

2 Groups

The concept of a group was first formalized by Cayley (1821–95) around 1854, but many mathematicians computed with group-like structures before that. In fact one of the main results in introductory group theory (see Theorem 2.2.8 below) was already known to Lagrange (1736–1813) in 1771. At this point we need to introduce groups in order to have a language that makes life easier. Dealing with numbers, we have encountered group-like structures several times already. By introducing the basic notions of group theory we get very simple (and nice) proofs of Euler’s and Fermat’s theorems on congruences (Theorem 1.7.2 and Corollary 1.9.2). By some mystery you are able to do much more powerful mathematics by introducing the three simple axioms defining a group. One point is worth singling out in this chapter: you will increase your level of abstraction from computing with elements in a set to computing with subsets of a set. In fact group theory puts the theory of congruences in a natural context and it will make sense to add and multiply subsets of \mathbb{Z} consisting of numbers with the same remainder with respect to a positive integer. Groups are also useful outside the world of numbers. Using symmetric and alternating groups we will give a complete treatment of the 15-puzzle invented by Sam Loyd in 1878. Loyd offered a 1000-dollar prize for a correct solution. You can understand why this puzzle usually drives people nuts by reading subsection 2.9.5.

At the end of the chapter we treat actions of groups on sets. This is an extremely useful notion. We will apply actions of groups to combinatorics and counting and in the proof of the celebrated Sylow theorems.

2.1 Definition

A *composition* on a set G is a map $\circ : G \times G \rightarrow G$. The composition $\circ(g, h)$ is often written $g \circ h$ or gh .

Definition 2.1.1 A pair (G, \circ) consisting of a set G and a composition $\circ : G \times G \rightarrow G$ is called a *group* if it satisfies the following three properties.

(i) The composition is *associative*:

$$s_1 \circ (s_2 \circ s_3) = (s_1 \circ s_2) \circ s_3$$

for every $s_1, s_2, s_3 \in G$.

(ii) There is a *neutral* element $e \in G$ such that

$$e \circ s = s \quad \text{and} \quad s \circ e = s$$

for every $s \in G$.

(iii) For every $s \in G$ there is an *inverse* element $t \in G$ such that

$$s \circ t = e \quad \text{and} \quad t \circ s = e.$$

A group G is called *abelian* if $x \circ y = y \circ x$ for every $x, y \in G$. The number of elements $|G|$ in G is called the *order* of G .

The first few examples of groups arise in the world of numbers. The set of natural numbers $(\mathbb{N}, +)$ with the composition $+$ is not a group, since the neutral element would have to be 0, but then 1, for example, would not have an inverse element (there would not exist $x \in \mathbb{N}$ such that $x + 1 = 0$). This defect is repaired by introducing the set of integers \mathbb{Z} , which is an abelian group with the composition $+$. The rational numbers $(\mathbb{Q}, +)$ and the real numbers $(\mathbb{R}, +)$ are also abelian groups. The sets of non-zero rational numbers $(\mathbb{Q} \setminus \{0\}, \cdot)$ and non-zero real numbers $(\mathbb{R} \setminus \{0\}, \cdot)$ are abelian groups with multiplication as composition.

The axioms defining a group resemble the rules of chess. You can learn them in a few minutes. To become a skilled player, however, you need to see lots of examples of groups in many contexts. You have little or no insight in the concept of a group by just knowing (i)–(iii) above. The first question to ask is, why do we introduce this abstraction? To begin with let us see how congruences fit into this framework.

2.1.1 Groups and congruences

A group is a vast generalization of the integers \mathbb{Z} with $+$. The advantage of working with \mathbb{Z} instead of \mathbb{N} is that every number $x \in \mathbb{Z}$ has an inverse $y = -x$, so that $x + y = 0$. In this context 0 is a neutral element for $+$, in that $x + 0 = x$ for every $x \in \mathbb{Z}$. One very important property is associativity, as mentioned above. This concept arises as an attempt to give meaning to the

expression $x + y + z$, where $x, y, z \in \mathbb{Z}$. This expression only makes sense when we insert parentheses, to give $(x + y) + z$ or $x + (y + z)$, because $+$ is a map $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$. Associativity states that $(x + y) + z = x + (y + z)$ – it does not matter how you insert the parentheses.

Granting that \mathbb{Z} is a group with the composition $+$, let us see how to build some new groups tied up with congruence modulo an integer. We will define addition, $+$, on subsets of \mathbb{Z} given by $a + n\mathbb{Z} = \{a + nx \mid x \in \mathbb{Z}\}$, where $a, n \in \mathbb{Z}$. As an example we have

$$2 + 5\mathbb{Z} = \{\dots, -8, -3, 2, 7, \dots\}.$$

When working with numbers it was easy to spot when two elements were identical. Now, we will work with subsets. Two subsets are identical when they contain the same elements. You may check for example that $5 + 7\mathbb{Z} = 19 + 7\mathbb{Z}$. This is a special case of the following proposition.

Proposition 2.1.2 *Let $a, b, c \in \mathbb{Z}$. Then $a + c\mathbb{Z} = b + c\mathbb{Z}$ if and only if $a \equiv b \pmod{c}$. Also $(a + c\mathbb{Z}) \cap (b + c\mathbb{Z}) = \emptyset$ if and only if $a \not\equiv b \pmod{c}$.*

Proof. If $m \in a + c\mathbb{Z}$ then $m = a + cx$, where $x \in \mathbb{Z}$. If $a + c\mathbb{Z} = b + c\mathbb{Z}$ then $m \in b + c\mathbb{Z}$. This shows that $m = a + cx = b + cy$ for $y \in \mathbb{Z}$. Therefore $a - b = c(y - x)$ and $a \equiv b \pmod{c}$. However, if $a \equiv b \pmod{c}$ then $a = b + cx$ for $x \in \mathbb{Z}$. Therefore $a + c\mathbb{Z} = b + cx + c\mathbb{Z} = b + c\mathbb{Z}$, since $cx + c\mathbb{Z} = c\mathbb{Z}$. If $(a + c\mathbb{Z}) \cap (b + c\mathbb{Z}) \neq \emptyset$, then we may find $m, x, y \in \mathbb{Z}$ such that $m = a + cx = b + cy$. This gives $a - b = c(y - x)$ and therefore $a \equiv b \pmod{c}$. This proves that if $(a + c\mathbb{Z}) \cap (b + c\mathbb{Z}) \neq \emptyset$ then $a + c\mathbb{Z} = b + c\mathbb{Z}$. \square

If $c > 0$ we have $a + c\mathbb{Z} = b + c\mathbb{Z}$ if and only if $[a]_c = [b]_c$, by Proposition 1.3.2(i). In this context we let $[x]$ denote the subset $x + c\mathbb{Z}$. Then $[x] = [[x]_c]$, so there can be only finitely many different subsets of the form $[x]$. These are given by the remainders $[0], [1], \dots, [c - 1]$ after division by c . Denote the set of these subsets by $\mathbb{Z}/c\mathbb{Z}$.

Example 2.1.3 Let $c = 3$. Then $\mathbb{Z}/3\mathbb{Z} = \{[0], [1], [2]\}$, where

$$[0] = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1] = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2] = \{\dots, -4, -1, 2, 5, 8, \dots\}.$$

Armed with these definitions we can add subsets $[x], [y] \in \mathbb{Z}/c\mathbb{Z}$ simply by defining $[x] + [y] = [x + y]$.

Notice the problem here! We need to check that if $[x] = [x']$ and $[y] = [y']$ then $[x + y] = [x' + y']$. But we have already done that in Proposition 1.3.4(i), where we proved that $x \equiv x' \pmod{c}$ and $y \equiv y' \pmod{c}$ implies that $x + y \equiv x' + y' \pmod{c}$. So by Proposition 2.1.2, the composition $+$ is well defined. Make sure you understand that there really is something to be checked here.

With the composition $+$ constructed in this way, $(\mathbb{Z}/c\mathbb{Z}, +)$ is a group of order c . The neutral element is the subset $[0] = c\mathbb{Z}$. The inverse element of $[x]$ is $[-x]$, and associativity holds because

$$\begin{aligned} ([x] + [y]) + [z] &= [x + y] + [z] = [(x + y) + z] = [x + (y + z)] \\ &= [x] + [y + z] = [x] + ([y] + [z]) \end{aligned}$$

for $[x], [y], [z] \in \mathbb{Z}/c\mathbb{Z}$. Here we have used the fact that associativity holds in $(\mathbb{Z}, +)$. The group $(\mathbb{Z}/c\mathbb{Z}, +)$ is abelian since $[x] + [y] = [x + y] = [y + x] = [y] + [x]$ for every $[x], [y] \in \mathbb{Z}/c\mathbb{Z}$. If $c = 0$ then $x + c\mathbb{Z} = \{x\}$ and we simply recover $(\mathbb{Z}, +)$ as the group $(\mathbb{Z}/0\mathbb{Z}, +)$.

2.1.2 The composition table

Definition 2.1.4 When dealing with a finite group $(\{e, g_1, \dots, g_r\}, \circ)$, the composition \circ is often displayed in a *composition table*:

\circ	e	g_1	\cdots	g_j	\cdots	g_r
e	e	g_1	\cdots	g_j	\cdots	g_r
g_1	g_1	$g_1 \circ g_1$	\cdots	$g_1 \circ g_j$	\cdots	$g_1 \circ g_r$
\vdots	\vdots	\vdots	\ddots	\vdots	\ddots	\vdots
g_i	g_i	$g_i \circ g_1$	\cdots	$g_i \circ g_j$	\cdots	$g_i \circ g_r$
\vdots	\vdots	\vdots	\ddots	\vdots	\ddots	\vdots
g_r	g_r	$g_r \circ g_1$	\cdots	$g_r \circ g_j$	\cdots	$g_r \circ g_r$

Example 2.1.5 The composition table for the finite group $(\mathbb{Z}/4\mathbb{Z}, +)$ with elements $[0], [1], [2], [3]$ is

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

2.1.3 Associativity

Suppose that S is a set with a composition $S \times S \rightarrow S$, where (x, y) maps to xy . Assume that $x(yz) = (xy)z$ for every $x, y, z \in S$ (the composition is associative). Writing an expression like $s_1s_2s_3$ for $s_1, s_2, s_3 \in S$ is clearly nonsense, since the composition is only defined given two elements from S . We can make sense of it by (1) first evaluating s_1s_2 and then composing with s_3 or (2) first evaluating s_2s_3 and then composing with s_1 (from the left). Associativity says that these two ways of evaluating give the same result. Similarly, for four elements s_1, s_2, s_3, s_4 of a group, we have five ways of evaluating $s_1s_2s_3s_4$:

$$\begin{aligned}s_1(s_2(s_3s_4)), \\ s_1((s_2s_3)s_4), \\ (s_1(s_2s_3))s_4, \\ ((s_1s_2)s_3)s_4, \\ (s_1s_2)(s_3s_4).\end{aligned}$$

You can use associativity to prove that these five different ways of evaluating $s_1s_2s_3s_4$ all give the same result. There are 4862 ways¹ of evaluating the product $s_1s_2 \cdots s_{10}$ of 10 elements. Associativity still proves that these are all the same. One can prove, using associativity, that any two ways of evaluating a product $s_1s_2 \cdots s_n$ lead to the same result.

In general it is difficult to decide whether a composition on a set is associative. There is one exceedingly important case for which we have an associative composition. This is the case where S is the set of maps from a set X to itself and the composition is the usual composition of maps, in which fg is defined by $(fg)(x) = f(g(x))$ for $f, g \in S$ and $x \in X$. In this case $f(gh) = (fg)h$, since $(f(gh))(x)$ and $((fg)h)(x)$ are identical for every $x \in X$:

$$\begin{aligned}(f(gh))(x) &= f((gh)(x)) = f(g(h(x))), \\ ((fg)h)(x) &= (fg)(h(x)) = f(g(h(x))).\end{aligned}$$

2.1.4 The first non-abelian group

To show the wide application of groups, we give an example of a non-abelian group with six elements. You should keep referring to this example

¹ Computing the number of ways C_{n-1} of evaluating the product of n elements $s_1s_2 \cdots s_n$ by inserting parentheses is a classical problem of combinatorics, referred to as Catalan's problem. One may prove that

$$C_n = \frac{1}{n+1} \binom{2n}{n}.$$

when new concepts are introduced. It contains all the ingredients of a good understanding.

Example 2.1.6 Let $X = \{1, 2, 3\}$ be a set consisting of three elements. Let G be the set of all bijective maps $X \rightarrow X$. Then G is a group with the usual composition of maps as composition (see the previous subsection). The neutral element e is the identity map $X \rightarrow X$. The element inverse to a given map $f : X \rightarrow X$ is the inverse map $f^{-1} : X \rightarrow X$, and the composition of maps is associative (we saw this in subsection 2.1.3). We can list the elements of G as follows:

$$\begin{aligned} e &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & a &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, & b &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \\ c &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, & d &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, & f &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}. \end{aligned}$$

where for example $c : X \rightarrow X$ is the bijective map given by $c(1) = 3$, $c(2) = 2$, $c(3) = 1$. To compute ab you simply find what the map $a \circ b$ does to 1, 2, 3. Now $ab(1) = a(b(1)) = 2$, $ab(2) = a(b(2)) = 3$ and $ab(3) = a(b(3)) = 1$. This shows that $ab = f$. The composition table (see subsection 2.1.2) is constructed using this reasoning.

\circ	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	d	e	f	a	c
c	c	f	d	e	b	a
d	d	b	c	a	f	e
f	f	c	a	b	e	d

The group G is also known as the symmetric group S_3 . It is non-abelian since $ab \neq ba$.

2.1.5 Uniqueness of neutral and inverse elements

There can be only one neutral element in a group G . If $e' \in G$ were another then $e = e'e = e'$ by Definition 2.1.1(ii). Also, to every $g \in G$ there can be only one inverse element, h . Suppose that h' is an element satisfying $gh' = e$. Then $e = hg$ implies that $h' = (hg)h' = h(gh') = he = h$ by Definition 2.1.1 (iii).

Definition 2.1.7 Let $g \in G$ be an element of a group. Then we let $g^{-1} \in G$ denote the unique inverse element of g .

Example 2.1.8 Finding the inverse element of a product ab in a group is similar to inverting a product of invertible matrices. In fact,

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a(ea^{-1}) = aa^{-1} = e$$

shows that $(ab)^{-1} = b^{-1}a^{-1}$. The computation for $(b^{-1}a^{-1})(ab)$ is similar.

2.1.6 Multiplication by $g \in G$ is bijective

Suppose that G is a group and $g \in G$. Then there is a map $\varphi : G \rightarrow G$ given by $\varphi(x) = gx$. This map is bijective. We can prove this by giving the inverse map $\psi : G \rightarrow G$ to φ . Consider the map $\psi(x) = g^{-1}x$ from G to G . Then $\psi(\varphi(x)) = g^{-1}(gx) = (g^{-1}g)x = ex = x$ and $\varphi(\psi(x)) = g(g^{-1}x) = (gg^{-1})x = ex = x$. This proves that ψ is the inverse map of φ and therefore that φ is a bijection. Notice how all the properties of the group composition in Section 2.1.1 come into play.

In the same way one can prove that the map $\xi : G \rightarrow G$ given by $\xi(x) = xg$ is a bijection (see Exercise 2.1).

Example 2.1.9 What does a group G of order three look like? There must be a (unique) neutral element $e \in G$ and two other elements $a, b \in G$. To describe the composition $\circ : G \times G \rightarrow G$ we fill out the composition table:

\circ	e	a	b
e	$e \circ e$	$e \circ a$	$e \circ b$
a	$a \circ e$	$a \circ a$	$a \circ b$
b	$b \circ e$	$b \circ a$	$b \circ b$

We know that $e \circ a = a \circ e = a$ and $e \circ b = b \circ e = b$. This gives us the partial table

\circ	e	a	b
e	e	a	b
a	a		
b	b		

An important point is that an element in a group can only occur once in a row (or a column) of the composition table. The reason is that multiplication by a group element is bijective. Using this fact, there is only one way to complete the table:

\circ	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

We have proved that there is only one way of filling out the composition table for a group of order three (the same holds for any prime number. We will prove this in Proposition 2.7.2).

2.1.7 More examples of groups

The only way to understand the concept of a group is to study its many incarnations. We give some more important examples in this subsection.

Example 2.1.10 Using matrices we will give an example of an infinite non-abelian group. Let

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

denote the set of 2×2 matrices with real entries and non-zero determinant. The multiplication of matrices gives a composition on $\mathrm{GL}_2(\mathbb{R})$ as $\det(AB) = \det(A)\det(B)$ for $A, B \in \mathrm{GL}_2(\mathbb{R})$. One may check that it is associative by explicit computation (or identify matrix multiplication with the composition of linear maps). The identity matrix is the neutral element in $\mathrm{GL}_2(\mathbb{R})$ and the inverse matrix A^{-1} is the inverse element of $A \in \mathrm{GL}_2(\mathbb{R})$; recall that $\det(A^{-1}) = \det(A)^{-1}$. This group is called the general linear group, or more precisely the 2×2 general linear group. It is a non-abelian group (can you find $A, B \in \mathrm{GL}_2(\mathbb{R})$ such that $AB \neq BA$?).

Example 2.1.11 Recall that the transpose of a 2×2 matrix is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

A matrix $A \in \mathrm{GL}_2(\mathbb{R})$ is called orthogonal if $AA^t = I$, where I is the identity matrix. The set of 2×2 orthogonal matrices is denoted $O_2(\mathbb{R})$. Matrix multiplication is in fact a composition on $O_2(\mathbb{R})$. This follows from the identity $(AB)^t = B^t A^t$ for $A, B \in O_2(\mathbb{R})$. Since $(A^{-1})^t = (A^t)^{-1}$, $O_2(\mathbb{R})$ is a group with matrix multiplication as composition. It is called the orthogonal group (or more precisely the 2×2 orthogonal group).

