

# ALGEBRA I

---

P. Steenhagen



INTERNATIONAL  
MATHEMATICS MASTER

2026



## TABLE OF CONTENTS ALGEBRA I

1. What Is Algebra?	7
Groups, Rings, and Fields • Symmetries of the Rhombus • Arithmetic Modulo 8 • Symmetries of the Square • Permutations of Four Elements • Spatial Symmetries • Exercises	
2. Permutation groups	17
The Group Axioms • Orders of Groups and Elements • Permutation Groups • Cycle Notation • Subgroups, Cyclic Groups • The Sign Map • 15 Puzzle • Exercises	
3. Plane Symmetries	31
Plane Geometry • Isometries • The Orthogonal Group • Plane Symmetry Groups • Sign of an Isometry • Geometry with Complex Numbers • Plane Transformation Groups • Exercises	
4. Homomorphisms	42
Homomorphisms, Isomorphisms, Automorphisms • Additive Notation • Kernel and Image • Injectivity • Cosets • The Isomorphism Theorem • Normal Subgroups • Quotient Groups • Exercises	
5. Group Actions	56
Cubic and Tetrahedral Groups • Orbit, Stabilizer, Fixed Point • Orbit Decomposition Formula • Combinatorial Applications • Regular Action • Conjugation Action • Cauchy's Theorem • Exercises	
6. Integers	71
Division with Remainder • GCD and LCM • Prime Numbers • Unique Prime Factorization • Rings • The ring $\mathbf{Z}/n\mathbf{Z}$ • Arithmetic Modulo $n$ • Euler's Theorem and Fermat's Little Theorem • Exercises	
7. Factorization and Cryptography.	84
Primality of Large Numbers • Large Number Factorization • Cryptography • The RSA Cryptosystem • Digital Signatures • Safety of RSA • discrete logarithms • Diffie–Hellman protocol • Exercises	
8. Quotients and Products.	94
Subgroups under Quotient Maps • Homomorphism Theorem • Commutator Subgroup • Direct Product • Semi-direct Product • Exercises	
9. Abelian Groups	108
Exact Sequences • Splitting Exact Sequences • Free Abelian Groups • Structure Theorem • The Group $(\mathbf{Z}/n\mathbf{Z})^*$ • Exercises	
10. Finite Groups	124
Non-abelian Exact Sequences • Classification for Simple Group Orders • Sylow $p$ -Subgroups • Construction of Normal Subgroups • Solvable Groups • Simple Groups • Exercises	
Table of Small Groups	138
Literature	139
The Greek Alphabet	147
Index	148

This is a preliminary version of the complete English translation, by Reinie Ern , of the Dutch original. The latest version will be made available on <https://websites.math.leidenuniv.nl/algebra/>.  
Publication date of this version: January 2026.

Each subsequent edition will, hopefully, contain fewer typos and inaccuracies than the current one—please send any comments to the author at [psh@math.leidenuniv.nl](mailto:psh@math.leidenuniv.nl).

Author's address:

Mathematisch Instituut  
Universiteit Leiden  
Postbus 9512  
2300 RA Leiden

## PREFACE

Algebra 1 is the first of the three courses making up the algebra curriculum at Leiden University. The distribution of algebra over the three courses roughly matches the traditional subdivision groups–rings–fields. This corresponds to increasing “specialization” rather than increasing difficulty: a ring is a group with an additional operation, and a field is a ring with special nice properties. These course notes, devoted mainly to group theory, are intended as a first introduction to algebra. Little prior knowledge is required, and certain interesting examples of groups, such as matrix groups over finite fields or fundamental groups of topological spaces, will therefore not be discussed in detail, if at all.

The reader is expected to have an idea of what a mathematical proof is, and in particular a proof *by complete induction* or *by contradiction*. Simple notions from set theory such as *injection*, *surjection*, *bijection*, and *equivalence relation* are used without further explanation. Prior knowledge of linear algebra is not strictly necessary, but some of the examples and exercises assume familiarity with basic concepts such as *linear map*, *matrix*, and *determinant*.

A characteristic property of these course notes is the abundance of *exercises*. There are more than can be given as homework or discussed, and students must each decide how many exercises they can handle. It is clear in practice that algebra is a subject in which it does not suffice to memorize theorems or tricks. It is more like swimming: you cannot learn it by watching others do it, and once you have mastered it, you often no longer understand what was so difficult about it. Selecting and trying as many exercises as possible without immediate help of modern AI is therefore essential. Exercises with a star are for those seeking (even) more challenge. They require an original idea or use concepts that are somewhat outside the scope of the course material.

These course notes contain more material than is usually covered in a single course in Leiden, and there are various ways in which material can be left out. The first eight sections form a reasonably well-rounded first introduction to abstract algebra. Section 7 can be skipped without any problem. It is possible to limit Section 3 to treating the orthogonal group and its finite subgroups and to not discuss the semi-direct product from Section 8. The resulting additional time may be spent on (parts of) the last two sections, which give a somewhat more mature look at group theory. Another possibility is to cut back the number-theoretic Section 6, which in a way is more on rings than on groups, in favor of the “purely group-theoretic” later sections.

The latest version of these Algebra 1 notes, the notes on ring and field theory in Algebra 2 and 3, and much more can be found online on the Leiden webpage [Various Algebra course notes](#).



# 1 WHAT IS ALGEBRA?

Somewhat inaccurately, one could say that algebra axiomatizes and studies in abstracto the “mathematical structures” that surround us.<sup>1</sup> In secondary school, where, in general, real numbers are the manipulated objects, algebra often means something like “doing arithmetic with letters,” where frequently parentheses are either eliminated or, conversely, added by either “expanding” or “factoring,” respectively. There are many more interesting objects in mathematics than just the real numbers and functions thereof. The algebra we will develop can be applied in all of these cases. This means that the symbols we will be “doing arithmetic” with will not always be numbers; they will often be matrices, geometric maps, permutations of sets, or whatever else we find useful for solving our problem.

An essential feature of modern mathematics is that it generally does not consider a single function, matrix, or equation but rather, if possible, a whole set of similar objects at once. Therefore, instead of functions and matrices, we encounter “function spaces” and “matrix groups”; these are large, often infinite collections of functions or matrices with certain common properties—for example, sets of differentiable functions or invertible matrices.

Algebra establishes axiomatic rules for “doing arithmetic” with the elements of such sets. At first glance, this may sound abstract and dull, more like something for taxonomists or aspiring accountants. However, the aim of such a minimalistic approach, where interesting results concerning the structure of the underlying set are deduced from a small number of axioms, is *applicability* and *clarity*. Therefore, the axioms we will encounter in this course are not arbitrary choices but serve to “model” interesting mathematics. The abstract way we will do this has significant advantages: with minor adjustments, eliminating redundant assumptions and coincidences in a given problem often leads to more transparent reasoning and a better understanding of the situation. Finally, and perhaps most importantly, it turns out that a generality discovered in this way also leads to results in what may seem to be completely different situations.

The price for discovering universal truths is the effort required to master a somewhat abstract way of thinking. This often takes time, which is why algebra sometimes seems “difficult” at first. However, history has shown that acquiring some algebraic skills is well worth the effort, and since the 1930s, “abstract algebra” has become an essential tool for both pure and applied mathematicians.

## ► GROUPS, RINGS, AND FIELDS

In these course notes, we will primarily study sets on which a single binary operation is defined. The elements of the set are generally numbers, matrices, or certain maps; the binary operation, which out of two given elements makes a third, is usually something such as addition, multiplication, or composition. We will provide the exact axioms in Definition 2.1 in §2. We summarize them by saying that the set in question becomes a

---

<sup>1</sup> For all references, see the section “Literature.”

*group* through the given binary operation.

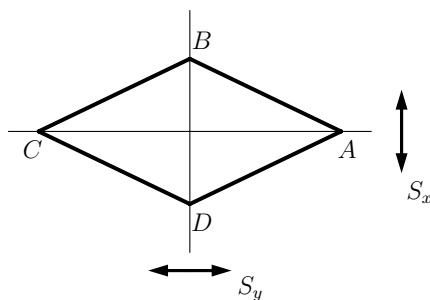
As we can already see from classic examples such as numbers, polynomials, and matrices, it is common for a set to be naturally endowed with both an addition and a multiplication; these satisfy simple rules such as  $a(b + c) = ab + ac$ . Such objects with two operations, called *rings*, are ubiquitous in mathematics. We define them in Definition 6.8 but will postpone a systematic study until the course Algebra 2. Popular examples of rings in analysis and linear algebra are  $\mathbf{R}$  and  $\mathbf{C}$ . In these rings, we can not only add and multiply but also *divide* by all elements (different from 0)—something that is much less straightforward in, for example, the case of matrix rings. Because of this nice property,  $\mathbf{R}$  and  $\mathbf{C}$  are typical examples of a kind of ring called a *field*.

The theory of fields and inclusions among them is called *Galois theory*, after its discoverer Évariste Galois (1810–1831), who died in a duel<sup>2</sup> at a young age. It was in this theory that the abstract notion of a group first manifested itself. Nowadays, mathematicians prefer to reverse the chronological order and first study abstract groups, to later apply these effectively in Galois theory. We will do so too. As it happens, group theory has simpler examples and applications than Galois theory, and these are better suited for expressing the unifying character of the notion of a group.

In this introductory section, we first present some examples that clarify why the axioms for a group given in 2.1 are rather obvious: they are simply the rules that most of the examples satisfy. The examples give a good idea of what we will encounter in this course and show that the same group structure can occur in different guises.

### ► SYMMETRIES OF THE RHOMBUS

We begin with a simple example from geometry that deals with the fundamental notion of *symmetry*. A symmetry of a plane figure is a map from the plane to itself that preserves the mutual distances between points and sends the given figure to itself. Let us consider the symmetries of the rhombus  $ABCD$  in the plane  $\mathbf{R}^2$  shown below.



Two symmetries stand out immediately: the rhombus is mapped to itself by the reflections in the  $x$ - and  $y$ -axes. Carrying out two symmetries consecutively always leads to a symmetry: the *composition*. It is easy to see that the composition  $h = s_x \circ s_y$  of the two reflections in the coordinate axes is a half turn about the origin. Note that the *order* in which we compose the reflections does not matter in this case. As we have chosen the rhombus to be symmetric about the origin, the symmetries  $s_x$ ,  $s_y$ , and  $h$  are *linear maps* from  $\mathbf{R}^2$  to itself. Those who like matrices can express these symmetries

in matrix form as

$$s_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad s_y = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

We can also observe that every symmetry of the rhombus is fixed by its action on the vertices and choose notation for that action that takes this into account, for example

$$s_x = (BD), \quad s_y = (AC), \quad h = (AC)(BD).$$

We can easily see that we cannot make a new symmetry through composition from the three we found. After all, the symmetries  $s_x$ ,  $s_y$ , and  $h$  are of *order 2*, which means that their “square” is the *identity*, the map that leaves all points in place. Moreover, the “product” of two distinct symmetries from our triple is always the third. If we count the identity as the “trivial symmetry,” then we have found a set of symmetries that is *closed* under composition of symmetries.

**1.1. Theorem.** *The set  $V_4 = \{\text{id}, s_x, s_y, h\}$  is the complete symmetry set of the rhombus  $ABCD$ . The three non-trivial symmetries in  $V_4$  are of order 2, and the product of two distinct non-trivial symmetries equals the third.*

**Proof.** We only need to show that there are no other symmetries than the four mentioned. So let  $s$  be an arbitrary symmetry of the rhombus. As  $s$  can only either fix the acute angle  $A$  of the rhombus or send it to the other acute angle  $C$ , we have  $s(A) = A$  or  $(s_y \circ s)(A) = A$ . A symmetry that fixes  $A$  must also fix  $C$ , which means that either it is the identity, or it only interchanges the obtuse angles  $B$  and  $D$  and therefore equals  $s_x$ . In the case  $s(A) = A$ , we have  $s = \text{id}$  or  $s = s_x$ , and we are done. In the case  $(s_y \circ s)(A) = A$ , we have  $s_y \circ s = \text{id}$  or  $s_y \circ s = s_x$ . In the identity  $s_y \circ s = \text{id}$ , we can compose on the left and right with  $s_y$ ; as  $s_y \circ s_y = \text{id}$ , this gives  $s = s_y$ . For  $s_y \circ s = s_x$ , composing with  $s_y$  gives  $s = s_y \circ s_x = h$ , the fourth and last possibility for  $s$ .  $\square$

**Exercise 1.** Determine which general properties of the composition of maps (in particular concerning “moving around parentheses”) we are using here.

The set  $V_4$  with four elements we just found consists of a “trivial element” and three elements of order 2 with the property that the product of two of those elements always gives the third. This “structure,” which is known as the *Klein four-group*, comes in many guises.

**Exercise 2.** Let  $ABCD$  be a rectangle which is not a square. Show that the set of symmetries of the rectangle  $ABCD$  is the Klein four-group.

## ► ARITHMETIC MODULO 8

Let us now show how the Klein four-group also occurs in number theory. We want to find all integers  $x$  and  $y$  that satisfy the equation

$$(1.2) \quad 3x^2 + 2 = y^2.$$

Geometers will recognize the equation of the hyperbola in the plane and say that we apparently want to determine the points on this hyperbola with integer coordinates.

**Exercise 3.** Draw the curve with equation  $3x^2 + 2 = y^2$  in the plane  $\mathbf{R}^2$ .

Looking at the equation, we can easily see that the numbers  $x$  and  $y$  that satisfy equation (1.2) are either both even or both odd. If we write the equation as  $2 = y^2 - 3x^2$ , then it becomes clear that  $x$  and  $y$  cannot both be even. After all, the square of an even number is divisible by 4 (why?), so if  $x$  and  $y$  are even, the number  $y^2 - 3x^2$  is divisible by 4 and therefore not equal to 2. We are left with the possibility that  $x$  and  $y$  are both odd.

When  $x$  and  $y$  are both odd, we apply a little trick called “arithmetic modulo 8,” about which we will first prove a theorem. Observe that when divided by 8, every odd number has remainder equal to 1, 3, 5, or 7. In other words, the odd numbers split up into *residue classes modulo 8* that we can evocatively denote by  $\bar{1}$ ,  $\bar{3}$ ,  $\bar{5}$ , and  $\bar{7}$ . If, for example, we take an element  $a$  from the class  $\bar{3}$  and an element  $b$  from the class  $\bar{5}$ , then it is not difficult to calculate in which class  $ab$  lies. After all, if we write  $a = 8a' + 3$  and  $b = 8b' + 5$  with  $a'$  and  $b'$  integer, then we find  $ab = (8a' + 3)(8b' + 5) = 8(8a'b' + 5a' + 3b') + 15$ , which shows that  $ab$  is an 8-tuple+15; this is exactly the same as an 8-tuple+7, so  $ab$  lies in the residue class  $\bar{7}$ . As the result does not depend on exactly what element we choose in  $\bar{3}$  and  $\bar{5}$ , we often say, for short, that we can multiply the *classes*  $\bar{3}$  and  $\bar{5}$  and simply write the entire calculation as  $\bar{3} \cdot \bar{5} = \bar{15} = \bar{7}$ .

Similarly, we can multiply any two residue classes in the set  $V'_4 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ . Multiplying by  $\bar{1}$  does not change a residue class, so the class  $\bar{1}$  acts as a kind of identity. The class  $\bar{1}$  is often called a *unit element* for multiplication in  $V'_4$ . For other products, we first find

$$\bar{3} \cdot \bar{3} = \bar{5} \cdot \bar{5} = \bar{7} \cdot \bar{7} = \bar{1},$$

so the elements  $\bar{3}$ ,  $\bar{5}$ , and  $\bar{7}$  are each “of order 2.” The identities

$$\bar{3} \cdot \bar{5} = \bar{7}, \quad \bar{3} \cdot \bar{7} = \bar{5}, \quad \text{and} \quad \bar{5} \cdot \bar{7} = \bar{3}$$

show that the product of two distinct classes in  $\{\bar{3}, \bar{5}, \bar{7}\}$  always yields the third. This gives us the following “structure theorem” for the odd residue classes modulo 8.

**1.3. Theorem.** *The set  $V'_4 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$  of odd residue classes modulo 8 has a natural multiplication. Under this multiplication,  $\bar{1}$  is a unit element, and the three remaining elements are of order 2. The product of two distinct elements of order 2 in  $V'_4$  is equal to the third element of order 2.  $\square$*

We now return to our equation  $3x^2 + 2 = y^2$ . If  $x$  and  $y$  are odd, then the structure theorem 1.3 shows that  $x^2$  and  $y^2$  are in the class  $\bar{1}$ . But if  $x^2$  is in  $\bar{1}$ , then  $3x^2 + 2$  is in  $\bar{3} \cdot \bar{1} + \bar{2} = \bar{5}$ . We conclude that  $3x^2 + 2$  cannot equal  $y^2$  and that equation (1.2) has no integer solutions.

**Exercise 4.** Show that the equation  $11x^2 + 1002 = 87y^2$  does not have any integer solutions.

Comparing Theorems 1.1 and 1.3, we see that  $V_4$  and  $V'_4$  apparently have “the same structure.” This becomes even clearer if we make *multiplication tables* for the values

of the “products”  $ab$  of elements of  $V_4$  and  $V'_4$ :

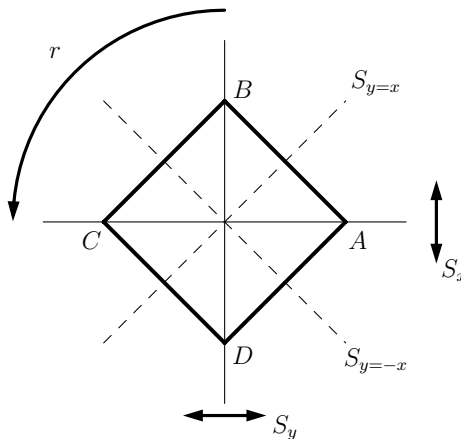
$a \downarrow b \rightarrow$	id	$s_x$	$s_y$	$h$
id	id	$s_x$	$s_y$	$h$
$s_x$	$s_x$	id	$h$	$s_y$
$s_y$	$s_y$	$h$	id	$s_x$
$h$	$h$	$s_y$	$s_x$	id

$a \downarrow b \rightarrow$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{3}$	$\bar{5}$	$\bar{7}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{7}$	$\bar{5}$
$\bar{5}$	$\bar{5}$	$\bar{7}$	$\bar{1}$	$\bar{3}$
$\bar{7}$	$\bar{7}$	$\bar{5}$	$\bar{3}$	$\bar{1}$

The bijection  $f : V_4 \rightarrow V'_4$  defined by  $\text{id} \mapsto \bar{1}$ ,  $s_x \mapsto \bar{3}$ ,  $s_y \mapsto \bar{5}$ , and  $h \mapsto \bar{7}$  has the property that it “respects” multiplication. Such an  $f$  is called an *isomorphism*, and the symmetry group  $V_4$  and the multiplicative group  $V'_4$  are said to be *isomorphic*.

