.

Since A_4 has a normal Sylow 2-subgroup, the required conclusion now follows from Example 4.94.

We saw in Theorem 4.76 that A_5 is a simple group. We may now show that:

Proposition 4.96. *If G is a simple group of order* 60 *then it is isomorphic to* A_5.

Proof. The number n_2 must divide 15, so $n_2 \in \{3, 5, 15\}$. Fix a Sylow 2-subgroup of G and sey $N := N_G(P)$, so that $[G : N] = n_2$. Note for later use that n_5 must be equal to 6.

We first claim that G has no proper subgroup of index less than 5. If H had index $2, 3$ or 4, then by Exercise 4.55, G would have a normal subgroup K contained in H for which G/K is isomorphic to a subgroup of S_2, S_3 or S_4. Since $K \neq G$, simplicity would force $K = \{1\}$. This is impossible since 60 does not divide 4!.

The above claim implies in particular that $n_2 = [G : N] \neq 3$. We now assume that $n_2 = [G : N] = 5$. In this case, again by Exercise 4.55, the action of G by left multiplication on the set of left cosets of N in G gives a permutation representation of $\rho : G \to S_5$. Since the kernel of this action is a proper normal subgroup of G and G is simple, the representation must be injective so $G \cong \mathrm{im}(\rho) \leq S_5$.

We aim to show that $\mathrm{im}(\rho)$ must be A_5, thus giving an isomorphism $G \cong A_5$. The subset $\mathrm{im}(\rho)A_5$ is a subgroup of S_5 because A_5 is normal in S_5. If $\mathrm{im}(\rho)$ were not contained in A_5, then the only option would be $\mathrm{im}(\rho)A_5 = S_5$ and, by the Second Isomorphism Theorem 3.56, $\mathrm{im}(\rho) \cap A_5$ is of index 2 in $\mathrm{im}(\rho)$. Since G, and therefore $\mathrm{im}(\rho)$, has no normal subgroup of index 2, this is a contradiction.

Therefore we must have had $\mathrm{im}(\rho) \subseteq A_5$ and, by cardinality, also $\mathrm{im}(\rho) = A_5$, showing that $G \cong A_5$ if $n_2 = 5$.

We must finally show that one cannot have $n_2 = 15$. We argue by contradiction. Assume $n_2 = 15$. If for every pair of Sylow 2-subgroups P and Q one had $P \cap Q = \{1\}$ then the number of non-identity elements in Sylow 2-subgroups of G would be $(4-1) \cdot 15 = 45$. Since we know $n_5 = 6$, the number of elements of order 5 in G must be $(5-1) \cdot 6 = 24$, accounting for $45 + 24 = 69$ elements of G, a clear contradiction.

Thus there must be distinct Sylow 2-subgroups P and Q with $|P \cap Q| = 2$. Set $M := N_G(P \cap Q)$. Since P and Q are abelian (being groups of order 4), P and Q are subgroups of M and since G is simple, $M \neq G$. Thus 4 divides $|M|$ and $|M| > 4$ (otherwise $P = M = Q$). The only possibility is $|M| = 12$, so M has index 5 in G (recall that M cannot have index 1 or 3 in G). But now the argument of the preceding paragraph applied to M in place of N gives $G \cong A_5$. This leads to a contradiction in this case because $n_2(A_5) = 5$. □

Remark 4.97. One may also show that any group of order 60 that has more than one Sylow 5-subgroup is necessarily simple, hence isomorphic to A_5.

Remark 4.98. You may now try to prove that if G is a non-abelian simple group with $|G| < 100$ then $G \cong A_5$, by eliminating all orders other than 60 as possibilities.

4.4. **(More) Exercises.** Don't forget to think about the exercises given throughout the rest of section 4.

Exercise 4.99. Recall from Exercise 1.107 that any group G has associated a group of automorphisms $\mathrm{Aut}(G)$. Prove that $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$ (or see [2, Prop. 4.16, p. 135] for a proof, or use the strategy of Exercise 2.101).

Exercise 4.100. Write each of the permutations considered in Exercises 1.86 and 1.87 as a product of transpositions, and determine their signs.

Exercise 4.101. Prove that the square of every permutation is even.

Exercise 4.102. Prove that $S_n = \langle U \rangle$ for $U := \{(i, i+1) : 1 \leq i \leq n-1\}$.

Exercise 4.103. Prove that $S_n = \langle (1, 2), (1, 2, 3, \ldots, n) \rangle$.

Exercise 4.104. Let p be a prime. Let $\sigma \in S_p$ be a transposition and let $\tau \in S_p$ be a p-cycle. Prove that $S_p = \langle \sigma, \tau \rangle$.

Exercise 4.105. Show that $\langle (1, 3), (1, 2, 3, 4) \rangle$ is a proper subgroup of S_4.

Exercise 4.106.
(i) Find all subgroups of A_4 that have order 2.
(ii) Find all subgroups of A_4 that have order 4. Determine which of them are normal in A_4 and what their isomorphism class is.
(iii) Prove that A_4 is solvable.

Exercise 4.107. Find all elements of order 4 in S_4. Prove that S_4 contains no subgroup that is isomorphic to Q_8.

Exercise 4.108. Prove that the function $f : S_{n-2} \to A_n$ given by $f(\sigma) = \sigma$ if σ is even, and by $f(\sigma) = \sigma \circ (n+1, n+2)$ if σ is odd, is an injective homomorphism. Find generators of $\mathrm{im}(f)$.

Exercise 4.109. Prove that every element of order 2 in A_n is the square of an element of order 4 of S_n.

Exercise 4.110. Let $\sigma \in A_4$ have order 2 and let $\tau \in A_4$ have order 3. Prove that $\langle \sigma, \tau \rangle = A_4$.

Exercise 4.111. Let σ and τ be 3-cycles in S_4 with $\sigma \neq \tau$ and $\sigma \neq \tau^{-1}$. Prove that $\langle \sigma, \tau \rangle = A_4$.

Exercise 4.112.
(i) Find 3-cycles σ and τ in S_5 with $\sigma \neq \tau$, $\sigma \neq \tau^{-1}$ and $\langle \sigma, \tau \rangle \cong A_4$.
(ii) Find 3-cycles σ and τ in S_5 with $\sigma \neq \tau$, $\sigma \neq \tau^{-1}$ and $\langle \sigma, \tau \rangle = A_5$.

Exercise 4.113. Let G act on A. Prove that if $a, b \in A$ with $a = gb$ for some $g \in G$ then $G_b = gG_ag^{-1}$. Deduce that if G acts transitively on A then the kernel of the action is $\bigcap_{g \in G} gG_ag^{-1}$, for any given $a \in A$.

Exercise 4.114. Let A be a non-empty set and let G be a subgroup of S_A, acting on A via evaluation. Fix $\sigma \in G$ and $a \in A$. Prove that $\sigma G_a \sigma^{-1} = G_{\sigma(a)}$. Deduce that if the action of G on A is transitive then

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \{1\}.$$

Exercise 4.115. Let A be a set and let G be an abelian subgroup of S_A that acts transitively on A via evaluation. Show that $\sigma(a) \neq a$ for every $\sigma \in G \setminus \{1\}$ and every $a \in A$. Deduce that the order of G must be equal to the cardinality of A.

Exercise 4.116. Let S_3 act on $\{1, 2, 3\} \times \{1, 2, 3\}$ via

$$\sigma((i, j)) := (\sigma(i), \sigma(j)).$$

Find all the orbits and all the stabilisers associated to this action.

Exercise 4.117. Fix a different bijection between $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\{1, 2, 3, 4\}$ than the one used on Example 4.51. Show that, although the homomorphism $G \to S_4$ that you obtain from the (left) regular representation is different from the one described there, its image in S_4 is the same subgroup.

Exercise 4.118. Use the (left) regular representation of Q_8 to find two elements of x and y of S_8 with the property that the subgroup $\langle x, y\rangle$ of S_8 is isomorphic to Q_8.

Exercise 4.119. (i) Show that if Q_8 acts on a set A of cardinality less than or equal to 7 then the stabiliser of each element of A is non-trivial.
(ii) Show that if Q_8 acts on a set A of cardinality less than or equal to 7 then the kernel of the action must contain the subgroup $\langle -1\rangle$ of Q_8.
(iii) Show that Q_8 cannot be isomorphic to a subgroup of S_n for any $n \leq 7$.

Exercise 4.120. Let G be a finite group and let $\rho : G \to S_{|G|}$ be the (left) regular representation of G. Fix an element x of G and set $n := \mathrm{o}(x)$ and $m := |G|/n$. Prove that $\rho(x)$ is a product of m n-cycles. Deduce that $\rho(x)$ is an odd permutation if and only if $\mathrm{o}(x)$ is even and $|G|/\mathrm{o}(x)$ is odd.

Exercise 4.121. Let G be a finite group and let $\rho : G \to S_{|G|}$ be the (left) regular representation of G. Use Exercise 3.115 to prove that if $\mathrm{im}(\rho)$ contains an odd permutation then G has a subgroup of index 2.

Exercise 4.122. Use Cauchy's Theorem (for general finite groups) and the previous two exercises to show that if G is a finite group for which 2 divides $|G|$ but 4 does not divide $|G|$, then G has a subgroup of index 2.

Exercise 4.123. Let G be a finite group. Assume that $|G|$ is not prime and that, for every natural number k dividing $|G|$, G has a subgroup of order k. Prove that G is not simple.

Exercise 4.124. Find all conjugacy classes, and their cardinalities, in each of the groups

$$D_8,\ D_{10},\ Q_8,\ A_4,\ \mathbb{Z}/2\mathbb{Z} \times S_3,\ S_3 \times S_3,\ \mathbb{Z}/3\mathbb{Z} \times A_4.$$

Exercise 4.125. Show that for any element g and subset S of a group G one has $gN_G(S)g^{-1} = N_G(gSg^{-1})$ and $gC_G(S)g^{-1} = C_G(gSg^{-1})$.

Exercise 4.126. Prove that every conjugacy class in a group G has cardinality less than or equal to $[G : Z(G)]$.

Exercise 4.127. Let G be a non-abelian group of order 15. Use Exercise 3.102 to prove that $Z(G) = 1$. Prove also that the Class Equation of G must be $15 = 1 + 3 + 3 + 3 + 5$.

Exercise 4.128. For $n = 3, 4, 6, 7$, make lists of all the partitions of n and give representatives of the corresponding conjugacy classes of S_n.

Exercise 4.129. Prove that $Z(S_n) = 1$ for all $n \geq 3$.

Exercise 4.130. Set $\sigma := (1, 2, 3, 4, 5) \in S_5$. In each of the following, find an element τ of S_5 which stisfies the given equality.
(i) $\tau\sigma\tau^{-1} = \sigma^2$.
(ii) $\tau\sigma\tau^{-1} = \sigma^{-1}$.

(iii) $\tau\sigma\tau^{-1} = \sigma^{-2}$.

Exercise 4.131. In each of the following, determine whether σ and σ' are conjugate or not. If they are, find an element τ for which $\sigma' = \tau\sigma\tau^{-1}$.

(i) $\sigma = (1,2)(3,4,5)$ and $\sigma' = (1,2,3)(4,5)$ in S_5.
(ii) $\sigma = (1,5)(2,3,7)(6,8,11,10)$ and $\sigma' = (2,13,11)(3,7,5,10)(4,9)$ in S_{13}.
(iii) $\sigma = (1,5)(2,3,7)(6,8,11,10)$ and $\sigma' = \sigma^3$ in S_{13}.
(iv) $\sigma = (1,3)(2,4,6)$ and $\sigma' = (2,4)(3,5,6)$ in S_6.

Exercise 4.132. Find a representative of each conjugacy class of elements of order 4 in S_8, and also in S_{12}.

Exercise 4.133. Find all finite groups which have exactly two conjugacy classes.

Exercise 4.134. Let p be a prime and let G be a group of order p^n for some natural number n. Prove (by induction on n) that G has a subgroup of order p^m for every $0 \leq m \leq n$.

Exercise 4.135. Let G be a group of odd order. Let $g \neq 1$ be an element of G. Prove that g and g^{-1} are not conjugate in G.

Exercise 4.136. Let σ be an element of S_n. Let $m_1, m_2, \ldots, m_s$ be the *distinct* integers which occur in the cycle type of σ. For each $i = 1, \ldots, s$, assume that σ has q_i cycles of length m_i. Prove that the number of conjugates of σ is

$$\frac{n!}{(q_1! m_1^{q_1})(q_2! m_2^{q_2}) \ldots (q_s! m_s^{q_s})}.$$

Exercise 4.137. Let p be a prime. Let P be a subgroup of S_p that has order p. Show that every subgroup of S_p conjugate to P contains exactly $p-1$ p-cycles. Deduce that $|N_{S_p}(P)| = p(p-1)$.

Exercise 4.138. Let p be a prime. Find a formula for the number of conjugacy classes of elements of order p in S_n.

In the remaining exercises we let G denote a finite group and we let p denote a prime number.

Exercise 4.139. Fix $P \in \mathrm{Syl}_p(G)$ and let H be a subgroup of G containing P. Show that P belongs to $\mathrm{Syl}_p(H)$. Give an example of group G, subgroup H and element Q of $\mathrm{Syl}_p(H)$ that is not in $\mathrm{Syl}_p(G)$.