Example 2.1.12 An isometry of the plane \mathbb{R}^2 is a map $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ preserving the Euclidean distance between any two points in \mathbb{R}^2 :

$$|\varphi(x) - \varphi(y)| = |x - y|$$

for every $x, y \in \mathbb{R}^2$. One can prove that an isometry fixing the origin $(0, 0)$ is a linear invertible map (see Exercise 2.8). We call such an isometry linear. The set L of linear isometries of \mathbb{R}^2 is a group with respect to the usual composition of maps. Let us prove this in detail. First we need to see that the composition $\varphi_1 \circ \varphi_2$ of two linear isometries $\varphi_1, \varphi_2 \in L$ is again a linear isometry. This is to make sure that \circ really is a composition on L . Given $x, y \in \mathbb{R}^2$,

$$|\varphi_1(\varphi_2(x)) - \varphi_1(\varphi_2(y))| = |\varphi_2(x) - \varphi_2(y)| = |x - y|.$$

This proves that $\varphi_1 \circ \varphi_2$ is an isometry. Since $\varphi_1(\varphi_2((0, 0))) = \varphi_1((0, 0)) = (0, 0)$, it must be linear. The neutral element in L with respect to \circ is the identity map. Also, if $\varphi \in L$ then $\varphi^{-1} \in L$ (we know that φ is bijective): we need to prove that

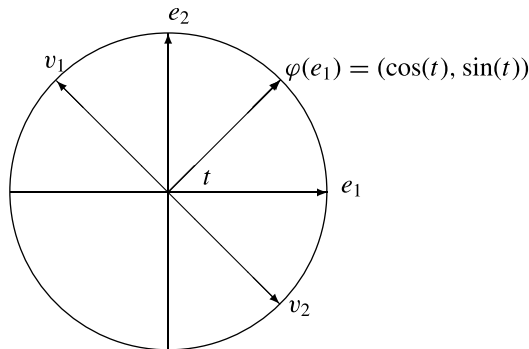
$$|\varphi^{-1}(x) - \varphi^{-1}(y)| = |x - y|$$

for every $x, y \in \mathbb{R}^2$. But since φ is surjective we can find $x', y' \in \mathbb{R}^2$ such that $x = \varphi(x')$ and $y = \varphi(y')$. Therefore

$$|\varphi^{-1}(x) - \varphi^{-1}(y)| = |x' - y'| = |\varphi(x') - \varphi(y')| = |x - y|.$$

This shows that $\varphi^{-1} \in L$. We know from subsection 2.1.3 that the composition of maps is associative. Therefore \circ is associative on L . In total we have proved that (L, \circ) really is a group. But what are the maps in L ? Let us compute the matrix of a linear isometry $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ in the standard basis $e_1 = (1, 0)$ and $e_2 = (0, 1)$ of \mathbb{R}^2 .

We know that $|\varphi(e_1)| = |\varphi(e_1) - \varphi((0, 0))| = |e_1| = 1$. This implies that $\varphi(e_1) = (\cos(t), \sin(t))$ for $t \in \mathbb{R}$. However, since $|e_1 - e_2| = |(1, -1)| = \sqrt{2}$, we get $|(\cos(t), \sin(t)) - \varphi(e_2)| = \sqrt{2}$. This gives $\varphi(e_2) = (-\sin(t), \cos(t)) = v_1$ or $\varphi(e_2) = (\sin(t), -\cos(t)) = v_2$, as seen in the following diagram:



So, given a linear isometry φ we have two possibilities for its matrix when $\varphi(e_1)$ is determined by $\varphi(e_1) = (\cos(t), \sin(t))$. The first is represented by the matrix

$$\begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix};$$

this corresponds to a rotation. The second one is given by the matrix

$$\begin{pmatrix} \cos(t) & \sin(t) \\ \sin(t) & -\cos(t) \end{pmatrix};$$

this corresponds to a reflection in the line $L = \{(r \cos(t/2), r \sin(t/2)) \mid r \in \mathbb{R}\}$.

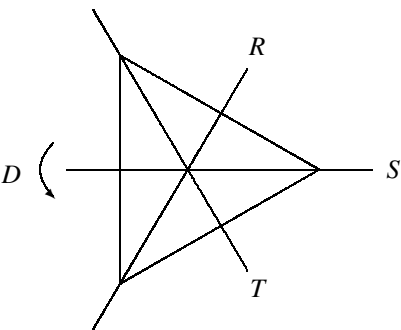
We have demystified the “complicated” term linear isometry and proved that we are dealing with rotations and reflections of the plane. Since L is a group the composition of a rotation and a reflection must be a reflection or a rotation. Which one is it?

If you prefer a more algebraic way of looking at the group L , you may prove that matrices of linear isometries are orthogonal (see Example 2.1.11). In fact, as we will see later, in Example 2.4.7, L is, in a specific sense, the same group as $O_2(\mathbb{R})$ from Example 2.1.11.

Example 2.1.13 Consider the subset $G \subset L$ of linear isometries (see Example 2.1.12) of \mathbb{R}^2 mapping an equilateral triangle K centered at $(0, 0)$ to itself. Thus

$$G = \{\varphi \in L \mid \varphi(K) = K\}.$$

Let us check that G is a group with respect to the composition of maps. First (as in Example 2.1.12) we need to check that $\varphi_1 \circ \varphi_2 \in G$ when $\varphi_1, \varphi_2 \in G$. This is definitely true, since $\varphi_1(\varphi_2(K)) = \varphi_1(K) = K$ when $\varphi_1, \varphi_2 \in G$. The identity map is the neutral element in G . If $\varphi \in G$, we need to prove that $\varphi^{-1} \in G$. This also holds, since $\varphi^{-1}(K) = \varphi^{-1}(\varphi(K)) = K$. Again, we know from subsection 2.1.3 that composition of maps is associative. Therefore \circ is an associative composition, just as in Example 2.1.12. We have proved that (G, \circ) is a group. What are the maps in G ? These are the rotations and reflections preserving the equilateral triangle.



The only reflections preserving K are the reflections in the lines R , S and T above. The only rotations preserving K are I , D , D^2 , where I is the identity map, D is a rotation of $2\pi/3$ (depicted above) and $E = D^2$ is a rotation of $4\pi/3$. Now it follows that

$$G = \{I, R, S, T, D, E\}$$

and that this finite subset of L really is a group. The composition table can be written down through explicit sketching:

\circ	I	R	S	T	D	E
I	I	R	S	T	D	E
R	R	I	D	E	S	T
S	S	E	I	D	T	R
T	T	D	E	I	R	S
D	D	T	R	S	E	I
E	E	S	T	R	I	D

Usually G is denoted D_3 and called the dihedral group of order 6. We will see later, in Example 2.4.6, that it is in a specific sense the same group as the group S_3 from Example 2.1.6 .

2.2 Subgroups and cosets

In Example 2.1.12 we saw an example of a group L containing a subset G that is a group with respect to the composition of L . Again in Example 2.1.11, the subset $O_2(\mathbb{R})$ of $GL_2(\mathbb{R})$ turned out to be a group with respect to the composition of $GL_2(\mathbb{R})$. This leads us to the concept of a subgroup.

Definition 2.2.1 A *subgroup* of a group G is a non-empty subset $H \subseteq G$ such that the composition of G makes H into a group, i.e. H is a subgroup of G if and only if

- (i) $e \in H$,
- (ii) $x^{-1} \in H$ for every $x \in H$,
- (iii) $xy \in H$ for every $x, y \in H$.

If you revisit Example 2.1.13, you will see that we actually proved there that G is a subgroup of L , by verifying steps (i)–(iii) above.

Example 2.2.2 Returning to the group S_3 from Example 2.1.6, you can check that the two subsets $\{e, a\}$ and $\{e, f, d\}$ are subgroups by looking at the composition table for S_3 .

2.2.1 Subgroups of \mathbb{Z}

We know that $(\mathbb{Z}, +)$ is a group. In the language of groups, division with remainder (Theorem 1.2.1) has a very pretty consequence.

Proposition 2.2.3 Let H be a subgroup of $(\mathbb{Z}, +)$. Then

$$H = d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\} = \{\dots, -2d, -d, 0, d, 2d, \dots\}$$

for a unique natural number $d \in \mathbb{N}$.

Proof. If $H = \{0\}$ we may put $d = 0$. Assume that $H \neq \{0\}$. Then $\mathbb{N} \cap H$ contains a smallest natural number $d > 0$ (why?). We claim that $H = d\mathbb{Z}$. It follows that $-d \in H$, since $d \in H$ and H is a subgroup. Again using that H is a subgroup, we get $-d + (-d) = -2d \in H$ and $d + d = 2d \in H$, $-2d + (-d) = -3d \in H$ and $2d + d = 3d, \dots$. This shows that $nd \in H$ for every $n \in \mathbb{Z}$. Therefore $d\mathbb{Z} \subseteq H$.

Now let $m \in H$. Division with remainder gives $m = qd + r$, where $0 \leq r < d$. Since H is a subgroup, $m \in H$ and $d \in H$, we get $-qd \in H$ and $r = m - qd \in H$. But $r \geq 0$ is a natural number $< d$ in H . This means that $r = 0$, so that $m = qd$ and $H \subseteq d\mathbb{Z}$. Therefore $H = d\mathbb{Z}$. \square

2.2.2 Cosets

Let H be a subgroup of G and $g \in G$. Then the subset

$$gH = \{gh \mid h \in H\} \subseteq G$$

is called a *left coset* of H . Similarly we call the subset

$$Hg = \{hg \mid h \in H\} \subseteq G$$

a *right coset* of H . The set of left cosets of H is denoted G/H . The set of right cosets of H is denoted $H \backslash G$.

Example 2.2.4 If $G = (\mathbb{Z}, +)$ and $H = 3\mathbb{Z}$ then

$$\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}.$$

Notice that $1 + 3\mathbb{Z} = 4 + 3\mathbb{Z}$. This illustrates the fact that you can have different ways of representing the same left coset: if H is a subgroup of G and $g_1H = g_2H$ then g_1 and g_2 are not necessarily equal.

Example 2.2.5 Let H denote the subgroup $\{e, a\}$ of the group S_3 from Example 2.1.6. Let us list all the left and right cosets of H just using the definitions. First the left cosets:

$$eH = \{ee, ea\} = \{e, a\},$$

$$aH = \{ae, aa\} = \{a, e\},$$

$$bH = \{be, ba\} = \{b, d\},$$

$$cH = \{ce, ca\} = \{c, f\},$$

$$dH = \{de, da\} = \{d, b\},$$

$$fH = \{fe, fa\} = \{f, c\}.$$

We can already spot some interesting phenomena. It seems that left cosets are either equal or disjoint. Also, $eH = aH$, $bH = dH$ and $cH = fH$. This means that $G/H = \{H, bH, cH\}$. Let us carry out the same computations for the right cosets:

$$He = \{ee, ae\} = \{e, a\},$$

$$Ha = \{ea, aa\} = \{a, e\},$$

$$Hb = \{eb, ab\} = \{b, f\},$$

$$Hc = \{ec, ac\} = \{c, d\},$$

$$Hd = \{ed, ad\} = \{d, c\},$$

$$Hf = \{ef, af\} = \{f, b\}.$$

Here we have $He = Ha$, $Hb = Hf$ and $Hc = Hd$. This means that $H \backslash G = \{H, Hb, Hc\}$.

With this concrete example at hand, the following lemma should make sense, even though it might appear abstract at a first reading.

Lemma 2.2.6 *Let H be a subgroup of a group G and let $x, y \in G$. Then*

- (i) $x \in xH$,
- (ii) $xH = yH \iff x^{-1}y \in H$,
- (iii) If $xH \neq yH$ then $xH \cap yH = \emptyset$,
- (iv) The map $\varphi : H \rightarrow xH$ given by $\varphi(h) = xh$ is bijective.

Proof. Clearly $x \in xH$, since $x = xe$ and $e \in H$. This proves (i). If $xH = yH$ then $xh = ye = y$ for some $h \in H$. This implies that $x^{-1}y = h \in H$. If $x^{-1}y = h \in H$ then $y = xh$. Therefore $yH \subseteq xH$. Since $x = yh^{-1}$, we get $xH \subseteq yH$, so that $xH = yH$. This proves (ii). Suppose that $z \in xH \cap yH$. Then $z = xh_1 = yh_2$ for suitable $h_1, h_2 \in H$. But this shows that $x^{-1}y \in H$ and thus that $xH = yH$ by (ii). Therefore (iii) holds. Since φ is multiplication by x it follows by from subsection 2.1.6 that φ is bijective. It is simply the multiplication map restricted to the subgroup H . This proves (iv). \square

To connect with the theory of numbers, look at the subgroup $d\mathbb{Z}$ of \mathbb{Z} , where $d \in \mathbb{N}$. In this context Lemma 2.2.6(ii) says that $a + d\mathbb{Z} = b + d\mathbb{Z}$ if and only if $b - a \in d\mathbb{Z}$. Now $b - a \in d\mathbb{Z}$ means that $d \mid b - a$ or $a \equiv b \pmod{d}$ in the language of congruences. This is what we obtained in Proposition 2.1.2 without knowing about cosets.

Corollary 2.2.7 *Let H be a subgroup of G . Then*

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

and if $g_1H \neq g_2H$ then $g_1H \cap g_2H = \emptyset$.

Proof. Since $g \in gH$ (Lemma 2.2.6(i)) for every $g \in G$, we see that $G = \bigcup_{g \in G} gH$. If $g_1H \neq g_2H$ then $g_1H \cap g_2H = \emptyset$ by Lemma 2.2.6(iii). \square

We are now able to prove the Lagrange index theorem. Lagrange did not have the concept of an abstract group. He worked in the context of solutions to algebraic equations.

Theorem 2.2.8 (Lagrange) *If $H \subseteq G$ is a subgroup of a finite group G then*

$$|G| = |G/H||H|.$$

The order of a subgroup divides the order of the group.

Proof. Let gH be a coset in G/H . By Lemma 2.2.6(iv) there is a bijection between gH and H . This shows that gH has the same number of elements as H . Since G is the union of the cosets and different cosets are disjoint, by Corollary 2.2.7, the order of G must be the number of cosets times the order of H . This shows that $|G| = |G/H||H|$ and that $|H|$ divides $|G|$. \square

Definition 2.2.9 The number of cosets $|G/H|$ is called the *index* of H in G . It is denoted $[G : H]$.

Lagrange's theorem says that the order of a subgroup H divides the order of the group G . Suppose that d is a divisor in the order of a finite group G . Does G contain a subgroup of order d ? After having digested Section 2.9 you will be able to solve Exercise 2.41, which answers this question negatively.

2.3 Normal subgroups

Let H be a subgroup of a group G . In a very important special case it is possible to make the set of left cosets, G/H , into a group inheriting the composition of G . What is the natural way of doing this? The set G/H consists of certain subsets of G called left cosets. We would like to compose two left cosets and get a new left coset. Why not compose subsets of G ? Define

$$XY = \{xy \mid x \in X, y \in Y\}$$

for arbitrary subsets $X, Y \subseteq G$. This is a composition on the set of subsets of G , which is associative because the composition in G is associative. We would like this composition on subsets to give a composition on left cosets viewed as subsets. This is not necessarily so. Take a look back at Example 2.2.5. Here

$$(bH)(cH) = \{b, d\}\{c, f\} = \{bc, bf, dc, df\} = \{f, c, a, e\},$$

which is not a left coset. The key is the following.

Proposition 2.3.1 *Let H be a subgroup of a group G . If $gH = Hg$ for every $g \in G$ then*

$$(xH)(yH) = (xy)H$$

for every $x, y \in G$.

Proof. The inclusion $(xH)(yH) \supseteq (xy)H$ holds without any assumptions on H : if $(xy)h$ is an element of $(xy)H$ then $(xy)h = (xe)(yh) \in (xH)(yH)$. Let us show that $(xH)(yH) \subseteq (xy)H$. Let $(xh_1)(yh_2) \in (xH)(yH)$, where $h_1, h_2 \in H$. It follows that $(xh_1)(yh_2) = x((h_1y)h_2) = x((yh_3)h_2) = (xy)(h_3h_2)$ for a suitable $h_3 \in H$, since $Hy = yH$. This shows that $(xH)(yH) \subseteq (xy)H$. \square

This leads to the following definition.

Definition 2.3.2 A subgroup N of a group G is called *normal* if

$$gNg^{-1} = \{gng^{-1} \mid n \in N\} = N$$

for every $g \in G$.

A normal subgroup N of G satisfies $gN = Ng$ for every $g \in G$ (see Exercise 2.13).

Corollary 2.3.3 Let N be a normal subgroup of the group G . Then the composition of subsets makes G/N into a group and

$$(g_1N)(g_2N) = (g_1g_2)N$$

for $g_1N, g_2N \in G/N$.

Proof. We know that composition of subsets is associative and we have verified the above identity $(g_1N)(g_2N) = (g_1g_2)N$ for arbitrary $g_1, g_2 \in G$ in Proposition 2.3.1. So, the multiplication of subsets of G gives a composition on G/N (notice once more that it is crucial that N is normal). The neutral element is the left coset $eN = N$. The inverse element $(gN)^{-1}$ is $g^{-1}N$ for $gN \in G/N$. Therefore G/N is a group with this composition. \square

Definition 2.3.4 Let N be a normal subgroup of G . The group G/N is called a *quotient group*.