### ► SYMMETRIES OF THE SQUARE

We obtain a slightly more complicated example, which at first glance looks very similar to that of the rhombus  $ABCD$ , by deforming the rhombus to a square  $ABCD$  and asking again what the symmetries are. The symmetries in 1.1 are obviously also symmetries of the square  $ABCD$ , but there are more.



Striking “new” symmetries are the rotation  $r$  by a quarter turn about the origin and the reflections in the lines  $y = x$  and  $y = -x$ . The quarter turn  $r$  is a symmetry of order 4: only after applying  $r$  four times do we obtain the identity. The “three-quarter turn”  $r^3 = r \circ r \circ r$ , which is the *inverse* of  $r$ , is also a symmetry of order 4. The symmetry  $r^2$ , which is nothing but  $h$ , has order 2. In addition to the four “old” symmetries from Theorem 1.1, we have found four new ones, namely  $r$ ,  $r^3$ , and the reflections mentioned above. Through some trial and error, we can see that we cannot make any new symmetries from these eight through composition.

**1.4. Theorem.** *The set  $D_4$  of symmetries of the square  $ABCD$  has eight elements: the four rotations about the origin by multiples of  $\pi/2$  and the reflections in the four lines connecting the origin to a vertex or the midpoint of a side.*

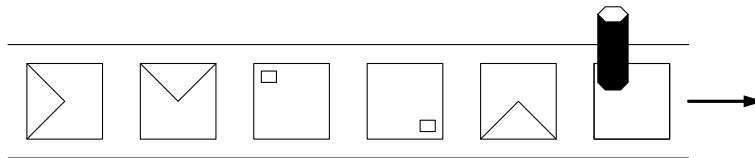
**Proof.** Let  $s$  be a symmetry of the square. By composing  $s$  with a number of quarter turns, we can obtain a symmetry that leaves the vertex  $A$  in place. Then this symmetry

also leaves the vertex  $C$  in place—after all,  $B$  and  $D$  are closer to  $A$  than  $C$ , so a symmetry (which preserves distances) cannot send  $C$  to either of them. There are only two possibilities for a symmetry of the square that leaves  $A$  and  $C$  in place: the identity and the reflection  $s_x$ , which interchanges  $B$  and  $D$ . We conclude that by composing  $s$  with a “power” of  $r$ , we can transform it into the identity or the reflection  $s_x$ . In the first case,  $s$  itself is one of the four powers of  $r$  and therefore equal to one of the four listed rotations about the origin. In the second case, we have an identity of the type

$$r^j \circ s = s_x,$$

where we can take  $j \in \{0, 1, 2, 3\}$ . By composing with a power of  $r$  on both sides, we can ensure that we have  $r^4 \circ s = \text{id} \circ s = s$  on the left, which gives  $s = r^k \circ s_x$  for some  $k$ . Again, there are four choices for  $k$ , which gives four elements, and the reader can verify that these are the four listed reflections.  $\square$

**Exercise 5.** A *postmarking machine* is a machine that is fed square envelopes on a conveyor belt. While the envelope is transported on the belt, a robot arm can turn it a quarter turn clockwise or “flip” it over (in a fixed way) so that the front of the envelope faces the top. The “treatment” of an envelope consists in putting a postmark over a stamp in a fixed corner (the upper right one on the front).



Show that the machine can postmark an envelope with a stamp in the upper right corner. What is the maximal number of actions the robot arm needs to perform?

The proof of 1.4 shows that all symmetries of the square can be made by repeatedly composing  $r$  and  $s_x$ . The group  $D_4$  of symmetries of the square is said to be *generated* by  $r$  and  $s_x$ .

A complication with the symmetry group  $D_4$  that does not occur with the symmetry group  $V_4$  of the rhombus is that the *order* of the composition now plays an important role. For example,  $r \circ s_x$  and  $s_x \circ r$  are *not* the same reflection in  $D_4$ . Anyone who has ever done matrix calculations will not be surprised, but those who have only done arithmetic with real numbers must keep this in mind. We say that the elements  $r$  and  $s_x$  of  $D_4$  do not *commute*.

By writing the elements of  $D_4$  as  $r^i s_x^j$  with  $i \in \{0, 1, 2, 3\}$  and  $j \in \{0, 1\}$ , we can multiply elements in  $D_4$  quickly. The rules

$$(1.5) \quad r^{i_1} \cdot r^{i_2} = r^{i_1+i_2} \quad \text{and} \quad s_x^{j_1} \cdot s_x^{j_2} = s_x^{j_1+j_2}$$

are obvious. We take the exponents modulo 4 and modulo 2, respectively. The “not commuting” of  $r$  and  $s_x$  is expressed by the rule

$$(1.6) \quad s_x \circ r^i = r^{-i} \circ s_x,$$

left as an exercise to the reader to deduce from the relation  $(r^i \circ s_x) \circ (r^i \circ s_x) = \text{id}$ . (After all,  $r^i \circ s_x$  is a reflection and therefore has order 2.) Note that the elements  $s_x$  and  $r^2 = h$ , which we know from  $V_4$ , do commute.

**Exercise 6.** Write the product  $s_x \circ r \circ s_x \circ r^2 \circ r^{-1} \circ s_x$  in the form  $r^i s_x^j$ .

As with the rhombus, we can denote the symmetries of the square using their action on the vertices. In the *cycle notation* already suggested for the rhombus, we then get

$$\begin{aligned} r^0 &= \text{id} = (A), & s_x &= (BD), \\ r &= (ABCD), & r \circ s_x &= s_{y=x} = (AB)(CD), \\ r^2 &= h = (AC)(BD), & r^2 \circ s_x &= s_y = (AC), \\ r^3 &= r^{-1} = (ADCB), & r^3 \circ s_x &= s_{y=-x} = (AD)(BC). \end{aligned}$$

Within a cycle, the symmetry maps each point onto the next point of the cycle, and the last point is mapped onto the first one. For example,  $(ABCD)$  represents the permutation  $A \mapsto B \mapsto C \mapsto D \mapsto A$ . Points that remain in place are not mentioned in the notation—except in the case of the identity, which we write as  $(A)$ .

### ► PERMUTATIONS OF FOUR ELEMENTS

We can view the sets  $V_4$  and  $D_4$  we have looked at as subsets of the set  $S_4$  of *all* permutations of the four points in the set  $\{A, B, C, D\}$ . As is well known, a permutation of a set is a bijective map from the set to itself, and for the set  $\{A, B, C, D\}$ , there are  $4! = 24$  distinct permutations. The cycle notation we just introduced gives us a compact way to write them down.

**Exercise 7.** Write the 24 elements of  $S_4$  in cycle notation and determine their orders.

The inclusions  $V_4 \subset D_4 \subset S_4$  lead to a *divisibility* of the sets' cardinalities 4, 8, and 24. Moreover, the order of an element in each of the sets  $V_4$ ,  $D_4$ , and  $S_4$  turns out to always be a divisor of the number of elements of the set. In 4.9, we will see that these are general properties of group inclusions and orders.

On the set  $S_4$ , just as on  $V_4$  and  $D_4$ , we have a natural composition of elements. After all, the “product” of two permutations is also a permutation. We write  $\alpha \circ \beta$ , or  $\alpha\beta$  for short, for the composition of the permutations  $\alpha$  and  $\beta$ ; we also call this the *product* of  $\alpha$  and  $\beta$ . Note that  $\alpha\beta$  means: first apply  $\beta$ , then  $\alpha$ . As we have seen,  $\alpha\beta$  and  $\beta\alpha$  are not always the same.

**Exercise 8.** Make a multiplication table for  $D_4$ . How does such a table show that there are elements that do not commute?

We already observed that the elements  $r = (ABCD)$  and  $s_x = (BD)$  *generate* all symmetries in  $D_4$ : this means that every symmetry can be obtained by repeatedly applying  $r$  and  $s_x$ . We can ask whether the set  $S_4$  can similarly be generated using a few elements; this is, for example, interesting for those who want to build a sorting machine. The number of possible choices is vast. We can, for example, take the *transpositions* in  $S_4$ . By definition, these are permutations that interchange two elements and leave all others in place. The number of such elements of  $S_4$  is  $\binom{4}{2} = 6$ .

**1.7. Theorem.** *Let  $\sigma$  be a permutation of a finite set  $X$ . Then  $\sigma$  is a product of transpositions.*

**Proof.** Denote the elements of the set by  $1, 2, 3, \dots, n$ , where  $n$  is the number of elements of  $X$ . We carry out the proof using induction on  $n$ . For  $n \leq 1$ , the permutation  $\sigma$  is the identity, which is the product of 0 transpositions.

Now, suppose that every permutation in a set with  $n - 1$  elements is a product of transpositions. If our permutation satisfies  $\sigma(n) = n$ , then  $\sigma$  can be viewed as a permutation of a set with  $n - 1$  elements, and we are done. So assume  $\sigma(n) = k \neq n$ . Then the product  $(kn) \circ \sigma$  of  $\sigma$  and the transposition  $(kn)$  is a permutation that leaves  $n$  in place (why?), and we just saw that this means that  $(kn) \circ \sigma$  is a product of transpositions. If we multiply this product by  $(kn)$ , then we have a product of transpositions equal to  $(kn) \circ (kn) \circ \sigma = \sigma$ .  $\square$

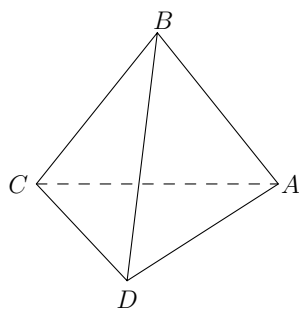
**Exercise 9.** Show that every element of  $S_4$  can be written as a product of no more than three transpositions.

The proof of Theorem 1.7, in which we took  $n$  arbitrary and not  $n = 4$ , shows that it can sometimes be easy to prove a *more general* statement. This is also called *simplification by generalization*. A slightly more subtle example of this phenomenon is given in the last exercise of this section.

### ► SPATIAL SYMMETRIES

We introduced  $V_4$  and  $D_4$  as symmetry sets, which leads to the question of whether the abstract “permutation set”  $S_4$  of  $\{A, B, C, D\}$  can also be interpreted in this way. It is not so easy to do this using points in the plane, but it can easily be done using spatial symmetries. Such symmetries, generally more difficult to visualize and classify than plane symmetries, are extensively studied in crystallography. The occurring symmetry sets are called *crystallographic groups*.

If we view the points  $A, B, C, D$  as vertices of a tetrahedron, then  $S_4$  acts as the symmetry set of the tetrahedron. After all, as every symmetry is uniquely determined by its action on the vertices, the symmetries of the tetrahedron form a subset of  $S_4$ . As compositions of symmetries are symmetries, by 1.7, it suffices to show that the transpositions occur as symmetries.



For example, to make the transposition  $(AB)$ , we take the plane that cuts  $AB$  perpendicularly through its midpoint. As the triangles  $ABC$  and  $ABD$  are equilateral,  $C$  and  $D$  lie in this plane. If we reflect in this plane, we obtain the symmetry that interchanges  $A$  and  $B$  and leaves  $C$  and  $D$  in place.

The example of the tetrahedron shows that we can use “abstract arguments” about permutation sets to prove something about the symmetries of a tetrahedron.

Those who do not like such an indirect approach may, of course, also try imagining what spatial transformation interchanges, for example, the vertices  $A, B, C, D$  in a 4-cycle  $(ABCD)$ .

## EXERCISES.

10. The *symmetric difference* of two sets  $A$  and  $B$  is defined as

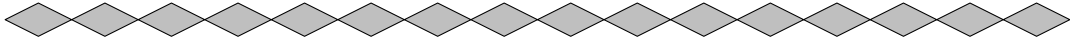
$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

Let  $X$  be a set with two elements and  $V$  the collection of subsets of  $X$ . Show that  $V$  is a set with four elements and that the action  $\Delta$  gives this set the structure of a Klein four-group.

11. Show that the set of integers not divisible by 2 or 3 splits up into four residue classes modulo 12. Is the natural multiplicative structure on these four classes that of the Klein four-group? Answer the same question for the four residue classes of the integers that are not divisible by 5.
12. Show that the equation  $3x^2 + 2 = y^2$  has no solutions with  $x$  and  $y$  odd by writing  $x = 2a + 1$  and  $y = 2b + 1$  and using a parity argument. (*Parity argument* is a proper word for “even/odd consideration”.)
13. Show that the equation  $3x^2 + 2 = y^2$  has no integer solutions by calculating modulo 3. Also prove that the equation has no *rational* solutions.
14. Define  $V_4$  and  $V'_4$  as in Theorems 1.1 and 1.3. Show that there exist exactly six different isomorphisms  $V_4 \rightarrow V'_4$ .
15. Give the matrix representations of the elements of  $D_4$ . Does matrix multiplication lead to a faster way to multiply the elements of  $D_4$  than the rules (1.5) and (1.6)?
16. Determine the symmetry set of an equilateral triangle in the plane. Do these symmetries commute under composition?
17. Can every permutation of  $\{A, B, C, D\}$  also be obtained from the transpositions  $(AB)$ ,  $(BC)$ , and  $(CD)$ ? Or from the transposition  $(AB)$  and the 4-cycle  $(ABCD)$ ? If so, how many multiplications are needed, at most, in these cases to obtain a permutation?
18. Show that the subset  $H \subset D_4$  generated by the symmetries  $r \circ s_x$  and  $r^3 \circ s_x$  of the square is a Klein four-group and is not equal to  $V_4 = \{\text{id}, s_x, s_y, h\}$ .  
[So we cannot speak of *the* inclusion  $V_4 \subset D_4$ .]
19. Determine the subset of  $S_4$  generated by the eight 3-cycles in  $S_4$ .  
\*Can you prove that your answer is correct?
20. Does there exist a quadrilateral  $ABCD$  in the plane with symmetry set  $S_4$ ? Explain.
21. Let  $n > 2$  be an integer. Show that the symmetry set of a regular  $n$ -gon about the origin in the plane consists of  $2n$  elements: the  $n$  rotations about the origin by multiples of  $2\pi/n$  and the reflections in the  $n$  lines connecting the origin to a vertex or the midpoint of an edge.
22. Show that the symmetry set of the unit circle in the plane consists of the rotations about the origin and the reflections in lines through the origin.

\*23. Can the set in the previous exercise be generated by a *finite* number of symmetries?

24. Determine the symmetry set of the infinite diamond pattern below.



Show that the set can be generated by three reflections.

25. Show that there are exactly 48 spatial symmetries that map a given cube to itself. Do two of these symmetries always commute?

26. Show that the equation  $55x^3 + 3 = y^3$  has no integer solutions.  
[Hint: Look at residue classes modulo 7 or 9.]

\*27. New Year's puzzle: prove that the equation

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} + \cdots + \frac{1}{x_{2025}} + \frac{1}{x_{2026}} = 1$$

has only finitely many solutions in positive integers  $x_i$ .

## 2 PERMUTATION GROUPS

The sets  $V_4$ ,  $D_4$ , and  $S_4$  from §1 are concrete examples of *groups*, of which we will now give a general definition. After that, we will give some details on the important example of the *permutation group*.

### ► THE GROUP AXIOMS

A *binary operation* or *composition law* on a set  $G$  is a map

$$\begin{aligned} G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \circ b, \end{aligned}$$

that is, a function that assigns to each ordered pair  $(a, b)$  of elements of  $G$  the *composition*  $a \circ b$  of  $a$  and  $b$  in  $G$ . We can use an arbitrary symbol instead of “ $\circ$ ” to denote  $a \circ b$ , for example  $a * b$  or  $a \# b$ . However, as there is no advantage to using exotic symbols, we often simply write  $ab$  for  $a \circ b$  and call the composition of  $a$  and  $b$  the *product*.

A *unit element* or *identity* for a binary operation on  $G$  is an element  $e \in G$  with the property that for all  $a \in G$ , we have  $e \circ a = a \circ e = a$ . Note that there can be only one such element: if  $e_1, e_2 \in G$  are both unit elements, then we have  $e_1 = e_1 \circ e_2 = e_2$ .

**2.1. Definition.** A set  $G$  endowed with a binary operation  $\circ$  is called a *group* if the following conditions are satisfied:

(G1) The set  $G$  contains a unit element  $e$  for the binary operation  $\circ$ .

(G2) For any three elements  $a, b, c \in G$ , we have the associative property:

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

(G3) For every element  $a \in G$ , there exists an element  $a^\dagger \in G$  with

$$a \circ a^\dagger = a^\dagger \circ a = e.$$

The element  $a^\dagger$  in (G3), called the *inverse* of  $a$ , is uniquely determined by  $a$ . After all, if  $a^\dagger$  and  $a^\ddagger$  are both inverses of  $a \in G$ , then by (G1) and (G2), we have

$$a^\dagger = a^\dagger \circ e = a^\dagger \circ (a \circ a^\ddagger) = (a^\dagger \circ a) \circ a^\ddagger = e \circ a^\ddagger = a^\ddagger.$$

So from now on, we can speak of *the* inverse of an element, just as we have *the* unit element of the group.

The *group axioms* (G1), (G2), and (G3) in 2.1 are chosen in such a way that many “natural examples” satisfy them. The reader can, for example, check that this includes, in particular, the examples  $V_4$ ,  $D_4$ , and  $S_4$  from the previous section.