Exercise 4.140. For $H \leq G$ and $Q \in \mathrm{Syl}_p(H)$, show that gQg^{-1} belongs to $\mathrm{Syl}_p(gHg^{-1})$ for any $g \in G$.

Exercise 4.141. Find all Sylow 2-subgroups and all Sylow 3-subgroups of D_{12} and of $S_3 \times S_3$.

Exercise 4.142. Show that if p is odd then every Sylow p-subgroup of D_{2n} is both normal in D_{2n} and cyclic.

Exercise 4.143. Find the Sylow 3-subgroups of A_4 and of S_4.

Exercise 4.144. Prove that if n is odd then $n_2(D_{2n}) = n$.

Exercise 4.145. Prove that a group of order 56 must have a normal Sylow p-subgroup for some prime $p \mid 56$.

Exercise 4.146. Prove that a group of order 312 must have a normal Sylow p-subgroup for some prime $p \mid 312$.

Exercise 4.147. Prove that a group of order 351 must have a normal Sylow p-subgroup for some prime $p \mid 351$.

Exercise 4.148. Show that if $|G|$ is the product of three distinct primes, then it has a normal Sylow subgroup for one of the three primes.

Exercise 4.149. Prove that a group of order 200 must have a normal Sylow 5-subgroup.

Exercise 4.150. Prove that there is no simple group of order 6545.

Exercise 4.151. Prove that there is no simple group of order 1365.

Exercise 4.152. Prove that there is no simple group of order 2907.

Exercise 4.153. Prove that there is no simple group of order 132.

Exercise 4.154. Prove that there is no simple group of order 462.

Exercise 4.155. Let P be a normal Sylow p-subgroup of G and let $H \leq G$. Show that $P \cap H$ is a normal Sylow p-subgroup of H.

Exercise 4.156. Let P be a Sylow p-subgroup of G and let N be a normal subgroup of G. Show that $P \cap N$ is a Sylow p-subgroup of N and that PN/N is a Sylow p-subgroup of G/N.

Exercise 4.157. Let P be a Sylow p-subgroup of G and let $H \leq G$. Prove that $gPg^{-1} \cap H$ is a Sylow p-subgroup of H for some $g \in G$. Give an explicit example in which $hPh^{-1} \cap H$ is not a Sylow p-subgroup for any $h \in H$.

Exercise 4.158. Prove that if N is a normal subgroup of G then $n_p(G/N) \leq n_p(G)$.

Exercise 4.159. Let R be a normal p-subgroup of G (not necessarily of maximal order).

(i) Prove that R is contained in every Sylow p-subgroup of G.

(ii) If S is also a normal p-subgroup of G, prove that RS is also a normal p-subgroup of G.

(iii) Set

$$O_p(G) := \langle \bigcup_Q Q \rangle$$

where Q runs over all normal p-subgroups of G. Prove that $O_p(G)$ is the unique largest normal p-subgroup of G and also that

$$O_p(G) = \bigcap_P P$$

where P runs over all Sylow p-subgroups of G.

(iv) Set $\overline{G} := G/O_p(G)$. Prove that $O_p(\overline{G}) = \{O_p(G)\}$, that is, $\overline{G}$ has no non-trivial normal p-subgroup.

Exercise 4.160. Use the same method we used in the proof of Sylow's Theorem to show that, if n_p is not congruent to 1 modulo p^2, then there are distinct Sylow p-subgroups P and Q of G for which $[P : P \cap Q] = [Q : P \cap Q] = p$.

Exercise 4.161. Assume that p is odd. Find generators for a Sylow p-subgroup of S_{2p}. Show that this is an abelian group of order p^2.

Exercise 4.162. Assume that p is odd. Find generators for a Sylow p-subgroup of S_{p^2}. Show that this is a non-abelian group of order p^{p+1}.

5. Classification and products

5.1. **Products.**

5.1.1. *Direct products.* In §1.1.5 we already defined the direct product of two groups and discussed its basic properties.

Definition 5.1. For any finite collection of groups $G_1, \dots, G_n$ we define their direct product to be the group

$$\prod_{i=1}^{i=n} G_i = G_1 \times \ldots \times G_n,$$

defined through the binary operation

$$(g_1, \dots, g_n)(g_1', \dots, g_n') = (g_1 g_1', \dots, g_n g_n').$$

Exercise 5.2. Prove that $\prod_{i=1}^{i=n} G_i$ is a group, and determine its identity element and the inverse of each of its elements. Prove that it is abelian of and only if each group G_i is abelian. Prove that

$$|\prod_{i=1}^{i=n} G_i| = \prod_{i=1}^{i=n} |G_i|,$$

and in particular that $\prod_{i=1}^{i=n} G_i$ is finite if and only if each group G_i is finite.

Exercise 5.3. Let $G_1, \dots, G_n$ be groups and let σ be an element of S_n. Prove that the function

$$f_\sigma : \prod_{i=1}^{i=n} G_i \to \prod_{i=1}^{i=n} G_{\sigma(i)}$$

given by

$$f_\sigma((g_1, \dots, g_n)) := (g_{\sigma(1)}, \dots, g_{\sigma(n)})$$

is an isomorphism.

Exercise 5.4. Let $G_1, \dots, G_n$ be groups. Prove that

$$G_1 \times (\prod_{i=2}^{i=n} G_i) \cong \prod_{i=1}^{i=n} G_i \cong (\prod_{i=1}^{i=n-1} G_i) \times G_n.$$

Come up with additional similar relations in the case $n = 4$.

Lemma 5.5. *Let $G_1, \dots, G_n$ be groups. Fix j with $1 \leq j \leq n$.*

(i) *The subgroup*

$$\{(1, 1, \dots, 1, g_j, 1, \dots, 1) : g_j \in G_j\} \tag{31}$$

is normal in $\prod_{i=1}^{i=n} G_i$, and is also canonically isomorphic to G_j. By abuse of notation we denote the subgroup (31) by G_j.

(ii) *In the notation of claim (i) we have a canonical isomorphism*

$$(\prod_{i=1}^{i=n} G_i)/G_j \cong \prod_{i\neq j} G_i$$

(with i running over the integers from 1 *to n that are different from j).*

(iii) *The surjective homomorphism*

$$\pi_j : \prod_{i=1}^{i=n} G_i \to G_j$$

defined by

$$\pi_j((g_1, \dots, g_n)) := g_j$$

has

$$\ker(\pi_j) \cong \prod_{i\neq j} G_i.$$

(iv) *In the notation of claim (i), if x belongs to the subgroup G_j of $\prod_{i=1}^{i=n} G_i$ and y belongs to the subgroup G_k of $\prod_{i=1}^{i=n} G_i$ for some $k \neq j$, then $xy = yx$.*

Proof. It is very easy to see that the subset (31) is a subgroup of $\prod_{i=1}^{i=n} G_i$. The map

$$g_i \mapsto (1, 1, \dots, 1, g_j, 1, \dots, 1)$$

is also easily seen to give an isomorphism between G_i and the subgroup (31).

To prove both claims (i) and (ii) it is enough, by the First Isomorphism Theorem 3.44, to show that there is a surjective homomorphism

$$\mu_j : \prod_{i=1}^{i=n} G_i \to \prod_{i\neq j} G_i$$

with $\ker(\mu_j)$ equal to the subgroup G_i of $\prod_{i=1}^{i=n} G_i$.

To do this we set

$$\mu_j((g_1, \dots, g_n)) := (g_1, \dots, g_{j-1}, g_{j+1}, \dots, g_n).$$

This map is a homomorphism since

$$\begin{aligned}\mu_j((g_1, \dots, g_n)(g_1', \dots, g_n')) =& \mu_j((g_1g_1', \dots, g_ng_n'))\\ =&(g_1g_1', \dots, g_{j-1}g_{j-1}', g_{j+1}g_{j+1}', \dots, g_ng_n')\\ =&(g_1, \dots, g_{j-1}, g_{j+1}, \dots, g_n)(g_1', \dots, g_{j-1}', g_{j+1}', \dots, g_n')\\ =&\mu_j((g_1, \dots, g_n))\mu_j((g_1', \dots, g_n')).\end{aligned}$$

It is clear that the function μ_j is surjective, and also that $\ker(\mu_j)$ is the subgroup (31) (which we have identified with G_i), as required.

The proof of claim (iii) is given by an argument almost identical to the one given above, and we leave it to the reader.

We finally prove claim (iv). Let

$$x = (1, \dots, 1, g_j, 1, \dots, 1) \in G_j$$

and let

$$y = (1, \dots, 1, g_k, 1, \dots, 1) \in G_k.$$

Then

$$xy = (1, \dots, 1, g_j, 1, \dots, 1, g_k, 1, \dots, 1) = yx,$$

provided that $j < k$, or

$$xy = (1, \dots, 1, g_k, 1, \dots, 1, g_j, 1, \dots, 1) = yx,$$

provided that $k < j$. In either case, we get that x and y commute, as required. □

Notation 5.6. Given groups $G_1, \dots, G_n$, an index j with $1 \leq j \leq n$ and an element g_j of G_j, we often denote the element

$$(1, \dots, 1, g_j, 1, \dots, 1)$$

of $\prod_{i=1}^{i=n} G_i$ simply by g_j.

Remark 5.7. For each $1 \leq i \leq n$ fix an element g_i of G_i. Then, using the notation introduced in 5.6, Lemma 5.5 (iv) implies that

$$(g_1 \cdot g_2 \cdot \dots \cdot g_n)^k = g_1^k \cdot g_2^k \cdot \dots \cdot g_n^k \tag{32}$$

in $\prod_{i=1}^{i=n} G_i$, for any $k \in \mathbb{Z}$.

In particular

$$\mathrm{o}(g_1 \cdot g_2 \cdot \dots \cdot g_n) = \mathrm{lcm}(\mathrm{o}(g_1), \mathrm{o}(g_2), \dots, \mathrm{o}(g_n)),$$

where this order is infinite if and only if one the elements g_i has infinite order.

Example 5.8. Let p be a prime and n be a natural number. Then

$$E_{p^n} := \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \dots \mathbb{Z}/p\mathbb{Z}$$

(with n factors in the right-hand side) is an abelian group of order p^n, that moreover has isomorphism class $C_p \times \dots C_p$. This group is called the 'elementary abelian group of order p^n'.

We compute the number of subgroups of E_{p^2}. Since each non-trivial element of E_{p^2} has order p, each of these generates a cyclic subgroup of order p. By Lagrange's Theorem, the intersection of distinct subgroups of order p must be trivial. Thus the $p^2 - 1$ non-identity elements of E_{p^2} are partitioned into subsets of size $p - 1$ (each of these subsets comprises the non-identity elements of some subgroup of order p). Therefore there must be

$$\frac{p^2 - 1}{p - 1} = p + 1$$

subgroups of order p. There are hence $p + 3$ subgroups of E_{p^2}.

Definition 5.9. We extend Definition 3.47. Given a group G and subgroups $H_1, \dots, H_k$ of G we define a subset

$$H_1 \dots H_k := \{h_1 \cdot \dots \cdot h_k : h_i \in H_i\}$$

of G.

Remark 5.10. It is easy to extend Corollary 3.53 and Corollary 3.54 by induction. In particular, if each subgroup H_i is normal in G then $H_1 \dots H_n$ is a normal subgroup of G.

Exercise 5.11. Let H and K be subgroups of a group G and assume that $H \cap K = \{1\}$. Show that every element of HK has a unique expression as a product hk with $h \in H$ and $k \in K$.

Theorem 5.12. *Let G be a group and let $H_1, \dots, H_n$ be* **normal** *subgroups of G with the property that*

$$H_j \cap (H_1 \dots H_{j-1} H_{j+1} \dots H_n) = \{1\} \tag{33}$$

for each $1 \leq j \leq n$. Then

$$H_1 \dots H_n \cong H_1 \times \dots \times H_n. \tag{34}$$

Proof. We observe that, for any $k \leq n$, the subset $H_1 \dots H_k$ is a normal subgroup of G and hence a group, by Remark 5.10.

We prove the result by induction on n. For $n = 1$ it is trivial. We assume that the result holds for collections of $n-1$ subgroups. We set $H := H_1 \dots H_{n-1}$ and $K := H_n$.

For any $1 \leq j \leq n-1$ we have

$$H_1 \dots H_{j-1} H_{j+1} \dots H_{n-1} \subseteq H_1 \dots H_{j-1} H_{j+1} \dots H_{n-1} H_n$$

and therefore also

$$(H_j \cap (H_1 \dots H_{j-1} H_{j+1} \dots H_{n-1})) \subseteq (H_j \cap (H_1 \dots H_{j-1} H_{j+1} \dots H_{n-1} H_n)) = \{1\}.$$

By the inductive hypothesis we get

$$H \cong H_1 \times \dots \times H_{n-1}. \tag{35}$$

If we can prove that

$$HK \cong H \times K, \tag{36}$$

then we would get

$$H_1 \dots H_{n-1} H_n = HK \cong H \times K \cong (H_1 \times \dots \times H_{n-1}) \times H_n \cong H_1 \times \dots \times H_{n-1} \times H_n,$$

with the isomorphisms by (36), (35) and Exercise 5.4 respectively.