Example 2.3.5 The subset $H = \{e, a\} \subseteq S_3$ is a subgroup of S_3 (using the notation of Example 2.1.6). It is not normal, since the left coset $bH = \{b, ba\}$ is not equal to the right coset $Hb = \{b, ab\}$. This follows from the fact that $ab \neq ba$ as we have already seen. However, $K = \{e, d, f\}$ is a normal subgroup of S_3 .

A subgroup of an abelian group is normal (see Exercise 2.14). Suppose that G is a group with the property that every subgroup in it is normal. Is G abelian? The answer is a somewhat surprising “no.” The smallest non-abelian group for which every subgroup is normal is the quaternion group with eight elements (see Exercise 2.17).

Lemma 2.3.6 *Let H and K , where H is normal, be subgroups of a group G . Then HK is a subgroup of G .*

Proof. Clearly $e \in HK$. If $x \in H, y \in K$ then $(xy)^{-1} = (y^{-1}x^{-1})y^{-1} \in HK$. If furthermore $x' \in H, y' \in K$ then $(xy)(x'y') = (x(yx'y^{-1}))yy' \in HK$. \square

2.3.1 Quotient groups of the integers

Consider the subgroup $n\mathbb{Z}$ of \mathbb{Z} . This is a normal subgroup since \mathbb{Z} is abelian. The quotient group $\mathbb{Z}/n\mathbb{Z}$ may appear abstract until you realize that it is exactly the same group as that defined at the start of subsection 2.1.1. The elements of $\mathbb{Z}/n\mathbb{Z}$ have the form $[x] = x + n\mathbb{Z}$, where $x \in \mathbb{Z}$. They are composed (here, added) using the familiar rule $[x] + [y] = [x + y]$. This is an application of Corollary 2.3.3.

The elements $[a] = a + n\mathbb{Z}$ of $\mathbb{Z}/n\mathbb{Z}$, where $a \in \mathbb{Z}$, are called *residue classes*. If $n > 0$ the residue classes of $\mathbb{Z}/n\mathbb{Z}$ are $\{[0], [1], \dots, [n-1]\}$ – represented by the remainders after dividing by n .

2.3.2 The multiplicative group of prime residue classes

Looking at the set $\mathbb{Z}/n\mathbb{Z}$, where $n > 0$, can we multiply residue classes via $[a][b] = [ab]$ using ordinary multiplication in \mathbb{Z} and get a group? We need to check that this makes sense. It may be possible that $[a] = [a']$ and $[b] = [b']$ but $[ab] \neq [a'b']$. This would make our definition meaningless. It would mean that $[a][b]$ has several values depending on the elements you choose in $[a]$ and $[b]$. Fortunately it does make sense since $[a] = [a']$ and $[b] = [b']$ can be rewritten as $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$. Now Proposition 1.3.4 implies that $ab \equiv a'b' \pmod{n}$ or $[ab] = [a'b']$. So we get a well defined composition on $\mathbb{Z}/n\mathbb{Z}$. It is associative with neutral element $[1] = 1 + n\mathbb{Z}$, but not every element has an inverse. To begin with, $[a][0] = [0]$ for every $[a] \in \mathbb{Z}/n\mathbb{Z}$, so $[0]$ cannot have an inverse. Suppose we put $G = \mathbb{Z}/n\mathbb{Z} \setminus \{[0]\}$. This is still not good enough. Take the example $n = 4$; here $[2][2] = [0] \notin G$. The answer is to

look at residue classes $[a] = a + n\mathbb{Z}$ with $\gcd(a, n) = 1$. You can easily check that if $a + n\mathbb{Z} = b + n\mathbb{Z}$ and $\gcd(a, n) = 1$ then $\gcd(b, n) = 1$. These residue classes are called *prime residue classes*. We let

$$(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$$

for $n \in \mathbb{N}$. The composition $[a][b] = [ab]$ is a composition on $(\mathbb{Z}/n\mathbb{Z})^*$, since $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ implies that $\gcd(ab, n) = 1$ (Corollary 1.5.11). Let $[a] \in (\mathbb{Z}/n\mathbb{Z})^*$. Then we can find $\lambda, \mu \in \mathbb{Z}$ such that $\lambda a + \mu n = 1$ by Lemma 1.5.7. In particular this gives $\gcd(\lambda, n) = 1$ and $[\lambda a] = [1]$, since $[\lambda a + \mu n] = [\lambda a] + [\mu n] = [\lambda a] + [0] = [\lambda a]$. But then $[\lambda]$ is the inverse element of $[a]$, since $[a][\lambda] = [a\lambda] = [1]$. We have proved that $(\mathbb{Z}/n\mathbb{Z})^*$ is a group with multiplication of residue classes as composition. The order of $(\mathbb{Z}/n\mathbb{Z})^*$ is $\varphi(n)$ for $n > 0$.

Example 2.3.7 Consider the group $(\mathbb{Z}/34\mathbb{Z})^*$. Then $[13] \in (\mathbb{Z}/34\mathbb{Z})^*$. In Example 1.5.3 we saw using the extended Euclidean algorithm that

$$5 \cdot 34 - 13 \cdot 13 = 1.$$

This implies that the inverse element of $[13]$ in $(\mathbb{Z}/34\mathbb{Z})^*$ is $[13]^{-1} = [21]$ (why?).

Example 2.3.8 If $n = 8$ then $(\mathbb{Z}/n\mathbb{Z})^*$ has the composition table

\cdot	[1]	[3]	[5]	[7]
[1]	[1]	[3]	[5]	[7]
[3]	[3]	[1]	[7]	[5]
[5]	[5]	[7]	[1]	[3]
[7]	[7]	[5]	[3]	[1]

The group $(\mathbb{Z}/n\mathbb{Z})^*$ is a much more subtle abelian group than $\mathbb{Z}/n\mathbb{Z}$. For one thing, the order of $(\mathbb{Z}/n\mathbb{Z})^*$ is $\varphi(n)$, a quantity difficult to compute as we have seen in Chapter 1. Later $(\mathbb{Z}/n\mathbb{Z})^*$ will appear more elegantly as the group of units in the ring $\mathbb{Z}/n\mathbb{Z}$.

The two groups $\mathbb{Z}/4\mathbb{Z}$ and $(\mathbb{Z}/8\mathbb{Z})^*$ both have four elements. They are abelian but quite different. In fact $G = (\mathbb{Z}/8\mathbb{Z})^*$ has the property that $g \cdot g = [1] = e$ for every $g \in G$. This is not shared by $\mathbb{Z}/4\mathbb{Z}$, where $[1] + [1] = [2] \neq [0] = e$. We require a tool to distinguish groups. We need to study maps between them that preserve their respective compositions.

2.4 Group homomorphisms

In what follows we will abuse notation somewhat by not writing the composition of elements explicitly. As before, we will write e for the neutral element in a group. It will be clear from the context to which group the composition and the neutral element refer.

Definition 2.4.1 Let G and K be groups. A map $f : G \rightarrow K$ is called a *group homomorphism* if $f(xy) = f(x)f(y)$ for every $x, y \in G$.

Example 2.4.2 The exponential function e^x is a group homomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \cdot)$, where $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$. This is the well known rule $e^{x+y} = e^x e^y$ for every $x, y \in \mathbb{R}$.

Example 2.4.3 The determinant

$$\det : \mathrm{GL}_2(\mathbb{R}) \rightarrow (\mathbb{R} \setminus \{0\}, \cdot)$$

is a group homomorphism (here \cdot denotes multiplication). This is the well known rule $\det(AB) = \det(A)\det(B)$ for $A, B \in \mathrm{GL}_2(\mathbb{R})$.

Example 2.4.4 Let N be a normal subgroup of the group G . Then $\pi : G \rightarrow G/N$ given by $\pi(g) = gN$ is a group homomorphism. This follows from Corollary 2.3.3.

Definition 2.4.5 The kernel of a group homomorphism $f : G \rightarrow K$ is

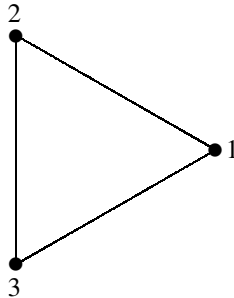
$$\mathrm{Ker} f = \{g \in G \mid f(g) = e\}.$$

The image of f is $f(G) = \{f(g) \mid g \in G\} \subseteq K$. A bijective group homomorphism is called a *group isomorphism*. A group isomorphism $f : G \rightarrow K$ is denoted $f : G \xrightarrow{\sim} K$ and we write $G \cong K$ and say that G and K are *isomorphic*.

Isomorphisms between groups may appear a bit abstract at first. In the world of groups, isomorphic groups are considered as the same. For all practical purposes they have the same composition tables.

Example 2.4.6 Recall the groups S_3 (Example 2.1.6) and D_3 (Example 2.1.13). They are isomorphic. To prove this we give a map $f : D_3 \rightarrow S_3$ and prove that it is a group isomorphism. We number the corners in the equilateral

triangle by 1, 2 and 3:



Given a rotation or a reflection $\sigma \in D_3$ it is easy to see that it must map a corner to a corner (if you do not believe this, you can go through the elements I, R, S, T, D, E of D_3 and check it). This enables us to construct a homomorphism φ from D_3 to S_3 given by

$$\varphi(\sigma) = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix},$$

where $\sigma \in D_3$. Since σ is a bijective map $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ it must also give a bijective map $\{1, 2, 3\} \rightarrow \{1, 2, 3\}$. Thus $\varphi(\sigma) \in S_3$. In order for φ to be a homomorphism, we must prove that $\varphi(\sigma_1 \circ \sigma_2) = \varphi(\sigma_1) \circ \varphi(\sigma_2)$. If you plug in the above form for $\varphi(\sigma)$, you will see that $\varphi(\sigma_1 \circ \sigma_2)(i) = (\varphi(\sigma_1) \circ \varphi(\sigma_2))(i) = \sigma_1(\sigma_2(i))$ for $i = 1, 2, 3$, so that φ really is a group homomorphism. Since a linear map $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ is uniquely determined by its values on two linearly independent vectors, φ must be injective. So we have an injective group homomorphism $\varphi : D_3 \rightarrow S_3$. Since D_3 and S_3 are both of order 6, φ must be a group isomorphism.

Example 2.4.7 Let us prove that the groups L (Example 2.1.12) and $O_2(\mathbb{R})$ (Example 2.1.11) are isomorphic. There is a natural map $\varphi : L \rightarrow O_2(\mathbb{R})$. This is given simply by defining $\varphi(f)$ to be the matrix representing f in the natural basis e_1 and e_2 . So if $f(e_1) = ae_1 + be_2$ and $f(e_2) = ce_1 + de_2$, where $a, b, c, d \in \mathbb{R}$, we put

$$\varphi(f) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

From linear algebra it is known that $\varphi(f \circ g) = \varphi(f)\varphi(g)$ – composition of linear maps corresponds to multiplication of their matrices. So φ is a group homomorphism. From Example 2.1.12 you see that $\varphi(f) \in O_2(\mathbb{R})$. Given an

orthogonal matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

we know that $a^2 + b^2 = 1$ and $ac + bd = 0$. Thus the two vectors (a, b) and (c, d) are orthogonal and $(a, b) = (\cos(t), \sin(t))$ for some $t \in \mathbb{R}$. This ultimately tells us that an orthogonal matrix is a rotation or a reflection – it represents a linear isometry. Therefore φ is surjective. Since φ is also injective (why?) it follows that it is a group isomorphism.

Example 2.4.8 The exponential function is a group isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \cdot)$. So $(\mathbb{R}, +)$ and $(\mathbb{R}_{>0}, \cdot)$ are isomorphic groups. This would have been impossible to prove without knowledge of the exponential function.

Notice that the kernel of the group homomorphism $G \rightarrow G/N$ is N and that the kernel of the determinant homomorphism from $\text{GL}_2(\mathbb{R})$ to $(\mathbb{R} \setminus \{0\}, \cdot)$ consists of matrices in $\text{GL}_2(\mathbb{R})$ with determinant 1.

We have the following general result on images and kernels of group homomorphisms.

Proposition 2.4.9 *Let $f : G \rightarrow K$ be a group homomorphism.*

- (i) *The image $f(G) \subseteq K$ is a subgroup of K .*
- (ii) *The kernel $\text{Ker } f \subseteq G$ is a normal subgroup of G .*
- (iii) *f is injective if and only if $\text{Ker } (f) = \{e\}$.*

Proof. First we prove that $f(G) = \{f(g) \mid g \in G\}$ is a subgroup of K . Since $f(e) = f(ee) = f(e)f(e)$, it follows that $e = f(e)$ by subsection 2.1.6. This shows that $e \in f(G)$. Let $x \in G$. Then $e = f(e) = f(xx^{-1}) = f(x)f(x^{-1})$ and $e = f(e) = f(x^{-1}x) = f(x^{-1})f(x)$. This shows that $f(x^{-1}) = f(x)^{-1}$. Thus if $f(x) \in f(G)$ then $f(x)^{-1} \in f(G)$. Finally if $f(x), f(y) \in f(G)$ then $f(x)f(y) = f(xy) \in f(G)$. This finishes the proof of (i).

Let us now prove that $\text{Ker } (f)$ is a normal subgroup. We have already seen that $e \in \text{Ker } (f)$ since $f(e) = e$. If $x \in \text{Ker } (f)$ then $e = f(x) = f(x)^{-1} = f(x^{-1})$, showing that $x^{-1} \in \text{Ker } (f)$. If $x, y \in \text{Ker } (f)$ then $f(xy) = f(x)f(y) = ee = e$, showing that $xy \in \text{Ker } (f)$. So $\text{Ker } (f)$ is a subgroup of G . Let $N = \text{Ker } (f)$. For every $g \in G$ and $x \in N$ we have $f((gx)g^{-1}) = (f(g)f(x))f(g^{-1}) = f(g)f(g)^{-1} = e$. This shows that $gNg^{-1} \subseteq N$. The inclusion $N \subseteq gNg^{-1}$ for every $g \in G$ follows from the fact that we have the inclusion $g^{-1}Ng \subseteq N$ for every $g \in G$. This finishes the proof of (ii).

Finally let us prove (iii). Since $f(e) = e$ it follows that $\text{Ker}(f) = \{e\}$ if f is injective. Conversely, assume that $\text{Ker}(f) = \{e\}$ and $f(x) = f(y)$. Then $f(y)^{-1}f(x) = f(y^{-1})f(x) = f(y^{-1}x) = e$. Therefore $y^{-1}x \in \text{Ker}(f)$. This implies that $y^{-1}x = e$ or $x = y$. \square

2.5 The isomorphism theorem

Now suppose that N is a normal subgroup of G . How do we find out more about the quotient group G/N ? The answer is that we identify the cosets G/N with some other known group using what is known as the isomorphism theorem.

Theorem 2.5.1 *Let G and K be groups and $f : G \rightarrow K$ a group homomorphism with kernel $N = \text{Ker}(f)$. Then*

$$\tilde{f} : G/N \rightarrow f(G)$$

given by $\tilde{f}(gN) = f(g)$ is a well defined map and a group isomorphism.

Proof. First notice that $f(x) = f(y)$ if and only if $f(y)^{-1}f(x) = f(y^{-1}x) = e$ if and only if $y^{-1}x \in N$ for every $x, y \in G$. By Lemma 2.2.6(ii) this implies that $f(x) = f(y)$ if and only if $xN = yN$. We get thus that \tilde{f} given by $\tilde{f}(gN) = f(g)$ is a well defined and injective map. It is a group homomorphism since

$$\begin{aligned}\tilde{f}((g_1N)(g_2N)) &= \tilde{f}((g_1g_2)N) \\ &= f(g_1g_2) = f(g_1)f(g_2) \\ &= \tilde{f}(g_1N)\tilde{f}(g_2N)\end{aligned}$$

for $g_1N, g_2N \in G/N$. It is surjective because f is surjective onto $f(G)$. Thus \tilde{f} is a group isomorphism $G/N \rightarrow f(G)$. \square

One usually understands a quotient group G/N by finding a surjective group homomorphism $f : G \rightarrow K$ for a suitable group K such that $N = \text{Ker}(f)$. Then Theorem 2.5.1 gives an isomorphism

$$\tilde{f} : G/N \xrightarrow{\sim} K.$$

Here are two examples of this.

Example 2.5.2 The subgroup $N = 2\pi\mathbb{Z} = \{2\pi m \mid m \in \mathbb{Z}\}$ of $(\mathbb{R}, +)$ is normal since $(\mathbb{R}, +)$ is an abelian group. What is \mathbb{R}/N ? The strategy is to find

a surjective group homomorphism $f : \mathbb{R} \rightarrow K$, with kernel $2\pi\mathbb{Z}$, onto some known group K . Here we can put $K = \{z \in \mathbb{C} \mid |z| = 1\}$, which is a group with multiplication as composition and use $f(x) = e^{ix}$ as the group homomorphism (recall that $e^{i(x+y)} = e^{ix}e^{iy}$). Then $\text{Ker } f = \{x \in \mathbb{R} \mid e^{ix} = 1\}$. Since $e^{ix} = \cos x + i \sin x$, this means that $x = 2\pi m$ for some $m \in \mathbb{Z}$. Now we can identify the quotient group $\mathbb{R}/2\pi\mathbb{Z}$ with the group of unit vectors in the complex plane by using the isomorphism

$$\tilde{f} : \mathbb{R}/2\pi\mathbb{Z} \xrightarrow{\sim} K$$

given in Theorem 2.5.1.