**Exercise 1.** Is the set  $\mathbf{R}$  of real numbers a group under addition? And under multiplication?

In the *multiplicative notation* for the group operation, which we will use in this section, we denote the inverse of  $a$  by  $a^{-1}$ . We write  $a^n$  for a product  $a \circ a \circ \dots \circ a$  of  $n$  factors  $a$  and  $a^{-n}$  for the  $n$ -fold product  $a^{-1} \circ a^{-1} \circ \dots \circ a^{-1}$ . Note that by the associativity

(G2), there is no need for parentheses in a product with multiple factors: the outcome does not depend on any.

We define  $a^0 = e$  for all  $a \in G$ , so that for all  $m, n \in \mathbf{Z}$ , the identity  $a^m a^n = a^{m+n}$  holds. More generally, it is convenient to define the product of zero factors, the *empty product*, to be equal to the unit element  $e$ .

A product  $a_1 a_2 a_3 \dots a_n$  of  $n$  elements  $a_i \in G$  is sometimes written as  $\prod_{i=1}^n a_i$ . The *order* of the factors of such a product is important: the product  $ab$  is not, in general, equal to  $ba$ . If it is, then we say that  $a$  and  $b$  *commute*. For non-commuting elements  $a$  and  $b$ , the products  $(ab)^n = ababab \dots ab$  and  $a^n b^n = a a a \dots a b b b \dots b$  may be completely different.

Groups in which all elements commute with one another are called *abelian groups*, after the Norwegian mathematician Niels Henrik Abel<sup>2</sup> (1802–1829).

**Exercise 2.** Show that the inverse of the product  $ab$  of two elements  $a$  and  $b$  is equal to

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

This “shoe-sock rule” says that to undo putting on socks and shoes, you must first take off your shoes and then your socks: the order is reversed.

## ► ORDERS OF GROUPS AND ELEMENTS

The number of elements of  $G$ , which can be either finite or infinite, is called the *order* of  $G$  and denoted by  $\#G$ . The *trivial group*, which consists of only the unit element, has order 1 and is therefore the “smallest possible group.” Notation:  $G = 1$ .

The *order* of an element  $a \in G$  is the least positive number  $n$  such that  $a^n = e$ . If such an  $n$  does not exist, then we say that  $a$  has infinite order. In a finite group, all elements have finite order. We have the following more precise statement.

**2.2. Proposition.** *Let  $G$  be a group and  $a \in G$  an element.*

1. *If  $a$  has infinite order, then all elements in the sequence  $(a^k)_{k \in \mathbf{Z}}$  of integer powers of  $a$  are different.*
2. *If  $a$  has finite order  $n$ , then there are exactly  $n$  different powers of  $a$ , and the sequence  $(a^k)_{k \in \mathbf{Z}}$  of integer powers of  $a$  is periodic with period  $n$ .*

**Proof.** Suppose that there exist two distinct values  $i, j \in \mathbf{Z}$  with, say,  $i > j$ , such that  $a^i = a^j$ . If we multiply either side by  $a^{-j}$ , then we obtain  $a^{i-j} = a^{j-j} = a^0 = e$ , so  $a$  has finite order. This proves (1).

If  $a$  has finite order  $n$ , then the argument above shows that the powers  $a^i$  for  $i = 0, 1, 2, \dots, n-1$  are all different. For  $i \in \mathbf{Z}$ , the equality  $a^{i+n} = a^i a^n = a^i e = a^i$  holds, so the sequence of powers of  $a$  is periodic with period  $n$ , and there are exactly  $n$  different powers.  $\square$

An element  $a \in G$  of finite order is also called a *torsion element*: the powers of  $a$  “rotate in a circle.” In a finite group, all elements are torsion.

**Exercise 3.** For  $a$  of order  $n$ , which power in the sequence  $e, a, a^2, \dots, a^{n-1}$  is the inverse of  $a$ ?

In the examples in the previous section, we frequently used the three *group axioms* (G1), (G2), and (G3). As the proofs of 1.1, 1.4, and 2.2 show, we often use them in the form of the equivalence

$$(2.3) \quad ax = b \iff x = a^{-1}b$$

for elements  $a, b, x \in G$ . This equivalence allows us to take an identity in a group and move elements to the other side of the equal sign. In fact, what we do—and that is the proof of (2.3)—is multiply by the same group element on both sides. If we multiply both sides of the identity  $ax = b$  on the left by the element  $a^{-1}$ , then we see that  $a^{-1}(ax) = (a^{-1}a)x = ex = x$  is equal to  $a^{-1}b$ . Conversely, the identity  $x = a^{-1}b$  gives the identity  $ax = b$  by multiplying on the left by  $a$ .

It follows from (2.3) that the map  $\lambda_a : G \rightarrow G$  given by  $x \mapsto ax$ , the *left multiplication* by  $a \in G$ , is bijective: for every  $b \in G$ , there is a unique element  $x \in G$  sent to  $b$  by left multiplication by  $a$ . The inverse of this map is given by left multiplication by  $a^{-1}$ , and by (G2), we have  $\lambda_a \circ \lambda_b = \lambda_{ab}$ .

**Exercise 4.** Prove the equivalence  $xa = b \iff x = ba^{-1}$ . Conclude that the right multiplication  $x \mapsto xa$  by  $a \in G$  gives a bijection  $\rho_a : G \rightarrow G$ . Prove:  $\rho_a \circ \rho_b = \rho_{ba}$ .

## ► PERMUTATION GROUPS

All groups in §1 consist of bijections from some set to itself. In the remainder of this section, we consider the “standard example” consisting of the group of *all* bijections from a set to itself.

**2.4. Theorem.** *Let  $X$  be a set. Then the set  $S(X)$  of bijections  $X \rightarrow X$  endowed with the composition of maps as its binary operation is a group.*

**Proof.** First, note that composing two bijections  $X \rightarrow X$  gives a bijection. To prove (G1), note that the identity  $\text{id}_X$  indeed behaves as a unit element for composition:  $f \circ \text{id}_X = \text{id}_X \circ f = f$  for all  $f \in S(X)$ . In this case, the associativity is a general property of the composition of maps. Namely, for any three maps

$$X_1 \xrightarrow{f} X_2 \xrightarrow{g} X_3 \xrightarrow{h} X_4$$

between sets, the identity  $h \circ (g \circ f) = (h \circ g) \circ f$  holds. If we take  $X_1 = X_2 = X_3 = X_4 = X$ , then we obtain (G2) for  $S(X)$ . The inverse  $f^{-1}$  of a bijection  $f \in S(X)$  is the inverse map in the sense of set theory, which is defined exactly by property (G3):  $f \circ f^{-1} = f^{-1} \circ f = \text{id}_X$ .  $\square$

The group  $S(X)$  in 2.4 is a very general example of a group because as *Cayley’s theorem* in 5.8 shows, *every* group  $G$  can be seen as a group of bijections from  $G$  to itself.

The group  $S(X)$  associated with a set  $X$  is called<sup>3</sup> the *permutation group* or *symmetric group* on  $X$ . When  $X$  is a finite set of  $n$  elements, we denote this group by  $S_n$ . The set  $S_4$  of permutations of the set  $\{A, B, C, D\}$  in §1 is indeed the permutation group  $S_4$  on four letters. As we saw, the order of this group is  $4! = 24$ . More generally,

the permutation group  $S_n$  has order  $n!$ . After all, for a bijection from a set with  $n$  elements to itself, there are  $n$  possibilities for the image of the first element, then  $n - 1$  left for the image of the second element,  $n - 2$  for the third, and so on, until there is only one possibility for the  $n$ -th element. This gives  $n(n - 1)(n - 2) \dots 2 \cdot 1 = n!$  possibilities.

**Exercise 5.** Show that  $S_n$  is not abelian for  $n \geq 3$ .

► CYCLE NOTATION

In §1, we introduced a cycle notation for the elements of  $S_4$ , which is considerably more practical than giving a complete list of arguments and images. An element  $\sigma \in S(X)$  is called a  $k$ -cycle or *cyclic permutation* of length  $k$  if there exist  $k$  different elements  $x_1, x_2, \dots, x_k \in X$  such that  $\sigma$  is the identity on  $X \setminus \{x_1, x_2, \dots, x_k\}$  and acts on  $\{x_1, x_2, \dots, x_k\}$  as the cyclic shift

$$\begin{array}{ccccccc} x_1 & \mapsto & x_2 & \mapsto & x_3 & \mapsto & \dots & \mapsto & x_{k-1} & \mapsto & x_k \\ \uparrow & & & & & & & & & & \downarrow \\ & & & & & & & & & & \end{array}$$

We denote such an element by  $\sigma = (x_1 \ x_2 \ x_3 \ \dots \ x_{k-1} \ x_k)$ . This notation is unique up to cyclic shifts because, for example,  $(x_1 \ x_2 \ x_3)$  and  $(x_2 \ x_3 \ x_1)$  indicate the same permutation. A 1-cycle is the same as the identity  $\text{id}_X$ .

Two cycles  $(x_1 \ x_2 \ x_3 \ \dots \ x_{k-1} \ x_k)$  and  $(x'_1 \ x'_2 \ x'_3 \ \dots \ x'_{\ell-1} \ x'_\ell)$  in  $S(X)$  are called *disjoint* if no element  $x_i$  is equal to an  $x'_j$ . Note that disjoint cycles always commute.

Our introductory section already used the following intuitively clear theorem for  $X = \{A, B, C, D\}$ .

**2.5. Theorem.** *Let  $X$  be a finite set. Then every permutation  $\sigma \in S(X)$  can be written as a product of disjoint cycles.*

**Proof.** We carry out the proof by induction on  $n = \#X$ . For the trivial group  $S_1$ , there is nothing to prove. After all, by our convention on the empty product, the unit element is equal to the product of *zero* disjoint cycles. (Those uncomfortable with this can also write the unit element as a 1-cycle.) In any case, the theorem is correct for  $n = 1$ .

Assume that the theorem is true for sets with fewer than  $n$  elements, and take a permutation  $\sigma \in S(X)$  for a set  $X$  with  $n$  elements. If we choose an  $x \in X$ , then only finitely many different elements occur in the infinite sequence  $x, \sigma(x), \sigma^2(x), \dots$

Let  $k > 0$  be the least positive number such that  $\sigma^j(x) = \sigma^k(x)$ , where  $j \in \{0, 1, 2, \dots, k - 1\}$ . Applying  $\sigma^{-j}$  to this equality gives  $\sigma^{k-j}(x) = \sigma^{j-j}(x) = x$ , so by the minimality of  $k$ , we have  $j = 0$  and  $\sigma^k(x) = x$ . The elements of the set  $X_0 = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{k-1}(x)\}$  are now distinct, and  $\sigma$  acts on this as the  $k$ -cycle

$$\sigma_0 = (x \ \sigma(x) \ \sigma^2(x) \ \dots \ \sigma^{k-2}(x) \ \sigma^{k-1}(x)).$$

As  $\sigma$  is a bijection on  $X$  that maps the subset  $X_0 \subset X$  onto itself, the complement  $X \setminus X_0$  is also mapped onto itself by  $\sigma$ . As  $X \setminus X_0$  consists of  $n - k < n$  elements, the

restriction of  $\sigma$  to this set can be written as a product of disjoint cycles. Multiplying this product by the cycle  $\sigma_0$ , we obtain a presentation of  $\sigma$  as a product of disjoint cycles.  $\square$

**Exercise 6.** Calculate the product  $(1\ 2)(2\ 3)(3\ 4)\dots(n-1\ n)$ , and use it to deduce 1.7 from 2.5.

To denote the elements of  $S_n$  in cycle notation, we must choose a set with  $n$  elements. A standard choice for such a set is  $\{1, 2, 3, \dots, n-1, n\}$ .

**2.6. Example.** We can denote an element of  $S_{12}$  by a  $2 \times 12$  matrix

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 1 & 11 & 10 & 3 & 4 & 7 & 2 & 12 & 6 & 8 & 9 \end{pmatrix}.$$

Each column consists of an element and its image. We can find the disjoint cycle representation of  $\sigma$  by choosing an element, say 1, and looking at its image under successive applications of  $\sigma$ . We find  $1 \mapsto 5 \mapsto 3 \mapsto 11 \mapsto 8 \mapsto 2 \mapsto 1$ , a cycle of length 6. Now choose an element outside this cycle, say 4, and repeat the procedure. We find  $4 \mapsto 10 \mapsto 6 \mapsto 4$ , a 3-cycle. There are still elements outside these cycles because we have only had  $6 + 3 = 9$  of the 12 elements. We do not need to write down the element 7, which stays in place and gives a 1-cycle. If we take 9, we find the 2-cycle  $(9\ 12)$ . The result of the calculation is

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

**Exercise 7.** Show that the element  $\sigma \in S_{12}$  above has order 6, and calculate the different powers of  $\sigma$ .

Similarly, we can find the disjoint cycle representation of an element given as a product of non-disjoint cycles, such as  $\tau = (1\ 4\ 3\ 6)(7\ 1\ 6)(2\ 7\ 6\ 5) \in S_7$ . We determine the image of 1 under  $\tau$  by first applying  $(2\ 7\ 6\ 5)$  (result: 1), then  $(7\ 1\ 6)$  (result: 6), and finally  $(1\ 4\ 3\ 6)$  (result: 1). So  $\tau$  leaves 1 in place. For 2, we find  $2 \mapsto 7 \mapsto 1 \mapsto 4$ , so  $\tau(2) = 4$ . Continuing in this way, we get  $\tau(4) = 3$ ,  $\tau(3) = 6$ ,  $\tau(6) = 5$ , and finally  $\tau(5) = 2$ . This gives the 5-cycle  $(2\ 4\ 3\ 6\ 5)$ , and as in addition to 1, the element 7 is also fixed by  $\tau$ , the element  $\tau$  is equal to this 5-cycle.

**Exercise 8.** Write the elements  $\sigma, \tau \in S_{12}$  given by, respectively,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 5 & 1 & 11 & 10 & 3 & 4 & 7 & 2 & 12 & 6 & 8 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 2 & 12 & 6 & 8 & 9 & 5 & 1 & 11 & 10 & 3 & 4 \end{pmatrix}$$

as products of disjoint cycles, and do the same for  $\sigma\tau$  and  $\tau\sigma$ .

The disjoint cycle representation of an element  $\sigma \in S_n$  is essentially unique: two such representations can only differ in the order of the cycles and whether they include the cycles of length 1. The cycles in the disjoint cycle representation of  $\sigma$  correspond to the *orbits* the set  $\{1, 2, \dots, n\}$  splits up into under repeatedly applying  $\sigma$ :  $i$  and  $j$  occur in the same cycle if and only if  $i$  can be mapped to  $j$  by repeatedly applying  $\sigma$ . A point in an orbit of length 1 corresponds to an element left in place by  $\sigma$  and is called a *fixed point* of the permutation  $\sigma$ .

If  $\sigma \in S_n$  is a product of  $t$  disjoint cycles of lengths  $k_1, k_2, \dots, k_t$ , where we also count the cycles of length 1, then we have  $k_1 + k_2 + k_3 + \dots + k_t = n$ . We call the sequence  $(k_1, k_2, k_3, \dots, k_t)$  the *cycle type* of  $\sigma$ ; the order of the terms does not matter. A cycle type  $(k_1, k_2, k_3, \dots, k_t)$  is in fact nothing but a way to write  $n$  as a sum of positive numbers  $k_i$ . We therefore also call the “splitting”  $(k_1, k_2, k_3, \dots, k_t)$  of  $n$  a *partition* of  $n$ . For the element  $\sigma \in S_{12}$  in 2.6, the cycle type is  $(6, 3, 2, 1)$ , which corresponds to the partition  $12 = 6 + 3 + 2 + 1$ .

**Exercise 9.** Determine all cycle types that occur in  $S_4$  and  $S_5$ , and for each cycle type, determine how many permutations there are of this type.

### ► SUBGROUPS, CYCLIC GROUPS

From the example of the group  $S_4$  in §1, which contained  $D_4$  and  $V_4$ , we see that a group can have various subsets that are themselves groups. In such a case, we speak of *subgroups*.

**2.7. Definition.** A subset  $H$  of a group  $G$  is called a *subgroup* of  $G$  if it satisfies the following conditions:

- (H1) The subset  $H$  contains the unit element of  $G$ .
- (H2) For any two elements  $a, b \in H$ , we have  $ab \in H$ .
- (H3) For every element  $a \in H$ , we have  $a^{-1} \in H$ .

Condition (H2) says that the restriction of the binary operation  $G \times G \rightarrow G$  to  $H \times H$  has image in  $H$  and therefore defines a binary operation on  $H$ . By (H1) and (H3), the subset  $H$  contains a unit element and inverses for this binary operation. The associativity of the binary operation on  $H$  follows from the associativity on  $G$ . We conclude that a subgroup  $H \subset G$  endowed with the binary operation of  $G$  is again a group. Conversely, we can easily see that every subset of a group  $G$  that forms a group when endowed with the binary operation of  $G$  is a subgroup of  $G$  in the sense of 2.7.

Every group  $G$  contains a *trivial subgroup*  $H = \{e\}$ . We generally denote it by  $H = 1$  for short. The “whole group”  $H = G$  is always a subgroup of  $G$ .

**Exercise 10.** Show that a subset  $H \subset G$  is a subgroup of  $G$  if and only if it satisfies the following conditions:

- (H1') The subset  $H$  is non-empty.
- (H2') For any two elements  $a, b \in H$ , we have  $ab^{-1} \in H$ .

Given one or more elements of a group, there is an easy way to construct the smallest subgroup that contains those elements.

**2.8. Lemma.** Let  $S$  be a subset of a group  $G$  and  $S^{-1} = \{s^{-1} : s \in S\}$ . Let  $\langle S \rangle \subset G$  be the set of elements that can be written as a finite product of elements  $s \in S \cup S^{-1}$ . Then  $\langle S \rangle$  is a subgroup of  $G$ , the smallest subgroup of  $G$  that contains every element of  $S$ .

**Proof.** Let us verify conditions (H1)–(H3) for the subset  $\langle S \rangle \subset G$ .

If  $S$  is empty, then  $\langle S \rangle$  contains only the empty product, which is equal to  $e$ , and  $\langle S \rangle$  is the trivial subgroup of  $G$ . In general, (H1) is automatically satisfied.