We finally prove (36). We first note that both H and K are normal in G (by Remark 5.10) and also that the condition (33) with $j = n$ states that

$$H \cap K = \{1\}. \tag{37}$$

We first claim that for any $h \in H$ and $k \in K$ we have

$$hk = kh. \tag{38}$$

Indeed, $k^{-1}hk$ belongs to H so $h^{-1}(k^{-1}hk)$ belongs to H. Similarly, $h^{-1}k^{-1}h$ belongs to K so $(h^{-1}k^{-1}h)k$ belongs to K. From (37) we get

$$h^{-1}k^{-1}hk = 1$$

or equivalently $hk = kh$, as claimed in (38).

By Exercise 5.11 combined with (37), every element of HK has a unique expression as a product hk with $h \in H$ and $k \in K$. This fact in turn means that the association $f(hk) := (h, k)$ gives a well-defined function

$$f : HK \to H \times K.$$

To conclude the proof of (36) and therefore of the theorem, we are hence reduced to showing that f is an isomorphism. It is a homomorphism because

$$\begin{aligned} f((hk)(h'k')) = f(h(kh')k') = f(h(h'k)k') = f((hh')(kk')) \\ = (hh', kk') = (h,k)(h',k') = f(hk)f(h'k'), \end{aligned}$$

where the second equality follows from (38). Since f is clearly both injective and surjective, this concludes the proof. □

Notation 5.13. Under the hypotheses of Theorem 5.12 we feel free to write $\prod_{i=1}^{i=n} H_i$ for either side of the isomorphism (34). The left-hand side of this isomorphism is sometimes called the 'internal direct product' of $H_1, \dots, H_n$ while the right-hand side is called the 'external direct product' of $H_1, \dots, H_n$. The notation introduced in 5.6 is consistent with our identification of both direct products.

We immediately get the following special case of Theorem 5.12, which is sometimes referred to as the 'Recognition Theorem'.

Corollary 5.14. *Let G be a group and let H and K be normal subgroups of G which satisfy both*

$$H \cap K = \{1\}$$

and

$$HK = G.$$

Then G is isomorphic to $H \times K$.

Examples 5.15.
(i) In $G = \mathbb{Z}/30\mathbb{Z}$ we set

$$H_1 := \{0, 15\}, \;\; H_2 := \{0, 10, 20\}, \;\; H_3 := \{0, 6, 12, 18, 24\}.$$

These are obviously normal subgroups of G which are cyclic, with isomorphism classes C_2, C_3 and C_5 respectively. In addition we have

$$\begin{aligned} H_1 + H_2 &= \{0, 5, 10, 15, 20, 25\}, \\ H_1 + H_3 &= \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\}, \\ H_2 + H_3 &= \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\}, \\ H_1 + H_2 + H_3 &= G. \end{aligned}$$

In particular

$$H_1 \cap (H_2 + H_3) = H_2 \cap (H_1 + H_3) = H_3(H_2 + H_3) = \{0\}.$$

We get that

$$\mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

or, in terms of isomorphism classes, that

$$C_{30} = C_2 \times C_3 \times C_5.$$

(ii) If n is an **odd** natural number then one can use Corollary 5.14 to show that $D_{4n} \cong D_{2n} \times \mathbb{Z}/2\mathbb{Z}$. Let $H := \langle s_{4n}, r_{4n}^2 \rangle$ and $K := \langle r_{4n}^n \rangle$ be subgroups of $D_{4n} = \langle s_{4n}, r_{4n} \rangle$. Then the map $H \to D_{2n} = \langle s_{2n}, r_{2n} \rangle$ that sends s_{4n} to s_{2n} and r_{4n}^2 to r_{2n} is easily seen to be an isomorphism, while $K = \{1, r_{4n}^n\}$ is clearly isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

The subgroup H is normal in D_{4n} as it can be shown to have index 2, while K can be seen to be normal by direct computation. Also r_{4n}^n does not belong to H because n is assumed to be odd, so $H \cap K = \{1\}$. The final condition to verify is that $HK = D_{4n}$, and for this it is enough to note that $r_{4n} = (r_{4n}^2)^{(n+1)/2} r_{4n}^n$ belongs to HK.

5.1.2. *Semidirect products.* Semidirect products of two groups H and K will be a generalisation of the direct product $H \times K$ which will still allow us to describe larger groups in terms of their subgroups H and K. The key difference is that both H and K are normal in $H \times K$, and in practice this condition is often too restrictive when trying to study certain groups through specific subgroups which may not be normal. We may even describe non-abelian groups as semidirect products of abelian subgroups H and K.

Example 5.16. Let G be a group, let H be a normal subgroup of G and let K be any subgroup of G for which $H \cap K = \{1\}$. From Corollary 3.53 (and Proposition 3.51) we know that HK is a subgroup of G. In addition the function

$$f : HK \to H \times K$$

given by $f(hk) := (h, k)$ for $h \in H$ and $k \in K$ is still a well-defined bijection of sets. However, as we are not assuming that K is normal in G, f is not necessarily a group homomorphism if we endow the cartesian product $H \times K$ with the usual direct product binary operation.

In general we have

$$(hk)(h'k') = (h(kh'k^{-1}))(kk'), \tag{39}$$

where $kh'k^{-1}$ belongs to H because H is normal in G.

So f would be a homomorphism of groups if the set $H \times K$ were considered as a group with the binary operation $(h, k) \star (h', k') = (h(kh'k^{-1}))(kk')$. Of course one would first have to verify that $\star$ does indeed make the set $H \times K$ into a group. We will prove a more general statement below.

For general groups G_1 and G_2, we would like to use the formula (39) to define a binary operation on the cartesian product $G_1 \times G_2$. In this way we would obtain a group in which we can identify both G_1 and G_2 as subgroups, intersecting only in the identity element, and with G_1 a normal subgroup (but with G_2 not necessarily normal). The only obstacle is how to define an element $g_2 g_1' g_2^{-1}$ of G_1. After that, for $g_1, g_1' \in G_1$ and $g_2, g_2' \in G_2$ we could just set $(g_1, g_2) \star (g_1', g_2') = (g_1(g_2 g_1' g_2^{-1}))(g_2 g_2')$.

Note that in (39), the term $kh'k^{-1} \in H$ is obtained through the action of $k \in K$ by conjugation on $h' \in H$ (which is indeed a well-defined action because H is normal in G). So a natural attempt to define $g_2 g_1' g_2^{-1} \in G_1$ is to interpret such an action in a more abstract way.

We already encountered the group of automorphisms of a group earlier, see for instance Exercise 1.107.

Definition 5.17. Let G be a group. An isomorphism from G to G is called an automorphism of G. The set of automorphisms of G is denoted $\mathrm{Aut}(G)$.

Exercise 5.18. Prove that $\mathrm{Aut}(G)$ is a group, with the binary operation given by composition of automorphisms (in particular $\mathrm{Aut}(G)$ is a subgroup of S_G).

Exercise 5.19. Let G be a group and let H be a normal subgroup of G. Prove that the permutation representation associated to the action of G via conjugation on the set H gives a well-defined group homomorphism

$$\rho : G \to \mathrm{Aut}(H)$$

that has $\ker(\rho) = C_G(H)$.

Theorem 5.20. *Let H and K be groups and let*

$$\rho : K \to \mathrm{Aut}(H)$$

be a group homomorphism. We define a binary operation $\star_\rho$ on the set $H \times K$ by

$$(h, k) \star_\rho (h', k') := (h \cdot (\rho(k)(h')), k \cdot k').$$

Then the following claims are valid.

(i) *The pair $(H \times K, \star_\rho)$ is a group of order $|H||K|$.*

(ii) *The sets*

$$\tilde{H} := \{(h, 1) : h \in H\} \text{ and } \tilde{K} := \{(1, k) : k \in K\}$$

are subgroups of $(H \times K, \star_\rho)$ and the maps $h \mapsto (h, 1)$ for $h \in H$ and $k \mapsto (1, k)$ for $k \in K$ define isomorphisms

$$H \cong \tilde{H} \text{ and } K \cong \tilde{K}.$$

(iii) *The subgroup $\tilde{H}$ is normal in $(H \times K, \star_\rho)$.*

(iv) *$\tilde{H} \cap \tilde{K} = \{1\}$ and $\tilde{H} \star_\rho \tilde{K} = (H \times K, \star_\rho)$.*

(v) *For $x = (h, 1) \in \tilde{H}$ and $y = (1, k) \in \tilde{K}$ one has*

$$y \star_\rho x \star_\rho y^{-1} = (\rho(k)(h), 1).$$

Proof. We first show $\star_\rho$ is associative. Let $a, b, c \in H$ and $x, y, z \in K$. Then

$$\begin{aligned}
((a, x) \star_\rho (b, y)) \star_\rho (c, z) =& (a(\rho(x)(b)), xy) \star_\rho (c, z) \\
=& (a(\rho(x)(b))(\rho(xy)(c)), xyz) \\
=& (a(\rho(x)(b))(\rho(x)(\rho(y)(c))), xyz) \\
=& (a(\rho(x)(b(\rho(y)(c)))), xyz) \\
=& (a, x) \star_\rho (b(\rho(y)(c)), yz) \\
=& (a, x) \star_\rho ((b, y) \star_\rho (c, z)).
\end{aligned}$$

The element $(1, 1)$ is the identity because

$$\begin{aligned}
(h, k) \star_\rho (1, 1) &= (h(\rho(k)(1)), k1) = (h1, k1) = (h, k) \\
&= (\rho(1)(h), k) = (1(\rho(1)(h)), 1k) = (1, 1) \star_\rho (h, k).
\end{aligned}$$

Given $(h, k) \in H \times K$ the inverse element is

$$(h, k)^{-1} := (\rho(k^{-1})(h^{-1}), k^{-1}).$$

Indeed,

$$\begin{aligned}(h,k)\star_\rho (h,k)^{-1} =&(h,k)\star_\rho (\rho(k^{-1})(h^{-1}),k^{-1})\\ =&(h(\rho(k)(\rho(k^{-1})(h^{-1})),kk^{-1})\\ =&(h(\rho(k)(\rho(k)^{-1}(h^{-1})),kk^{-1})\\ =&(hh^{-1},kk^{-1})\\ =&(1,1)\\ =&(\rho(k^{-1})(1),1)\\ =&(\rho(k^{-1})(h^{-1}h),k^{-1}k)\\ =&((\rho(k^{-1})(h^{-1}))(\rho(k^{-1})(h)),k^{-1}k)\\ =&(\rho(k^{-1})(h^{-1}),k^{-1})\star_\rho (h,k)\\ =&(h,k)^{-1}\star_\rho (h,k).\end{aligned}$$

The order of the group $(H\times K,\star_\rho)$ is just the cardinality of $H\times K$ which is just $|H||K|$. This completes the proof of claim (i).

We have

$$(h,1)\star_\rho (h',1) = (h(\rho(1)(h')),11) = (hh',1) \tag{40}$$

and

$$(h,1)^{-1} = (\rho(1)(h^{-1}),1) = (h^{-1},1)$$

so $\tilde{H}$ is a subgroup of G. Moreover the function $f_H : H \to \tilde{H}$ given by $f_H(h) = (h,1)$ is a homomorphism because (40) implies that

$$f_H(hh') = (hh',1) = (h,1)\star_\rho (h',1) = f_H(h)\star_\rho f_H(h').$$

Since f_H is clearly a bijection, it is an isomorphism $H\cong\tilde{H}$.

We have

$$(1,k)\star_\rho (1,k') = (1(\rho(k)(1)),kk') = (11,kk') = (1,kk') \tag{41}$$

and

$$(1,k)^{-1} = (\rho(k^{-1})(1),k^{-1}) = (1,k^{-1})$$

so $\tilde{K}$ is a subgroup of G. Moreover the function $f_K : K \to \tilde{K}$ given by $f_K(k) = (1,k)$ is a homomorphism because (41) implies that

$$f_K(kk') = (1,kk') = (1,k)\star_\rho (1,k') = f_K(k)\star_\rho f_K(k').$$

Since f_K is clearly a bijection, it is an isomorphism $K\cong\tilde{K}$. This completes the proof of claim (ii).

It is clear that $\tilde{H}\cap\tilde{K} = \{1\}$ and also that $\tilde{H}\star_\rho\tilde{K} = (H\times K,\star_\rho)$, so (iv) is valid.

We prove claim (v) before proving claim (iii). We have

$$\begin{aligned}(1,k)\star_\rho(h,1)\star_\rho(1,k)^{-1}=&(1(\rho(k)(h)),k1)\star_\rho(1,k)^{-1}\\=&(\rho(k)(h),k)\star_\rho(1,k^{-1})\\=&((\rho(k)(h))(\rho(k)(1)),kk^{-1})\\=&(\rho(k)(h)1,kk^{-1})\\=&(\rho(k)(h),1).\end{aligned}$$

This proves claim (v).

Now claim (v) implies in particular that $\tilde{K}\subseteq N_{(H\times K,\star_\rho)}(\tilde{H})$. Since $(H\times K,\star_\rho)=\tilde{H}\star_\rho\tilde{K}$, and since obviously $\tilde{H}\subseteq N_{(H\times K,\star_\rho)}(\tilde{H})$, we get that

$$N_{(H\times K,\star_\rho)}(\tilde{H})=(H\times K,\star_\rho).$$

This means that $\tilde{H}$ is normal in $(H\times K,\star_\rho)$, which proves claim (iii) and completes the proof. □

Definition 5.21. Let H and K be groups and let

$$\rho:K\to\mathrm{Aut}(H)$$

be a group homomorphism. The group $(H\times K,\star_\rho)$ is the 'semidirect product of H and K with respect to ρ' and is denoted by $H\rtimes_\rho K$, or simply by $H\rtimes K$ when ρ is clear from context.