Example 2.5.3 Denote by A_3 the (normal) subgroup $\{e, d, f\}$ of S_3 (in the notation of Example 2.1.6). Then

$$S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z},$$

since $|S_3/A_3| = |S_3|/|A_3| = 2$ and $\mathbb{Z}/2\mathbb{Z}$ is the only group of order 2 up to isomorphism. Can you construct an explicit surjective group homomorphism $\text{sgn} : S_3 \rightarrow \mathbb{Z}/2\mathbb{Z}$ such that $\text{Ker}(f) = A_3$?

2.6 Order of a group element

In a group G we can compose an element $g \in G$ with itself an arbitrary number of times $g, gg, (gg)g, \dots$. Let us introduce the precise notion of powers of elements in groups. Define $g^0 = e$, $g^n = g^{n-1}g$ for $n > 0$ and $g^n = (g^{-1})^{-n}$ for $n < 0$ and every $g \in G$. Then we have a well defined map $f_g : \mathbb{Z} \rightarrow G$ given by $f_g(n) = g^n$.

Proposition 2.6.1 Let G be a group and $g \in G$. The map

$$f_g : \mathbb{Z} \rightarrow G$$

given by $f_g(n) = g^n$ is a group homomorphism from $(\mathbb{Z}, +)$ to G .

Proof. By the definition of g^n , where $n \in \mathbb{Z}$, we have $f_{g^{-1}}(-m) = f_g(m)$ for every $g \in G, m \in \mathbb{Z}$, along with $f_g(m+1) = f_g(m)f_g(1)$ and $f_g(m-1) = f_g(m)f_g(-1)$ for every $g \in G, m \geq 0$. This gives the identity $f_g(m+1) = f_g(m)f_g(1)$ for every $g \in G, m \in \mathbb{Z}$. From this we deduce that $f_g(m+n) = f_g(m)f_g(n)$ for every $g \in G, m \in \mathbb{Z}$ and $n \geq 0$. If $m < 0$ and $n < 0$ then $f_g(m+n) = f_{g^{-1}}(-m+(-n)) = f_{g^{-1}}(-m)f_{g^{-1}}(-n) = f_g(m)f_g(n)$.

This completes the proof that $f_g(m+n) = f_g(m)f_g(n)$ for every $m, n \in \mathbb{Z}$, showing that f_g is a group homomorphism. \square

The image $f_g(\mathbb{Z}) = \{g^n \mid n \in \mathbb{Z}\}$ is denoted $\langle g \rangle$. It is an abelian subgroup of G (see Exercise 2.26). The number of elements in $\langle g \rangle$ is called the *order* of g . It is denoted $\text{ord}(g)$. One usually thinks of the order of an element g as the smallest positive power of g giving the neutral element. If no such power exists, g is said to have infinite order.

Example 2.6.2 In the notation of Example 2.1.6, a has order 2 and f has order 3 in S_3 . This follows from the composition table: $a \neq e$ but $a^2 = e$. Similarly $f \neq e$ and $f^2 = d \neq e$ but $f^3 = f^2 f = df = e$.

The element $[2] \in \mathbb{Z}/8\mathbb{Z}$ has order 4 and $[2] \in \mathbb{Z}/5\mathbb{Z}$ has order 5. However, the matrix

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

has infinite order in the group $\text{GL}_2(\mathbb{R})$.

The following fundamental result turns out to be very useful for later computations in group theory (with applications to prime numbers and polynomials).

Proposition 2.6.3 *Let G be a finite group and let $g \in G$.*

- (i) *The order $\text{ord}(g)$ of g divides $|G|$.*
- (ii) *$g^{|G|} = e$.*
- (iii) *If $g^n = e$ for some $n > 0$ then $\text{ord}(g) \mid n$.*

Proof. This is an application of Theorem 2.2.8. Let H denote the subgroup $\langle g \rangle$ generated by g . Since $\text{ord}(g) = |H|$, we get that $|G| = |G/H| \text{ord}(g)$. This proves (i). In the same way we have

$$g^{|G|} = g^{\text{ord}(g)|G/H|} = (g^{\text{ord}(g)})^{|G/H|} = e^{|G/H|} = e.$$

This proves (ii). If $g^n = e$ then $n \in \text{Ker}(f_g)$. But $\text{Ker}(f_g) = n_g\mathbb{Z}$ and since $n > 0$ it follows that $n_g > 0$ and that g has finite order $\text{ord}(g) = n_g$. Since $n \in n_g\mathbb{Z} = \text{ord}(g)\mathbb{Z}$ we get that $\text{ord}(g) \mid n$. This proves (iii). \square

2.7 Cyclic groups

Definition 2.7.1 A *cyclic group* is a group G containing an element g such that $G = \langle g \rangle$. The element g is called a *generator* of G (we say that G is *generated* by g).

Cyclic groups are very concrete objects. We can easily identify them with groups we know very well. Let $G = \langle g \rangle$ be a cyclic group and consider the group homomorphism $f_g : \mathbb{Z} \rightarrow G$. The kernel $\text{Ker}(f_g)$ is a subgroup of \mathbb{Z} . Thus $\text{Ker}(f_g) = n_g \mathbb{Z}$ for some unique natural number $n_g \geq 0$ by Proposition 2.2.3. By Theorem 2.5.1 we have a group isomorphism

$$\mathbb{Z}/n_g \mathbb{Z} \xrightarrow{\sim} \langle g \rangle = G.$$

This shows that a cyclic group is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$. Now we are in a position to illuminate the explicit computation in Example 2.1.9.

Proposition 2.7.2 A group G of prime order $|G| = p$ is isomorphic to the cyclic group $\mathbb{Z}/p\mathbb{Z}$.

Proof. Let $g \in G$ be an element in G different from the neutral element e . Then $f_g(\mathbb{Z})$ is a subgroup H of G with more than one element. Since $|H|$ divides $|G| = p$ (by Theorem 2.2.8) it follows that $|H| = |G|$ and therefore that $H = G$. This means that $f_g : \mathbb{Z} \rightarrow G$ is a surjective homomorphism. The kernel of f_g is $p\mathbb{Z}$ by Proposition 2.6.3. Now the result follows from Theorem 2.5.1. \square

Cyclic groups are in some sense the easiest groups to work with. Proposition 2.7.4 below tells almost the whole story about them. Before this let us go through an illustrative example.

Example 2.7.3 Let $[a] = a + 12\mathbb{Z}$, where $a \in \mathbb{Z}$. Then

$$\mathbb{Z}/12\mathbb{Z} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]\}.$$

The order of $[3]$ is 4, since $\langle [3] \rangle = \{[0], [3], [6], [9]\}$. The orders of the elements in the group (appearing as above) are

$$1, 12, 6, 4, 3, 12, 2, 12, 3, 4, 6, 12$$

respectively. Notice that for every (natural) divisor d of 12, there is a unique subgroup of order d . This is the subgroup generated by $[12/d]$. Notice also that there are $\varphi(d)$ elements of order d .

Proposition 2.7.4 *Let G be a cyclic group.*

- (i) *Every subgroup of G is cyclic.*
- (ii) *Suppose that G is finite and that d is a divisor in $|G|$. Then G contains a unique subgroup H of order d .*
- (iii) *There are $\varphi(d)$ elements of order d in G . These are the generators of H .*

Proof. If G is infinite then $G \cong \mathbb{Z}$. We know that every subgroup of \mathbb{Z} has the form $d\mathbb{Z}$ for some $d \in \mathbb{N}$. Such a subgroup is cyclic and generated by d . Suppose that G is finite and that $|G| = N > 0$. We may assume that $G = \mathbb{Z}/N\mathbb{Z} = \{[0], [1], \dots, [N-1]\}$. Let H be a subgroup of G . If $H \neq \{[0]\}$ we pick the smallest natural number $d > 0$ such that $[d] \in H$. If $[n] \in H$ then division with remainder gives $n = qd + r$, where $0 \leq r < d$. If $r > 0$ then $[n - qd] = [r] \in H$, contradicting the minimality of d . So $r = 0$ and $H = \langle [d] \rangle$. This proves (i).

Next, assume that d is a divisor in N . Let $m = N/d$. Then $[m]$ is an element of order d in G . If $[n]$ is another element of order d then $[dn] = [0]$. Thus $N \mid nd$ and so $m \mid n$. So every element in G of order d is some multiple of $[m]$. Since subgroups are cyclic, it follows that the only subgroup of order d is $H = \langle [m] \rangle$. This proves (ii).

Since H is the unique subgroup of order d , the elements of order d in G must be in one-to-one correspondence with the generators of H . We write $H = \{[0], [1], \dots, [d-1]\}$ since $H \cong \mathbb{Z}/d\mathbb{Z}$. If $[a]$ is a generator of H then $\gcd(a, d) = 1$, because if $\gcd(a, d) = s > 1$, $a = bs$, $d = cs$ then we get $ca = cbs = bd$. Thus $[ca] = [0]$, where $1 \leq c < d$, contradicting that $[a]$ is a generator of H . However, if $\gcd(a, d) = 1$, $[a]$ has to be a generator of H : if $[ia] = [0]$ then $d \mid ia$ and therefore $d \mid i$, since $\gcd(a, d) = 1$. This proves (iii). \square

Remark 2.7.5 In the notation of the proof of Proposition 2.7.4, the $\varphi(d)$ elements of order d in $\mathbb{Z}/N\mathbb{Z}$ are $\{[km] \mid 0 \leq k < N, \gcd(k, N) = 1\}$, where $m = N/d$.

Using the language of group theory we can now produce a very simple proof of an identity that seems related only to numbers.

Corollary 2.7.6 *Let N be a positive integer. Then*

$$\sum_{d|N} \varphi(d) = N,$$

where the sum is over $d \in \text{div}(N)$.

Proof. Let G be the cyclic group $\mathbb{Z}/N\mathbb{Z}$. Then

$$N = \sum_{g \in G} 1 = \sum_{d|N} \sum_{g \in G, \text{ord}(g)=d} 1 = \sum_{d|N} \varphi(d)$$

by Proposition 2.7.4. □

2.8 Groups and numbers

Let us see how Euler's theorem (Theorem 1.7.2) and the Chinese remainder theorem (Theorem 1.6.4) fit into the framework of groups.

2.8.1 Euler's theorem

Recall Euler's theorem. If a, n are relatively prime integers, where $n > 0$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$. In the framework of groups we consider the finite group $G = (\mathbb{Z}/n\mathbb{Z})^*$ from subsection 2.3.2. The order of G is $\varphi(n)$. The integer a is relatively prime to n . Therefore $[a] \in G$. Now we can apply Proposition 2.6.3(ii) to obtain

$$[a]^{|G|} = [a]^{\varphi(n)} = [1].$$

This means that $a^{\varphi(n)} - 1 \in n\mathbb{Z}$ and therefore that $a^{\varphi(n)} \equiv 1 \pmod{n}$. You should really compare this with our original proof of Theorem 1.7.2. Where did all the computations go? The answer is that groups form another level of abstraction. Proofs become simpler.

Before moving on to the group version of the Chinese remainder theorem we need to define product groups.

2.8.2 Product groups

If G_1, G_2, \dots, G_n are groups then the product

$$G = G_1 \times G_2 \times \cdots \times G_n = \{(g_1, g_2, \dots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \dots, g_n \in G_n\}$$

has the natural composition

$$(g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n) = (g_1h_1, g_2h_2, \dots, g_nh_n).$$

You can easily check that this composition is associative (it is associative at each component). The neutral element is (e, e, \dots, e) and the inverse of the group element $g = (g_1, \dots, g_n)$ is $g^{-1} = (g_1^{-1}, \dots, g_n^{-1})$. So G is a group called the *product group* of G_1, \dots, G_n . Also, if H is a group and we have group homomorphisms $\varphi_i : H \rightarrow G_i, i = 1, \dots, n$, then

$$\varphi(g) = (\varphi_1(g), \dots, \varphi_n(g))$$

is a group homomorphism from H to $G = G_1 \times \dots \times G_n$. Before giving the group version of the Chinese remainder theorem, let us record the following lemma on product groups.

Lemma 2.8.1 *Let M, N be normal subgroups of a group G with $M \cap N = \{e\}$. Then MN is a subgroup of G and*

$$\pi : M \times N \rightarrow MN$$

given by $\pi(x, y) = xy$ is an isomorphism.

Proof. Lemma 2.3.6 tells us that MN is a subgroup. In order for π to be a homomorphism we must prove that $(xy)(x'y') = (xx')(yy')$, where $x, x' \in M$ and $y, y' \in N$. This is seen by rewriting $(xy)(x'y')$ as $(xx')(x'^{-1}yx'y^{-1})(yy')$ and noticing that $x'^{-1}yx'y^{-1} \in M \cap N = \{e\}$, since M and N are normal subgroups of G . Since the kernel of π is isomorphic to $M \cap N$ and the image of π is MN , π has to be bijective and therefore an isomorphism. \square

2.8.3 The Chinese remainder theorem

Here is the group version of the Chinese remainder theorem (Theorem 1.6.4).

Proposition 2.8.2 *Let $n_1, \dots, n_r \in \mathbb{Z}$ be pairwise relative prime integers and let $N = n_1 \dots n_r$. If φ_i denotes the canonical group homomorphism $\pi_{n_i\mathbb{Z}} : \mathbb{Z} \rightarrow \mathbb{Z}/n_i\mathbb{Z}$ then the map*

$$\tilde{\varphi} : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$$

given by $\varphi(x + N\mathbb{Z}) = (\varphi_1(x), \dots, \varphi_r(x))$ is a group isomorphism.

Proof. The map

$$\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

given by $\varphi(x) = (\varphi_1(x), \dots, \varphi_r(x))$ is a group homomorphism by subsection 2.8.2. If $n \in \text{Ker}(\varphi)$ then $\varphi_1(n) = 0, \dots, \varphi_r(n) = 0$. This means that $n \in n_1\mathbb{Z}, \dots, n \in n_r\mathbb{Z}$ or that $n_1 \mid n, \dots, n_r \mid n$. By Corollary 1.5.11 we get that $N = n_1 \cdots n_r \mid n$ so that $n \in N\mathbb{Z}$. This proves that $\text{Ker}(\varphi) \subseteq N\mathbb{Z}$. The other inclusion is left to the reader. Now Theorem 2.5.1 tells us that we have an isomorphism

$$\tilde{\varphi} : \mathbb{Z}/N\mathbb{Z} \rightarrow \varphi(\mathbb{Z}) \subseteq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}.$$

But since the number of elements in $\mathbb{Z}/N\mathbb{Z}$ equals the number of elements in $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, we get that $\varphi(\mathbb{Z}) = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ and $\tilde{\varphi}$ is thus an isomorphism. \square

Using the notation of Proposition 2.8.2 we have actually proved that

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

is a cyclic group $\cong \mathbb{Z}/N\mathbb{Z}$.

Example 2.8.3 The product group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not cyclic, since the maximal order of an element is 2. One may prove that $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2.9 Symmetric and alternating groups

In Example 2.1.6 we constructed the group S_3 of bijective maps of a set M of three elements to itself. The composition in S_3 is the composition of maps. The bijective map given by $1 \mapsto 2, 2 \mapsto 3$ and $3 \mapsto 1$ was denoted

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Of course, the same construction makes sense for a set $M_n = \{1, 2, \dots, n\}$ with n elements and this leads to the so-called *symmetric group* S_n on n elements. Thus S_n consists of the bijective maps from M_n to itself. It is a group with composition of maps as the composition, and one may show that $|S_n| = n!$ by counting permutations of the numbers $1, \dots, n$. The elements (bijective maps) of S_n are called *permutations*. As in the S_3 setting, a bijective map $\sigma \in S_n$ will

be denoted

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

Symmetric groups are in general non-abelian. We have for example

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

since the map on the left hand side assumes the value 3 at 2 and the map on the right hand side assumes the value 1 at 2. In an important special case one can actually prove that $\sigma\tau = \tau\sigma$, where σ, τ are certain permutations in S_n .

Definition 2.9.1 Suppose that $\sigma \in S_n$. Then we define

$$M_\sigma = \{x \in M_n \mid \sigma(x) \neq x\}.$$

Permutations $\sigma, \tau \in S_n$ are called disjoint if $M_\sigma \cap M_\tau = \emptyset$.

One may say loosely that disjoint permutations move different numbers. They have the following pleasant property.

Proposition 2.9.2 Let $\sigma, \tau \in S_n$ be disjoint permutations in S_n . Then

$$\sigma\tau = \tau\sigma.$$

Proof. We must prove that $\sigma(\tau(x)) = \tau(\sigma(x))$ for every $x \in M_n$. If $x \notin M_\sigma \cup M_\tau$ then $\sigma(x) = x$ and $\tau(x) = x$ and both sides are equal to x . If $x \in M_\sigma$ then $\sigma(x) \in M_\sigma$ (why?). Therefore we have $\tau(\sigma(x)) = \sigma(x)$ and similarly $\sigma(\tau(x)) = \sigma(x)$. So both sides are equal in this case. The case $x \in M_\tau$ is treated in the same way. \square

2.9.1 Cycles

Some permutations in S_n deserve special attention. Suppose we are given k different elements x_1, x_2, \dots, x_k of M_n . A permutation $\sigma \in S_n$ given by

$$\sigma(x_1) = x_2, \quad \sigma(x_2) = x_3, \quad \dots, \quad \sigma(x_{k-1}) = x_k, \quad \sigma(x_k) = x_1$$

and $\sigma(x) = x$ if $x \notin \{x_1, \dots, x_k\}$ is called a k -cycle. It is denoted

$$\sigma = (x_1 \ x_2 \ \dots \ x_k)$$

to indicate that $x_2 = \sigma(x_1), \dots, x_1 = \sigma(x_k)$. In this notation σ may be written in the following k different ways:

$$\begin{aligned} &(x_1 x_2 \dots x_{k-1} x_k), \\ &(x_2 x_3 \dots x_k x_1), \\ &\vdots \\ &(x_k x_1 \dots x_{k-2} x_{k-1}). \end{aligned}$$

Notice that $M_\sigma = \{x_1, x_2, \dots, x_k\}$ and that the order of a k -cycle in S_n is k .