If  $a$  and  $b$  are products of elements  $s \in S \cup S^{-1}$ , then  $ab$  is also such a product, so  $\langle S \rangle$  satisfies (H2). If  $a = s_1 s_2 \dots s_t$  is a product of elements  $s_i \in S \cup S^{-1}$ , then by the “shoe-sock rule,”  $a^{-1} = s_t^{-1} s_{t-1}^{-1} \dots s_2^{-1} s_1^{-1}$ . For every element  $s_i \in S \cup S^{-1}$ , the inverse  $s_i^{-1}$  is also in  $S \cup S^{-1}$ , so we have  $a^{-1} \in \langle S \rangle$ , and (H3) is satisfied. We conclude that  $\langle S \rangle$  is a subgroup of  $G$ .

Every subgroup  $H \subset G$  that contains the elements of  $S$  contains  $S^{-1}$  by (H3), and  $(S \cup S^{-1}) \subset H$  implies  $\langle S \rangle \subset H$  by (H2).  $\square$

**Exercise 11.** Show that for  $S \subset G$ , the set of finite products of elements of  $S$  is not necessarily a subgroup of  $G$ . Is it always a subgroup if  $G$  is finite?

The subgroup  $\langle S \rangle$  in 2.8 is called the subgroup of  $G$  *generated by*  $S$ . If  $\langle S \rangle = G$ , then we say that  $G$  is *generated by*  $S$  or that  $S$  is a set of *generators* of  $G$ . A group generated by a finite set of elements is called *finitely generated*. Finite groups are always finitely generated: we can simply take  $S = G$ . For small  $S$ , such as  $S = \{a\}$  or  $S = \{a, b\}$ , the braces are generally left out, and  $\langle S \rangle$  is written as  $\langle a \rangle$  or  $\langle a, b \rangle$ . So for the subgroups  $V_4$  and  $D_4$  of  $S_4$  in §1, if we number the vertices  $A, B, C, D$  as  $A = 1, B = 2, C = 3$ , and  $D = 4$ , then we have

$$\begin{aligned} V_4 &= \langle (1\ 3), (2\ 4) \rangle, \\ D_4 &= \langle (2\ 4), (1\ 2\ 3\ 4) \rangle, \\ S_4 &= \langle (1\ 2), (1\ 2\ 3\ 4) \rangle. \end{aligned}$$

Note that the obtained injections  $V_4 \rightarrow S_4$  and  $D_4 \rightarrow S_4$  depend on a *choice* of the numbering of the vertices. See Exercise 48.

**Exercise 12.** Give an explicit numbering of  $\{A, B, C, D\}$  that leads to injections  $V_4 \rightarrow S_4$  and  $D_4 \rightarrow S_4$  with a *different* image.

A group generated by one element is called a *cyclic group*. It consists of the integer powers of the generator. If  $a \in G$  has infinite order, then by 2.2.1, the cyclic subgroup  $\langle a \rangle \subset G$  also has infinite order. If  $a \in G$  has finite order  $n$ , then by 2.2.2, the subgroup  $\langle a \rangle$  also has order  $n$ . For example,  $C_4 = \langle (1\ 2\ 3\ 4) \rangle$  is a cyclic subgroup of  $S_4$  of order 4. In 4.9, we will see that in a finite group, the order of any subgroup divides the group order. By considering cyclic subgroups, it follows that the orders of the elements of a finite group always *divide* the group order.

**Exercise 13.** Show that the groups  $V_4, D_4$ , and  $S_4$  are not cyclic.

For a subset  $S \subset S_n$  of more than one element, we often have (in a sense that must be made precise<sup>4</sup>)  $\langle S \rangle = S_n$ . See Exercises 54–56 for examples of small sets that generate  $S_n$ .

## ► THE SIGN MAP

We conclude this section by constructing a subgroup  $A_n \subset S_n$  called the *alternating group* on  $n$  elements. The construction relies on assigning a *sign*  $\varepsilon(\sigma) \in \{\pm 1\}$  to a permutation  $\sigma \in S_n$ .

**2.9. Lemma.** *There exists a unique map  $\varepsilon : S_n \rightarrow \{\pm 1\}$  with the following two properties:*

- 1) *If  $\sigma$  is a transposition, then we have  $\varepsilon(\sigma) = -1$ .*
- 2) *For any elements  $\sigma, \tau \in S_n$ , we have  $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$ .*

**Proof.** If we take  $\sigma = \tau = \text{id} \in S_n$  in (2), then we see that  $\varepsilon$  always sends the identity to 1, and we are immediately done for  $n = 1$ . For  $n \geq 2$ , we know by 1.7 that every element can be written as a non-empty product of transpositions, so it is clear that there is *at most* one map  $\varepsilon$  with properties (1) and (2). However, as a given permutation can be written as a product of transpositions in many different ways, it is not obvious that such a map exists.

We define  $\varepsilon$  by looking at the function  $F : \mathbf{R}^n \rightarrow \mathbf{R}$  given by

$$F(x_1, x_2, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

First, observe that  $F$  is not the zero function. For  $\sigma \in S_n$ , consider the function  $\sigma f : \mathbf{R}^n \rightarrow \mathbf{R}$  given by

$$(\sigma f)(x_1, x_2, \dots, x_n) = F(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = \prod_{1 \leq i < j \leq n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Up to a sign, this function is equal to  $F$ , and we define  $\varepsilon(\sigma)$  by

$$\sigma f = \varepsilon(\sigma)F.$$

If we take  $\sigma$  equal to a transposition  $(i j)$ , then  $\sigma f$  arises from  $F$  by replacing the factor  $x_i - x_j$  in the definition of  $F$  by  $x_j - x_i$ . After all, all other factors that contain  $x_i$  or  $x_j$  can be combined pairwise, with one pair per element  $k \neq i, j$ . For every  $k$ , we obtain one of the four pairs below, depending on the position of  $k$  with respect to  $i$  and  $j$ ,

$$(x_i - x_k)(x_j - x_k), \quad (x_i - x_k)(x_k - x_j), \quad (x_k - x_i)(x_j - x_k), \quad (x_k - x_i)(x_k - x_j),$$

and every one of these factors is invariant under the transposition  $(i j)$ . This shows that we have  $\varepsilon(\sigma) = -1$  for a transposition  $\sigma$ .

The relation  $(\sigma\tau)(F) = \sigma(\tau F)$  easily gives  $\varepsilon(\sigma\tau)F = \varepsilon(\sigma)\varepsilon(\tau)F$ ; it follows that  $\varepsilon$  also satisfies (2).  $\square$

Instead of the sign, we also speak of the *parity* of a permutation. Permutations  $\sigma \in S_n$  with  $\varepsilon(\sigma) = 1$  are called *even*, those with  $\varepsilon(\sigma) = -1$  *odd*. Theorem 1.7 says that every permutation is a product of transpositions, but its presentation as such a product is not unique. For example, the 4-cycle  $(1\ 2\ 3\ 4)$  can be written as

$$(1\ 2\ 3\ 4) = (1\ 4)(1\ 3)(1\ 2) = (2\ 3)(1\ 2)(1\ 3)(2\ 4)(2\ 3).$$

However, 2.9 implies that the *parity* of the number of transpositions in such a presentation is uniquely determined:  $(1\ 2\ 3\ 4)$  *cannot* be written as the product of two, four,

or six transpositions. Therefore, the parity of a permutation is the same as the parity of the number of transpositions needed to get this permutation.

For a  $k$ -cycle, the parity  $\varepsilon(\sigma)$  depends only on  $k$ . The identity

$$(1\ 2)(2\ 3)(3\ 4)(4\ 5)\dots(k-1\ k) = (1\ 2\ 3\ 4\ \dots\ k-1\ k)$$

shows that a  $k$ -cycle  $\sigma \in S_n$  has parity  $\varepsilon(\sigma) = (-1)^{k-1}$ . For  $\sigma \in S_n$  of cycle type  $(k_1, k_2, k_3, \dots, k_t)$ , we find

$$\varepsilon(\sigma) = (-1)^{\sum_{i=1}^t (k_i-1)} = (-1)^{n-t}.$$

The proof of 2.9 also shows that the parity of a permutation  $\sigma$  is also the parity of the number of *inversions* induced by  $\sigma$ . An inversion is a pair  $(i, j)$  of indices in  $\{1, 2, \dots, n\}$  for which the inequalities  $i < j$  and  $\sigma(i) > \sigma(j)$  hold.

By the *multiplicativity* of the sign map stated in 2.9.2, we easily see that the subset  $A_n$  of even permutations in  $S_n$  is a subgroup. First, the identity  $\text{id} \in S_n$  is a product of zero transpositions and therefore an even permutation, so (H1) is satisfied. For all  $\sigma \in S_n$ , we now have the identity  $1 = \varepsilon(\text{id}) = \varepsilon(\sigma\sigma^{-1}) = \varepsilon(\sigma)\varepsilon(\sigma^{-1})$ . This shows that  $\sigma$  and  $\sigma^{-1}$  have the same sign. Property (H3) follows. Finally, (H2) is also a direct consequence of the multiplicativity in 2.9.2: the product of two even permutations is also even.

Later, we will see that the alternating group  $A_n$  occurs in various situations. For  $n = 4$ , we saw in Exercise 1.19 that  $A_4$  is generated by 3-cycles.

**2.10. Theorem.** *The alternating group  $A_n$  is the subgroup of  $S_n$  generated by the 3-cycles. The order of  $A_n$  is  $\frac{1}{2} \cdot n!$  for all  $n \geq 2$ .*

**Proof.** The first statement is correct (but trivial) for  $n \leq 2$ . To show for  $n \geq 3$  that  $A_n$  is generated by the 3-cycles, we first note that by the identity

$$(*) \quad (x\ y\ z) = (x\ y)(y\ z),$$

every 3-cycle  $(x\ y\ z) \in S_n$  is an even permutation. As an even permutation is the product of an even number of transpositions, it now suffices to show that every product of two transpositions  $\sigma, \tau \in S_n$  can be written as a product of 3-cycles. For  $\sigma = \tau$ , this is clear because  $\sigma\tau = \text{id}$ , and for distinct but not disjoint  $\sigma$  and  $\tau$ , it follows from (\*). In the disjoint case, we can also apply (\*) with a sleigh of hand:

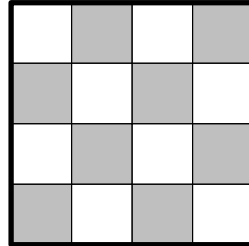
$$(a\ b)(c\ d) = (a\ b)(b\ c) \cdot (b\ c)(c\ d) = (a\ b\ c)(b\ c\ d).$$

To see that for  $n \geq 2$ , there are as many even as odd permutations in  $S_n$ , we choose a transposition in  $S_n$  (this is where we need  $n \geq 2$ ) and consider the bijection  $S_n \rightarrow S_n$  given by left multiplication by this transposition. This bijection interchanges the even and odd permutations, so there must be equal numbers of both kinds. As  $S_n$  has order  $n!$ , it follows immediately that  $A_n$  has order  $\frac{1}{2} \cdot n!$ .  $\square$

## ► 15 PUZZLE

As a recreational application of the notion of parity for permutations, we look at a well-known little puzzle known as the 15 puzzle.<sup>5</sup> The idea is to slide 15 tiles in a square box to move them in numerical order. If, in the end, the situation is as shown below on the left, then the puzzle cannot be solved because it is impossible to interchange tiles 14 and 15 through skillful sliding.

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



SO	WH	ER	EI
ST	HE	PA	RI
TY	PR	OB	LE
MH	E?	ER	

To *prove* that this is impossible, we give the “missing tile” the number 16 and note that a “move” in this game consists of interchanging tile 16 and an adjacent tile. We are apparently doing transpositions in the permutation group  $S_{16}$ . If, after several moves, tile 16 is again at the bottom right, then this number of moves was *even*: after all, in the given “checkerboard pattern,” tile 16 always moves from a white square to a black square, and vice versa, so after an odd number of moves, it will never be back on the bottom right white square. The product of an even number of transpositions is an *even* permutation, and that cannot be the desired transposition (14 15).

**Exercise 14.** Show that the other puzzle, in which “ER” and “E?” must be interchanged, is solvable.

Many puzzles of this type, such as the well-known *Rubik’s cube*<sup>6</sup> and its variants, have considerably more complicated symmetry groups than the 15 puzzle. However, we can often prove the impossibility of solving puzzles with certain initial positions in a similar way.

## EXERCISES.

In the exercises below,  $G$  always denotes a group.

15. In each of the following cases, check whether the binary operation  $*$  defines the structure of a group on  $X$  and, if so, whether the group is abelian:

$$a * b = ab \quad \text{for } a, b \in X = \mathbf{R} \setminus \{0\},$$

$$a * b = a + b - 1 \quad \text{for } a, b \in X = \mathbf{R},$$

$$a * b = a^{\log b} \quad \text{for } a, b \in X = \mathbf{R}_{>1},$$

$$a * b = \max\{a, b\} \quad \text{for } a, b \in X = \mathbf{R}.$$

16. The *commutator* of two elements  $a, b \in G$  is the element  $[a, b] = aba^{-1}b^{-1}$ . Show that we have  $ab = [a, b]ba$ , and conclude that  $a$  and  $b$  commute if and only if the commutator  $[a, b]$  is equal to  $e$ .
17. Suppose that we have  $(ab)^{-1} = a^{-1}b^{-1}$  for all  $a, b \in G$ . Prove that  $G$  is abelian.
18. Suppose that we have  $(ab)^n = a^n b^n$  for all  $a, b \in G$  and all  $n > 1$ . Prove that  $G$  is abelian.
19. Suppose that we have  $a^2 = e$  for all  $a \in G$ . Prove that  $G$  is abelian.
20. Show that we have  $a^4 = e$  for all  $a \in D_4$  and that  $D_4$  is not abelian.
- \*21. Does there exist a non-abelian group  $G$  such that we have  $a^3 = e$  for all  $a \in G$ ?
22. Show that each element occurs exactly once in every row and column of the group table (that is, multiplication table) of a finite group.
23. Let  $G$  be a group of order 4. Prove:  $G$  is either cyclic or the Klein four-group.
24. Let  $G$  be a set with an element  $e \in G$  and a binary operation  $\circ$  that satisfy (G2) and the following *right axioms*:
- (G1') For all  $a \in G$ , we have  $a \circ e = a$ .
- (G3') Every element  $a \in G$  has a right inverse  $a^\dagger \in G$  with the property  $a \circ a^\dagger = e$ .
- Prove that  $G$  endowed with the binary operation  $\circ$  is a group.  
[Hint: show first that any element  $a \in G$  satisfying  $a^2 = a$  is equal to  $e$ .]
25. Let  $X$  be a set. The collection  $P(X)$  of subsets of  $X$  is called the *power set* of  $X$ . Define the product of two subset  $A, B \in P(X)$  as the symmetric difference  $A \Delta B$ . Show that this makes  $P(X)$  into an abelian group.
26. Let  $X$  be a finite set. Calculate the order of the group  $P(X)$  from the previous exercise and the orders of the elements of  $P(X)$ .
27. Prove that every intersection  $\bigcap_i H_i$  of subgroups  $H_i \subset G$  is a subgroup of  $G$ .
28. Show that the union  $H_1 \cup H_2$  of two subgroups  $H_1$  and  $H_2$  of  $G$  is a subgroup if and only if we have  $H_1 \subset H_2$  or  $H_2 \subset H_1$ .
29. A *chain* of subgroups of  $G$  is a collection  $\{H_i\}_{i \in I}$  of subgroups  $H_i \subset G$  such that for any two subgroups  $H_i, H_j$  in the collection, we have an inclusion  $H_i \subset H_j$  or  $H_j \subset H_i$ . Show that for a suitably chosen indexation, a finite chain of  $n \geq 1$  subgroups satisfies

$$H_1 \subset H_2 \subset H_3 \subset \dots \subset H_{n-1} \subset H_n$$

and prove, in general, that the union  $\bigcup_{i \in I} H_i$  of a non-empty chain is a subgroup of  $G$ .

30. Determine all subgroups of  $S_3$ . What are the orders of these subgroups?
31. Let  $G$  be a finite *abelian* group and  $x \in G$  arbitrary. Prove:  $\prod_{g \in G} xg = \prod_{g \in G} g$ . Deduce from this that the order of  $x$  divides the group order. [The latter is also true if  $G$  is not abelian; see 4.9.]
32. Define  $\sigma, \tau \in S_5$  by  $\sigma = (1\ 5)(2\ 4)$  and  $\tau = (1\ 2\ 3\ 4\ 5)$ . Determine the commutator  $[\sigma, \tau]$  and the order of the subgroup  $H = \langle \sigma, \tau \rangle \subset S_5$ .
33. As in the previous exercise, but now with  $\sigma = (1\ 5)$ .
34. Show that in Definition 2.7, condition (H3) can be left out for *finite* subsets  $H \subset G$ . Also show that this does not hold in general.
35. Let  $a$  and  $b$  be torsion elements of an abelian group  $G$ . Prove:  $ab$  is a torsion element.
36. Let  $X = \mathbf{Z}$  be the set of integers, and let  $\sigma, \tau \in S(X)$  be given by, respectively,  $\sigma(x) = -x$  and  $\tau(x) = 1 - x$  for  $x \in \mathbf{Z}$ . Show that  $\sigma$  and  $\tau$  have order 2 and that  $\sigma\tau$  and  $\tau\sigma$  have infinite order.
37. Give an example of an infinite group  $G$  in which every element has finite order.
38. Let  $G$  be a finitely generated *abelian* group in which every element has finite order. Prove that  $G$  is finite.
39. Let  $G$  be a finite group and  $S \subset G$  a subset of order  $\#S > \frac{1}{2}\#G$ . Prove:  $G = \langle S \rangle$ .
40. Let  $G$  be a group of order  $\#G < 1000$ . Prove that  $G$  can be generated by fewer than ten elements.
- \*41. Let  $G$  be an infinite group. Prove:  $G$  is finitely generated  $\Rightarrow G$  is countably infinite. Does the converse hold?
- \*42. Let  $X$  be an infinite set. Prove that  $S(X)$  is not finitely generated.
43. Two elements  $x, y \in G$  are called *conjugate* if we have  $y = gxg^{-1}$  for some  $g \in G$ . Prove that “being conjugate” is an *equivalence relation* on the set of elements of  $G$ . The equivalence classes are called the *conjugacy classes* of  $G$ .
44. Let  $G$  be a finite group. Prove that all conjugacy classes of  $G$  have the same number of elements if and only if  $G$  is abelian.
45. Show that conjugate elements of a group have the same order.
46. Show that for  $\tau \in S_n$  arbitrary and a  $k$ -cycle  $\sigma = (x_1\ x_2\ \dots\ x_k) \in S_n$ , the conjugate  $\tau\sigma\tau^{-1}$  is equal to
- $$(\tau(x_1)\ \tau(x_2)\ \dots\ \tau(x_k)).$$
- Deduce that two elements of  $S_n$  are conjugate if and only if they have the same cycle type.
47. Let  $H \subset G$  be a subgroup and  $g \in G$  an element. Prove that the subgroup  $gHg^{-1} = \{ghg^{-1} : h \in H\}$  *conjugate* to  $H$  is again a subgroup of  $G$ .
48. Show that different choices of the numbering in Exercise 12 lead to images of  $V_4$  in  $S_4$  that are conjugate, and likewise for  $D_4$ . How many possible images do we get in each case? \*Are these *all* possible images by group embeddings of  $V_4$  and  $D_4$  into  $S_4$ ?