Notation 5.22. We use the canonical isomorphisms described in Theorem 5.20 (ii) to identify both H of K with subgroups of $H\rtimes_\rho K$, and so we henceforth drop the notation $\tilde{H}$, $\tilde{K}$ and simply write H and K in their place. As usual, we often drop the binary operation $\star_\rho$ from all notation.

We sometimes also write $k\cdot h:=\rho(k)(h)$ for $h\in H$, $k\in K$, whenever ρ is clear from context. With this notation, the formula for the binary operation in $H\rtimes K$ becomes

$$(h,k)(h',k')=(h(k\cdot h'),kk')$$

and the formula of Theorem 5.20 (v) becomes

$$khk^{-1}=k\cdot h$$

for any $h\in H$ and $k\in K$.

Remark 5.23. The symbol $H\rtimes K$ reminds us that, under the identifications of Notation 5.22, H is a normal subgroup of $H\rtimes K$, while K is not necessarily normal in $H\rtimes K$. Unlike the direct product $\times$, the semidirect product $\rtimes$ is certainly not symmetric.

The following result clarifies when exactly K can be normal in $H\rtimes K$.

Proposition 5.24. *Let H and K be groups and let*

$$\rho:K\to\mathrm{Aut}(H)$$

be a group homomorphism. Then the following conditions are equivalent.

(i) *The identity function between $H\rtimes K$ and $H\times K$ is a group homomorphism.*

(ii) *The identity function between $H \rtimes K$ and $H \times K$ is a group isomorphism.*

(iii) *ρ is the trivial homomorphism from K to $\mathrm{Aut}(H)$ (meaning $\rho(k) = \mathrm{id}_H$ for every $k \in K$).*

(iv) *K is normal in $H \rtimes K$.*

Proof. It is clear that (i) and (ii) are equivalent, since the equality of underlying cartesian products $H \times K = H \times K$ is obviously bijective.

Now condition (i) holds if and only if

$$(h(\rho(k)(h')), kk') = (h, k) \star_\rho (h', k') = (h, k)(h', k') = (hh', kk')$$

for every h, h', k, k'. Equivalently $h(\rho(k)(h')) = hh'$ for every h, h', k. Equivalently $\rho(k)(h') = h'$ for every $k \in K$ and every $h' \in H$. Equivalently $\rho(k) = \mathrm{id}_H$ for every $k \in K$. This proves that conditions (i) and (iii) are equivalent.

We now prove that conditions (iii) and (iv) are equivalent. Since $H \rtimes K = HK$ and trivially K normalises K, we know that K is normal in $H \rtimes K$ if and only if H normalises K. it is enough to prove that H normalises K if and only if $\rho(k) = \mathrm{id}_H$ for every $k \in K$.

Now H normalises K if and only if for every $x \in H$ and $y \in K$ the element xyx^{-1} belongs to K, if and only if $(xyx^{-1})y^{-1}$ belongs to K. But $x(yx^{-1}y^{-1})$ always belongs to H (since H is normal), so H normalises K if and only if for every $x \in H$ and $y \in K$ the element $xyx^{-1}y^{-1}$ belongs to $H \cap K = \{1\}$, if and only $xy = yx$ for every $x \in H$ and $y \in K$, if and only $x = yxy^{-1}$ for every $x \in H$ and $y \in K$.

To conclude the proof or the equivalence of (iii) and (iv) we use Theorem 5.20 (v). For $x = (h, 1) \in H$ and $y = (1, k) \in K$ one has $yxy^{-1} = (\rho(k)(h), 1)$. Therefore $x = yxy^{-1}$ for every $x \in H$ and $y \in K$ if and only if $\rho(k)(h) = h$ for every $k \in K$ and every $h \in H$, if and only if $\rho(k) = \mathrm{id}_H$ for every $k \in K$. This completes the proof. □

Examples 5.25.

(i) Let G be a group. The homomorphism $\rho : G \to \mathrm{Aut}(G)$ given by $\rho(g)(g') = gg'g^{-1}$ for all $g, g' \in G$ defines a group $G \rtimes G = G \rtimes_\rho G$ in which $(g_1, g_2)(g_3, g_4) = (g_1g_2g_3g_2^{-1}, g_2g_4)$. The identity map $G \rtimes G \to G \times G$ is an isomorphism if and only if G is abelian.

(ii) Let

$$\rho : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$$

be given by $\rho(0)(x) = x$ and by $\rho(1)(x) = -x$ for $x \in \mathbb{Z}/3\mathbb{Z}$. It is easy to see that ρ is a homomorphism. Then the group $\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ is a non-abelian group of order 6 and contains $H = \{(0, 0), (1, 0), (2, 0)\}$ as a normal subgroup. In fact, it is easy to see that the map

$$\mathbb{Z}/3\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} \to D_6$$

given by

$$(0, 0) \mapsto 1,\ \ (1, 0) \mapsto r,\ \ (2, 0) \mapsto r^2,\ \ (0, 1) \mapsto s,\ \ (1, 1) \mapsto sr,\ \ (2, 1) \mapsto sr^2$$

is an isomorphism.

(iii) More generally, let

$$\rho : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$$

be given by $\rho(0)(x) = x$ and by $\rho(1)(x) = -x$ for $x \in \mathbb{Z}/n\mathbb{Z}$. It is easy to see that ρ is a homomorphism. Then the group $\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ is a non-abelian group of order $2n$

and contains $H = \{(0,0),(1,0),(2,0),\dots,(n-1,0)\}$ as a normal subgroup. In fact, as a straightforward generalisation of part (ii), one sees that

$$\mathbb{Z}/n\mathbb{Z} \rtimes_\rho \mathbb{Z}/2\mathbb{Z} \cong D_{2n}.$$

(iv) More generally, for any abelian group H, let

$$\rho : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(H)$$

be given by $\rho(0)(x) = x$ and by $\rho(1)(x) = -x$ for $x \in H$. It is easy to see that ρ is a homomorphism. Then the group $H \rtimes_\rho \mathbb{Z}/2\mathbb{Z}$ contains H as a normal subgroup of index 2.

As an example one may consider the case $H = \mathbb{Z}$ and obtain the group

$$D_\infty := \mathbb{Z} \rtimes_\varrho \mathbb{Z}/2\mathbb{Z}.$$

This group is non-abelian, so in particular it is not isomorphic to $\mathbb{Z}$. For instance one has

$$(6,1)(2,0) = (6+\rho(1)(2), 1+0) = (6-2,1) = (4,1)$$

and

$$(2,0)(6,1) = (2+\rho(0)(6), 0+1) = (2+6,1) = (8,1).$$

(v) More generally, for any abelian group H, let

$$\rho : \mathbb{Z}/2n\mathbb{Z} \to \mathrm{Aut}(H)$$

be given by $\rho(k)(x) = (-1)^k x$ for $0 \leq k \leq 2n-1$ and for $x \in H$. It is easy to see that ρ is a homomorphism.

As an example we consider the case $H = \mathbb{Z}/3\mathbb{Z}$ and $n = 2$. The group $\mathbb{Z}/4\mathbb{Z} \rtimes_\rho \mathbb{Z}/3\mathbb{Z}$ has order 12 and we claim that it is non-abelian, so for instance it cannot have isomorphism class C_{12}, or isomorphism class $C_2 \times C_6$. We also claim that it is not isomorphic to D_{12} or to A_4. In this way, we have used the semidirect product to construct a genuinely new group that we had not encountered previously.

We have

$$(1,1)(2,0) = (1+\rho(1)(2), 1+0) = (1-2,1) = (2,1)$$

while

$$(2,0)(1,1) = (2+\rho(0)(1), 0+1) = (2+1,1) = (0,1),$$

so $\mathbb{Z}/4\mathbb{Z} \rtimes_\rho \mathbb{Z}/3\mathbb{Z}$ is non-abelian.

In addition D_{12} and A_4 do not have any elements of order 4, but $\mathbb{Z}/4\mathbb{Z} \rtimes_\rho \mathbb{Z}/3\mathbb{Z}$ contains the cyclic subgroup $\mathbb{Z}/4\mathbb{Z}$ of order 4 (which in fact is the unique Sylow 2-subgroup). Therefore $\mathbb{Z}/4\mathbb{Z} \rtimes_\rho \mathbb{Z}/3\mathbb{Z}$ cannot be isomorphic to either D_{12} or A_4.

(vi) Let H be a group. Let

$$\rho = \mathrm{id} : \mathrm{Aut}(H) \to \mathrm{Aut}(H)$$

be the identity map. The semidirect product

$$\mathrm{Hol}(H) := H \rtimes_{\mathrm{id}} \mathrm{Aut}(H)$$

is called the 'holomorph' of H.

(vii) Let p and q be distinct primes with, say, $p < q$. We note that, by [2, Prop. 4.16, p. 135] (or Exercise 2.101), the group $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ is cyclic of order $q-1$, with each element given by multiplication by an element of $\{1,2,\dots,q-1\}$.

We saw in Example 4.91 that if $p \nmid q-1$ then any group of order pq is necessarily cyclic. This is consistent with the fact that there is no non-trivial homomorphism from $\mathbb{Z}/p\mathbb{Z}$ to $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$.

If on the other hand $p \mid q-1$, then one may use [2, Prop. 4.16, p. 135] and Cauchy's Theorem to show that there is a non-trivial homomorphism

$$\rho : \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}).$$

It can further be proved that the associated semidirect product $\mathbb{Z}/q\mathbb{Z} \rtimes_\rho \mathbb{Z}/p\mathbb{Z}$ is the unique (up to isomorphism) non-abelian group of order pq.

Exercise 5.26. Prove that $\mathrm{Hol}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_4$.

Exercise 5.27. Construct a non-abelian group of order 21 and a non-abelian group of order 39.

Exercise 5.28. Construct two non-isomorphic non-abelian groups of order 27.

As in the case of direct products, we have a Recognition Theorem for semidirect products.

Theorem 5.29. *Let G be a group. Let H be a normal subgroup of G. Let K be a subgroup of G. Assume that*

$$H \cap K = \{1\}.$$

Let

$$\rho : K \to \mathrm{Aut}(H)$$

be given by

$$\rho(k)(h) := khk^{-1}.$$

Then $HK \cong H \rtimes_\rho K$.

If in particular $G = HK$ then $G \cong H \rtimes_\rho K$.

Proof. We know HK is a subgroup of G by Corollary 3.53 and Proposition 3.51 (since H is normal in G). By Exercise 5.11, each element of HK has a unique expression of the form hk with $h \in H$ and $k \in K$. The function $hk \mapsto (h,k)$ is a well-defined bijection $HK \to H \rtimes_\rho K$. The fact that it is a group homomorphism now follows from (39). □

The above result is linked to a general bit of terminology, which we include here only for completeness.

Definition 5.30. Let G be a group and let H be a subgroup of G. A subgroup K of G is called a 'complement for H in G' if both $G = HK$ and $H \cap K = \{1\}$.

Example 5.31. In Example 4.91 we saw that, if a group G has order pq for distinct primes p and q, with $p < q$, then G has a normal Sylow q-subgroup Q. We also saw that if $p \nmid q-1$, then G is necessarily cyclic.

Let P be a Sylow p-subgroup of P. In either case, one has $Q \cap P = \{1\}$ by Lagrange's Theorem. One also has that $QP = G$ and therefore Theorem 5.29 implies that G is isomorphic to a semidirect product $Q \rtimes_\rho P$.

We note that by Theorem 5.33 and Proposition 5.46 below, the unique isomorphism class of abelian groups of order pq is C_{pq}.

In the case $p \nmid q-1$ we already know that G is also isomorphic to $Q \times P$, and Proposition 5.24 shows that $\rho : P \to \mathrm{Aut}(Q)$ must be the trivial homomorphism.

Suppose now that $p \mid q-1$. In this case, in addition to the isomorphism class C_{pq}, there is a unique non-abelian group of order pq up to isomorphism. This claim is equivalent to verifying that all non-trivial homomorphisms $\rho : P \to \mathrm{Aut}(Q)$ lead to isomorphic semidirect products.

Let y be a generator of P. By [2, Prop. 4.16, p. 135] (or Exercise 2.101) we know that $\mathrm{Aut}(Q)$ is cyclic of order $q-1$. Therefore it contains a unique subgroup of order p. Let γ be any element of $\mathrm{Aut}(Q)$ of order p. Then any homomorphism $\rho : P \to \mathrm{Aut}(Q)$ must map y to a power of γ. The possibilities are $\rho_j(y) := \gamma^j$ for each $0 \leq j \leq p-1$, with ρ_0 the trivial homomorphism.

Set $G_j := Q \rtimes_{\rho_j} P$ for some j with $2 \leq j \leq p-1$. We explain why G_j is isomorphic to G_1. Fix k with jk congruent to 1 modulo p. Then the map $G_1 \to G_j$ given by

$$(x, y^l) \mapsto (x, y^{lk}),$$

for $x \in Q$, is easily seen to be a group homomorphism and therefore also a group isomorphism.

This shows that all non-abelian groups of order pq must be isomorphic.