Example 2.9.3 Consider

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

This is the 3-cycle $(1\ 2\ 3)$ in S_3 . As an element in the group S_3 it has order 3. Notice that $(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2)$.

A 1-cycle is literally translated as the identity map. A 2-cycle is called a *transposition*. Notice that a transposition is its own inverse in S_n . A transposition of the form $s_i = (i\ i+1)$, where $i = 1, \dots, n-1$, is called a *simple* transposition.

Example 2.9.4 In S_3 we have

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = s_1 s_2.$$

This follows by evaluating $(1\ 2\ 3)$ and the composition $s_1 s_2$ on 1, 2 and 3 and seeing that they give the same result.

It turns out that every permutation can be expressed as a product of disjoint cycles. Such an expression is useful, for example, in the following proposition.

Proposition 2.9.5 *Let $\sigma \in S_n$ be written as a product of disjoint cycles $\sigma_1 \cdots \sigma_r$. Then the order of σ is the least common multiple of the orders of the cycles $\sigma_1, \dots, \sigma_r$.*

Proof. Since $\sigma_i \sigma_j = \sigma_j \sigma_i$ when $i \neq j$ we get $\sigma^n = \sigma_1^n \cdots \sigma_r^n$ for $n \in \mathbb{N}$. If $\sigma^n = e$ then $\sigma_i^n = e$ for $i = 1, \dots, r$, as $\sigma_1^n, \dots, \sigma_r^n$ are disjoint permutations. Therefore n is divisible by the orders of the cycles, by Proposition

2.6.3(iii). This means that the least common multiple m of the orders of the cycles is $\leq \text{ord}(\sigma)$. However, $\sigma_i^m = e$ for every $i = 1, \dots, r$. Therefore $\text{ord}(\sigma) = m$. \square

We have the following fundamental proposition.

Proposition 2.9.6 *Every permutation $\sigma \in S_n$ is a product of unique disjoint cycles.*

Proof. The proof of the existence uses induction on the number of elements in M_σ . If $|M_\sigma| = 0$ then σ is a product of disjoint 1-cycles. Assume that $|M_\sigma| > 0$. Pick $x \in M_\sigma$. Then $x \neq \sigma(x)$. Form the sequence $x = \sigma^0(x), \sigma(x), \sigma^2(x), \dots$ of elements in M_n and stop when you encounter the first repetition $\sigma^k(x)$, where $\sigma^k(x) = \sigma^j(x)$ for some $0 \leq j < k$. Then $j = 0$ (why?). Define the cycle $\tau = (x_1 x_2 \dots x_k)$ by

$$x_1 = x, \quad x_2 = \sigma(x_1), \quad \dots, \quad x_k = \sigma(x_{k-1}) \quad \text{and} \quad x_1 = \sigma(x_k).$$

Now $M_{\sigma\tau^{-1}} = M_\sigma \setminus \{x_1, \dots, x_k\}$, because if $x \notin \{x_1, \dots, x_k\}$ then $\tau^{-1}(x) = x$. Such an x will satisfy $\sigma(\tau^{-1}(x)) \neq x$ if and only if $\sigma(x) \neq x$. However, if $x \in \{x_1, \dots, x_k\}$ then $\sigma(x) \neq x$ but $\sigma(\tau^{-1}(x)) = x$, since x can be written $\tau(y)$ for $y \in \{x_1, \dots, x_k\}$ with $\sigma(y) = x$. By induction $\sigma\tau^{-1}$ is a product of disjoint cycles $\tau_1 \dots \tau_r$. Since τ must be disjoint from τ_1, \dots, τ_r , it follows that

$$\sigma = \tau_1 \dots \tau_r \tau$$

is a product of disjoint cycles. This proves that a permutation can be written as a product of disjoint cycles. The uniqueness part can be deduced from the existence proof. In fact, if $\sigma = \sigma_1 \dots \sigma_r$ is written as a product of disjoint cycles $\sigma_1, \dots, \sigma_r$ then $M_\sigma = M_{\sigma_1} \cup \dots \cup M_{\sigma_r}$ and $M_{\sigma_i} \cap M_{\sigma_j} = \emptyset$ if $i \neq j$, since σ_i and σ_j are disjoint permutations if $i \neq j$. So, if $x \in M_\sigma$ then $x \in M_{\sigma_j}$ for a unique $j = 1, \dots, r$ and $\sigma_j = (x \sigma(x) \sigma^2(x) \dots)$ since $\sigma(x) = \sigma_j(x)$, when $x \in M_{\sigma_j}$. In this way the cycles occurring in σ written as a product of disjoint cycles are uniquely determined by σ . \square

Example 2.9.7 The element

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix} \in S_6$$

can be written as the product $(1623)(45)$ of disjoint cycles. One simply mimics the procedure outlined in the proof of Proposition 2.9.6: $\sigma(1) = 6$, $\sigma(6) = 2$,

$\sigma(2) = 3$, $\sigma(3) = 1$ gives the 4-cycle (1623) and $\sigma(4) = 5$, $\sigma(5) = 4$ gives the transposition (45). The order of σ is $\text{lcm}(2, 4) = 4$.

The following lemma will be very important for later computations.

Lemma 2.9.8 Suppose that $\tau = (i_1 i_2 \dots i_k)$ is a k -cycle and σ a permutation in S_n . Then

$$\sigma(i_1 i_2 \dots i_k)\sigma^{-1} = (\sigma(i_1) \sigma(i_2) \dots \sigma(i_k)).$$

Proof. Let $J = \{\sigma(i_1), \dots, \sigma(i_k)\}$. Then the left and right hand sides assume the same value on $i \in J$. Since they both map $i \notin J$ to itself, they must be the same permutations. \square

2.9.2 Simple transpositions and “bubble sort”

Let us describe one of the simplest sorting algorithms (“bubble sort”) for sorting n numbers a_1, \dots, a_n . You run through the list a_1, \dots, a_n . Each time you encounter a neighboring pair $a_i > a_{i+1}$ that is not in (ascending) order, you switch the two numbers and go back to the beginning. Do this until there are no more unordered neighboring pairs. Then the sequence has been sorted into ascending order. How does this relate to permutations? Take a look at the example below.

Example 2.9.9 Suppose that we consider the permutation 631542 of the sequence 123456. Using “bubble sort” you can reorder the permuted sequence by switching neighbors:

631542	361542	316542	136542	135642
135462	134562	134526	134256	132456
123456.				

The process of switching neighbors corresponds to the simple transpositions

$$(12)(23)(12)(34)(45)(34)(56)(45)(34)(23),$$

where the numbers refer to the positions in the sequence. In the language of permutations and S_6 you may express the first step of the bubble sort as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix} (12) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 4 & 2 \end{pmatrix}.$$

In total we have proved that

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix} (12)(23)(12)(34)(45)(34)(56)(45)(34)(23) \\ = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

and therefore that

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix} = (23)(34)(45)(56)(34)(45)(34)(12)(23)(12).$$

You should check this by evaluating the permutations on the left and right hand side on 1, 2, 3, 4, 5 and 6.

Example 2.9.9 illustrates the result that every permutation is a product of simple transpositions. What is the minimal number of simple transpositions needed for writing a permutation σ as a product in this way? Surprisingly, the answer lies in counting the number of ordered pairs (i, j) , $i < j$, for which the values $\sigma(i) > \sigma(j)$ are in the wrong order. This is the reasoning behind the following definition.

Definition 2.9.10 Let $\sigma \in S_n$ be a permutation. A pair of indices (i, j) , where $1 \leq i < j \leq n$, is called an *inversion* (of σ) if $\sigma(i) > \sigma(j)$. Let

$$I_\sigma = \{(i, j) \mid 1 \leq i < j \leq n \text{ and } \sigma(i) > \sigma(j)\}$$

denote the set of inversions and let $n(\sigma) = |I_\sigma|$ be the number of inversions of σ .

Example 2.9.11 We have that

$$n\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right) = 2,$$

since $(1, 3)$ and $(2, 3)$ are the only inversions (corresponding to $2 > 1$ and $3 > 1$). Again counting inversions we find that

$$n\left(\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 5 & 4 & 2 \end{pmatrix}\right) = 10.$$

This agrees with the number of simple transpositions we found in Example 2.9.9.

Proposition 2.9.12 *The permutation $\sigma \in S_n$ is the identity map if and only if $n(\sigma) = 0$. If σ is not the identity map then there exists $i = 1, \dots, n-1$ such that $\sigma(i) > \sigma(i+1)$.*

Proof. If σ is the identity map then it has no inversions. Therefore $n(\sigma) = 0$. If $n(\sigma) = 0$ and σ is not the identity map then there exists a smallest $i \in M_n$ such that $\sigma(i) > i$. The pair $(i, \sigma^{-1}(i))$ is an inversion for σ , contradicting that $n(\sigma) = 0$. If σ is a permutation satisfying $\sigma(1) < \sigma(2) < \dots < \sigma(n)$ then σ has to be the identity map, since $n(\sigma) = 0$. This proves the last part of the proposition. \square

The following lemma is crucial.

Lemma 2.9.13 *Let $s_i \in S_n$ be a simple transposition and $\sigma \in S_n$. Then*

$$n(\sigma s_i) = \begin{cases} n(\sigma) + 1 & \text{if } \sigma(i) < \sigma(i+1), \\ n(\sigma) - 1 & \text{if } \sigma(i) > \sigma(i+1). \end{cases}$$

Proof. Assume that $\sigma(i) < \sigma(i+1)$. Since $(i, i+1)$ is an inversion for σs_i (why?) we only need to establish a bijective map

$$\varphi : I_\sigma \rightarrow I_{\sigma s_i} \setminus \{(i, i+1)\}.$$

Such a bijective map is given by $\varphi((k, l)) = (s_i(k), s_i(l))$. If $(k, l) \in I_\sigma$ then $s_i(k) < s_i(l)$, because the only way this can fail is if $k = i$ and $l = i+1$ and, by assumption, $(i, i+1) \notin I_\sigma$. Now $(s_i(k), s_i(l)) \in I_{\sigma s_i}$, since $(k, l) \in I_\sigma$. In the same way, if $(k, l) \in I_{\sigma s_i} \setminus \{(i, i+1)\}$ then $(s_i(k), s_i(l)) \in I_\sigma$. This proves that φ is a bijective map. If $\sigma(i) > \sigma(i+1)$ then we work with the permutation σs_i . In this case we know that $(\sigma s_i)(i) < (\sigma s_i)(i+1)$ and therefore it follows that $n((\sigma s_i)s_i) = n(\sigma) = n(\sigma s_i) + 1$ by what we have already proved. \square

Proposition 2.9.14 *Let $\sigma \in S_n$. Then*

- (i) σ is a product of $n(\sigma)$ simple transpositions.
- (ii) $n(\sigma)$ is the minimal number of simple transpositions needed in writing σ as a product of simple transpositions.

Proof. We will use induction on $n(\sigma)$ for proving (i). If $n(\sigma) = 0$ then σ is the identity map by Proposition 2.9.12 and we are done (σ is the empty product of simple transpositions, which is the identity by definition). If not, we

may find $i = 1, \dots, n-1$ such that $\sigma(i) > \sigma(i+1)$ according to Proposition 2.9.12. Then $n(\sigma s_i) = n(\sigma) - 1$ by Lemma 2.9.13. By induction $\eta = \sigma s_i$ can be written as a product of $n(\sigma) - 1$ simple transpositions. Then $\sigma = \eta s_i$ is a product of $n(\sigma)$ simple transpositions. This proves (i).

Let $\ell(\sigma)$ denote the minimal number of simple transpositions needed in writing σ as a product of simple transpositions. Then $n(\sigma) \geq \ell(\sigma)$ by (i). We will prove that $\ell(\sigma) = n(\sigma)$ using induction on $\ell(\sigma)$. The case $\ell(\sigma) = 0$ follows as in the proof of (i). Assume that $\ell(\sigma) > 0$. Then we may find a simple transposition s_i such that $\ell(\sigma s_i) = \ell(\sigma) - 1$. Therefore $\ell(\sigma s_i) = n(\sigma s_i)$ by induction and $\ell(\sigma) \geq n(\sigma)$ by Lemma 2.9.13. This proves (ii). \square

2.9.3 The alternating group

Definition 2.9.15 The sign of a permutation $\sigma \in S_n$ is

$$\text{sgn}(\sigma) = (-1)^{n(\sigma)}.$$

A permutation with positive sign is called even. A permutation with negative sign is called odd.

Proposition 2.9.16 *The sign*

$$\text{sgn} : S_n \rightarrow \{\pm 1\}$$

of a permutation is a group homomorphism, where the composition in $\{\pm 1\}$ is multiplication.

Proof. We must prove that $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$, where $\sigma, \tau \in S_n$. Since τ is a product of simple transpositions we may assume that τ itself is a simple transposition s_i . By Lemma 2.9.13 we have $n(\sigma s_i) = n(\sigma) \pm 1$, so that $\text{sgn}(\sigma s_i) = -\text{sgn}(\sigma)$. Thus $\text{sgn}(\sigma s_i) = \text{sgn}(\sigma)\text{sgn}(s_i)$, as $n(s_i) = 1$. \square

The set of even permutations in S_n is denoted A_n and called the *alternating group*. It follows by Proposition 2.9.16 that A_n is a normal subgroup of S_n , being the kernel of sgn . By Theorem 2.5.1, we get the group isomorphism

$$S_n/A_n \xrightarrow{\sim} \{\pm 1\},$$

showing that $|A_n| = |S_n|/2 = n!/2$ for $n > 1$. Before moving on, let us see how one can determine $\text{sgn}(\sigma)$ for a permutation $\sigma \in S_n$ from its disjoint cycle decomposition (Proposition 2.9.6). Since sgn is a group homomorphism, we only need to compute the sign of a cycle.

Proposition 2.9.17 *Let $n \geq 2$. A transposition $\tau = (i\ j) \in S_n$ is an odd permutation. The sign of an r -cycle $\sigma = (x_1\ x_2\ \dots\ x_r) \in S_n$ is $(-1)^{r-1}$.*

Proof. We can find a permutation $\eta \in S_n$ such that $\eta(1) = i$ and $\eta(2) = j$. This implies that $-1 = \text{sgn}(1\ 2) = \text{sgn}(\eta(1\ 2)\eta^{-1}) = \text{sgn}((\eta(1)\ \eta(2))) = \text{sgn}(\tau)$. Therefore τ is odd. To see that the sign of σ is $(-1)^{r-1}$, we simply write

$$(x_1\ x_2\ \dots\ x_r) = (x_1\ x_2)(x_2\ x_3)\dots(x_{r-1}\ x_r).$$

We have expressed σ as a product of $r - 1$ transpositions. Therefore $\text{sgn}(\sigma) = (-1)^{r-1}$. \square

2.9.4 Simple groups

A group N is called *simple* if $\{e\}$ and N are the only normal subgroups of N . One can prove that any finite group G has a decreasing sequence of subgroups,

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \dots \supseteq G_{n-1} \supseteq G_n = \{e\},$$

such that G_{i+1} is a normal subgroup of G_i and the quotient group G_i/G_{i+1} is a simple finite group. One may also prove that the simple quotient groups occurring in such a decreasing sequence are uniquely determined up to isomorphism. In this sense the simple finite groups form the building blocks for all finite groups.

Here we prove the following classical result due to E. Galois (1811–32). When developed a little further, into Galois theory, it accounts for the miraculous fact that there is no formula (involving the usual arithmetical operations and extracting roots) for the solution of a general algebraic equation of degree ≥ 5 . First we need a simple but important lemma.

Lemma 2.9.18 *Every permutation in A_n is a product of 3-cycles if $n \geq 3$.*

Proof. A permutation in A_n is a product of an even number of transpositions. Consider four distinct numbers a, b, c and d . Then $(a\ b)(c\ d) = (a\ d\ c)(a\ b\ c)$ and $(a\ b)(b\ c) = (a\ b\ c)$. So we may replace consecutive pairs of transpositions with products of 3-cycles. This proves the claim. \square

Theorem 2.9.19 *The alternating group A_n is simple for $n \geq 5$.*

Proof. We will prove that

- (i) Given a 3-cycle $\tau \in A_n$, there is a permutation $\sigma \in A_n$ such that $\sigma\tau\sigma^{-1} = (123)$.
(ii) A non-trivial normal subgroup N of A_n must contain a 3-cycle.

We now go through these two steps. (i) Let $\tau = (ijk)$ be a 3-cycle. We can find a permutation $\sigma \in S_n$ such that $\sigma(i) = 1$, $\sigma(j) = 2$ and $\sigma(k) = 3$. Now Lemma 2.9.8 gives

$$\sigma(ijk)\sigma^{-1} = (123).$$

We may assume that $\sigma \in A_n$ by replacing σ with $(45)\sigma$ in the case $\sigma \notin A_n$: $((45)(123)(45))^{-1} = (123)$. This proves (i).