49. Let  $\sigma \in S_n$  be a product of  $t$  disjoint cycles of lengths  $k_1, k_2, \dots, k_t$ . Prove that the order of  $\sigma$  is equal to the least common multiple of the numbers  $k_i$ . Conclude that for every element  $\sigma \in S_n$ , the order of  $\sigma$  divides the order of  $S_n$ .
50. Let  $X$  be a set and  $H \subset S(X)$  a subgroup. Show that the relation  $\sim$  on  $X$  defined by

$$x \sim y \iff (\exists \tau \in H : y = \tau x)$$

is an equivalence relation, and conclude that  $X$  is a disjoint union of  $H$ -orbits. What are these orbits if  $X$  is finite and  $H$  is the cyclic subgroup generated by an element  $\sigma \in S(X)$ ?

51. Let  $X = \{1, 2, 3, \dots\}$  be the set of positive natural numbers, and view  $S_n$  as a subgroup of  $S(X)$  through its natural action on  $\{1, 2, 3, \dots, n\}$ . Show that  $H = \bigcup_{n>0} S_n$  is a subgroup of  $S(X)$ . Is  $H$  equal to  $S(X)$ ?
52. Let  $n > 1$  be an integer, and let  $f : S_n \rightarrow \mathbf{R}$  be a *non-constant* real-valued function on  $S_n$  that satisfies the multiplicativity 2.9.2. Prove that  $f$  is the sign map.
53. Are two elements conjugate in the group  $A_n$  if they have the same cycle type?
54. Show that  $S_n$  is generated by the set  $\{(1\ i) : i = 2, 3, \dots, n\}$ .
55. Show that  $A_n$  is generated by the set  $\{(1\ 2\ i) : i = 3, 4, \dots, n\}$ .
56. Show that for  $n \geq 2$ , the group  $S_n$  is generated by  $(1\ 2)$  and  $(1\ 2\ 3\ \dots\ n)$ .
57. Determine the sizes of all conjugacy classes in  $S_n$  for  $n \leq 6$ . \*Can you formulate and prove a divisibility property for the sizes of conjugacy classes in  $S_n$ ?
58. Let  $p(n)$  be the number of possible cycle types of elements of  $S_n$ . Calculate  $p(n)$  for  $n \leq 8$ .
- \*59. Prove that the *partition function*<sup>7</sup> in the previous exercise satisfies the power series identity

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{k \geq 1} \frac{1}{1 - x^k}.$$

Take  $p(0) = 1$  by definition. \*For what real values of  $x$  do these expressions converge?

60. Let  $g(n)$  be the maximal order of an element of  $S_n$ . Determine  $g(n)$  for  $n \leq 20$ . \*How could we determine  $g(n)$  for large  $n$ ?<sup>8</sup>
61. For  $\sigma \in S_n$ , define  $d(\sigma)$  as the number of fixed points of  $\sigma$ . Determine the average value

$$\delta_n = \frac{1}{n!} \sum_{\sigma \in S_n} d(\sigma)$$

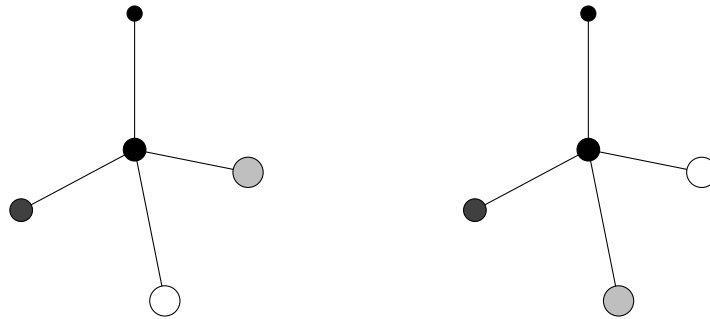
of the function  $d$  on  $S_n$  for  $n \leq 5$ . \*Can you prove a general formula for  $\delta_n$ ?

62. For  $\sigma \in S_n$ , define  $t(\sigma)$  as the *number* of cycles in the cycle type  $(k_1, k_2, \dots, k_t)$  of  $\sigma$ . Determine the average value

$$\tau_n = \frac{1}{n!} \sum_{\sigma \in S_n} 2^{t(\sigma)}$$

of the function  $2^t$  on  $S_n$  for  $n \leq 4$ . \*Can you prove a general formula for  $\tau_n$ ?

63. Show that the number of permutations in  $S_n$  without fixed points is equal to  $n! \cdot \sum_{k=0}^n \frac{(-1)^k}{k!}$ . Calculate what fraction of the elements this is for  $n \leq 6$ , and conclude that when randomly drawing names for Sinterklaas (Saint Nicholas' Eve) or Secret Santa<sup>9</sup> in a group that is not too small, the probability that no one draws themselves is approximately equal to  $1/e = 0.367879\dots$
64. Let  $e_1, e_2, e_3, \dots, e_n$  be a standard basis of  $\mathbf{R}^n$ . For  $\sigma \in S_n$ , define the linear map  $M_\sigma : \mathbf{R}^n \rightarrow \mathbf{R}^n$  by  $\sum_i a_i e_i \mapsto \sum_i a_i e_{\sigma(i)}$ . Prove that the sign  $\varepsilon(\sigma)$  of  $\sigma$  is equal to the determinant  $\det(M_\sigma)$ .  
[The matrix corresponding to  $M_\sigma$  is also called a *permutation matrix*.]
65. View the group  $S_4$  as the symmetry group of the tetrahedron  $ABCD$  as in §1. Prove that the subgroup  $A_4 \subset S_4$  is equal to the group of symmetries of  $ABCD$  generated by rotations, that is, the “physically realizable” symmetries. Conclude that the molecules below are *enantiomers*,<sup>10</sup> congruent molecules that cannot be transformed into each other through rotations.



- \*66. Prove that the 15 puzzle is solvable for half of all possible initial positions. How many are these? Show that the remaining positions can be transformed into one another through sliding.  
[We say that this puzzle has two *orbits* under sliding.]
- \*67. Define what we mean by a “position” of the Rubik’s cube, and calculate the number of possible positions. Can all these positions be transformed into one another through “legal rotations”? Can the set of positions be endowed with the structure of a group so that the set of “solvable positions” becomes a subgroup?

### 3 PLANE SYMMETRIES

If  $X$  is an arbitrary infinite set, then the permutation group  $S(X)$  is usually too large and too “structureless” to be interesting. However,  $X$  is often not just any infinite set but a set with “additional structure.” In this case, instead of studying the group of all bijections, we study a subgroup of bijections that behave well in some way for the structure of  $X$ .

#### ► PLANE GEOMETRY

In this section,  $X$  is the plane. This case played a central role in Greek mathematics, and from Euclid ( $\pm 325$ – $\pm 265$  BCE) until well into the 20th century, *plane geometry* was the staple of any introduction to mathematics. The plane is the two-dimensional case of what is nowadays called a *Euclidean space*, and much of what we treat in this section can be generalized to the  $n$ -dimensional Euclidean space for arbitrary  $n \geq 1$ . The three-dimensional case, which leads to *solid geometry* or *stereometry*, is applied in *crystallography*, among other things.

Group theory plays a fundamental role not only in Euclidean geometry, but also in the variants discovered only in the 19th century such as *hyperbolic* and *elliptic* geometry. With every “geometric space,” we associate the *transformation groups* of maps from the space to itself that preserve structural quantities such as distance or volume. This approach to geometry, presented in 1872 by the German Felix Klein (1849–1925) in his inaugural lecture in Erlangen, is sometimes referred to as the *Erlanger Programm*.<sup>11</sup> In the case of the plane, *angles* and *distances* are important structural quantities, so we will look at groups that leave these unchanged (“invariant”).

From the 17th century on, geometry has been increasingly described in terms of chosen *coordinates*, allowing us to verify geometric facts through algebraic manipulations. For the plane, such a choice leads to an identification with the set  $\mathbf{R}^2$  of ordered pairs of real numbers. We choose a *coordinate system* consisting of two lines intersecting perpendicularly in the plane, also called the  $x_1$ -axis and  $x_2$ -axis, and call their intersection point the *origin* of the plane. Once a unit of length is chosen, every point in the plane can be written as an ordered pair  $x = (x_1, x_2) \in \mathbf{R}^2$ . Such pairs can be added coordinatewise; the resulting summation in the plane is also called *vector addition*.

**Exercise 1.** Verify that vector addition gives rise to the structure of a group on  $\mathbf{R}^2$ .

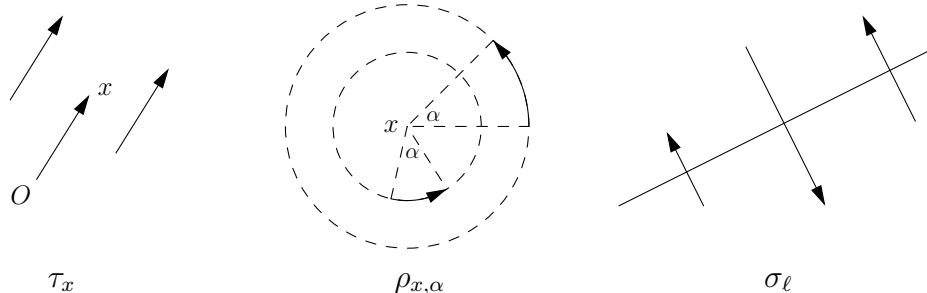
Besides vector addition, we have *scalar multiplication*, which allows us to multiply the points of  $\mathbf{R}^2$  by a real constant. This is summarized in linear algebra by saying that  $\mathbf{R}^2$  is a *vector space* over  $\mathbf{R}$ . Every point is a unique  $\mathbf{R}$ -linear combination of the points  $e_1 = (1, 0)$  and  $e_2 = (0, 1)$ , which together form the *standard basis* of  $\mathbf{R}^2$ . A point  $(x_1, x_2) \in \mathbf{R}^2$  is also denoted by the column vector  $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ .

Linear algebra shows how to express classic geometric concepts such as the distance between points and the angle between lines in  $\mathbf{R}^2$  in terms of the *inner product*  $\langle \cdot, \cdot \rangle : \mathbf{R}^2 \times \mathbf{R}^2 \rightarrow \mathbf{R}$  given by the formula  $\langle \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle = x_1 y_1 + x_2 y_2$ .

**Exercise 2.** Do the inner product and scalar multiplication give group operations on  $\mathbf{R}^2$ ?

► ISOMETRIES

Well-known examples of maps  $\mathbf{R}^2 \rightarrow \mathbf{R}^2$  from plane geometry are the *translation*  $\tau_x$  over a vector  $x \in \mathbf{R}^2$ , the *rotation*  $\rho_{x,\alpha}$  about a point  $x$  by an angle  $\alpha$ , and the *reflection*  $\sigma_\ell$  in a line  $\ell$ . We came across such maps in §1 when considering *symmetry groups* of plane figures such as the rhombus and the square.



The examples mentioned above are all bijections from the plane to itself, with inverses, respectively, the translation  $\tau_{-x}$ , the rotation  $\rho_{x,-\alpha}$ , and the reflection  $\sigma_\ell$ . Since they do not necessarily map the origin to itself, they are not, in general, linear. They are examples of what are called *plane symmetries*, *congruences*, or *isometries*. The definition is entirely in the spirit of the Erlanger Programm.

**3.1. Definition.** A *plane symmetry* or *isometry* is a map  $\varphi : \mathbf{R}^2 \rightarrow \mathbf{R}^2$  that preserves distances:

$$|\varphi(x) - \varphi(y)| = |x - y| \quad \text{for all points } x, y \in \mathbf{R}^2.$$

If we have  $\varphi(O) = O$  for an isometry  $\varphi$ , with  $O \in \mathbf{R}^2$  the origin, then  $\varphi$  is called an *orthogonal map*.

We denote the set of isometries of the plane by  $I_2(\mathbf{R})$  and the subset of orthogonal maps by  $O_2(\mathbf{R})$ . Note that in 3.1, we do not require explicitly that  $\varphi$  is a bijection. In 3.4, we will see that this is a *consequence* of the definition and that  $I_2(\mathbf{R})$  is in fact a subgroup of the permutation group  $S(\mathbf{R}^2)$ .

We first prove that every isometry is the product of a translation, a rotation about the origin, and possibly a reflection in the  $x_1$ -axis. The proof, strongly reminiscent of the proofs of 1.1 and 1.4, relies on a lemma from plane geometry.

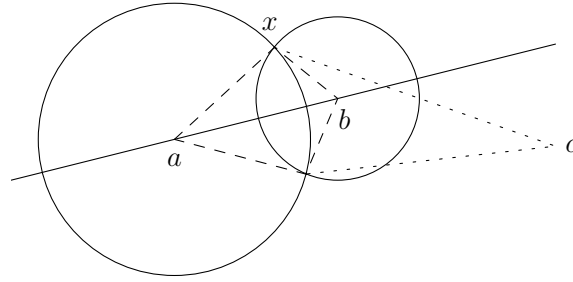
We call points in the plane *collinear* if there is a line in the plane on which they all lie. If we have  $\varphi(x) = x$  for  $x \in \mathbf{R}^2$  and  $\varphi : \mathbf{R}^2 \rightarrow \mathbf{R}^2$ , then we say that  $\varphi$  leaves the point  $x$  *invariant* or that  $x$  is a *fixed point* of  $\varphi$ .

**3.2. Lemma.** 1. An isometry that leaves two distinct points invariant is either the identity or the reflection in the line through these two points.

2. An isometry that leaves three non-collinear points invariant is the identity.

**Proof.** Suppose that  $\varphi$  leaves two distinct points  $a$  and  $b$  invariant. We first show that for any point  $x \in \mathbf{R}^2$ ,  $\varphi$  either leaves it invariant or reflects it in the line  $\ell$  through  $a$  and  $b$ . Since  $\varphi$  is an isometry, the distances from  $\varphi(x)$  to  $a$  and  $b$  must, respectively,

equal  $|x - a|$  and  $|x - b|$ . As shown in the figure below,  $x$  and its mirror image  $\sigma_\ell(x)$  in  $\ell$  are the only points that satisfy this. In particular,  $\varphi$  leaves all points on  $\ell$  invariant.



First, suppose that  $\varphi$  leaves a point  $c$  outside the line  $\ell$  invariant. If  $x$  is a point outside  $\ell$ , then  $x$  and  $\sigma_\ell(x)$  have different distances to  $c$ , so  $\varphi(x) = x$ . In this case,  $\varphi$  is the identity, and we obtain the second statement of the lemma. Now, suppose that  $\varphi$  does not leave any point outside  $\ell$  invariant. Then we have  $\varphi(x) = \sigma_\ell(x)$  for all points  $x$  outside  $\ell$ , and we obtain  $\varphi = \sigma_\ell$ .  $\square$

**3.3. Proposition.** 1. Every isometry can be written uniquely as a product  $\tau\psi$  of a translation  $\tau$  and an orthogonal map  $\psi$ .

2. An orthogonal map is either a rotation about the origin or the product of a rotation about the origin and a reflection in the  $x_1$ -axis.

**Proof.** We begin with the last statement. Let  $\psi$  be an orthogonal map and  $a$  a point on the  $x_1$ -axis different from the origin  $O$ . Then  $\psi(a)$  is a point on the circle with its center at the origin and radius  $|a|$ , so there exists a rotation  $\rho$  about  $O$  with  $\rho(a) = \psi(a)$ . The isometry  $\rho^{-1}\psi$  now leaves  $O$  and  $a$  invariant, so by 3.2.1, the map  $\rho^{-1}\psi$  is equal to either the identity or the reflection  $\sigma$  in the  $x_1$ -axis. In the first case,  $\psi = \rho$  is a rotation about the origin; in the second case, the relation  $\rho^{-1}\psi = \sigma$  gives the identity  $\psi = \rho\sigma$ , so that  $\psi$  is the product of a reflection in the  $x_1$ -axis and a rotation about the origin. In particular, this shows that orthogonal maps are bijections.

Now, let  $\varphi$  be an arbitrary isometry and  $\tau = \tau_{\varphi(O)}$  the translation over  $\varphi(O)$ . Then  $\psi = \tau^{-1}\varphi$  leaves the origin invariant, so  $\psi$  is an orthogonal map, and  $\varphi = \tau\psi$  is a product of the required kind.

Suppose that there exist translations  $\tau_1, \tau_2$  and orthogonal maps  $\psi_1, \psi_2$  with  $\tau_1\psi_1 = \tau_2\psi_2$ . Since translations and orthogonal maps are bijections, they have inverses, and by multiplying the previous identity successively on the left by  $\tau_2^{-1}$  and on the right by  $\psi_1^{-1}$ , we obtain  $\tau_2^{-1}\tau_1 = \psi_2\psi_1^{-1}$ . We have a translation on the left and an orthogonal map on the right. Since the identity is the only translation that is orthogonal, we find that  $\tau_2^{-1}\tau_1 = \text{id} = \psi_2\psi_1^{-1}$ , and so  $\tau_1 = \tau_2$  and  $\psi_1 = \psi_2$ . Thus, the product representation  $\varphi = \tau\psi$  found above is unique.  $\square$

**Exercise 3.** Show that every isometry can be written uniquely as a product  $\varphi = \psi\tau$  with  $\psi$  an orthogonal map and  $\tau$  a translation. Does this give the same  $\tau$  and  $\psi$  as in 3.3.1?