Example 5.32. One can show that any group G of order 30 has a subgroup H of order 15 (see [2, p. 143,144]). Such a subgroup H is necessarily both normal (by Lemma 3.31) and cyclic (by Example 4.91).

By Sylow's Theorem, G also has a subgroup K of order 2, and again by Theorem 5.29, G must be isomorphic to a semidirect product $H \rtimes_\rho K$ for some $\rho : K \to \mathrm{Aut}(H)$.

We note that by Theorem 5.33 and Proposition 5.46 below, the unique isomorphism class of abelian groups of order 30 is C_{30}.The trivial homomorphism corresponds to this class.

Any non-trivial ρ must map the non-trivial element of K to an element of order 2 in $\mathrm{Aut}(H)$. Now using the fact that H is cyclic of order 15 one may show, either directly or via the general result [2, Prop. 4.16, p. 135], that $\mathrm{Aut}(H)$ only contains three elements of order 2. In this way we see that, up to isomorphism, there are (at most) three non-abelian groups of order 30.

In fact there are exactly three non-abelian groups of order 30 up to isomorphism, because the groups $\mathbb{Z}/5\mathbb{Z} \times D_6$, $\mathbb{Z}/3\mathbb{Z} \times D_{10}$ and D_{30} are pairwise non-isomorphic.

5.2. **The Fundamental Theorem of finite abelian groups.**

5.2.1. *The statements.* In this section we state the Fundamental Theorem, which we shall prove in section 5.2.3 below. In fact we will discuss two different but equivalent formulations of this result.

Theorem 5.33. *Let G be a finite abelian group. Then G has isomorphism class*

$$C_{n_1} \times C_{n_2} \times \ldots \times C_{n_s}$$

for some integers $s \in \mathbb{N}$ and $n_j \geq 2$ with the property that n_{j+1} divides n_j for all $1 \leq j \leq s-1$.

This description of the isomorphism class of G is unique: if G has isomorphism class

$$C_{m_1} \times C_{m_2} \times \ldots \times C_{m_t}$$

for some integers $m_i \geq 2$ with the property that m_{i+1} divides m_i for all $1 \leq i \leq t-1$, then

$$t = s \text{ and } m_i = n_i \text{ for all } 1 \leq i \leq s.$$

Definition 5.34. The integers $n_1, \dots, n_s$ are the 'invariant factors' of G. One sometimes says that G has 'type' $(n_1, \dots, n_s)$.

Remark 5.35. One has $|G| = n_1 \dots n_s$. Theorem 5.33 thus states that, for a fixed $n \in \mathbb{N}$, there is a bijection between the sets of isomorphism classes of finite abelian groups of order n, and the set of all finite sequences of integers $n_1, \dots, n_s$ (greater than 1) which satisfy $n_{j+1} \mid n_j$ for all j as well as $n_1 \dots n_s = n$.

In any such sequence we have $n_1 \geq \dots \geq n_s$, and each n_j divides n. So any prime factor p of n must divide some invariant factor n_j, and then it must also divide $n_{j-1}, \dots, n_1$. In particular, every prime divisor of n must divide n_1.

Corollary 5.36. *If G is a finite abelian group and $|G|$ is square-free then G is cyclic.*

Proof. As explained in Remark 5.35, if $|G| = p_1 \dots p_m$ for distinct primes p_i, then each p_i must divide the first invariant factor n_1. Therefore $|G| \mid n_1 \mid |G|$ so $n_1 = |G|$, It follows that $s = 1$ and that G has isomorphism class $C_{n_1} = C_{|G|}$, so G is cyclic. □

Example 5.37. We determine the isomorphism classes of all abelian groups of order $180 = 2^2 \cdot 3^2 \cdot 5$. We must have $30 = 2 \cdot 3 \cdot 5 \mid n_1$ so the only possibilities for n_1 are

$$180 = 2^2 \cdot 3^2 \cdot 5, \;\; 60 = 2^2 \cdot 3 \cdot 5, \;\; 90 = 2 \cdot 3^2 \cdot 5, \;\; 30 = 2 \cdot 3 \cdot 5.$$

We consider each of these cases individually. If $n_1 = 180$ then $s = 1$ and we are done.

If $n_1 = 90$ then the only number $n_2 \geq 2$ dividing n_1 with the property that $n_1 n_2$ divides 180 is $n_2 = 2$. In this case $n_1 n_2 = 180$ so $s = 2$ and we are done.

If $n_1 = 60$ then the only number $n_2 \geq 2$ dividing n_1 with the property that $n_1 n_2$ divides 180 is $n_2 = 3$. In this case $n_1 n_2 = 180$ so $s = 2$ and we are done.

We finally consider the case $n_1 = 30$. A priori, the only candidates for n_2 are $2, 3$ or 6. But if $n_2 = 2$ then since $n_3 \mid n_2$ we would have $n_3 = 2$, but then $n_1 n_2 n_3$ would be divisible by 2^3, which is impossible. Similarly if $n_2 = 3$ then since $n_3 \mid n_2$ we would have $n_3 = 3$, but then $n_1 n_2 n_3$ would be divisible by 3^3, which is impossible. Therefore the only possibility is $n_2 = 6$ and then $s = 2$ and we are done.

We have proved that all possible isomorphism classes of abelian groups of order 180 are

$$C_{180}, \;\; C_{90} \times C_2, \;\; C_{60} \times C_3, \;\; C_{30} \times C_6. \tag{42}$$

We now give another formulation of the Fundamental Theorem.

Theorem 5.38. *Let G be a finite abelian group and let*

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

be the prime decomposition of $|G|$. Then

$$G \cong A_1 \times A_2 \times \dots \times A_k \tag{43}$$

where each group A_i is the Sylow p_i-subgroup of G and has isomorphism class

$$C_{p_i^{\beta_{1,i}}} \times C_{p_i^{\beta_{2,i}}} \times \dots \times C_{p_i^{\beta_{t_i,i}}}$$

for natural numbers t_i and $\beta_{j,i}$ with

$$\beta_{1,i} \geq \beta_{2,i} \geq \ldots \geq \beta_{t_i,i}. \tag{44}$$

This decomposition is unique: if $G \cong B_1 \times B_2 \times \ldots \times B_k$ with $|B_i| = p^{\alpha_i}$ then for all i we have $B_i \cong A_i$ and B_i and A_i have the same sequence of invariant factors $\beta_{1,i}, \beta_{2,i}, \ldots, \beta_{t_i,i}$.

Remark 5.39. Obviously one has $|A_i| = p_i^{\alpha_i}$ and $\beta_{1,i} + \beta_{2,i} + \ldots \beta_{t_i,i} = \alpha_i$. Also since G is abelian each group A_i is the *unique* Sylow p_i-subgroup of G. The fact that G is isomorphic to the direct product of its own Sylow subgroups is sometimes referred to as the Primary Decomposition Theorem for finite abelian groups.

Definition 5.40. The integers $p_i^{\beta_{j,i}}$, for $1 \leq i \leq k$ and $1 \leq j \leq t_i$, are called the 'elementary divisors' of G. The description given in Theorem 5.38 is then the 'elementary divisor decomposition' of G.

Remark 5.41. The elementary divisors of G are thus partitioned into the invariant factors of each of its Sylow subgroups A_i. Beware, however, that the elementary divisors of G are in general not the invariant factors of G itself.

Exercise 5.42.
(i) Let p be a prime number. Prove that the number of isomorphism classes of abelian groups of order p^α is equal to the number of partitions of α, in the sense of Definition 4.69 (ii). Determine all isomorphism classes of abelian groups of order p^α for each of $\alpha = 1, 2, 3, 4, 5$.
(ii) Let $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Let a_k be the number of partitions of α_k. Show that the number of isomorphism classes of abelian groups of order n is $a_1 \ldots a_k$.

Remark 5.43. In particular, the number of isomorphism classes of abelian groups of order p^α is independent of p.

Examples 5.44.
(i) As we already verified in Example 5.37, if we consider $n = 180 = 2^2 \cdot 3^2 \cdot 5$, since the number of partitions of 2 is 2 and the number of partitions of 1 is 1, we get that there are $2 \cdot 2 \cdot 1 = 4$ isomorphism classes of abelian groups of order 180. These were already listed in (42).
(ii) For $n = 1800 = 2^3 \cdot 3^2 \cdot 5^2$ we have 3 partitions of 3 and 2 partitions of 2 and hence 12 isomorphism classes of abelian groups of order 1800. The possible isomorphism classes of Sylow 2-subgroups of such a group are

$$C_8, \quad C_4 \times C_2, \quad C_2 \times C_2 \times C_2.$$

The possible isomorphism classes of Sylow 3-subgroups of such a group are C_9 or $C_3 \times C_3$. The possible isomorphism classes of Sylow 5-subgroups of such a group are C_{25} or $C_5 \times C_5$. Thus the 12 isomorphism classes of abelian groups of order 1800 are

$$C_8 \times C_9 \times C_{25},\ C_8 \times C_9 \times C_5 \times C_5,\ C_8 \times C_3 \times C_3 \times C_{25},$$
$$C_8 \times C_3 \times C_3 \times C_5 \times C_5,\ C_4 \times C_2 \times C_9 \times C_{25},\ C_4 \times C_2 \times C_9 \times C_5 \times C_5,$$
$$C_4 \times C_2 \times C_3 \times C_3 \times C_{25},\ C_4 \times C_2 \times C_3 \times C_3 \times C_5 \times C_5,\ C_2 \times C_2 \times C_2 \times C_9 \times C_{25},$$
$$C_2 \times C_2 \times C_2 \times C_9 \times C_5 \times C_5,\ C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_{25},\ C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5 \times C_5.$$

Remark 5.45. As we already mentioned in Remark 5.41, the elementary divisors of G are invariant factors of the Sylow subgroups of G but not of G itself. For instance in the above list of classes, we have not expressed the given isomorphism classes in terms of the corresponding invariant factors. The next result gives us a crucial step in translating decompositions in terms of invariant factors into decompositions in terms of elementary divisors, and vice versa.

Proposition 5.46. *Fix $m, n \in \mathbb{N}$.*

(i) *The group $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is isomorphic to the group $\mathbb{Z}/(mn)\mathbb{Z}$ if and only if m and n are coprime.*

(ii) *If $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ then*

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}.$$

Proof. Claim (ii) follows from claim (i) through a straightforward induction argument. We leave the details to the reader and only discuss the proof of claim (i).

Set $l := \operatorname{lcm}(m, n)$, so that $l = mn$ if and only if $(m, n) = 1$. Then for any $(a, b) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ we have

$$l(a, b) = (la, lb) = (0, 0).$$

So if $(m, n) \neq 1$, every element of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has order at most $l < mn$. Then $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ does not contain any elements of order mn and therefore it cannot be isomorphic to $\mathbb{Z}/(mn)\mathbb{Z}$.

Conversely if $(m, n) = 1$ then

$$\mathrm{o}(([1]_m, [1]_n)) = \operatorname{lcm}(\mathrm{o}([1]_m), \mathrm{o}([1]_m)) = l = mn$$

so the cyclic subgroup $\langle([1]_m, [1]_n)\rangle$ of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has order mn, and thus $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ must in fact be cyclic, as required. □

Remarks 5.47.

(i) We may use Proposition 5.46 to obtain the elementary divisors of a finite abelian group G from its sequence of invariant factors $n_1, n_2, \dots, n_s$. Let

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = n_1 n_2 \dots n_s.$$

Write down the prime factorisation of each n_j as

$$n_j = p_1^{\beta_{j,1}} p_2^{\beta_{j,2}} \dots p_k^{\beta_{j,k}},$$

for integers $\beta_{j,i} \geq 0$. Then Proposition 5.46 implies that

$$\mathbb{Z}/n_j\mathbb{Z} \cong \mathbb{Z}/p_1^{\beta_{j,1}}\mathbb{Z} \times \mathbb{Z}/p_2^{\beta_{j,2}} \times \dots \times \mathbb{Z}/p_k^{\beta_{j,k}},$$

where any factor of the form $\mathbb{Z}/p^0\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = \{1\}$ may obviously be deleted from the above decomposition. Then the elementary divisors of G are precisely the integers $p_i^{\beta_{j,i}}$ for each $1 \leq i \leq k$ and each $1 \leq j \leq s$ that satisfies $\beta_{j,i} \neq 0$.