(ii) Let N be a non-trivial normal subgroup of A_n . We need to show that N contains a 3-cycle τ . Let $\sigma \in N$ denote an element $\neq e$. Write σ as a product $\tau_1\tau_2 \cdots \tau_r$ of disjoint cycles. If two of the disjoint cycles are transpositions, we may assume that $\tau_1 = (12)$ and $\tau_2 = (34)$ and thus $\sigma = (12)(34)\eta$ for some $\eta \in S_n$. Putting $\tau = (123)$ we get a new permutation $\sigma_1 = \tau\sigma\tau^{-1}\sigma^{-1}$ that also lies in N , since N is a normal subgroup. Composing permutations we get (using Lemma 2.9.8)

$$\sigma_1 = \tau\sigma\tau^{-1}\sigma^{-1} = (13)(24).$$

Now using the same trick with $\rho = (245)$, we get

$$\sigma_2 = \rho\sigma_1\rho^{-1}\sigma_1^{-1} = (254).$$

So σ_2 is the desired 3-cycle in N . If σ contains a cycle $(1234 \dots)$ of length at least 4 we get the 3-cycle

$$\tau\sigma\tau^{-1}\sigma^{-1} = (124)$$

in N , where $\tau = (123)$. The only case left is where σ contains a 3-cycle (123) and another cycle $(45 \dots)$. In this case we get, using $\tau = (234)$, that

$$\tau\sigma\tau^{-1}\sigma^{-1} = (14235),$$

which is a cycle of length 5. We already know why this implies that N contains a 3-cycle.

We know that, for every 3-cycle τ , there is an element $\sigma \in A_n$ such that

$$\sigma\tau\sigma^{-1} = (123).$$

This means that, given two arbitrary 3-cycles τ_1 and τ_2 , there is a $\sigma \in A_n$ such that $\sigma\tau_1\sigma^{-1} = \tau_2$. Thus if a normal subgroup N of A_n contains just one 3-cycle, it will have to contain all 3-cycles! In this way we have proved that a normal

subgroup N of A_n is either $\{e\}$ or A_n , as we know that every element of A_n is a product of 3-cycles by Lemma 2.9.18. □

One of the milestones of modern group theory is the theorem of Feit and Thompson. They proved in 1963 that the order of a non-abelian finite simple group must be even. The proof of this takes up more than 250 pages [9]. Simple finite groups fall into some well defined families except for 26 finite simple groups, the sporadic groups. The largest sporadic group is called the monster group. It has

$$8080174247945128758864599049617107570057543680000000000 \\ = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

elements. The classification of the finite simple groups was completed in 1980 (but has not yet been written up completely!).

2.9.5 The 15-puzzle

Can you interchange the empty square successively with adjacent squares so that the configuration on the left gets changed into the “correct” configuration, the one on the right below?

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

This is the classical 15-puzzle, as published by the American puzzlemaker Sam Loyd in 1878. He offered a prize of 1000 dollars for the first correct solution to the problem. He went on to write (see [10])

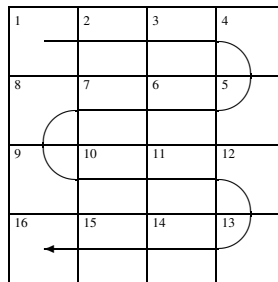
People became infatuated with the puzzle and ludicrous tales are told of shopkeepers who neglected to open their stores; of a distinguished clergyman who stood under a street lamp all through a wintry night trying to recall the way he had performed the feat. The mysterious feature of the puzzle is that none seem to be able to remember the sequence of moves whereby they feel sure they succeeded in solving the puzzle. Pilots are said to have wrecked their ships, and engineers rush

their trains past stations. A famous Baltimore editor tells how he went for his noon lunch and was discovered by his frantic staff long past midnight pushing little pieces of pie around on a plate! Farmers are known to have deserted their plows . . .

The frustrated farmer below appeared in Loyd's original article on the puzzle.



Following [2] we will go through a method of analyzing this problem using symmetric and alternating groups. Each square (including the empty square) occupies one of the 16 numbered *cells* below.



(2.1)

A configuration C maps to a permutation σ_C in S_{15} defined by writing the squares according to their order along the snake pattern in (2.1) (forgetting the empty square). For example, the “correct” configuration maps to

$$\begin{aligned}
 & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 2 & 3 & 4 & 8 & 7 & 6 & 5 & 9 & 10 & 11 & 12 & 15 & 14 & 13 \end{pmatrix} \\
 &= (5\ 8)(6\ 7)(13\ 15)
 \end{aligned}$$

and the “evil” Loyd configuration maps to

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 1 & 2 & 3 & 4 & 8 & 7 & 6 & 5 & 9 & 10 & 11 & 12 & 14 & 15 & 13 \end{pmatrix} \\ = (5\ 8)(6\ 7)(13\ 14\ 15).$$

The correct configuration maps to an odd permutation and the “evil” Loyd configuration maps to an even permutation. We will see shortly that this is the reason why the original 15-puzzle was unsolvable, so that Loyd was sure never to lose his 1000 dollars.

The mapping of a configuration to a permutation in S_{15} using the snake pattern is not a one-to-one correspondence. The configurations you get by moving the empty square along the snake all map to the same permutation in S_{15} . If C is a configuration where the blank square occupies cell b and square i occupies cell j then

$$\sigma_C^{-1}(i) = \begin{cases} j & \text{if } j < b, \\ j - 1 & \text{if } j > b. \end{cases}$$

Suppose that we have a configuration C_1 where the empty square occupies cell i . By moving the empty square (legally) to cell j we get a new configuration C_2 , where the blank square occupies cell j . Then σ_{C_1} and σ_{C_2} are related through a fixed permutation $\sigma_{i,j} \in S_{15}$ via $\sigma_{C_2}^{-1} = \sigma_{i,j} \sigma_{C_1}^{-1}$. The permutations corresponding to the legal moves can be read off from (2.1). They are

$$\sigma_{1,2}, \sigma_{2,3}, \dots, \sigma_{15,16}, \sigma_{1,8}, \sigma_{2,7}, \sigma_{3,6}, \sigma_{7,10}, \sigma_{6,11}, \sigma_{5,12}, \sigma_{11,14}, \sigma_{10,15}, \sigma_{9,16} \quad (2.2)$$

along with their inverse permutations. It is easy to see that $\sigma_{1,2} = \sigma_{2,3} = \dots = \sigma_{15,16} = 1$. These moves do not affect σ_C for a given configuration C for which the empty square is positioned in the appropriate cell. Let us have a closer look at $\sigma_{1,8}$. After having done this move, which consists in moving the empty square from cell 1 to cell 8, the square that was number 1 becomes number 2, the square that was number 2 becomes number 3, \dots , the square that was number 7 becomes number 1. This proves that

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

Just as in the $\sigma_{1,8}$ case we can easily compute the permutations corresponding to the other legal moves. Below we list the permutations corresponding to the

legal moves in (2.2) other than $\sigma_{i,i+1}$, $1 \leq i \leq 15$:

$$\begin{aligned}\sigma_{1,8} &= (1\ 2\ 3\ 4\ 5\ 6\ 7), \\ \sigma_{2,7} &= (2\ 3\ 4\ 5\ 6), \\ \sigma_{3,6} &= (3\ 4\ 5), \\ \sigma_{7,10} &= (7\ 8\ 9), \\ \sigma_{6,11} &= (6\ 7\ 8\ 9\ 10), \\ \sigma_{5,12} &= (5\ 6\ 7\ 8\ 9\ 10\ 11), \\ \sigma_{9,16} &= (9\ 10\ 11\ 12\ 13\ 14\ 15), \\ \sigma_{10,15} &= (10\ 11\ 12\ 13\ 14), \\ \sigma_{11,14} &= (11\ 12\ 13).\end{aligned}$$

The permutations corresponding to the legal moves are all cycles of odd length. By Proposition 2.9.17 a cycle of odd length is an even permutation. The upshot is that if we have a configuration C_1 and perform a series of legal moves corresponding to permutations τ_1, \dots, τ_n and finally reaching the configuration C_2 then

$$\sigma_{C_2}^{-1} = \tau_n \cdots \tau_1 \sigma_{C_1}^{-1},$$

and therefore $\text{sgn}(\sigma_{C_2}) = \text{sgn}(\sigma_{C_1})$. So unless two configurations map to permutations of the same sign you cannot come from one to the other through a sequence of legal moves. This proves that the original Loyd puzzle is unsolvable. This could have been verified without going through the machinery of writing legal moves as permutations in A_{15} . Using the permutation description of the legal moves we can actually prove more, as follows.

A surprising fact is that if two configurations map to permutations of the same sign then you can come from one to the other using a sequence of legal moves. We will give a simple proof of this here. First we need a small lemma. We call a 3-cycle *simple* if it has the form $(k\ k+1\ k+2)$.

Lemma 2.9.20 *Every 3-cycle is a product of simple 3-cycles in A_n if $n \geq 3$.*

Proof. This is proved by induction. For $n = 3$ one gets all 3-cycles as powers of the simple 3-cycle $(1\ 2\ 3)$. If $n > 3$ we may assume by induction that every 3-cycle not containing both 1 and n can be written as a product of simple 3-cycles. Consider the 3-cycle $(1\ x\ n)$ containing both 1 and n . Choose $y \notin \{1, x, n\}$. Then $(1\ x\ n) = (1\ x\ y)(x\ n\ y)$ and $(1\ n\ x) = (1\ x\ n)^2$. This proves by induction that every 3-cycle in A_n can be written as a product of simple 3-cycles. \square

Now we get by Lemma 2.9.18 that every even permutation is a product of simple 3-cycles. This leads us to the main result:

Theorem 2.9.21 *Every permutation in A_{15} is a product of permutations corresponding to legal moves in the 15-puzzle.*

Proof. It suffices to prove that all the simple 3-cycles can be written as products of the legal moves. We will show how to get the simple 3-cycles $(1\ 2\ 3)$, \dots , $(5\ 6\ 7)$ and leave the rest to the reader. Consider the two legal moves $\tau = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ and $\sigma = (3\ 4\ 5)$. Then

$$\tau\sigma\tau^{-1} = (\tau(3)\ \tau(4)\ \tau(5)) = (4\ 5\ 6)$$

by Lemma 2.9.8. Similarly $\tau^2\sigma\tau^{-2} = (5\ 6\ 7)$, $\tau^5\sigma\tau^{-5} = (1\ 2\ 3)$ and $\tau^6\sigma\tau^{-6} = (2\ 3\ 4)$. \square

Suppose we have two configurations C_1, C_2 for which $\text{sgn}(\sigma_{C_1}) = \text{sgn}(\sigma_{C_2})$. Then $\sigma_{C_2}^{-1}\sigma_{C_1} \in A_{15}$. This means that $\sigma_{C_2}^{-1}\sigma_{C_1}$ can be written as a product $\tau_1 \cdots \tau_r$ of permutations corresponding to legal moves, by Theorem 2.9.21. Thus $\sigma_{C_2}^{-1} = \tau_1 \cdots \tau_r \sigma_{C_1}^{-1}$. We can translate this back into a sequence of legal moves turning C_1 into C_2 . This is done by placing the empty square in the appropriate cell according to each permutation (recall that the permutation does not change when the empty square is moved along the snake pattern). For example for $\tau = \sigma_{i,j}$ we move the empty square to cell i in order to carry out the move from cell i to cell j .

2.10 Actions of groups

Groups are very powerful algebraic objects in themselves, but most of the time it is more interesting to know how they interact with the world around them. The relevant notion is that of a group acting on a set. In this section we will apply actions of groups to combinatorics and counting, to conjugacy classes in the symmetric groups and to the proof of the Sylow theorems.

Definition 2.10.1 Let G be a group and S a set. We will say that G acts (from the left) on S if there is a map

$$\alpha : G \times S \rightarrow S,$$

denoted $\alpha(g, s) = g \cdot s$, such that

- (i) $e \cdot s = s$ for every $s \in S$,
- (ii) $(g \cdot h) \cdot s = g \cdot (h \cdot s)$ for every $g, h \in G$ and every $s \in S$.

When no confusion is likely to arise we will leave out the multiplication point from $g \cdot s$ and just write gs .

Definition 2.10.2 Let $\alpha : G \times S \rightarrow S$ be an action of G on S , $X \subseteq S$ a subset of S and $s \in S$ an element of S . Then $G \cdot s = Gs = \{gs \mid g \in G\}$ is called the *orbit* of s (under the action of G). The set of orbits $\{Gs \mid s \in S\}$ is denoted S/G . Let $g \cdot X = gX = \{gx \mid x \in X\}$, where $g \in G$. Then

$$G_X = \{g \in G \mid gX = X\}$$

is called the stabilizer of X . If $X = \{x\}$ we denote G_X by G_x . A fixed point for the action is an element $s \in S$ such that $gs = s$ for every $g \in G$. The set of fixed points is denoted S^G .

Example 2.10.3 The above definitions may seem abstract, but we have already seen many examples of them.

- (i) The symmetric group S_n acts on the set $M_n = \{1, 2, \dots, n\}$ in the natural way $\sigma i = \sigma(i)$, where $\sigma \in S_n$ and $i \in M_n$. The stabilizer $(S_n)_i$ consists of the permutations fixing i . Let $\sigma \in S_n$ and let H denote the subgroup $\langle \sigma \rangle$. Then we have an action $\alpha_H : H \times S \rightarrow S$ (given by $\sigma^n i = \sigma^n(i)$, where $n \in \mathbb{N}$ and $i \in S$). The orbits of this action are in one-to-one correspondence with the disjoint cycles of σ (see Proposition 2.9.6).
- (ii) Let H be a subgroup of a group G . Then we have an action $\alpha : H \times G \rightarrow G$ given by

$$\alpha(h, g) = h \cdot g = gh^{-1} \text{ (why do we need } h^{-1} \text{ and not just } h?).$$

The orbit $H \cdot g$ is the left coset gH . The set of orbits of this action is the set G/H of left cosets of H . Notice that this action does not have any fixed points.

- (iii) Let L be the group of linear isometries of \mathbb{R}^2 (Example 2.1.12). Then there is a natural action $\alpha : L \times \mathbb{R}^2 \rightarrow \mathbb{R}^2$ given by $\alpha(\varphi, v) = \varphi(v)$. The stabilizer L_K of $K \subseteq \mathbb{R}^2$ is the group D_3 , where K is the triangle in Example 2.1.13. The origin $(0, 0)$ is the only fixed point of this action. The orbit $L(x, y)$ is the circle centered in the origin with radius $\sqrt{x^2 + y^2}$.

We have singled out the following example of a group action, because it is important in almost all mathematics. We will make use of it later when proving the Sylow theorems.

Example 2.10.4 Let G be a group and H a subgroup. We may not be able to make G/H into a group (H is not necessarily normal), but there is an action $\alpha : G \times G/H \rightarrow G/H$ of G , on the left cosets of H , given by $\alpha(g, g'H) = (gg')H$ where $g, g' \in G$. This is an action with only one orbit.

Proposition 2.10.5 Let $\alpha : G \times S \rightarrow S$ be an action.

- (i) Let $X \subseteq S$ be a subset of S . Then G_X is a subgroup of G .
- (ii) The set S is the union of G -orbits

$$S = \bigcup_{s \in S} Gs,$$

where $Gs \neq Gt$ implies $Gs \cap Gt = \emptyset$ if $s, t \in S$.

- (iii) Let $x \in S$. Then

$$\tilde{f} : G/G_x \rightarrow Gx$$

given by $\tilde{f}(gG_x) = gx$ is a well defined and bijective map between the left cosets of G_x and the orbit Gx .

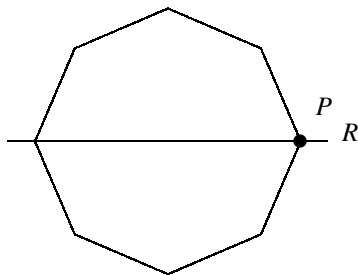
Proof. (i) Clearly $e \in G_X$, and if $g, h \in G_X$ then $gh \in G_X$. If $g \in G_X$ then $g^{-1}X = g^{-1}(gX) = eX = X$, so that $g^{-1} \in G_X$. This shows that G_X is a subgroup of G .

(ii) If $s \in S$ then $es \in S$, so that $s \in Gs$. This shows that $S = \cup_{s \in S} Gs$. Let us prove that $Gs \neq Gt$ gives $Gs \cap Gt = \emptyset$. Suppose that $z \in Gs \cap Gt \neq \emptyset$. Then we can find $g_1, g_2 \in G$ such that $z = g_1s = g_2t$. This implies that $s = es = g_1^{-1}(g_1s) = g_1^{-1}(g_2t) = (g_1^{-1}g_2)t$, so that $s \in Gt$ and thereby $Gs \subseteq Gt$. In the same way we get that $Gt \subseteq Gs$, so that $Gs = Gt$.

(iii) Let $g_1, g_2 \in G$. Then $g_1x = g_2x$ if and only if $x = (g_1^{-1}g_2)x$ if and only if $g_1^{-1}g_2 \in G_x$. By Lemma 2.2.6 we get $g_1x = g_2x$ if and only if $g_1G_x = g_2G_x$. So $\tilde{f}(gG_x) = gx$ is a well defined and injective map. Since it is also surjective, it is a bijective map. \square

Example 2.10.6 Recall that the group L of linear isometries acts naturally on \mathbb{R}^2 via $\varphi v = \varphi(v)$, where $\varphi \in L$ and $v \in \mathbb{R}^2$. Suppose that $O \subseteq \mathbb{R}^2$ is

an octagon



centered at $(0, 0)$. We consider the set G of linear isometries mapping O to itself:

$$G = \{\varphi \in L \mid \varphi(O) = O\}.$$

In the language of group actions G is the stabilizer of O , i.e. $G = L_O$. How do we determine the order $|G|$ of G ? Let us first see that $|G|$ is finite. The following argument is quite general and can be used in many other circumstances. Let the vertices of O be listed as $V = \{1, 2, \dots, 8\}$. If $g \in G$ and $v \in V$ then $gv \in V$, since g is a reflection or a rotation by Example 2.1.12. This shows that G acts on V and that we have a group homomorphism $\varphi : G \rightarrow S_8$ given by $\varphi(g)(v) = gv$. If $gv = v$ for every $v \in V$ then g must be the identity, since g is a linear map fixing a basis of \mathbb{R}^2 . Therefore φ is injective and $|G| \leq 8!$. The orbit of the vertex P is $GP = V$. Now we can use the formula $|G/G_P| = |GP| = |V|$ from Proposition 2.10.5(iii) to compute the order of G . The stabilizer G_P consists only of the identity and the reflection in the line R . So $|G_P| = 2$. Therefore $|V| = |G/G_P| = |G|/2$ and thus $|G| = 2 \cdot 8 = 16$.