The product representation  $\varphi = \tau\psi$  will prove to be useful in various situations.

**3.4. Corollary.** The set  $I_2(\mathbf{R})$  of plane symmetries forms a group under composition, and  $O_2(\mathbf{R})$  is the subgroup of linear maps in  $I_2(\mathbf{R})$ .

**Proof.** It follows from 3.3 that every plane symmetry is a composition of bijections  $\mathbf{R}^2 \rightarrow \mathbf{R}^2$  and therefore itself a bijection. Under the inclusion  $I_2(\mathbf{R}) \subset S(\mathbf{R}^2)$ ,  $I_2(\mathbf{R})$  becomes a subgroup of  $S(\mathbf{R}^2)$  in the sense of 2.7: the identity is an isometry, the composition of two isometries is also an isometry, and if a bijection preserves distances, then so does its inverse. Similarly, we can see that the subset  $O_2(\mathbf{R}) \subset I_2(\mathbf{R})$  of isometries that preserve the origin is a subgroup of  $I_2(\mathbf{R})$ . By 3.3.2, every orthogonal map is a product of linear maps and therefore linear. Conversely, a linear map in  $I_2(\mathbf{R})$  leaves the origin invariant and is therefore orthogonal.  $\square$

**3.5. Corollary.** For an isometry  $\varphi$  and points  $x_1, x_2, \dots, x_n \in \mathbf{R}^2$ , we have

$$\varphi\left(\frac{x_1 + x_2 + \dots + x_n}{n}\right) = \frac{\varphi(x_1) + \varphi(x_2) + \dots + \varphi(x_n)}{n}.$$

**Proof.** It is admittedly intuitively clear that isometries “preserve averages” in the sense of this corollary, but this is not an immediate consequence of Definition 3.1. However, we can observe that the desired identity is correct for a linear map and also for a translation. If we apply these special cases successively, we see that the identity holds for every composition  $\varphi = \tau\psi$  in 3.3.1.  $\square$

### ► THE ORTHOGONAL GROUP

The *orthogonal group*  $O_2(\mathbf{R})$  of linear plane isometries consists of two types of elements. As matrices, the rotations about  $O$  in  $O_2(\mathbf{R})$  are of the form

$$\rho_\alpha = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix},$$

where  $\alpha$  is the rotation angle. The remaining elements of  $O_2(\mathbf{R})$  follow from this by multiplication by the reflection  $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ . This gives matrices of the form

$$\rho_\alpha\sigma = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}.$$

The map  $\rho_\alpha\sigma$  sends the line  $\ell$  at an angle  $\alpha/2$  to the positive  $x_1$ -axis to itself; it is the reflection in  $\ell$ .

**Exercise 4.** Verify this using a sketch.

For every rotation  $\rho \in O_2(\mathbf{R})$ , the reflection  $\rho\sigma$  is of order 2 and therefore equal to its inverse:  $(\rho\sigma)^{-1} = \rho\sigma$ . Since we also have  $(\rho\sigma)^{-1} = \sigma^{-1}\rho^{-1} = \sigma\rho^{-1}$ , we find that

$$(3.6) \quad \rho\sigma = \sigma\rho^{-1},$$

an extremely useful rule that we already came across in §1 (for Exercise 6), using Latin letters instead of Greek ones. It shows that the reflection  $\sigma$  does not commute with all rotations. Together, the relation  $\rho_\alpha\sigma = \sigma\rho_{-\alpha}$  in (3.6) and the “commutativity relation”  $\rho_\alpha\rho_\beta = \rho_\beta\rho_\alpha$  suffice to do arithmetic in  $O_2(\mathbf{R})$  without ever using matrices.

**Exercise 5.** Deduce (3.6) using a sketch or an explicit matrix multiplication. Does the same identity hold if we replace  $\sigma$  with an arbitrary reflection in  $O_2(\mathbf{R})$ ?

As for the permutation group  $S_n$ , we have a *sign map*  $O_2(\mathbf{R}) \rightarrow \{\pm 1\}$  for the orthogonal group  $O_2(\mathbf{R})$ ; this sign map sends each map in  $O_2(\mathbf{R})$  to the *determinant* of the corresponding matrix. The orthogonal maps of determinant 1 are the rotations; those of determinant  $-1$  are the reflections. They are called, respectively, *orientation-preserving* and *orientation-reversing* maps.

**Exercise 6.** Try to explain these names. What is the connection to Exercise 2.64?<sup>12</sup>

As in the case of the alternating group  $A_n \subset S_n$ , it follows from the multiplicativity of the determinant that the orientation-preserving orthogonal maps form a subgroup  $O_2^+(\mathbf{R}) \subset O_2(\mathbf{R})$ . This subgroup consists of the rotations about  $O$ .

### ► PLANE SYMMETRY GROUPS

The orthogonal group, which already appears implicitly in Exercise 1.22, is the *symmetry group* of the unit circle in the plane. If we define, very generically, a *plane figure* as a subset  $F \subset \mathbf{R}^2$ , then we have the following definition of the symmetry group of  $F$ .

**3.7. Definition.** Let  $F \subset \mathbf{R}^2$  be a plane figure. The subgroup

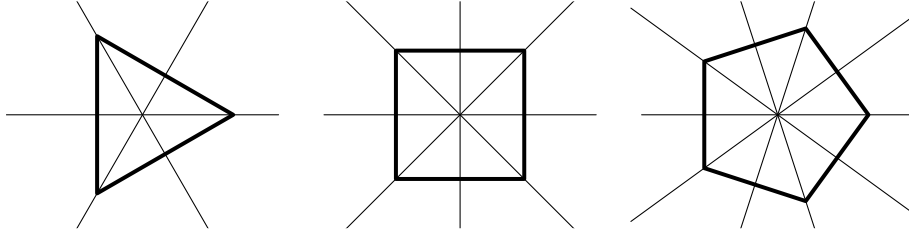
$$\text{Sym}(F) = \{\varphi \in I_2(\mathbf{R}) : \varphi[F] = F\}$$

is called the *symmetry group of the figure  $F$* .

Note that the set  $\text{Sym}(F)$  in 3.7 is indeed a subgroup of  $I_2(\mathbf{R})$  and therefore itself also a group. In §1, we already encountered the special cases where  $F$  is a rhombus or a square with the origin as its center. For  $F = \{O\}$ , the group  $\text{Sym}(F)$  is the orthogonal group  $O_2(\mathbf{R})$ .

**Exercise 7.** If in 3.7, we require only an inclusion  $\varphi[F] \subset F$  instead of equality, do we still get a group?

In §1, we studied the symmetry group  $D_4$  of the square. More generally, for arbitrary  $n \geq 2$ , we have the symmetry group  $D_n$  of the regular  $n$ -gon. Since for every symmetry of a regular  $n$ -gon, the center is a fixed point by 3.5, we obtain an inclusion  $D_n \subset O_2(\mathbf{R})$  by taking  $O$  as the center. The rotations in  $D_n$  are now the  $n$  rotations about  $O$  by the angles  $2k\pi/n$  for integer  $k$ . They form a cyclic subgroup  $C_n \subset O_2(\mathbf{R})$  of order  $n$  that is generated by the rotation  $\rho = \rho_{2\pi/n}$  by the angle  $2\pi/n$ . As in 1.4, we deduce  $D_n$  from  $C_n$  by adding the compositions with a reflection in the line through  $O$  and a vertex. This gives the  $n$  reflections in the lines through  $O$  and a vertex and in the lines through  $O$  and the midpoint of an edge. We sometimes call  $D_n$  the *dihedral group* of order  $2n$ .



If we choose a vertex on the  $x_1$ -axis and let  $\sigma$  be the reflection in the  $x_1$ -axis, we find

$$\begin{aligned} D_n &= \langle \rho, \sigma \rangle = C_n \cup \sigma C_n \\ &= \{\rho^k : k = 0, 1, 2, \dots, n-1\} \cup \{\sigma \rho^k : k = 0, 1, 2, \dots, n-1\}. \end{aligned}$$

Using relation (3.6), we can now do arithmetic in  $D_n$  in terms of  $\rho$  and  $\sigma$ .

For  $n = 1$ , the group  $D_n$  is by definition equal to the group  $D_1 = \langle \sigma \rangle$  of order 2 generated by  $\sigma$ . Its subgroup of rotations is the trivial group  $C_1$ .

**Exercise 8.** Show that  $D_1$  and  $D_2$  are the only abelian dihedral groups.

The groups  $C_n$  and  $D_n$  are the only examples of finite symmetry groups.

**3.8. Theorem.** Every finite subgroup of  $I_2(\mathbf{R})$  is equal to  $C_n$  or  $D_n$  for a suitable choice of coordinates.

**Proof.** Let  $G \subset I_2(\mathbf{R})$  be finite. We first show that there is a point in the plane that is invariant under all  $\varphi \in G$ . Take an arbitrary point  $x \in \mathbf{R}^2$ , and look at the *orbit* of  $x$  under  $G$ , that is, the set of images of  $x$  under the symmetries in  $G$ . Since  $G$  is finite, this orbit is also finite, say equal to  $\{x_1, x_2, \dots, x_n\}$ . The orbit of  $x$  is mapped to itself by the elements of  $G$ , and by the bijectivity of symmetries, these maps are permutations. By 3.5, the “average” of the points in the orbit of  $x$  is now a fixed point:

$$\varphi \left( \frac{x_1 + x_2 + \dots + x_n}{n} \right) = \frac{\varphi(x_1) + \varphi(x_2) + \dots + \varphi(x_n)}{n} = \frac{x_1 + x_2 + \dots + x_n}{n}.$$

If we take this point as the origin, then  $G$  becomes a finite subgroup of the orthogonal group  $O_2(\mathbf{R})$ .

We first determine the subgroup  $G^+ = G \cap O_2^+(\mathbf{R})$  of rotations in  $G$ . Since  $G^+$  is finite, there is a *minimal* value  $\alpha \in (0, 2\pi]$  for which  $\rho = \rho_\alpha$  is contained in  $G$ . Let  $n$  be the least positive number such that we have  $n\alpha \geq 2\pi$ . Then  $\rho^n \in G^+$  is a rotation by  $n\alpha \in [2\pi, 2\pi + \alpha)$ , and by the minimality of  $\alpha$ , we have  $n\alpha = 2\pi$ , so  $\rho_\alpha = \rho_{2\pi/n}$ . After multiplication by a suitable power of  $\rho_{2\pi/n}$ , every other rotation in  $G^+$  is of the form  $\rho_\beta$  with  $0 \leq \beta < 2\pi/n$ , and it then follows from the minimality of  $\alpha = 2\pi/n$  that  $\beta = 0$  and  $\rho_\beta = \text{id}$ . We conclude that  $G^+$  consists of the powers of  $\rho_{2\pi/n}$  and is therefore equal to  $C_n$ .

If  $G$  also contains a reflection, then by taking the reflection axis as the  $x_1$ -axis, we obtain  $\sigma \in G$ . For every other reflection  $\tilde{\sigma} \in G$ , the product  $\sigma\tilde{\sigma} = \rho$  is a rotation in  $G$ , so the reflections in  $G$  are the elements  $\sigma\rho$  with  $\rho$  in the subgroup  $G^+$  of rotations in  $G$ . We have already seen that  $G^+$  is equal to  $C_n = \langle \rho_{2\pi/n} \rangle$  for some  $n$ , so in this case, we get  $G = D_n$ .  $\square$

The technique used in the proof of 3.8 to show that the group  $G^+$  of rotations is cyclic occurs in many forms. A variant for integers can be found in 6.2.

**Exercise 9.** Show that the set  $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$  of non-zero complex numbers forms a group under multiplication and that every *finite* subgroup  $H \subset \mathbf{C}^*$  is cyclic.

There is an analog of 3.8 for symmetries of the three-dimensional space. Somewhat surprisingly, it turns out that in dimension three, there are not that many more possibilities than in dimension two.<sup>13</sup>

### ► SIGN OF AN ISOMETRY

We attach a sign to an arbitrary isometry using the decomposition  $\varphi = \tau\psi$  from 3.3.1. We refer to the orthogonal map  $\psi$  in such a decomposition as the *linear component*  $\psi = L(\varphi)$  of the isometry  $\varphi$ .

**3.9. Proposition.** *The map  $L : I_2(\mathbf{R}) \rightarrow O_2(\mathbf{R})$  that sends an isometry to its linear component is multiplicative; that is, we have*

$$L(\varphi_1\varphi_2) = L(\varphi_1)L(\varphi_2) \quad \text{for } \varphi_1, \varphi_2 \in I_2(\mathbf{R}).$$

**Proof.** Write  $\varphi_1 = \tau_1\psi_1$  and  $\varphi_2 = \tau_2\psi_2$  for the decompositions of  $\varphi_1$  and  $\varphi_2$ . Since translations and orthogonal maps do not, in general, commute, we must put in some effort to find the decomposition of  $\varphi_1\varphi_2 = \tau_1\psi_1\tau_2\psi_2$ .

If  $\tau_a$  is the translation over  $a$  and  $\psi$  is an arbitrary linear map, we have

$$(\psi\tau_a)(x) = \psi(x+a) = \psi(x) + \psi(a) = (\tau_{\psi(a)}\psi)(x)$$

for every point  $x \in \mathbf{R}^2$ . The resulting relation

$$(3.10) \quad \psi\tau_a = \tau_{\psi(a)}\psi$$

shows that we have  $\psi_1\tau_2 = \tau'_2\psi_1$  for some translation  $\tau'_2$  and that the desired decomposition is given by  $\varphi_1\varphi_2 = (\tau_1\tau'_2)(\psi_1\psi_2)$ . In particular, we have  $L(\varphi_1\varphi_2) = \psi_1\psi_2 = L(\varphi_1)L(\varphi_2)$ .  $\square$

We define the *sign map*  $I_2(\mathbf{R}) \rightarrow \{\pm 1\}$  by  $\varphi \mapsto \det L(\varphi)$ . It follows from 3.9 that this map, as the composition of two multiplicative maps, is itself also multiplicative:

$$\det L(\phi_1\phi_2) = \det(L(\phi_1)L(\phi_2)) = \det L(\phi_1) \cdot \det L(\phi_2).$$

As for the orthogonal group, we find that  $I_2(\mathbf{R})$  contains a subgroup  $I_2^+(\mathbf{R})$  of orientation-preserving isometries, consisting of the isometries with sign 1.

### ► GEOMETRY WITH COMPLEX NUMBERS

We can give a description of  $I_2(\mathbf{R})$  in terms of complex numbers that, at first glance, looks somewhat different from 3.3 but is, in fact, equivalent to it when we identify the plane  $\mathbf{R}^2$  with the complex numbers  $\mathbf{C}$  in the usual way. The elements of the standard basis become 1 and  $i$ , and the isometries take on the following form.

**3.11. Theorem.** *The orientation-preserving isometries of the complex plane  $\mathbf{C}$  are the maps*

$$\varphi_{a,b}^+ : z \mapsto az + b \quad \text{with } a, b \in \mathbf{C} \text{ and } |a| = 1,$$

*and the orientation-reversing isometries are the maps*

$$\varphi_{a,b}^- : z \mapsto a\bar{z} + b \quad \text{with } a, b \in \mathbf{C} \text{ and } |a| = 1.$$

Here,  $\bar{z}$  denotes the complex conjugate of  $z \in \mathbf{C}$ .

**Proof.** Under the identification of  $\mathbf{R}^2$  with  $\mathbf{C}$ , the reflection in the  $x_1$ -axis corresponds to complex conjugation, the rotation about  $O$  by an angle  $\alpha$  with multiplication by the complex number  $a = e^{i\alpha}$  of absolute value 1, and the translation over a point  $b$  with the addition  $z \mapsto z + b$ . If we write the decompositions in 3.3 in terms of complex numbers, we find exactly the maps mentioned in the theorem. The map  $z \mapsto az + b$  is a composition of a rotation and a translation and therefore has sign 1. Preceding it by the reflection  $z \mapsto \bar{z}$  with sign  $-1$ , we obtain the map  $z \mapsto a\bar{z} + b$ , which thus has sign  $-1$ .  $\square$

The identification of  $\mathbf{R}^2$  with  $\mathbf{C}$ , which unlike most other arguments in this section has no analog in higher dimensions, can sometimes be used efficiently in plane geometry. As an application, we prove that the “type” of an isometry is determined as below by its sign and whether it has a fixed point.

	With fixed point	Without fixed point
det = +1	rotation	true translation
det = -1	reflection	true glide reflection

In the column “without fixed point,” the term “true translation” means a translation over a non-zero vector. Likewise, a true *glide reflection* is a reflection followed by a true translation parallel to the reflection axis.

Isometries with a fixed point are orthogonal if we take the fixed point as the origin. We have already seen that these are rotations and reflections and that we can distinguish between them using their signs. This gives the first column of the table.

An isometry with sign  $+1$  without fixed point corresponds to a map  $\phi_{a,b}^+ : z \mapsto az + b$  in 3.11 for which the equation  $z = az + b$  has no solution. For  $a \neq 1$ , there is the solution  $z = b/(1 - a) \in \mathbf{C}$ , so we have  $a = 1$ , and  $\phi_{a,b}^+ : z \mapsto z + b$  is a translation. For  $b \neq 0$ , this has no fixed point.