(ii) Conversely, given the elementary divisors of a finite abelian group G one easily obtains the invariant factors as follows. Suppose $|G| = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Set

$$s := \max(t_1, \dots, t_k).$$

Set $\beta_{j,i} := 0$ whenever $s \geq j > t_i$, thus adding 1's to the list of invariant factors $p_i^{\beta_{j,i}}$. Then for each $1 \leq j \leq s$ the j-th invariant factor n_j is

$$n_j := p_1^{\beta_{j,1}} p_2^{\beta_{j,2}} \ldots p_k^{\beta_{j,k}}.$$

Example 5.48. We may use the method outlined in Remarks 5.47(i) to obtain the elementary divisors of an abelian group G from *any* cyclic decomposition of G, not just from the decomposition in terms of invariant factors. For instance if $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ then the elementary divisors of G are $2, 3, 3, 5$ so in particular G also has isomorphism class

$$C_2 \times C_3 \times C_3 \times C_5.$$

Example 5.49. As in Example 5.44 (ii) we consider the case $n = 1800 = 2^3 \cdot 3^2 \cdot 5^2$. We already listed all possible sequences of elementary divisors of abelian groups of order 1800, through the corresponding isomorphism classes. Let us now re-write each such isomorphism class in terms of its corresponding sequence of invariant factors.

$$\begin{aligned}
C_8 \times C_9 \times C_{25} &= C_{1800}, & C_8 \times C_9 \times C_5 \times C_5 &= C_{360} \times C_5,\\
C_8 \times C_3 \times C_3 \times C_{25} &= C_{600} \times C_3, & C_8 \times C_3 \times C_3 \times C_5 \times C_5 &= C_{120} \times C_{15},\\
C_4 \times C_2 \times C_9 \times C_{25} &= C_{900} \times C_2, & C_4 \times C_2 \times C_9 \times C_5 \times C_5 &= C_{180} \times C_{10},\\
C_4 \times C_2 \times C_3 \times C_3 \times C_{25} &= C_{300} \times C_6, & C_4 \times C_2 \times C_3 \times C_3 \times C_5 \times C_5 &= C_{60} \times C_{30},\\
C_2 \times C_2 \times C_2 \times C_9 \times C_{25} &= C_{450} \times C_2 \times C_2, & C_2 \times C_2 \times C_2 \times C_9 \times C_5 \times C_5 &= C_{90} \times C_{10} \times C_2,\\
C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_{25} &= C_{150} \times C_6 \times C_2, & C_2 \times C_2 \times C_2 \times C_3 \times C_3 \times C_5 \times C_5 &= C_{30} \times C_{30} \times C_2.
\end{aligned}$$

Let us briefly indicate all the relevant computations involved in each of the 12 cases.

- The sequence of invariant factors $n_1 = 1800$ gives $n_1 = 2^3 \cdot 3^2 \cdot 5^2$ and thus elementary divisors $8, 9, 25$. Conversely, the elementary divisors $8, 9, 25$ give $s = 1$ and $n_1 = 8 \cdot 9 \cdot 25 = 1800$.
- The invariant factors $n_1 = 360 = 2^3 \cdot 3^2 \cdot 5$ and $n_2 = 5$ give elementary divisors $8, 9, 5, 5$. Conversely the elementary divisors $8, 9, 5, 5$ give $s = 2$, $n_1 = 8 \cdot 9 \cdot 5 = 360$ and $n_2 = 1 \cdot 1 \cdot 5 = 5$.
- The invariant factors $n_1 = 600 = 2^3 \cdot 3 \cdot 5^2$ and $n_2 = 3$ give elementary divisors $8, 3, 3, 25$. Conversely the elementary divisors $8, 3, 3, 25$ give $s = 2$, $n_1 = 8 \cdot 3 \cdot 25 = 600$ and $n_2 = 1 \cdot 3 \cdot 1 = 3$.
- The invariant factors $n_1 = 120 = 2^3 \cdot 3 \cdot 5$ and $n_2 = 15 = 3 \cdot 5$ give elementary divisors $8, 3, 3, 5, 5$. Conversely the elementary divisors $8, 3, 3, 5, 5$ give $s = 2$, $n_1 = 8 \cdot 3 \cdot 5 = 120$ and $n_2 = 1 \cdot 3 \cdot 5 = 15$.
- The invariant factors $n_1 = 900 = 2^2 \cdot 3^2 \cdot 5^2$ and $n_2 = 2$ give elementary divisors $4, 2, 9, 25$. Conversely the elementary divisors $4, 2, 9, 25$ give $s = 2$, $n_1 = 4 \cdot 9 \cdot 25 = 900$ and $n_2 = 2 \cdot 1 \cdot 1 = 2$.
- The invariant factors $n_1 = 180 = 2^2 \cdot 3^2 \cdot 5$ and $n_2 = 10 = 2 \cdot 5$ give elementary divisors $4, 2, 9, 5, 5$. Conversely the elementary divisors $4, 2, 9, 5, 5$ give $s = 2$, $n_1 = 4 \cdot 9 \cdot 5 = 180$ and $n_2 = 2 \cdot 1 \cdot 5 = 10$.
- The invariant factors $n_1 = 300 = 2^2 \cdot 3 \cdot 5^2$ and $n_2 = 6 = 2 \cdot 3$ give elementary divisors $4, 2, 3, 3, 25$. Conversely the elementary divisors $4, 2, 3, 3, 25$ give $s = 2$, $n_1 = 4 \cdot 3 \cdot 25 = 300$ and $n_2 = 2 \cdot 3 \cdot 1 = 6$.

- The invariant factors $n_1 = 60 = 2^2 \cdot 3 \cdot 5$ and $n_2 = 30 = 2 \cdot 3 \cdot 5$ give elementary divisors $4, 2, 3, 3, 5, 5$. Conversely the elementary divisors $4, 2, 3, 3, 5, 5$ give $s = 2$, $n_1 = 4 \cdot 3 \cdot 5 = 60$ and $n_2 = 2 \cdot 3 \cdot 5 = 30$.
- The invariant factors $n_1 = 450 = 2 \cdot 3^2 \cdot 5^2$, $n_2 = 2$ and $n_3 = 2$ give elementary divisors $2, 2, 2, 9, 25$. Conversely the elementary divisors $2, 2, 2, 9, 25$ give $s = 3$, $n_1 = 2 \cdot 9 \cdot 25 = 450$, $n_2 = 2 \cdot 1 \cdot 1 = 2$ and $n_3 = 2 \cdot 1 \cdot 1 = 2$.
- The invariant factors $n_1 = 90 = 2 \cdot 3^2 \cdot 5$, $n_2 = 10 = 2 \cdot 5$ and $n_3 = 2$ give elementary divisors $2, 2, 2, 9, 5, 5$. Conversely the elementary divisors $2, 2, 2, 9, 5, 5$ give $s = 3$, $n_1 = 2 \cdot 9 \cdot 5 = 90$, $n_2 = 2 \cdot 1 \cdot 5 = 10$ and $n_3 = 2 \cdot 1 \cdot 1 = 2$.
- The invariant factors $n_1 = 150 = 2 \cdot 3 \cdot 5^2$, $n_2 = 6 = 2 \cdot 3$ and $n_3 = 2$ give elementary divisors $2, 2, 2, 3, 3, 25$. Conversely the elementary divisors $2, 2, 2, 3, 3, 25$ give $s = 3$, $n_1 = 2 \cdot 3 \cdot 25 = 150$, $n_2 = 2 \cdot 3 \cdot 1 = 6$ and $n_3 = 2 \cdot 1 \cdot 1 = 2$.
- The invariant factors $n_1 = 30 = 2 \cdot 3 \cdot 5$, $n_2 = 30 = 2 \cdot 3 \cdot 5$ and $n_3 = 2$ give elementary divisors $2, 2, 2, 3, 3, 5, 5$. Conversely the elementary divisors $2, 2, 2, 3, 3, 5, 5$ give $s = 3$, $n_1 = 2 \cdot 3 \cdot 5 = 30$, $n_2 = 2 \cdot 3 \cdot 5 = 30$ and $n_3 = 2 \cdot 1 \cdot 1 = 2$.

Exercise 5.50. Prove that Theorem 5.33 is valid if and only if Theorem 5.38 is valid (you may and should, of course, use Proposition 5.46).

5.2.2. *The exponent.* In this section we briefly introduce a general notion, and some related results in the case of finite abelian groups, that will be useful in the sequel.

Definition 5.51. Let G be a finite group. The 'exponent' $e(G)$ of G is

$$e(G) := \min\{n \in \mathbb{N} : g^n = 1 \text{ for all } g \in G\}.$$

Remark 5.52. The exponents of isomorphic groups coincide.

Lemma 5.53. *Let G be a finite abelian group. Then*

$$e(G) = \max\{\mathrm{o}(g) : g \in G\}.$$

Proof. Obviously $e(G) \geq \max\{\mathrm{o}(g) : g \in G\}$. Let $x \in G$ be an element of maximal order. We must simply prove that $\mathrm{o}(x) = e(G)$.

Now $e(G)$ is the least common multiple of the finite set of natural numbers $\{\mathrm{o}(g) : g \in G\}$. If we can prove that $\mathrm{o}(g)$ divides $\mathrm{o}(x)$ for every $g \in G$ then we must have $e(G) = \mathrm{o}(x)$, as required.

To argue by contradiction, assume that we have $g \in G$ for which $\mathrm{o}(g) \nmid \mathrm{o}(x)$. Then there is a prime number p and a natural number j with the property that $p^j \mid \mathrm{o}(g)$ but $p^j \nmid \mathrm{o}(x)$. Write $\mathrm{o}(x) = p^i k$ with $p \nmid k$ and $i < j$.

We set $x' := x^{p^i}$ and $g' := g^{\mathrm{o}(g)/p^j}$. Then $\mathrm{o}(x') = k$ and $\mathrm{o}(g') = p^j$, so that $\mathrm{o}(x)$ and $\mathrm{o}(g')$ are coprime. Now since G is abelian, the order of the element $x'g'$ is

$$\mathrm{o}(x')\mathrm{o}(g') = kp^j > kp^i = \mathrm{o}(x).$$

This would contradict the maximality of $\mathrm{o}(x)$. □

Lemma 5.54. *If G is a finite abelian group then $\mathrm{o}(g)$ divides $e(G)$ for every $g \in G$.*

Proof. Fix $x \in G$ with the property that $\mathrm{o}(x) = e(G)$. To argue by contradiction we fix $y \in G$ for which $\mathrm{o}(y) \nmid \mathrm{o}(x)$.

Then there exists a prime number p and integers r and s, with $0 \leq r < s$, for which p^r is the power of p which occurs in the prime decomposition of $\mathrm{o}(x)$ but p^s is the power of p which occurs in the prime decomposition of $\mathrm{o}(y)$.

Now

$$\mathrm{o}(x^{p^r}) = \frac{\mathrm{o}(x)}{(\mathrm{o}(x), p^r)} = \frac{\mathrm{o}(x)}{p^r}$$

is not divisible by p but

$$\mathrm{o}(y^{\mathrm{o}(y)/p^s}) = \frac{\mathrm{o}(y)}{(\mathrm{o}(y), \mathrm{o}(y)/p^s)} = \frac{\mathrm{o}(y)}{\mathrm{o}(y)/p^s} = p^s.$$

In particular $\mathrm{o}(x^{p^n})$ and $\mathrm{o}(y^{\mathrm{o}(y)/p^s})$ are coprime.

Now, since G is assumed to be abelian, the product $z := x^{p^r} y^{\mathrm{o}(y)/p^s}$ has order

$$\mathrm{o}(z) = \mathrm{lcm}(\mathrm{o}(x^{p^n}), \mathrm{o}(y^{\mathrm{o}(y)/p^s})) = \mathrm{o}(x^{p^r})\mathrm{o}(y^{\mathrm{o}(y)/p^s}) = \frac{\mathrm{o}(x)}{p^r} p^s = \mathrm{o}(x)p^{s-r} > \mathrm{o}(x).$$

This contradicts the maximality of $\mathrm{o}(x)$ in the choice of the element x and thus completes the proof. □

The next result uses the existence claim of Theorem 5.33 to give another characterisation of the exponent of a finite abelian group. It also shows the uniqueness of the first invariant factor of a finite abelian group. In fact, we will use this result in the proof of the uniqueness claim of Theorem 5.33.

Proposition 5.55. *Let G be a finite abelian group. Then the first invariant factor n_1 of G is equal to $e(G)$.*

Proof. On the one hand, since G contains an element of order n_1, Lemma 5.54 implies that n_1 divides $e(G)$. On the other hand, for any element

$$(a_1, a_2, \ldots, a_s) \in \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

one has

$$n_1(a_1, a_2, \ldots, a_s) = (n_1 a_1, \frac{n_1}{n_2} n_2 a_s, \ldots, \frac{n_1}{n_s} n_s a_s) = (0, \frac{n_1}{n_2} 0, \ldots, \frac{n_1}{n_s} 0) = (0, 0, \ldots, 0), \tag{45}$$

because n_1 is divisible by every other invariant factor n_j of G.

Now (45) implies that $g^{n_1} = 1$ for every $g \in G$. Therefore $e(G) \leq n_1$. We conclude that $n_1 = e(G)$, as required. □

Lemma 5.56. *Let G be a finite abelian group. Fix an element x in G of maximal order $\mathrm{o}(x) = e(G)$. Fix $y \in G$ and consider the left coset $y\langle x \rangle \in G/\langle x \rangle$. Then there exists $z \in y\langle x \rangle$ with the property that $\mathrm{o}(z) = \mathrm{o}(y\langle x \rangle)$.*

Proof. We have

$$y^{\mathrm{o}(y\langle x \rangle)}\langle x \rangle = (y\langle x \rangle)^{\mathrm{o}(y\langle x \rangle)} = \langle x \rangle,$$

so $y^{\mathrm{o}(y\langle x \rangle)}$ belongs to $\langle x \rangle$ and there exists $r \in \mathbb{Z}$ such that

$$y^{\mathrm{o}(y\langle x \rangle)} = x^r. \tag{46}$$

Of course one always has $(y\langle x\rangle)^{\mathrm{o}(y)} = \langle x\rangle$ so $\mathrm{o}(y\langle x\rangle)$ divides $\mathrm{o}(y)$ and therefore

$$\frac{\mathrm{o}(y)}{\mathrm{o}(y\langle x\rangle)} = \frac{\mathrm{o}(y)}{(\mathrm{o}(y), \mathrm{o}(y\langle x\rangle)} = \mathrm{o}(y^{\mathrm{o}(y\langle x\rangle)}) = \mathrm{o}(x^r) = \frac{e(G)}{(e(G), r)}.$$

We get that

$$(e(G), r) = \mathrm{o}(y\langle x\rangle)\frac{e(G)}{\mathrm{o}(y)}$$

so Lemma 5.54 implies that $\mathrm{o}(y\langle x\rangle)$ divides $(e(G), r)$, and in particular divides r. We may and will then fix $s \in \mathbb{Z}$ for which

$$r = s\mathrm{o}(y\langle x\rangle). \tag{47}$$

We now set $z := yx^{-s} \in y\langle x\rangle$. We must prove that $\mathrm{o}(z) = \mathrm{o}(y\langle x\rangle)$.