The method illustrated in Example 2.10.6 becomes even more useful when computing orders of “symmetry” groups in \mathbb{R}^3 (such as stabilizers of the cube or the regular dodecahedron under the action of the group SO_3 of rotations of \mathbb{R}^3).

From Proposition 2.10.5 we can also deduce the following important counting formula.

Corollary 2.10.7 *Let $G \times S \rightarrow S$ be an action, where S is a finite set. Then*

$$|S| = |S^G| + \sum_x |G/G_x|,$$

where the summation is done by picking out an element x from each orbit with more than one element.

Proof. By Proposition 2.10.5(ii), we may count the number of elements in S by counting the number of elements in each orbit and adding these. The formula expresses this, in that we first count the orbits containing one point (this is the term $|S^G|$) and then the orbits containing two or more points (this is the summation). In the latter case we use the bijection $Gx \rightarrow G/G_x$ from Proposition 2.10.5(iii). \square

The following lemma is a very valuable tool for doing combinatorics and counting. Notice how having two different ways of counting leads to a surprising formula.

Lemma 2.10.8 (Burnside) *Let $G \times S \rightarrow S$ be an action, where G is a finite group and S a finite set. Then*

$$|S/G| = \frac{\sum_{g \in G} |S^g|}{|G|}$$

where $S^g = \{x \in S \mid gx = x\}$.

Proof. Define $T = \{(g, x) \in G \times S \mid gx = x\}$. We will count the elements in T in two different ways. For every $g \in G$ we count the number of $x \in S$ fixed by g . This is the same as for every $x \in S$ counting the number of $g \in G$ that fixes x . Thus we have the formula

$$|T| = \sum_{g \in G} |S^g| = \sum_{x \in S} |G_x|.$$

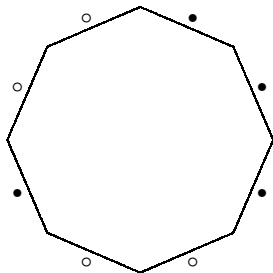
The last sum can be rewritten using Proposition 2.10.5(ii):

$$\sum_{x \in S} |G_x| = \sum_{\text{orbits } Gx} \sum_{y \in Gx} |G_y| = \sum_{\text{orbits } Gx} |Gx| |G_x| = \sum_{\text{orbits } Gx} |G| = |S/G| |G|,$$

since $Gy = Gx$ when $y \in Gx$ and therefore $|G_y| = |G_x|$, by Proposition 2.10.5(iii). This gives the desired result. \square

Example 2.10.9 Suppose that you color four of the edges of the octagon in Example 2.10.6 white and four black. You can do this in $\binom{8}{4} = 70$ ways, but some of them can be mapped to each other using reflections and rotations. We wish to count the number of essentially different colorings. The group G from Example 2.10.6 acts on the set S of colorings without taking into account that some of them are the same. So $|S| = 70$. The colorings in the same orbits of

this action are considered as the same (two colorings are in the same orbit if you can reflect or rotate one to the other).



We wish to find the number of orbits $|S/G|$ using Lemma 2.10.8. Now, G has 16 elements consisting of eight reflections and eight rotations. We need to find $|S^g|$ for $g \in G$. Let g be a reflection in a line through two opposite vertices of the octagon. Once we have chosen the colors of two edges of the four on one side of the line, the colors of the rest of the edges are determined if the coloring is invariant under g . This means that $|S^g| = \binom{4}{2} = 6$. Now let g be a reflection in a line through the midpoints of opposite edges. The color of these two opposite edges has to be the same for the coloring to be invariant under g . Therefore $|S^g| = 2 \cdot 3 = 6$.

Of course, $|S^e| = 70$. If g is a rotation of $\pi/4$, $3\pi/4$, $5\pi/4$ or $7\pi/4$ then $|S^g| = 0$. If g is a rotation of $\pi/2$ or $3\pi/2$ then $|S^g| = 2$. Finally, if g is a rotation of π then $|S^g| = \binom{4}{2} = 6$. Plugging these numbers into Burnside's formula gives

$$|S/G| = \frac{1}{16}(6 + 6 + 6 + 6 + 6 + 6 + 6 + 6 + 70 + 2 + 2 + 6) = 8.$$

Example 2.10.10 Let us look again at Example 2.10.9 but now consider only the group G of rotations acting on the set S of colorings. So G consists of rotations of $2k\pi/8$, where $k = 0, 1, \dots, 7$. Two colorings are considered the same if they are in the same orbit under the action of G . This means that you can map one to the other using a rotation in G . How many essentially different colorings are there now? Again this amounts to counting the number of orbits of G in S . We already have the relevant numbers $|S^g|$ for $g \in G$ from Example 2.10.9. Let us plug them into Burnside's formula and compute

$$|S/G| = \frac{1}{8}(70 + 0 + 2 + 0 + 6 + 0 + 2 + 0) = 10.$$

2.10.1 Conjugacy classes

The map $\alpha : G \times G \rightarrow G$ given by $\alpha(g, h) = ghg^{-1}$ is an action of G on G . It is called *conjugation*. The orbit

$$G \cdot h = C(h) = \{ghg^{-1} \mid g \in G\}$$

is denoted $C(h)$ and called the *conjugacy class* containing h . The stabilizer G_h is denoted $Z(h)$ and called the *centralizer* of h . Notice that

$$Z(h) = \{g \in G \mid gh = hg\}.$$

The set of fixed points

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

is denoted $Z(G)$ and called the *center* of G . There is at least one fixed point for the conjugation action, namely $e \in Z(G)$. In fact $Z(G)$ is an abelian normal subgroup of G (see Exercise 2.50). The stabilizer of a subgroup $H \subseteq G$,

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

is denoted $N_G(H)$ and called the *normalizer* of H in G . Notice that H is a normal subgroup if and only if $N_G(H) = G$ (see Exercise 2.51). If G is a finite group then we may write Corollary 2.10.7 as

$$|G| = |Z(G)| + \sum_{h \in G} |G/Z(h)|,$$

where the last sum is done by picking out one element h from each conjugacy class with more than one element.

2.10.2 Conjugacy classes in the symmetric group

Conjugacy classes in the symmetric group S_n have a very appealing description. Let $\sigma \in S_n$ and write $\sigma = \sigma_1 \sigma_2 \cdots \sigma_r$ as a product of disjoint cycles (Proposition 2.9.6) of increasing length $i_1 \leq i_2 \leq \cdots \leq i_r$. We get for example that

$$(34) = (1)(2)(34)$$

for $(34) \in S_4$, so that $i_1 = i_2 = 1$ and $i_3 = 2$. The increasing sequence $i_1 \leq \cdots \leq i_r$ is called the *cycle type* of σ . It follows by Lemma 2.9.8 that the conjugacy class $C(\sigma)$ consists of permutations with the same cycle type as σ . You may see this by writing on top of each other two permutations $\sigma_1, \sigma_2 \in S_n$ with the

same cycle type. Let $\tau \in S_n$ be given by mapping the elements on top to the elements below. Then $\tau\sigma_1\tau^{-1} = \sigma_2$. An example will clarify this.

Example 2.10.11 Let $\sigma_1 = (1\ 2)(3\ 4)$ and $\sigma_2 = (2\ 3)(4\ 1)$ be permutations in S_4 . Then we can write σ_1 and σ_2 on top of each other as follows:

$$\begin{array}{cccc} (1\ 2)(3\ 4) \\ (2\ 3)(4\ 1). \end{array}$$

Now define τ by

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Then we see that $\tau\sigma_1\tau^{-1}$ is given by

$$\tau(1\ 2)(3\ 4)\tau^{-1} = \tau(1\ 2)\tau^{-1}\tau(3\ 4)\tau^{-1} = (\tau(1)\ \tau(2))(\tau(3)\ \tau(4)) = \sigma_2.$$

Counting the number of elements in a conjugacy class is a combinatorial problem. The number of conjugacy classes in S_n is the number of sequences $1 \leq i_1 \leq i_2 \leq \cdots \leq i_r$ of integers with

$$i_1 + \cdots + i_r = n.$$

For example, there are five conjugacy classes in S_4 , corresponding to the sequences

$$\begin{array}{l} 1 \leq 1 \leq 1 \leq 1, \\ 1 \leq 1 \leq 2, \\ 1 \leq 3, \\ 2 \leq 2, \\ 4. \end{array}$$

The permutation $\sigma = (3\ 4)$ lies in the conjugacy class corresponding to $1 \leq 1 \leq 2$. The conjugacy class $C(\sigma)$ consists of the elements

$$\{(3\ 4), (2\ 4), (2\ 3), (1\ 4), (1\ 3), (1\ 2)\}.$$

Therefore $|Z(\sigma)| = |S_4|/|C(\sigma)| = 4$.

Remark 2.10.12 Counting the number of conjugacy classes in S_n translates into the problem of counting increasing sequences $1 \leq i_1 \leq i_2 \leq \cdots \leq i_r \leq n$ such that $i_1 + \cdots + i_r = n$. For example, when $n = 6$ there are the following

increasing sequences:

$$6 = 1 + 1 + 1 + 1 + 1 + 1,$$

$$6 = 1 + 1 + 1 + 1 + 2,$$

$$6 = 1 + 1 + 2 + 2,$$

$$6 = 2 + 2 + 2,$$

$$6 = 1 + 1 + 1 + 3,$$

$$6 = 1 + 2 + 3,$$

$$6 = 3 + 3,$$

$$6 = 1 + 1 + 4,$$

$$6 = 2 + 4,$$

$$6 = 1 + 5,$$

$$6 = 6.$$

This combinatorial problem was studied by Euler in his landmark work *Introductio in Analysin Infinitorum* (1748). Let $p(n)$ be the number of ways in which an integer n can be written as a sum of natural positive numbers. Note that $p(0) = 1$, counting the empty sum as a way of writing 0, and $p(n) = 0$ if $n < 0$. We have seen above that $p(6) = 11$. Euler proved the remarkable identity

$$\begin{aligned} p(n) = & p(n-1) + p(n-2) - p(n-5) - p(n-7) \\ & + p(n-12) + p(n-15) - \dots \end{aligned} \quad (2.3)$$

where the numbers subtracted from n are $\frac{1}{2}(3k^2 \mp k)$, $k = 1, 2, \dots$

2.10.3 Groups of order p^r

A finite group of order p^r , where p is a prime number and $r \in \mathbb{N}$, is called a *p-group*.

Proposition 2.10.13 *Let G be a non-trivial p -group acting on a finite set S . Then $|S| \equiv |S^G| \pmod{p}$.*

Proof. Corollary 2.10.7 gives

$$|S| = |S^G| + \sum_{x \in S} |G/G_x|,$$

where the summation on the right hand side is done by picking out an element x from each orbit with more than one element (x is not a fixed point). If $x \in S$ is not a fixed point then G_x is a proper subset of G . Therefore p divides $|G/G_x| = |G|/|G_x|$. Thus p divides every term in the summation on the right hand side. Therefore p divides $|S| - |S^G|$. \square

Corollary 2.10.14 *Let G be a non-trivial p -group of order p^r . Then*

$$|G| \equiv |Z(G)| \pmod{p}$$

and $|Z(G)| > 1$.

Proof. This is done simply by using Proposition 2.10.13 for the conjugation action. In this case the $Z(G)$ are the fixed points. Since $p \nmid p^r - 1$ we obtain $|Z(G)| > 1$. \square

Corollary 2.10.15 *Let p be a prime number. A group G of order $|G| = p^2$ is abelian.*

Proof. We will prove that $|Z(G)| = |G|$. By Corollary 2.10.14, we get $|Z(G)| > 1$. Since $|Z(G)|$ divides $|G|$, the only possibilities left are $|Z(G)| = p$ or $|Z(G)| = p^2$. We wish to exclude $|Z(G)| = p$. Suppose that this is the case. Since $Z(G) \subseteq G$ is a normal subgroup, $G/Z(G)$ is a group of order p . Therefore it has to be cyclic, by Proposition 2.7.2. Let $xZ(G)$ be a generator for $G/Z(G)$, where $x \in G$. Then every $gZ(G) = x^n Z(G)$ for some power $n \in \mathbb{N}$. In particular every element $g \in G$ can be written $g = x^n a$, where $a \in Z(G)$. But $(x^m a)(x^n b) = (x^n b)(x^m a)$ when $a, b \in Z(G)$. This proves that G is abelian, contradicting $|Z(G)| = p < |G|$. \square

Extending the method in the proof of Corollary 2.10.15 a little, one can show that $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ are the only groups of order p^2 up to isomorphism. There is also a small modification to the proof that makes it simpler: if $|Z(G)| = p$ then there must exist $g \in G \setminus Z(G)$. But then $Z(G) \subsetneq Z(g)$. This implies that $Z(g) = G$ or that $g \in Z(G)$, which is a contradiction.

2.10.4 The Sylow theorems

We now move on to the celebrated Sylow theorems. Sylow (1832–1918) published a 10-page paper [24] in *Mathematische Annalen* in 1872 containing

three theorems. His three theorems have survived to the present day and are of fundamental importance.

Definition 2.10.16 Let G be a finite group and p a prime number, and suppose that $|G| = p^r m$, where $p \nmid m$. A *Sylow p -subgroup* is a subgroup $H \subseteq G$ of order p^r .

Theorem 2.10.17 (First Sylow theorem) Let G be a finite group and p a prime number, and suppose that $|G| = p^r m$, where $p \nmid m$. Then G contains a Sylow p -subgroup.

Proof. Define a map $\alpha : G \times S \rightarrow S$, where $S = \{X \subseteq G \mid |X| = p^r\}$, given by $\alpha(g, X) = \{gx \mid x \in X\}$, where $X \in S$ and $g \in G$. It follows from subsection 2.1.6 that $\alpha(g, X) \in S$ when $g \in G$ and $X \in S$. It is easy to see that α is an action of G on S . The number of subsets with p^r elements in a set having $p^r m$ elements is given by the binomial coefficient

$$|S| = \binom{p^r m}{p^r} = \frac{p^r m (p^r m - 1) \cdots (p^r m - p^r + 1)}{p^r (p^r - 1) \cdots 1}.$$

Since $p^{r+1} \nmid p^r m - i$ and $p^{r+1} \nmid p^r - i$ for $i = 0, \dots, p^r - 1$, it follows that the highest power of p dividing $p^r - i$, is the highest power of p dividing $p^r m - i$, for $i = 0, \dots, p^r - 1$. From this we deduce the important fact that $p \nmid |S|$.

By Proposition 2.10.5(ii), there must exist an orbit $G \cdot X$, where $X \in S$, such that $p \nmid |G \cdot X|$. From $|G_X||G \cdot X| = |G|$ (Proposition 2.10.5(iii)), it follows that p^r divides $|G_X|$. We will show that $|G_X| = p^r$. To this end we use the action of G_X on X itself. The orbits of this action are the right cosets $G_X g$ of G_X . So the orbits each have $|G_X|$ elements (why?). Again by Proposition 2.10.5(ii) we get that $|G_X|$ divides $|X| = p^r$. This proves that $|G_X| = p^r$ and therefore that G_X is a Sylow p -subgroup of G . \square

Theorem 2.10.18 (Second Sylow theorem) Let G be a finite group and P, Q two Sylow p -subgroups. Then there exists $g \in G$ such that

$$gPg^{-1} = Q.$$

Furthermore, any p -subgroup H is contained in a Sylow p -subgroup.

Proof. The natural action of G on G/Q (Example 2.10.4) restricts to give an action of P on G/Q . Since p does not divide $|G/Q| = |G|/|Q|$, this action has

a fixed point by Proposition 2.10.13. Thus we can find a left coset xQ , $x \in G$, such that $gxQ = xQ$ for every $g \in P$. This means that $P \subseteq xQx^{-1}$. But since $|P| = |Q| = |xQx^{-1}|$, we must have $P = xQx^{-1}$.

Let H be a non-trivial p -subgroup and P a Sylow p -subgroup. As above H acts on G/P and has a fixed point yP , $y \in G$. This means that $hyP = yP$ for every $h \in H$ and therefore that $H \subseteq yPy^{-1}$, so that H is contained in the Sylow p -subgroup yPy^{-1} . \square

Theorem 2.10.19 (Third Sylow theorem) *Let G denote a finite group of order $p^r m$, where $p \nmid m$. Let $\text{Syl}_p(G)$ denote the set of Sylow p -subgroups. Then*

- (i) $|\text{Syl}_p(G)|$ divides m ,
- (ii) $|\text{Syl}_p(G)| \equiv 1 \pmod{p}$.