To see when the map  $\varphi_{a,b}^- : z \mapsto a\bar{z} + b$  with sign  $-1$  in 3.11 has a fixed point, we write  $a = w^2$  and note that  $\varphi_{a,b}^-$  is a reflection in the line  $w\mathbf{R}$  followed by a translation over  $b$ . Since  $|a| = |w| = 1$ , we have  $\bar{w} = w^{-1}$  and can rewrite the equation  $z = a\bar{z} + b$  as

$$2i \cdot \Im(z/w) = \bar{w}z - w\bar{z} = b/w.$$

This equation has a solution if and only if  $b/w$  is purely imaginary, which means that  $b$  is perpendicular to the reflection axis  $w\mathbf{R}$ . For such  $b$ , the map  $\varphi_{a,b}^-$  is the reflection in the line  $b/2 + w\mathbf{R}$ . More generally, we can write  $b = b_1 + b_2$  with  $b_1$  perpendicular to  $w\mathbf{R}$  and  $b_2 \in w\mathbf{R}$ . If there is no fixed point, then we have  $b_2 \neq 0$ , and  $\varphi_{a,b}^-$  is a reflection in the line  $b_1/2 + w\mathbf{R}$  followed by a translation parallel to that line. This proves that our table is correct.  $\square$

**Exercise 10.** Use a sketch to check the last argument.

### ► PLANE TRANSFORMATION GROUPS

To conclude this section, we note that other groups than  $I_2(\mathbf{R})$  can also be associated with the plane. In linear algebra, we often consider the set  $\text{GL}_2(\mathbf{R})$  of bijections of the plane that are *linear*. We can identify this set with the group of *invertible*  $2 \times 2$  matrices with real coefficients. The notation “GL” is an abbreviation of “general linear.” By 3.4, we have

$$\text{GL}_2(\mathbf{R}) \cap I_2(\mathbf{R}) = O_2(\mathbf{R}).$$

If we do not require as in 3.1 that all distances are preserved but instead require that the *ratios* between distances are, we obtain the group  $\text{Sim}_2(\mathbf{R})$  of plane *similarity transformations* or *similarities*. The similarities are the maps that transform straight lines into straight lines and preserve the angles between them.

Finally, if we allow not only compositions of translations and orthogonal maps as in 3.3.1, but also compositions of translations and arbitrary elements of  $\text{GL}_2(\mathbf{R})$ , we obtain (Exercise 32) the group  $\text{Aff}_2(\mathbf{R})$  of plane *affine* maps. These are the maps that transform straight lines into straight lines. There are (Exercise 32) natural inclusions

$$I_2(\mathbf{R}) \subset \text{Sim}_2(\mathbf{R}) \subset \text{Aff}_2(\mathbf{R}),$$

and every one of these groups consists of bijections of the plane that “leave something invariant” in the spirit of the Erlanger Programm. For further details, we refer to the exercises.

### EXERCISES.

11. Show that the set  $\text{GL}_2(\mathbf{R})$  of invertible linear maps  $\mathbf{R}^2 \rightarrow \mathbf{R}^2$  forms a group and that it consists of the  $2 \times 2$  matrices with non-zero determinant. Is  $O_2(\mathbf{R})$  a subgroup of  $\text{GL}_2(\mathbf{R})$ ?
12. Does the set  $\text{Mat}_2(\mathbf{R})$  of *all* real  $2 \times 2$  matrices form a group under multiplication? Is there a natural *addition* on  $\text{Mat}_2(\mathbf{R})$  that gives it the structure of a group?
13. Let  $\varphi : \mathbf{R}^2 \rightarrow \mathbf{R}^2$  be a linear map. Prove that the following are equivalent:
  1. The map  $\varphi$  is an isometry.
  2. For all  $x \in \mathbf{R}^2$ , we have  $|\varphi(x)| = |x|$ .
  3. For all  $x, y \in \mathbf{R}^2$ , the inner product satisfies  $\langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle$ .
14. Show that an isometry leaves angles between lines invariant.
15. Prove that an element of  $I_2(\mathbf{R})$  conjugate to a translation is itself a translation.

16. Write the elements of the group  $D_6 \subset O_2(\mathbf{R})$  explicitly in matrix form.
17. Show that  $D_2$  is “the same” group as the *Klein four-group* from §1.
18. Determine the symmetry groups of each of the letters in a simple block letter Roman alphabet. Which group is most common? For each symmetry group you find, can you make a *word* that has this symmetry group (as a word!)?
19. Let  $F$  be a “word in the plane” in the sense of the previous exercise, and assume that  $\text{Sym}(F)$  is the trivial group. Let  $G \subset I_2(\mathbf{R})$  be an arbitrary finite subgroup. Prove that  $F$  can be extended to a figure  $\overline{F} \supset F$  with symmetry group  $\text{Sym}(\overline{F}) = G$ .
20. Show that every symmetry of a plane figure  $F$  gives rise to a bijection  $F \rightarrow F$ , and let  $f : \text{Sym}(F) \rightarrow S(F)$  be the corresponding map. Prove that  $f$  is injective if and only if  $F$  is not contained in a line in  $\mathbf{R}^2$ . Conclude that for “true” plane figures,  $\text{Sym}(F)$  can be viewed as a subgroup of  $S(F)$ .
21. Define  $F = \{(k, 0) : k \in \mathbf{Z}\}$ . Determine  $\text{Sym}(F)$ , and the elements of  $\text{Sym}(F)$  that are mapped to the identity by the map  $f : \text{Sym}(F) \rightarrow S(F)$  from the previous exercise.
22. Let  $F$  be a plane figure with symmetry group  $S$  and  $\alpha \in I_2(\mathbf{R})$  an isometry. Prove that the symmetry group of the figure  $\alpha F = \{\alpha(x) : x \in F\}$  is equal to the conjugate subgroup  $\alpha S \alpha^{-1} = \{\alpha \sigma \alpha^{-1} : \sigma \in S\}$  of  $S$ .
23. Prove that the “structure” of the symmetry group of a figure does not depend on the choice of coordinates. [First, formulate *exactly* what this should mean.]
24. Use a sketch to show that the composition of a rotation about  $O$  by an angle  $\alpha \neq 0$  and a translation is again a rotation by  $\alpha$ , and determine the new center of rotation.
25. Prove the following theorems from plane geometry. There is always a “direct geometric” proof and a very short proof using 3.11.
  1. The composition of the reflections in two parallel lines is a translation.
  2. The square of a glide reflection is a translation.
  3. The composition of the reflections in two intersecting lines is a rotation.
  4. The composition of two rotations by angles  $\alpha$  and  $-\alpha$  is a translation.
  5. The composition of two rotations by angles  $\alpha$  and  $\beta \neq -\alpha$  is a rotation by  $\alpha + \beta$ .
26. For the items in the previous exercise, determine the translation vectors (in 1, 2, and 4), the rotation angle (in 3), and the center of rotation (in 5).
- \*27. Let  $F \subset \mathbf{R}^2$  be a non-empty subset of  $\mathbf{R}^2$  that is *bounded*. Prove that for a suitable choice of coordinates,  $\text{Sym}(F)$  is a subgroup of  $O_2(\mathbf{R})$ .
28. Let  $G \subset I_2(\mathbf{R})$  be a group of plane symmetries. Show that the set  $G_T = \{\phi \in G : L(\phi) = \text{id}\}$  of elements in  $G$  with trivial linear component is a subgroup of  $G$ , and that it consists of the translations in  $G$ ; it is called the *translation subgroup* of  $G$ . Also show that the *point group*  $\overline{G} = \{L(\phi) : \phi \in G\}$  of  $G$  is a subgroup of  $O_2(\mathbf{R})$ .
- \*29. A group  $G \subset I_2(\mathbf{R})$  of plane symmetries is called a *plane crystallographic group* if its translation subgroup is generated by two independent translations, that is, translations  $\tau_x$  and  $\tau_y$  such that  $x$  and  $y$  form a basis of  $\mathbf{R}^2$ . Prove that for a suitable choice of coordinates, the point group of a plane crystallographic group is equal to  $C_n$  or  $D_n$  with  $n \in \{1, 2, 3, 4, 6\}$ .

30. A *similarity* is a non-constant map  $\phi : \mathbf{R}^2 \rightarrow \mathbf{R}^2$  that leaves distance ratios invariant: for any four points  $a, b, c, d \in \mathbf{R}^2$  with  $a \neq b$  and  $c \neq d$ , we have

$$\frac{|\phi(a) - \phi(b)|}{|a - b|} = \frac{|\phi(c) - \phi(d)|}{|c - d|}.$$

Prove that a similarity multiplies all distances by the same positive factor and that the set  $\text{Sim}_2(\mathbf{R})$  of similarities is a subgroup of  $S(\mathbf{R}^2)$  that contains  $I_2(\mathbf{R})$ .

31. Show that the analog of 3.11 for similarities is obtained by replacing the condition  $|a| = 1$  by  $a \neq 0$ .
32. A *plane affine map* is a map  $\mathbf{R}^2 \rightarrow \mathbf{R}^2$  that can be obtained by composing an invertible linear map with a translation. Prove that the set  $\text{Aff}_2(\mathbf{R})$  of affine maps is a subgroup of  $S(\mathbf{R}^2)$  that contains  $\text{Sim}_2(\mathbf{R})$ .
33. Show that the determinant map on  $\text{GL}_2(\mathbf{R})$  has a canonical extension to a multiplicative function on  $\text{Aff}_2(\mathbf{R})$ .
34. Define the groups  $I_1(\mathbf{R})$ ,  $\text{Sim}_1(\mathbf{R})$ , and  $\text{Aff}_1(\mathbf{R})$  of *linear* isometries, similarities, and affine maps  $\mathbf{R} \rightarrow \mathbf{R}$ . Then prove the analogs of 3.3, 3.4, 3.9, and 3.11, and conclude that the affine group  $\text{Aff}_1(\mathbf{R})$  over  $\mathbf{R}$  coincides with  $\text{Sim}_1(\mathbf{R})$  and consists of the linear map  $x \mapsto ax + b$  with  $a, b \in \mathbf{R}$ ,  $a \neq 0$ .
35. Define a multiplication on the product set  $\mathbf{C} \times \mathbf{C}^*$  by

$$(b_1, a_1) \cdot (b_2, a_2) = (b_1 + a_1 b_2, a_1 a_2).$$

Prove that under this multiplication,  $\mathbf{C} \times \mathbf{C}^*$  forms a group; it is called the *affine group* over  $\mathbf{C}$ . Is this group abelian?

## 4 HOMOMORPHISMS

It is a general observation in mathematics that for every interesting category of objects, there is an “associated” type of *maps* between them. These maps, which, as a rule, in some way respect the structure of the objects in question, are called the *homomorphisms*, or *morphisms* for short, in the category.<sup>14</sup> For example, the morphisms in linear algebra are the *linear* maps, and those in topology are the *continuous* maps.

### ► HOMOMORPHISMS, ISOMORPHISMS, AUTOMORPHISMS

For groups, where the structure on the underlying set is given by a group operation, it makes sense to look at maps that respect that operation.

**4.1. Definition.** A homomorphism from a group  $G$  to a group  $G'$  is a map  $f : G \rightarrow G'$  such that for any two elements  $x, y \in G$ , the identity

$$f(xy) = f(x)f(y)$$

holds. A bijective homomorphism is called an *isomorphism*.

The set  $\text{Hom}(G, G')$  of homomorphisms from  $G$  to  $G'$  always contains the *trivial homomorphism*, which sends all elements of  $G$  to the unit element  $e' \in G'$ . Sometimes, this is the only homomorphism from  $G$  to  $G'$ .

If  $f : G \rightarrow G'$  is an isomorphism, we write  $f : G \xrightarrow{\sim} G'$  and say that the groups  $G$  and  $G'$  are *isomorphic*. Notation:  $G \cong G'$ . In this case,  $G$  and  $G'$  have “the same group structure.”

We have already seen several examples of isomorphisms. In §1, we observed that the symmetry group  $V_4$  of the rhombus is isomorphic to the multiplicative group  $\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$  of odd residue classes modulo 8. In this case, every bijection that sends the unit element  $\text{id} \in V_4$  to  $\bar{1}$  is an isomorphism.

The subgroup  $D_1 = \langle \sigma \rangle \subset O_2(\mathbf{R})$  of order 2 generated by the reflection  $\sigma$  in the  $x_1$ -axis is isomorphic to the *sign group*  $\{\pm 1\}$ . The determinant map gives an isomorphism  $\det : D_1 \xrightarrow{\sim} \{\pm 1\}$ . The subgroup  $C_2 \subset O_2(\mathbf{R})$  generated by the half turn is also isomorphic to  $\{\pm 1\}$ . However, the determinant map  $\det : C_2 \rightarrow \{\pm 1\}$  is the trivial homomorphism and therefore not an isomorphism.

**Exercise 1.** Prove that all groups of order 2 are isomorphic. Are all groups of order 3 also isomorphic?

Examples of homomorphisms from the previous sections are the sign map  $\varepsilon : S_n \rightarrow \{\pm 1\}$  in 2.9, the linear component map  $L : I_2(\mathbf{R}) \rightarrow O_2(\mathbf{R})$  in 3.9, and the determinant map  $\det : O_2(\mathbf{R}) \rightarrow \{\pm 1\}$ . The composition  $\det \circ L : I_2(\mathbf{R}) \rightarrow \{\pm 1\}$  also gives a homomorphism, the sign map for isometries. More generally, it is easy to check that the composition of a homomorphism  $G \rightarrow G'$  and a homomorphism  $G' \rightarrow G''$  gives a homomorphism  $G \rightarrow G''$ .

The homomorphisms  $G \rightarrow G$  from a group  $G$  to itself are called *endomorphisms*. The group  $\text{Hom}(G, G)$  is also denoted by  $\text{End}(G)$ . For *abelian* groups  $G$ , the map  $x \mapsto x^n$  is an endomorphism of  $G$  for every integer  $n$ . For non-abelian groups  $G$ , we

obtain interesting examples of endomorphisms by considering the *conjugation maps*  $\sigma_g : x \mapsto gxg^{-1}$  for  $g \in G$ . For  $\sigma_g$ , the *homomorphism property* stated in 4.1 follows from the identity

$$\sigma_g(xy) = gxyg^{-1} = gxg^{-1} \cdot gyg^{-1} = \sigma_g(x)\sigma_g(y).$$

Bijective endomorphisms  $G \rightarrow G$  are called *automorphisms* of  $G$ . The conjugation map  $\sigma_g$ , whose inverse is the conjugation map  $\sigma_{g^{-1}}$ , is an example of one. The automorphisms of  $G$  are the isomorphisms from  $G$  to itself; we can see them as abstract “symmetries” of the group  $G$ . Given this analogy, it should come as no surprise that the set  $\text{Aut}(G)$  of automorphisms of  $G$  forms a *group* under composition, the *automorphism group* of  $G$ . A useful exercise for the reader who is still hesitant about so much abstraction is to check that  $\text{Aut}(G)$  indeed satisfies all group axioms.

**Exercise 2.** Let  $G$  be a group for which  $\text{End}(G)$  is a group under composition. Prove:  $G = 1$ .

### ► ADDITIVE NOTATION

In the homomorphism property in 4.1, the multiplication  $xy$  takes place in  $G$  and the multiplication  $f(x)f(y)$  in  $G'$ . If the group operations in  $G$  and  $G'$  are not denoted the same way, the identity looks less “symmetric.”

The only other common way to denote a group operation is the *additive notation*. This notation is only used for abelian groups. In the additive notation, we write a *sum*  $x + y$  instead of a product  $xy$ , and the inverse  $x^{-1}$  of  $x$  is  $-x$ , also called the *opposite* of  $x$ . More generally, the notation for  $x^n$  with  $n \in \mathbf{Z}$  is  $nx$ . Instead of a unit element, additively, we prefer to speak of the *zero element* of the group and write it as 0.

As already noted, the choice of the symbol used to indicate the group operation is basically irrelevant, and we can denote abelian groups both additively and multiplicatively. However, many abelian groups have had a standard notation for their group operation since Euler (1707–1783). The best-known examples are the additive groups  $\mathbf{Z}$ ,  $\mathbf{Q}$ ,  $\mathbf{R}$ , and  $\mathbf{C}$  of, respectively, integer, rational, real, and complex numbers. No one will ever imagine using a symbol other than  $+$  for the addition in these additive groups, if only because a product operation is also defined on these sets. If we omit the zero element from the sets  $\mathbf{Q}$ ,  $\mathbf{R}$ , and  $\mathbf{C}$ , the “usual” multiplication gives the structure of a group. The corresponding groups  $\mathbf{Q}^*$ ,  $\mathbf{R}^*$ , and  $\mathbf{C}^*$  are the *multiplicative groups* of, respectively, rational, real, and complex numbers.

**Exercise 3.** Are there subsets  $\mathbf{Z}^* \subset \mathbf{Z} \setminus \{0\}$  on which multiplication induces the structure of a group? Is there a *largest* one?

Well-known examples of homomorphisms in analysis are the *exponential map*  $\exp : \mathbf{R} \rightarrow \mathbf{R}^*$  given by  $x \mapsto e^x$  and the *logarithm*  $\log : \mathbf{R}_{>0} \rightarrow \mathbf{R}$  given by  $x \mapsto \log x$ . The homomorphism property is then written as  $e^{x+y} = e^x e^y$  and  $\log(xy) = \log x + \log y$ .

### ► KERNEL AND IMAGE

Since a homomorphism respects the group operation, it must send a unit element to a unit element and preserve inverses.

**4.2. Lemma.** For a homomorphism  $f : G \rightarrow G'$ , we have

1.  $f(e) = e'$ , with  $e \in G$  and  $e' \in G'$  the unit elements;
2.  $f(x^{-1}) = f(x)^{-1}$  for all  $x \in G$ .

**Proof.** Using the equivalence (2.3), it easily follows from the identity  $f(e) = f(ee) = f(e)f(e)$  that  $f(e) = e'$ . For  $x \in G$ , we then have  $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$ , and so  $f(x^{-1}) = f(x)^{-1}$ .  $\square$

In the previous sections, we constructed subgroups  $A_n$  and  $I_2^+(\mathbf{R})$  using the sign maps  $S_n \rightarrow \{\pm 1\}$  and  $I_2(\mathbf{R}) \rightarrow \{\pm 1\}$ . This construction turns out to be very general: every homomorphism  $f : G \rightarrow G'$  leads to subgroups  $\ker(f) \subset G$  and  $f[G] \subset G'$  called the *kernel* and the *image* of  $f$ .

**4.3. Theorem.** For a homomorphism  $f : G \rightarrow G'$ ,

1. the kernel  $\ker(f) = \{x \in G : f(x) = e'\}$  of  $f$  is a subgroup of  $G$ ;
2. the image  $f[G] = \{f(x) : x \in G\}$  of  $f$  is a subgroup of  $G'$ .

**Proof.** Let us check properties (H1)–(H3) from 2.7 for  $\ker(f)$ . The kernel  $\ker(f)$  contains  $e$  by 4.2. For  $x, y \in \ker(f)$ , we have  $f(xy) = f(x)f(y) = e'e' = e'$ , so we have  $xy \in \ker(f)$ . For  $x \in \ker(f)$ , we have  $f(x^{-1}) = f(x)^{-1} = e'^{-1} = e'$ , so also  $x^{-1} \in \ker(f)$ , and we are done.