On the one hand, since G is abelian, we have

$$z^{\mathrm{o}(y\langle x\rangle)} = y^{\mathrm{o}(y\langle x\rangle)}x^{-s\mathrm{o}(y\langle x\rangle)} = y^{\mathrm{o}(y\langle x\rangle)}x^{-r} = 1,$$

where we have used both (47) and (46). Thus $\mathrm{o}(z)$ divides $\mathrm{o}(y\langle x\rangle)$.

On the other hand $(z\langle x\rangle)^{\mathrm{o}(z)} = \langle x\rangle$ so $\mathrm{o}(z)$ divides $\mathrm{o}(z\langle x\rangle) = \mathrm{o}(y\langle x\rangle)$ (here we have used that z is chosen to belong to the same left coset of $\langle x\rangle$ as y). This completes the proof. □

5.2.3. *The proof of Theorem 5.33.* In this section we prove the Fundamental Theorem of finite abelian groups, through its formulation in Theorem 5.33. Recall that, by Exercise 5.38, one then also obtains a proof of Theorem 5.38.

We prove the existence of the claimed decomposition by induction on $|G|$. We will later prove the uniqueness claim of Theorem 5.33.

If $|G| = 1$ then certainly G has isomorphism class C_1, which gives the claimed decomposition with $s = 1$ and $n_1 = 1$.

We now assume that $|G| > 1$ and that the existence claim of Theorem 5.33 is valid for every finite abelian group of order strictly less than $|G|$. We fix $z_1 \in G$ with maximal order $\mathrm{o}(z_1) = n_1 := e(G)$ and we set $H_1 := \langle z_1\rangle$.

The quotient group G/H_1 is abelian and has order $|G|/n_1 < |G|$. By the inductive hypothesis there exists $r \in \mathbb{N}$ and a sequence of integers $m_j \geq 2$ with the property that $m_{j+1} \mid m_j$ for all $1 \leq j \leq r-1$ and that G/H_1 has isomorphism class

$$C_{m_1} \times C_{m_2} \times \ldots \times C_{m_r}.$$

For notational simplicity we set $s := r + 1$ and $n_j := m_{j-1}$ for every $2 \leq j \leq r$. Then we have a sequence of integers $n_2, n_3, \ldots, n_s$, all greater than or equal to 2, all dividing the previous one, with the property that G/H_1 has isomorphism class

$$C_{n_2} \times C_{n_3} \times \ldots \times C_{n_s}.$$

We fix an isomorphism

$$f : G/H_1 :\to \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_3\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}.$$

For each $2 \leq j \leq s$ we set

$$u_j := (0, 0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{Z}/n_2\mathbb{Z}\times\mathbb{Z}/n_3\mathbb{Z}\times\ldots\mathbb{Z}/n_{j-1}\mathbb{Z}\times\mathbb{Z}/n_j\mathbb{Z}\times\mathbb{Z}/n_{j+1}\mathbb{Z}\times\ldots\times\mathbb{Z}/n_s\mathbb{Z}.$$

Then $\mathrm{o}(f^{-1}(u_j)) = \mathrm{o}(u_j) = n_j$ and, by Lemma 5.56, there is

$$z_j \in f^{-1}(u_j) \tag{48}$$

with the property that $\mathrm{o}(z_j) = n_j$.

For each $2 \le j \le s$ we set $H_j := \langle z_j \rangle$ and then also $K := H_2 \dots H_s$, which is a subgroup of G by Remark 5.10. We write ι_K for the inclusion $K \subseteq G$ and $\pi_{H_1} : G \to G/H_1$ for the projection map. We require the following intermediate result.

Lemma 5.57. *The composition*

$$(\pi_{H_1} \circ \iota_K) : K \to G/H_1$$

is surjective. In particular $|G/H_1| \le |K|$ *and* $|G/H_1| = |\operatorname{im}(\pi_{H_1} \circ \iota_K)| = |KH_1/H_1|$.

Proof. Fix a left coset xH_1 in G/H_1. Then for $2 \le j \le s$ there are integers a_j with the property that

$$\begin{aligned} xH_1 =& f^{-1}(([a_2]_{n_2}, \dots, [a_s]_{n_s})) \\ =& f^{-1}(\sum_{j=2}^{j=s} a_j u_j) \\ =& \prod_{j=2}^{j=s} f^{-1}(a_j u_j) \\ =& \prod_{j=2}^{j=s} f^{-1}(u_j)^{a_j} \\ =& \prod_{j=2}^{j=s} (z_j H_1)^{a_j} \\ =& (\prod_{j=2}^{j=s} z_j^{a_j}) H_1. \end{aligned}$$

Here the fifth equality holds by (48).

Now $k := \prod_{j=2}^{j=s} z_j^{a_j}$ belongs to K and so we finally get

$$xH_1 = kH_1 = \pi_{H_1}(k) = \pi_{H_1}(\iota_K(k)) = (\pi_{H_1} \circ \iota_K)(k).$$

This completes the proof of the lemma. □

We shall now use Lemma 5.57 to continue with our proof by induction of the existence claim of Theorem 5.33. We have that

$$|K| \le |H_2| \dots |H_s| = n_2 \dots n_s = |G/H_1| \le |K|,$$

with the last equality from Lemma 5.57. But then all the inequalities must be equalities, so we find that

$$|K| = |H_2| \dots |H_s| = |G/H_1|. \tag{49}$$

We wish to apply Theorem 5.12 to prove that

$$K \cong H_2 \times \ldots \times H_s. \tag{50}$$

To do so we only need to fix $2 \leq j \leq s$ and prove that

$$H_j \cap (H_2 \ldots H_{j-1} H_{j-1} \ldots H_s) = \{1\}.$$

But by Proposition 3.49 we have that

$$\begin{aligned} |H_j \cap (H_2 \ldots H_{j-1} H_{j-1} \ldots H_s)| =& \frac{|H_j||H_2 \ldots H_{j-1} H_{j-1} \ldots H_s|}{|H_j H_2 \ldots H_{j-1} H_{j-1} \ldots H_s|} \\ =& \frac{|H_j||H_2 \ldots H_{j-1} H_{j-1} \ldots H_s|}{|K|} \\ \leq& \frac{|H_j||H_2| \ldots |H_{j-1}||H_{j-1}| \ldots |H_s|}{|K|} = 1, \end{aligned}$$

with the last equality by (49). This proves that (50) is valid.

With a view to applying Theorem 5.12 again (or Corollary 5.14), this time to the subgroups H_1 and K, we next claim that

$$H_1 \cap K = \{1\}. \tag{51}$$

This is true because, by the Second Isomorphism Theorem 3.56 we have

$$\frac{|K|}{|H_1 \cap K|} = |KH_1/H_1| = |G/H_1| = |K|,$$

with the second equality by Lemma 5.57 and the third equality by (49).

Since in addition Proposition 3.49 gives

$$|H_1 K| = \frac{|H_1||K|}{|H_1 \cap K|} = |H_1||K| = |H_1||G/H_1| = |G|$$

we must have $H_1 K = G$ and so, applying Corollary 5.14 by keeping (51) in mind, we finally get that $G \cong H_1 \times K$ and therefore, by (50), also that

$$G \cong H_1 \cong H_2 \times \ldots \times H_s.$$

This proves that G has isomorphism class

$$C_{n_1} \times C_{n_2} \times \ldots \times C_{n_s}.$$

To conclude the proof of the existence claim of Theorem 5.33 it is enough to recall that $n_2 = \mathrm{o}(z_2)$ must divide $n_1 = e(G)$ by Lemma 5.54.

We now finally proceed to prove the uniqueness claim of Theorem 5.33. Applying Proposition 5.55 to any two sequences $n_1, n_2, \ldots, n_s$ and $m_1, m_2, \ldots, m_t$ of invariant factors of G we get that

$$n_1 = e(G) = m_1.$$

To now argue by contradiction we assume there is a natural number k with the property that

$$n_1 = m_1,\ n_2 = m_2, \ldots, n_{k-1} = m_{k-1}, n_k \neq m_k.$$

Without loss of generality we may also assume that $n_k > m_k$.

Now since both

$$G' := \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \ldots \times \mathbb{Z}/n_s\mathbb{Z}$$

and

$$G'' := \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \ldots \times \mathbb{Z}/m_t\mathbb{Z}$$

are isomorphic to G, we may fix an isomorphism

$$f : G' \xrightarrow{\sim} G''.$$

We also write

$$\alpha_{m_k} : G' \to G'$$

for the homomorphism given by $\alpha_{m_k}(x) = m_k x$ for $x \in G'$, and

$$\beta_{m_k} : G'' \to G''$$

for the homomorphism given by $\beta_{m_k}(y) = m_k y$ for $y \in G''$.

We claim that

$$f \circ \alpha_{m_k} = \beta_{m_k} \circ f. \tag{52}$$

Indeed for any $x \in G'$ one has

$$f(\alpha_{m_k}(x)) = f(m_k x) = m_k f(x) = \beta_{m_k}(f(x)).$$

Since f is an isomorphism, from (52) we then get that

$$\begin{aligned} |\operatorname{im}(\alpha_{m_k})| &= |f(\operatorname{im}(\alpha_{m_k}))| = |\operatorname{im}(f \circ \alpha_{m_k})| \\ &= |\operatorname{im}(\beta_{m_k} \circ f)| = |\beta_{m_k}(\operatorname{im}(f))| = |\beta_{m_k}(G'')| = |\operatorname{im}(\beta_{m_k})|. \end{aligned} \tag{53}$$

To finally arrive at a contradiction we will compute the order of the images of α_{m_k} and of β_{m_k}. We begin by considering the latter.

We have

$$\operatorname{im}(\beta_{m_k}) = m_k G'' = m_k\mathbb{Z}/m_1\mathbb{Z} \times m_k\mathbb{Z}/m_2\mathbb{Z} \times \ldots \times m_k\mathbb{Z}/m_{k-1}\mathbb{Z},$$

since all additional terms in the direct product G'' become trivial after multiplying by m_k. Recalling that for $1 \leq j \leq k-1$ the Third Isomorphism Theorem 3.58 gives

$$m_k = |\mathbb{Z}/m_k\mathbb{Z}| = \frac{|\mathbb{Z}/m_j\mathbb{Z}|}{|m_k\mathbb{Z}/m_j\mathbb{Z}|} = \frac{m_j}{|m_k\mathbb{Z}/m_j\mathbb{Z}|}$$

we get that

$$|\operatorname{im}(\beta_{m_k})| = \prod_{j=1}^{j=k-1} |m_k\mathbb{Z}/m_j\mathbb{Z}| = \prod_{j=1}^{j=k-1} \frac{m_j}{m_k} = \frac{\prod_{j=1}^{j=k-1} m_j}{m_k^{k-1}}. \tag{54}$$

Similarly we have that the subset

$$S := m_k\mathbb{Z}/n_1\mathbb{Z} \times m_k\mathbb{Z}/n_2\mathbb{Z} \times \ldots \times m_k\mathbb{Z}/n_{k-1}\mathbb{Z} \times \{[0]_{n_k}, [m_k]_{n_k}\}$$

of G' is contained in $\operatorname{im}(\alpha_{m_k})$, and we observe that $[0]_{n_k} \neq [m_k]_{n_k}$ as we have assumed that $m_k < n_k$. By an identical application of the Third Isomorphism Theorem 3.58 to compute the cardinality of the cartesian product S we get that

$$|\operatorname{im}(\alpha_{m_k})| \geq |S| = 2\prod_{j=1}^{j=k-1} |m_k\mathbb{Z}/n_j\mathbb{Z}| = 2\prod_{j=1}^{j=k-1} \frac{n_j}{m_k} = 2\frac{\prod_{j=1}^{j=k-1} n_j}{m_k^{k-1}}. \tag{55}$$

Recalling our choice of k and combining (53), (54) and (55) we finally get that

$$\prod_{j=1}^{j=k-1} n_j = \prod_{j=1}^{j=k-1} m_j = m_k^{k-1}|\operatorname{im}(\beta_{m_k})| = m_k^{k-1}|\operatorname{im}(\alpha_{m_k})| \geq 2\prod_{j=1}^{j=k-1} n_j.$$

Since $\prod_{j=1}^{j=k-1} n_j \geq 1$ for any sequence of invariant factors $n_1, \ldots, n_s$ and any index $k > 1$, we have arrived at the desired contradiction.