Proof. Let P be a Sylow p -subgroup. Then G acts on $\text{Syl}_p(G)$ by conjugation. This action has only one orbit, by the second Sylow theorem. Thus by Proposition 2.10.5(iii) we get

$$|\text{Syl}_p(G)| = |G/N_G(P)|,$$

where P is a Sylow p -subgroup. But since $P \subseteq N_G(P)$, it follows that $|G/P| = |G/N_G(P)| |N_G(P)/P|$ (see Exercise 2.18). Therefore $|\text{Syl}_p(G)|$ divides $|G/P| = m$. This proves (i).

The conjugation action of G on $\text{Syl}_p(G)$ restricts to give an action of P on $\text{Syl}_p(G)$. To prove (ii), it suffices by Proposition 2.10.13 to show that P is the only fixed point for this action. Suppose that $Q \in \text{Syl}_p(G)$ is a fixed point, i.e. $gQg^{-1} = Q$ for every $g \in P$. This means that $P \subseteq N_G(Q)$. Now using the second Sylow theorem on the Sylow p -subgroups P and Q of the group $N_G(Q)$, there must exist $g \in N_G(Q)$ such that $Q = gQg^{-1} = P$. This shows that P is the only fixed point. \square

A typical example of the use of the Sylow theorems is the following (more examples are found in Exercises 2.52–2.56).

Example 2.10.20 A group G of order 143 must be isomorphic to $\mathbb{Z}/143\mathbb{Z}$. Since $143 = 11 \cdot 13$, the third Sylow theorem tells us that

$$|\text{Syl}_{11}(G)| \in \{1, 13\}, \quad |\text{Syl}_{13}(G)| \in \{1, 11\}$$

and

$$|\text{Syl}_{11}(G)| \equiv 1 \pmod{11}, \quad |\text{Syl}_{13}(G)| \equiv 1 \pmod{13}.$$

So there is a unique Sylow 11-subgroup P and a unique Sylow 13-subgroup Q in G . These Sylow subgroups have to be normal (why?). The product PQ is a subgroup (see Lemma 2.3.6) and it contains P and Q . This implies that $PQ = G$, as $11 = |P|$ divides $|PQ|$ and $13 = |Q|$ divides $|PQ|$. Since $P \cap Q$ is a proper subgroup of Q , it follows that $P \cap Q = \{e\}$ by Theorem 2.2.8. This implies by Lemma 2.8.1 that

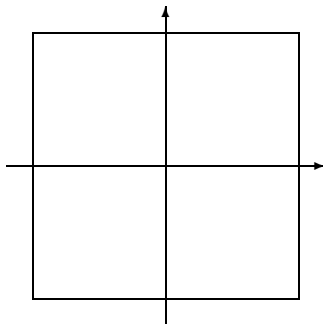
$$\pi : P \times Q \xrightarrow{\sim} G$$

given by $\pi(p, q) = pq$ is an isomorphism. So G is isomorphic to $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$, which by the Chinese remainder theorem (Proposition 2.8.2) is isomorphic to $\mathbb{Z}/143\mathbb{Z}$.

2.11 Exercises

1. Let G be a group and $g \in G$ an element of G . Prove that the map $\xi : G \rightarrow G$ given by $\xi(x) = xg$ is bijective.
2. Using subsection 2.1.6 construct the possible composition tables for a group with four elements.
3. Verify the composition table in Example 2.1.6.
4. Let G be a group and $H \subseteq G$ a non-empty subset. Prove that H is a subgroup if and only if $xy^{-1} \in H$ for all $x, y \in H$.
5. Let H be a non-empty finite subset of a group G . Prove that H is a subgroup if $xy \in H$ for every $x, y \in H$. Give an example where this breaks down if H is infinite. (Hint: consider e, x, x^2, \dots or use the fact that multiplication by $x \in H$ is bijective.)
6. Prove in detail that $\text{GL}_2(\mathbb{R})$ and $O_2(\mathbb{R})$ are groups and that they are non-abelian.
7. In the notation of Example 2.1.6, show that $\{e, d, f\}$ is a normal subgroup of S_3 . List the subgroups of order 2. Are any of these normal?
8. Let $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ be an isometry such that $\varphi((0, 0)) = (0, 0)$, as in Example 2.1.12.
 - (i) Prove that $\varphi(v_1) \cdot \varphi(v_2) = v_1 \cdot v_2$, where $v_1, v_2 \in \mathbb{R}^2$ and \cdot denotes the usual inner product on \mathbb{R}^2 (use $|v_1 - v_2|^2 = |v_1|^2 + |v_2|^2 - 2v_1 \cdot v_2$).
 - (ii) Show that $\varphi(e_1) \cdot \varphi(e_2) = 0$ and that $\varphi(\lambda e_1 + \mu e_2) = \lambda \varphi(e_1) + \mu \varphi(e_2)$, where e_1, e_2 is the usual basis of \mathbb{R}^2 and $\lambda, \mu \in \mathbb{R}$.
 - (iii) Prove that φ is a homomorphism (linear map) of vector spaces, i.e.

- (a) $\varphi(\lambda v) = \lambda \varphi(v)$, where $\lambda \in \mathbb{R}$ and $v \in \mathbb{R}^2$,
 (b) $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$, where $v_1, v_2 \in \mathbb{R}^2$.
 (iv) Prove that φ is invertible by proving that its determinant is non-zero.
 9. Let L denote the group of linear isometries (rotations and reflections) of \mathbb{R}^2 (see Example 2.1.12). Consider the square $K \subseteq \mathbb{R}^2$.



- (i) List the elements of the group $G = \{\varphi \in L \mid \varphi(K) = K\}$.
 (ii) Write down the composition table for G .
 10. Write down the subgroups of $\mathbb{Z}/6\mathbb{Z}$.
 11. Why are $\{[0]\}$ and $\mathbb{Z}/7\mathbb{Z}$ the only subgroups of $\mathbb{Z}/7\mathbb{Z}$?
 12. Show that a group G is not the union of two proper subgroups $H_1, H_2 \subsetneq G$. Can a group be the union of three proper subgroups?
 13. Let N be a normal subgroup of a group G . Prove that $gN = Ng$ for every $g \in G$.
 14. Show that every subgroup of an abelian group is normal.
 15. Let H be a subgroup of the group G .
 (i) Show that H is a right coset and that distinct right cosets of H are disjoint.
 (ii) Show that the map $\Phi : G/H \rightarrow H \backslash G$ given by $\Phi(gH) = Hg^{-1}$ is well defined. Prove also that it is bijective.
 (iii) Prove that if H has index 2 in G (i.e. $|G/H| = 2$), then H is normal. Give an example of a subgroup of index 3 that is not normal.
 16. Consider the subset H of $\text{GL}_2(\mathbb{C})$ consisting of the eight matrices $\pm \mathbf{1}, \pm \mathbf{i}, \pm \mathbf{j}$ and $\pm \mathbf{k}$, where

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

Verify that H is a subgroup by constructing the composition table. This group is called the *quaternion group*.

17. Prove that the quaternion group H from Exercise 2.16 is not abelian, but that all its subgroups are normal.
18. Let G be a finite group and $H \supseteq K$ subgroups of G . Prove that $|G/K| = |G/H||H/K|$.
19. (i) Compute the inverse of $[3]$ in $(\mathbb{Z}/8\mathbb{Z})^*$.
(ii) Compute the inverse of $[5]$ in $(\mathbb{Z}/13\mathbb{Z})^*$.
20. Prove that the inverse map of a group isomorphism is also a group homomorphism.
21. Prove that G is abelian if and only if the map $f : G \rightarrow G$ given by $f(g) = g^2$ is a group homomorphism.
22. Prove that the exponential function $\xi(x) = e^x$ is a group isomorphism from $(\mathbb{R}, +)$ to $(\mathbb{R}_{>0}, \cdot)$.
23. Using the notation of Example 2.1.6, prove that the map $\text{sgn} : S_3 \rightarrow \mathbb{Z}/2\mathbb{Z}$, mapping e, d, f to $[0]$ and a, b, c to $[1]$, is a group homomorphism.
24. Prove that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R})$$

has infinite order in the group $\text{GL}_2(\mathbb{R})$.

25. Let V be a real vector space and W a subspace of V . Show that V is an abelian group with respect to $+$ and that W is a normal subgroup in V . Prove that the quotient group V/W is a real vector space with scalar multiplication $\lambda(v + W) = \lambda v + W$, where $\lambda \in \mathbb{R}$.
26. Let G be an abelian group, K a group and $f : G \rightarrow K$ a group homomorphism. Prove that $f(G) \subseteq K$ is an abelian subgroup of K .
27. Let $\text{SL}_2(\mathbb{R})$ be the subset of $\text{GL}_2(\mathbb{R})$ (see Example 2.1.10) consisting of matrices with determinant 1. Show that $\text{SL}_2(\mathbb{R})$ is a normal subgroup of $\text{GL}_2(\mathbb{R})$. Use the isomorphism theorem to determine the group

$$\text{GL}_2(\mathbb{R})/\text{SL}_2(\mathbb{R}).$$

28. Prove that $(\mathbb{Z}/13\mathbb{Z})^*$ is a cyclic group by finding a generator.
29. Let p be a prime number and suppose that q is a prime number such that $q \mid 2^p - 1$. Prove that $q > p$ (hint: consider the element $[2] \in (\mathbb{Z}/q\mathbb{Z})^*$). Use this to prove that there are infinitely many prime numbers.
30. Let $\pi : G \rightarrow G/N$ be the canonical group homomorphism where N is a normal subgroup of G .
(i) Prove that $\pi(K)$ is a subgroup of G/N if K is a subgroup of G .

- (ii) Prove that $\pi^{-1}(H)$ is a subgroup of G containing N if H is a subgroup of G/N .
- (iii) Prove that $\pi(\pi^{-1}(H)) = H$ and $\pi^{-1}(\pi(K)) = K$, where H is a subgroup of G/N and K is a subgroup of G containing N .
- (iv) Let G be a cyclic group and $f : G \rightarrow K$ a surjective group homomorphism. Prove that K is a cyclic group.
- (v) Let $N \in \mathbb{N}$. Prove using the canonical group homomorphism

$$\pi : \mathbb{Z} \rightarrow \mathbb{Z}/N\mathbb{Z}$$

that a subgroup H of $\mathbb{Z}/N\mathbb{Z}$ is cyclic.

- 31. (i) Write down all the elements of order 7 in $\mathbb{Z}/28\mathbb{Z}$.
- (ii) How many subgroups are there of order 7 in $\mathbb{Z}/28\mathbb{Z}$?
- 32. (i) Prove that the cyclic group $\mathbb{Z}/15\mathbb{Z}$ is isomorphic to the product group $\mathbb{Z}/3 \times \mathbb{Z}/5\mathbb{Z}$.
- (ii) Prove that the group $(\mathbb{Z}/15\mathbb{Z})^*$ is isomorphic to the product group $\mathbb{Z}/2 \times \mathbb{Z}/4\mathbb{Z}$. Conclude that $(\mathbb{Z}/15\mathbb{Z})^*$ is not cyclic.
- 33. Consider $\mathbb{Z} \subset \mathbb{Q}$ as abelian groups with $+$ as composition. Let $[q] = q + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, where $q \in \mathbb{Q}$.
- (i) Show that $\left[\frac{9}{4}\right]$ has order 4 in \mathbb{Q}/\mathbb{Z} .
- (ii) Determine the order of $\left[\frac{a}{b}\right]$ in \mathbb{Q}/\mathbb{Z} , where $a \in \mathbb{Z}$, $b \in \mathbb{N} \setminus \{0\}$ and $\gcd(a, b) = 1$. Conclude that every element in \mathbb{Q}/\mathbb{Z} has finite order and that there are elements in \mathbb{Q}/\mathbb{Z} of arbitrary large order.
- (iii) Show that \mathbb{Q}/\mathbb{Z} is an infinite group that is not cyclic.
- 34. Prove that $(\mathbb{Q} \setminus \{0\}, \cdot)$ is not a cyclic group.
- 35. Give an example of a non-cyclic group of order 8.
- 36. Let G be a finite group of order N . Let $\psi(d)$ be the number of elements in G of order d .
- (i) Prove that $\psi(d) = 0$ if $d \nmid N$ and that G is cyclic if and only if $\psi(N) > 0$.
- (ii) Prove that

$$\sum_{d|N} \psi(d) = N.$$

- (iii) Suppose that for every divisor d in N , there is a unique subgroup H in G of order d . Prove that $\psi(d) \leq \varphi(d)$ and that G is a cyclic group.
- 37. Prove that an even permutation cannot be the product of an odd number of transpositions.
- 38. Prove that the order of a k -cycle in S_n is k .

39. Let $\tau \in S_3$ denote the 3-cycle

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Show that the subgroup $\langle \tau \rangle = \{\tau^n \mid n \in \mathbb{Z}\}$ is normal in S_3 .

40. Let $\sigma \in S_5$ denote the 5-cycle

$$(1\ 2\ 3\ 4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}.$$

- (i) Show that σ is an even permutation and that $\langle \sigma \rangle = \{\sigma^n \mid n \in \mathbb{Z}\}$ has order 5 and write down the elements in $\langle \sigma \rangle$.
- (ii) Prove that $\langle \sigma \rangle$ is not a normal subgroup of S_5 .
- 41. (i) Let $\sigma, \tau \in S_4$. Show that $\text{sgn}(\tau\sigma\tau^{-1}) = \text{sgn}(\sigma)$.
- (ii) Write the 3-cycle $(1\ 2\ 3)$ as a product of two simple transpositions. Prove that for a general 3-cycle σ one can find a permutation $\tau \in S_4$ such that $\tau\sigma\tau^{-1} = (1\ 2\ 3)$. Use this to show that 3-cycles in S_4 are even. Prove that a 3-cycle has order 3 in A_4 .
- (iii) Show that the number of 3-cycles in A_4 is greater than six. Conclude that the only subgroup of A_4 containing every 3-cycle is A_4 .
- (iv) Let $\varphi : A_4 \rightarrow \mathbb{Z}/2\mathbb{Z}$ be a group homomorphism. Show that if σ is a 3-cycle then $\varphi(\sigma) = [0] = 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z}$. Use this to prove that $\varphi(\sigma) = [0]$ for every $\sigma \in A_4$.
- (v) Prove that A_4 does not contain a subgroup of order 6.
- 42. If you are more familiar with 3-cycles this is an easier way of doing Exercise 2.41. Prove that A_n does not contain a subgroup H of index 2 (hint: consider A_n/H and deduce that H must contain all 3-cycles).
- 43. Write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \in S_6$$

as a product of the minimal number of simple transpositions.

- 44. Prove that there are 45 elements of order 2 in A_6 .
- 45. Prove that A_3 is a simple group. Prove that A_4 is not simple by proving that the elements of order 2 along with the neutral element form a normal subgroup.
- 46. Let K be the equilateral triangle from Example 2.1.13. Suppose that you color each edge of K using k colors. Show that the number of

colorings is

$$\frac{1}{6}(k^3 + 3k^2 + 2k),$$

where two colorings are considered the same if they map to each other using rotations and reflections.

47. (i) Give a coloring from each orbit in Example 2.10.9.
 (ii) Give a coloring from each orbit in Example 2.10.10.
 (iii) Comparing Example 2.10.9 with Example 2.10.10, which colorings are invariant under rotations but not under reflections?
48. In how many ways can you color the 16 squares of a 4×4 board when half of them must be black and the other half white? Now answer the same question when colorings are considered the same if they map to each other using rotations and reflections.
49. Consider the permutations $\sigma_1 = (1)(2)(345)$, $\sigma_2 = (3)(4)(152)$ and $\tau = (13)(245)$ in S_5 .
 (i) What is the minimal number of simple transpositions needed in writing τ as a product of simple transpositions?
 (ii) Show that $\tau \notin A_5$ and that

$$\tau \sigma_1 \tau^{-1} = \sigma_2.$$

- (iii) Show that $\sigma_1, \sigma_2 \in A_5$, $\tau_1 = (34)\tau \in A_5$ and $\tau_1 \sigma_1 \tau_1^{-1} = \sigma_2$.
 - (iv) Now we know that σ_1, σ_2 are conjugate via a permutation τ_1 in A_5 . Show that a permutation of the cycle type (a) $1 \leq 1 \leq 1 \leq 1 \leq 1$, (b) $1 \leq 2 \leq 2$, (c) $1 \leq 1 \leq 3$ or (d) 5 is even. We know that permutations of the same cycle type are conjugate via a permutation in S_5 . Show that two permutations with the same cycle type, (a), (b) or (c), are conjugate via a permutation in A_5 .
 - (v) Give an example of two 5-cycles that cannot be conjugate via a permutation in A_5 .
 - (vi) Show that in general a normal subgroup N in a group G is a disjoint union of conjugacy classes $C(n)$, $n \in N$ (subsection 2.10.1).
 - (vii) One may prove on further inspection that A_5 is the disjoint union of conjugacy classes with 1, 12, 12, 15 and 20 elements (check that $1 + 12 + 12 + 15 + 20 = 60$). Thus show that A_5 is a simple group.
50. Let G be a group. Prove that the center $Z(G)$ of the group is an abelian normal subgroup of G .

51. Let $H \subseteq G$ be a subgroup of a group G . Prove that the normalizer $N_G(H)$ is a subgroup of G containing H . Prove that H is normal if and only if $G = N_G(H)$.
52. Let G be a finite group and p a prime number. Prove that G contains an element of order p if p divides $|G|$. (Hint: reduce to the situation where G is cyclic and of order p^r).
53. Prove that a group of order 15 is cyclic.
54. Does a group of order 14 have to be cyclic?
55. Compute the number of elements of order 5 in a group of order 20.
56. Let p and q be prime numbers. Prove that a finite group G of order pq cannot be simple.
57. **(HOF)** Prove using only ideas developed in Chapter 2 that a finite abelian group is isomorphic to a product of cyclic groups.