We have proved that $n_j = m_j$ for every $1 \leq j \leq \min(s, t)$. Since

$$n_1 \ldots n_s = |G| = m_1 \ldots m_t$$

we must have $s = t$. This completes the proof of the uniqueness claim and therefore also of Theorem 5.33.

5.2.4. *Groups of small order.* For $n \leq 19$ it is easy to list all isomorphism classes of groups of order n, except in the case $n = 16$, which is much more involved.

There are of course five isomorphism classes of *abelian* groups of order 16, namely

$$C_{16},\ C_8 \times C_2,\ C_4 \times C_4,\ C_4 \times C_2 \times C_2,\ C_2 \times C_2 \times C_2 \times C_2.$$

However there are an additional nine isomorphism classes of non-abelian groups of order 16, and fully justifying their classification can get tricky.

We give the complete list of isomorphism classes corresponding to each such $n \neq 16$. We leave, as an exercise for the reader, the proper verification that these lists are indeed complete!

- For $n = 1$ we only have the class C_1.
- For $n = 2$ we only have the class C_2.
- For $n = 3$ we only have the class C_3.
- For $n = 4$ we have the classes C_4 and $C_2 \times C_2$.
- For $n = 5$ we only have the class C_5.
- For $n = 6$ we have the class C_6 and also the class of $S_3 = D_6$.
- For $n = 7$ we only have the class C_7.
- For $n = 8$ we have the classes C_8, $C_4 \times C_2$ and $C_2 \times C_2 \times C_2$ and also the class of D_8 and the class of Q_8.
- For $n = 9$ we only have the classes C_9 and $C_3 \times C_3$.
- For $n = 10$ we have the class C_{10} and also the class of D_{10}.
- For $n = 11$ we only have the class C_{11}.

- For $n = 12$ we have the classes C_{12} and $C_6 \times C_2$ and also the class of A_4, the class of D_{12} and the class of
$$\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z},$$
where the semidirect product is as discussed in Examples 5.25 (v). See also Example 5.58 below for more details.
- For $n = 13$ we only have the class C_{13}.
- For $n = 14$ we have the class C_{14} and also the class of D_{14}.
- For $n = 15$ we only have the class C_{15}.
- For $n = 17$ we only have the class C_{17}.
- For $n = 18$ we have the classes C_{18} and $C_6 \times C_3$ and also the class of D_{18}, the class of $S_3 \times \mathbb{Z}/3\mathbb{Z}$ and the class of
$$(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z},$$
where the semidirect product is as discussed in Examples 5.25 (iv).
- For $n = 19$ we only have the class C_{19}.

Example 5.58. We give a sketch of the method to verify the case $n = 12$. Let G be a group of order 12. Let V be a Sylow 2-subgroup of G and let T be a Sylow 3-subgroup of G. The group V must have isomorphism class C_4 or $C_2 \times C_2$ while the group T must have isomorphism class C_3.

In Example 4.94 we already saw that either V or T must be normal in G. By Lagrange's Theorem we have $V \cap T = \{1\}$ so by Theorem 5.29 we know G is a semidirect product, either of the form $V \rtimes_\rho T$ or of the form $T \rtimes_\rho V$. In fact in Example 4.94 we proved a stronger statement: that either T is normal in G or $G \cong A_4$.

Assume for now that V is normal in G. We must determine all possible homomorphisms $\rho : T \to \mathrm{Aut}(V)$.

If V has isomorphism class C_4 then by [2, Prop. 4.16, p. 135] (or Exercise 2.101), $\mathrm{Aut}(V)$ has order 2, so there is no non-trivial homomorphism ρ. In this case the isomorphism class of G is C_{12} (since $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$).

If instead V has isomorphism class $C_2 \times C_2$ then one can show that $\mathrm{Aut}(V) \cong S_3$. Therefore $\mathrm{Aut}(V)$ has a unique subgroup of order 3. If we fix an element γ of $\mathrm{Aut}(V)$ of order 3 and a generator y of T then the possible homomorphisms $T \to \mathrm{Aut}(V)$ are ρ_j, defined by $\rho_j(y) := \gamma^j$, for each $j = 0, 1, 2$.

As usual ρ_0 is the trivial homomorphism and thus the corresponding semidirect product is actually a direct product with isomorphism class $C_6 \times C_2$ (since $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$). Both ρ_1 and ρ_2 give rise to semidirect products with isomorphism class A_4, as we already know from Example 4.94. It is also easy to prove this directly.

We now instead assume that T is normal in G. We must determine all possible homomorphisms $\rho : V \to \mathrm{Aut}(T)$. Since T has isomorphism class C_3, $\mathrm{Aut}(T)$ has order 2, again by [2, Prop. 4.16, p. 135] (or Exercise 2.101). In fact it is easy to see directly that $\mathrm{Aut}(T) = \{\mathrm{id}, \lambda\}$, where λ inverts the elements of T.

If V has isomorphism class C_4 then, in addition to the trivial homomorphism leading to the isomorphism class C_{12} again, there is one non-trivial homomorphism ρ, mapping any generator x of V to λ. The semidirect product $T \rtimes_\rho V$ corresponding to this homomorphism

ρ is easily seen to be isomorphic to the semidirect product $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ that is discussed in Examples 5.25 (v).

Finally we assume that $V = \langle a \rangle \times \langle b \rangle$ with isomorphism class $C_2 \times C_2$. The trivial homomorphism again leads to the isomorphism class $C_6 \times C_2$. There are three non-trivial homomorphisms $\rho_j : V \to \mathrm{Aut}(T)$ for $j = 1, 2, 3$, determined by the equalities

$$\rho_1(a) = \lambda = \rho_1(b), \quad \rho_2(a) = 1, \ \rho_2(b) = \lambda, \quad \rho_3(a) = \lambda, \ \rho_3(b) = 1.$$

All three of the corresponding semidirect products can be shown to be isomorphic to $D_6 \times \mathbb{Z}/2\mathbb{Z}$, which in turn is isomorphic to D_{12}.

5.3. **(More) Exercises.** Don't forget to think about the exercises given throughout the rest of section 5.

Exercise 5.59. Show that for groups $G_1, G_2, \ldots, G_n$ one has

$$Z(G_1 \times G_2 \times \ldots \times G_n) = Z(G_1) \times Z(G_2) \times \ldots \times Z(G_n).$$

Deduce that a direct product of groups is abelian if and only if each of the factors is abelian.

Exercise 5.60. Let G_1 and G_2 be groups and let p be a prime. Prove that any Sylow p-subgroup of $G_1 \times G_2$ is of the form $P_1 \times P_2$, where P_1 is a Sylow p-subgroup of G_1 and P_2 is a Sylow p-subgroup of G_2. Deduce that $n_p(G_1 \times G_2) = n_p(G_1)n_p(G_2)$. Generalise these statements to the direct product of n groups $G_1, G_2, \ldots, G_n$.

Exercise 5.61. Find a subgroup of $Q_8 \times \mathbb{Z}/4\mathbb{Z}$ that is not normal in $Q_8 \times \mathbb{Z}/4\mathbb{Z}$.

Exercise 5.62. For $n \in \mathbb{N}$ we recall that we write E_{2^n} for the direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \ldots \mathbb{Z}/2\mathbb{Z}$ of n copies of $\mathbb{Z}/2\mathbb{Z}$. Prove that all subgroups of $Q_8 \times E_{2^n}$ are normal.

Exercise 5.63. Let p be a prime and let n be a natural number. Find a formula for the number of subgroups of E_{p^n} that have order p.

Exercise 5.64. Prove that D_{8n} is not isomorphic to $D_{4n} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 5.65. Let F be a field. Let G be the following subgroup of $\mathrm{Gl}_n(F)$:

$$G := \{(a_{ij}) \in \mathrm{Gl}_n(F) : a_{ij} = 0 \text{ for } i > j \text{ and } a_{11} = a_{22} = \ldots = a_{nn}\}.$$

Let D be the following subgroup of $\mathrm{Gl}_n(F)$:

$$D := \{(a_{ij}) \in \mathrm{Gl}_n(F) : a_{ij} = 0 \text{ for } i \neq j \text{ and } a_{11} = a_{22} = \ldots = a_{nn}\}.$$

Let U be the following subgroup of $\mathrm{Gl}_n(F)$:

$$U := \{(a_{ij}) \in \mathrm{Gl}_n(F) : a_{ij} = 0 \text{ for } i > j \text{ and } a_{11} = a_{22} = \ldots = a_{nn} = 1\}.$$

Prove that $G \cong D \times U$.

Exercise 5.66. Give an example of a group G and normal subgroups $H_1, \ldots, H_n$ of G satisfying $G = H_1 \ldots H_n$ and satisfying $H_i \cap H_j = \{1\}$ for every $i \neq j$, for which G is not isomorphic to $H_1 \times \ldots \times H_n$.

In the following exercises we let H and K be groups, we let $\rho : K \to \mathrm{Aut}(H)$ be a homomorphism and we set $G := H \rtimes_\rho K$.

Exercise 5.67. Prove that $C_G(H) \cap K = \ker(\rho)$ and that $C_G(K) \cap H = N_G(K) \cap H$.

Exercise 5.68. Let H be abelian and consider the group $G := H \rtimes \mathbb{Z}/2\mathbb{Z}$ defined in Examples 5.25 (iv). Prove that every element of $G \setminus H$ has order 2. Prove that G is abelian if and only if every non-trivial element of H has order 2.

Exercise 5.69. Assume that K is cyclic, and suppose given two homomorphisms $\rho_1, \rho_2 : K \to \mathrm{Aut}(H)$ that satisfy $\mathrm{im}(\rho_1) = \mathrm{im}(\rho_2)$. Assume also that either K is finite, or both ρ_1 and ρ_2 are injective. Prove that $H \rtimes_{\rho_1} K \cong H \rtimes_{\rho_2} K$.

Exercise 5.70. For each of $n = 10, 576, 1155, 42875, 2704$, determine the number of isomorphism classes of abelian groups of order n.

Exercise 5.71. For each of $n = 270, 9801, 320, 105, 44100$, determine the possible sequences of invariant factors of an abelian group of order n. Determine also the possible sequences of elementary divisors of an abelian group of order n.

Exercise 5.72. In each of the following lists of isomorphism classes of abelian groups, determine how many of the given classes are *distinct*.

(i) $C_4 \times C_9$, $C_6 \times C_6$, $C_8 \times C_3$, $C_9 \times C_4$, $C_6 \times C_4$, C_{64}.
(ii) $C_4 \times C_{18}$, $C_{12} \times C_6$, C_{72}, $C_{36} \times C_2$.
(iii) $C_{5^2.7^2} \times C_{3^2.5.7}$, $C_{3^2.5^2.7} \times C_{5\cdot 7^2}$, $C_{3\cdot 5^2} \times C_{7^2} \times C_{3\cdot 5\cdot 7}$, $C_{5^2.7} \times C_{3^2.5\cdot 7^2}$.
(iv) $C_{2^2\dot{5}\cdot 7} \times C_{2^3.5^3} \times C_{2\cdot 5^2}$, $C_{2^3.5^3.7} \times C_{2^3.5^3}$, $C_{2^2} \times C_{2\cdot 7} \times C_{2^3} \times C_{5^3} \times C_{5^3}$, $C_{2\cdot 5^3} \times C_{2^2.5^3} \times C_{2^3} \times C_7$.

Exercise 5.73. Find a finite group G that has no element of order $e(G)$.

Exercise 5.74. Let p be a prime number and let G be a group with isomorphism class

$$C_{p^{a_1}} \times C_{p^{a_2}} \times \ldots \times C_{p^{a_n}}$$

for natural numbers n and $a_1, \ldots, a_n$. Define the p-th power map

$$f_p : G \to G$$

by setting $f_p(g) := g^p$.

(i) Prove that f_p is a homomorphism.
(ii) Prove that

$$\ker(f_p) \cong E_{p^n} \cong G/\,\mathrm{im}(f_p).$$

Exercise 5.75. Let G be a finite abelian group and let p be a prime. We set

$$G^p := \{g^p : g \in G\} \text{ and } G_p := \{g \in G : g^p = 1\}.$$

(i) Prove that $G/G^p \cong G_p$.
(ii) Prove that the number of subgroups of G that have order p is equal to the number of subgroups of G that have order p.

Exercise 5.76. Let G be a group with isomorphism class $C_{60} \times C_{45} \times C_{12} \times C_{36}$. Find the number of elements of G that have order 2 and the number of subgroups of G that have index 2 in G.

Exercise 5.77. Let Ω be a finite set of cardinality $n \in \mathbb{N}$. Let $(\mathcal{P}(\Omega), \star)$ be the abelian group considered in Exercise 1.85. Determine the sequence of invariant factors of this group.

Exercise 5.78. Show that S_9 does not contain an abelian subgroup of order 21.

Exercise 5.79. Prove that the groups D_{16}, $D_8 \times \mathbb{Z}/2\mathbb{Z}$, $Q_8 \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$, with the semidirect product as in Examples 5.25 (v), are pairwise non-isomorphic.

References

[1] J. Dorronsoro, E. Hernández, Números, grupos y anillos, Addison-Wesley Iberoamericana-UAM 2006.
[2] D. S. Dummit, R. M. Foote, Abstract Algebra, 3rd Edition, Wiley 2003.

Universidad Autónoma de Madrid, Madrid 28049, Spain
E-mail address: daniel.macias@uam.es