The proof of (2) is similar. Since  $e' = f(e) \in f[G]$ , we have (H1). The identity  $f(x)f(y) = f(xy)$  gives the closure condition (H2), and (H3) follows from  $f(x)^{-1} = f(x^{-1}) \in f[G]$ .  $\square$

In the main result of this section, the isomorphism theorem 4.10, we will see that there is a direct relation between the kernel and the image of a homomorphism.

**Exercise 4.** Prove that for a homomorphism  $f : G \rightarrow G'$  and subgroups  $H \subset G$  and  $H' \subset G'$ ,

1. the image  $f[H] = \{f(x) : x \in H\}$  of  $H$  is a subgroup of  $G'$ ;
2. the inverse image  $f^{-1}[H'] = \{x \in G : f(x) \in H'\}$  of  $H'$  is a subgroup of  $G$ .

As an illustration of 4.3 and the exercise above, consider the determinant map  $\det : \mathrm{GL}_2(\mathbf{R}) \rightarrow \mathbf{R}^*$ . This is a homomorphism that sends the group  $\mathrm{GL}_2(\mathbf{R})$  of invertible real  $2 \times 2$  matrices to the multiplicative group  $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$  of non-zero real numbers. The kernel of this homomorphism is the group  $\mathrm{SL}_2(\mathbf{R})$  of matrices with determinant 1. The image of the orthogonal group  $O_2(\mathbf{R}) \subset \mathrm{GL}_2(\mathbf{R})$  is the sign subgroup  $\{\pm 1\} \subset \mathbf{R}^*$ . The inverse image of the sign subgroup is the subgroup  $V \subset \mathrm{GL}_2(\mathbf{R})$  of linear maps with determinant 1 or  $-1$ . The orthogonal group  $O_2(\mathbf{R})$  is a subgroup of  $V$ .

**\*Exercise 5.** Show that  $V$  is the subgroup of area-preserving maps in  $\mathrm{GL}_2(\mathbf{R})$ .

### ► INJECTIVITY

For a homomorphism  $f : G \rightarrow G'$  and an arbitrary element  $y \in G'$ , the inverse image  $f^{-1}(y) = \{x \in G : f(x) = y\}$  of  $y \in G'$  is called the *fiber* of  $f$  over  $y$ . For elements  $y \notin f[G]$ , the fiber  $f^{-1}(y)$  is empty.

The fiber over the unit element  $e' \in G'$  is the kernel of  $f$ , which is a subgroup of  $G$ . We can tell from this fiber whether  $f$  is injective.

**4.4. Theorem.** For a homomorphism  $f : G \rightarrow G'$ , we have

$$f \text{ is injective} \iff \ker(f) = \{e\}.$$

**Proof.** For elements  $g_1, g_2 \in G$ , by the homomorphism property and 4.2, we have

$$(4.5) \quad f(g_1) = f(g_2) \iff f(g_1)^{-1}f(g_2) = e' \iff f(g_1^{-1}g_2) = e' \iff g_1^{-1}g_2 \in \ker(f).$$

If  $\ker(f) = \{e\}$ , it follows from the last identity that  $g_1 = g_2$ , so  $f$  is injective. Conversely, for an injective homomorphism  $f$ , we clearly have  $\ker(f) = \{e\}$ .  $\square$

**4.6. Example.** The real exponential map  $\exp : \mathbf{R} \rightarrow \mathbf{R}^*$  is an injective homomorphism with kernel  $\ker(\exp) = \{0\}$ . By Euler's formula  $e^{a+bi} = e^a(\cos b + i \sin b)$ , the complex exponential map  $\exp : \mathbf{C} \rightarrow \mathbf{C}^*$  has kernel  $2\pi i\mathbf{Z} = \{2k\pi i : k \in \mathbf{Z}\}$  and is therefore not injective.

**Exercise 6.** Are both exponential maps above surjective?

### ► COSETS

Theorem 4.4 says that if the fiber  $N = \ker(f)$  over the unit element consists of one element, then all non-empty fibers consist of one element. By taking a closer look at (4.5), we can show that the non-empty fibers are always “as large” as the kernel. After all, if we fix the element  $g_1$  in (4.5) and check what elements  $g_2 \in G$  are in the fiber over  $f(g_1)$ , we see that these are the  $g_2 \in G$  for which we have  $g_1^{-1}g_2 = n \in N$ , that is,  $g_2 = g_1n$  with  $n \in N$ . In other words, the fiber of a homomorphism  $f$  over a point  $f(g)$  in its image is the set

$$gN = \{gn \in G : n \in N\} = \{x \in G : x = gn \text{ for some } n \in N\}.$$

Such a set is called a *left coset* of the subgroup  $N \subset G$ . The left multiplication  $\lambda_g : G \rightarrow G$  by  $g$  is a bijection that maps  $N$  onto the coset  $gN$ . In the case where  $N$  is finite, this means that all cosets  $gN$  have the same number of elements. For infinite  $N$ , the existence of bijections between the cosets of  $N$  means that they are all “equal in size” in the sense of set theory: they all have the same *cardinality*.

The elements of  $G$  are apparently neatly distributed over the different cosets of  $N = \ker(f)$ . In the case where  $f$  is the sign map  $\varepsilon : S_n \rightarrow \{\pm 1\}$ , we already encountered this equal distribution in 2.10: for  $n > 1$ , the group  $S_n$  splits up into a subgroup  $A_n$  of even permutations and a left coset  $(1\ 2)A_n$  of odd permutations; each class gets half, namely  $n!/2$ , of the elements. The symmetry group  $D_n$  of the regular  $n$ -gon, which like every plane symmetry group admits a sign map, splits up into a subgroup  $C_n$  of  $n$  rotations with sign  $+1$  and a left coset  $\sigma C_n$  of  $n$  reflections with sign  $-1$ .

The name of the Frenchman Joseph Louis Lagrange (1736–1813) is associated with the equal distribution of the group elements over the cosets of a subgroup. Take an arbitrary subgroup  $H$  of a group  $G$ , and consider the collection  $G/H$  of left cosets of  $H$  in  $G$ , that is, the collection of subsets of  $G$  of the form

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

If two cosets  $g_1H$  and  $g_2H$  have a common element  $g_1h_1 = g_2h_2$ , we have  $g_1H = g_1h_1H = g_2h_2H = g_2H$ . So distinct left cosets are always disjoint, and since every element  $g \in G$  lies in a left coset of  $H$  (for example, in  $gH$ ), we see that  $G$  is a *disjoint union* of the left cosets in  $G/H$ . We have

$$(4.7) \quad g_1H = g_2H \iff g_1^{-1}g_2 \in H.$$

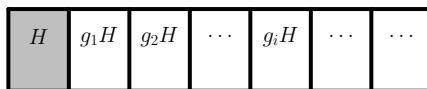
**Exercise 7.** Show that the relation  $g_1 \sim g_2 \iff g_1^{-1}g_2 \in H$  is an equivalence relation on  $G$  and that the equivalence classes for this relation are the left cosets of  $H$  in  $G$ .

The map  $G \rightarrow G/H$  from the *group*  $G$  to the *set*  $G/H$  given by  $g \mapsto gH$  is called the *canonical* or *natural map*. The number of distinct left cosets of  $H$  in  $G$  is the *index*  $[G : H] = \#(G/H)$  of  $H$  in  $G$ . For infinite  $G$ , this index can be infinite. If  $G$  is finite, the index is also finite, and the order of  $G$  can be found by multiplying the index by the number of elements per coset.

**4.8. Lagrange’s theorem.** *Let  $G$  be a finite group and  $H \subset G$  be a subgroup. Then we have*

$$\#G = [G : H] \cdot \#H. \quad \square$$

The graphically inclined can represent the location of a subgroup in a group schematically in the following way: a subgroup is a “building block”  $H$  that, together with its “translations”  $gH$ , neatly covers the group  $G$ . Those who want to draw a “real” example can take  $G = D_7$  and  $H = \langle \sigma \rangle$ , the subgroup generated by a reflection  $\sigma$ .



Theorem 4.8 explains the various divisibility relations for the orders of elements and subgroups we encountered in §1 and §2. In general, we have the following.

**4.9. Corollary.** *For a finite group  $G$ ,*

1. *the order  $\#H$  of a subgroup  $H \subset G$  divides  $\#G$ ;*
2. *the order of an element  $x \in G$  divides  $\#G$ .*

**Proof.** The first statement follows immediately from 4.8. For (2), we take  $H = \langle x \rangle$  and note that the order of the subgroup  $\langle x \rangle$  is equal to the order of the element  $x$ .  $\square$

**Exercise 8.** Prove that every group of *prime order*  $\#G = p$  is isomorphic to the cyclic group  $C_p$ .

#### ► THE ISOMORPHISM THEOREM

We have seen that for a homomorphism  $f : G \rightarrow G'$  with kernel  $N = \ker(f)$ , the set  $G/N$  of left cosets of  $N$  consists of the fibers of  $f$  over the points of the image of  $f$ . So we have a bijection  $G/N \leftrightarrow f[G]$  that sends the coset  $gN$  to the element  $f(g) \in f[G]$ . Now, by 4.3, the image  $f[G]$  is a subgroup of  $G'$  and so itself a group. By *transport of structure*, we conclude that  $G/N$  apparently *also* has the structure of a group. This observation is one of the basic theorems in group theory.

**4.10. Isomorphism theorem.** Let  $f : G \rightarrow G'$  be a homomorphism with kernel  $N$ , and define a binary operation on  $G/N$  by setting  $g_1N \cdot g_2N = g_1g_2N$ . This endows  $G/N$  with the structure of a group, and the map

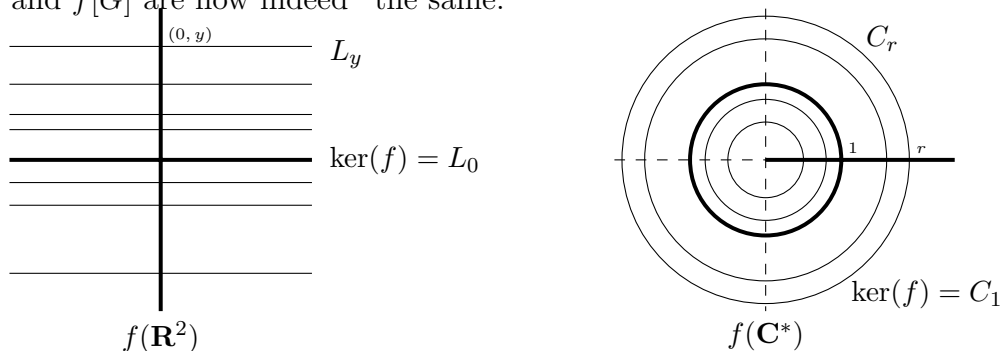
$$\bar{f} : G/N \xrightarrow{\sim} f[G]$$

given by  $gN \mapsto f(g)$  is a group isomorphism.

**Proof.** Since we already know that  $\bar{f} : G/N \rightarrow f[G]$  is a bijection from  $G/N$  to  $f[G]$ , we only need to check that the product class  $g_1N \cdot g_2N = g_1g_2N$  in  $G/N$  is the coset corresponding to the product  $f(g_1)f(g_2) \in f[G]$ . The desired relation  $f(g_1g_2) = f(g_1)f(g_2)$  is precisely the homomorphism property of  $f$ .  $\square$

The isomorphism theorem shows that the *image* of a homomorphism is determined, up to isomorphism, by its *kernel*. This is *the* fundamental homomorphism theorem, and we will frequently come across it.

**4.11. Examples.** To get a feel for what Theorem 4.10 tells us, we give three examples. First, take  $G = G' = \mathbf{R}^2$ , and let  $f : \mathbf{R}^2 \rightarrow \mathbf{R}^2$  be the map given by  $(x, y) \mapsto (0, y)$ . This is a linear map, so certainly a homomorphism; it describes the projection of the plane onto the  $y$ -axis. The kernel of this map is the subgroup  $N = \{(x, 0) : x \in \mathbf{R}\}$  of points on the  $x$ -axis, and the image is the subgroup  $f[G] = \{(0, y) : y \in \mathbf{R}\}$  of points on the  $y$ -axis. The fibers of  $f$  are the horizontal lines  $L_y = \{(x, y) : x \in \mathbf{R}\}$ ; these are the cosets of  $N$  in  $G = \mathbf{R}^2$ . The group  $G = \mathbf{R}^2$  is the disjoint union of the lines  $L_y$ , and each of these lines corresponds to a unique point  $(0, y) \in f[G]$ . The natural addition given by  $\bar{f}$  on the set  $G/N$  of horizontal lines in  $G = \mathbf{R}^2$  is the “addition of  $y$ -coordinates” defined by  $L_{y_1} + L_{y_2} = L_{y_1+y_2}$ . Under the identification  $L_y \leftrightarrow (0, y)$ ,  $G/N$  and  $f[G]$  are now indeed “the same.”



As a second example, we take the map  $f : \mathbf{C}^* \rightarrow \mathbf{R}^*$  given by  $z \mapsto |z|$ . The multiplicativity  $|z_1z_2| = |z_1||z_2|$  of the absolute value says that this is a homomorphism. The kernel  $N$  of  $f$  is the *circle group*  $\{z \in \mathbf{C}^* : |z| = 1\}$  of complex numbers with absolute value 1. Note that this is indeed a subgroup of  $G = \mathbf{C}^*$ . The image of  $f$  is the subgroup  $f[G] = \mathbf{R}_{>0} = \{r \in \mathbf{R} : r > 0\}$  of positive real numbers in  $\mathbf{R}^*$ , and the cosets of  $N$  in  $G = \mathbf{C}^*$  are the sets of complex numbers with given absolute value  $r > 0$ . In our figure, these are the circles  $C_r$  about the origin with radius  $r$ . We again see that  $G$  is a disjoint union of such circles. Each circle corresponds to a unique radius  $r \in f[G]$ , and the multiplication on the set  $G/N$  of circles obtained from  $\bar{f}$  gives  $C_{r_1} \cdot C_{r_2} = C_{r_1r_2}$ . As a group,  $G/N = \{C_r : r \in \mathbf{R}_{>0}\}$  is again the “same” as the group  $f[G] = \mathbf{R}_{>0}$ .

**Exercise 9.** Make a similar figure for the homomorphism  $\mathbf{C}^* \rightarrow \mathbf{C}^*$  given by  $z \mapsto \frac{z}{|z|}$ .

As the third and last example, we consider the “abstract” homomorphism

$$\begin{aligned} f : G &\longrightarrow \text{Aut}(G) \\ g &\longmapsto (\sigma_g : x \mapsto gxg^{-1}) \end{aligned}$$

that sends  $g \in G$  to the conjugation map  $\sigma_g : G \xrightarrow{\sim} G$  defined by  $\sigma_g(x) = gxg^{-1}$ . We have already seen that  $\sigma_g$  is indeed an automorphism of  $G$ . The homomorphism property of  $f$  corresponds to the identity  $\sigma_{g_1g_2} = \sigma_{g_1}\sigma_{g_2} \in \text{Aut}(G)$ . For all  $x \in G$ , we indeed have

$$\sigma_{g_1g_2}(x) = g_1g_2x(g_1g_2)^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = \sigma_{g_1}\sigma_{g_2}(x).$$

The kernel of  $f$  is the subgroup

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

of elements of  $G$  that commute with all elements of  $G$ . The set  $Z(G)$  is called the *center* of  $G$ . The image of  $f$  is the subgroup  $\text{Inn}(G) \subset \text{Aut}(G)$  of *inner automorphisms* of  $G$ . In this case, the isomorphism theorem gives an isomorphism

$$G/Z(G) \xrightarrow{\sim} \text{Inn}(G)$$

that is not easy to visualize. Intuitively, it is clear that there are “more” inner automorphisms the fewer elements of  $G$  commute with all group elements. For abelian groups, we have  $Z(G) = G$ , and  $G/Z(G)$  and  $\text{Inn}(G)$  are both the trivial group. For  $G = S_n$ , we have  $Z(S_n) = 1$  for  $n \neq 2$  (Exercise 29); in this case, conjugation gives an isomorphism  $S_n \xrightarrow{\sim} \text{Inn}(S_n)$ .

Inner automorphisms are common. In linear algebra, we encounter them when writing a linear map given by a matrix  $A$  as a matrix with respect to a basis other than the standard one: if  $T$  is the matrix describing the change of basis, then  $TAT^{-1}$  is the new matrix.

More generally, we find inner automorphisms in all sorts of situations involving a “choice of coordinates.” For the inclusions  $\text{Sym}(F) \rightarrow I_2(\mathbf{R})$  in §3 that occur for distinct choices of a “coordinate system” in  $\mathbf{R}^2$ , we saw this in Exercise 3.22; Exercise 2.48 is a discrete variant of this, and we will see other examples later on (Exercise 5.11). In physics, measurements from different observers are related in a similar way.

### ► NORMAL SUBGROUPS

The isomorphism theorem shows that for a subgroup  $H \subset G$ , the set  $G/H$  has the natural structure of a group if  $H$  acts as the kernel of a homomorphism  $f$ . In fact, 4.10 says that if  $H$  is the kernel of the homomorphism  $f : G \rightarrow f[G]$ , then  $f$  is obtained by composing a “canonical homomorphism”  $G \rightarrow G/H$  with an isomorphism. We will now determine for which subgroups  $H$  such a canonical homomorphism  $G \rightarrow G/H$  exists.

It turns out that problems only arise when the set  $G/H$  of *left* cosets, on which we have so far concentrated so asymmetrically, differs from the set  $H\backslash G$  of *right* cosets  $Hg = \{hg : h \in H\}$  of  $H$  in  $G$ . In the situations where we used left cosets up to now, as in the definition of the index  $[G : H]$  and the proofs of 4.8 and 4.9, we could just as well have used right cosets—see Exercises 44 and 45. In *abelian* groups, we have  $gH = Hg$ , and there is no need to distinguish between left and right cosets. In general, however, the distinction is necessary. For example, if we take the subgroup  $H = \langle(1\ 2)\rangle$  in  $G = S_3$ , then we see that the three left cosets

$$H = \{(1), (1\ 2)\}, \quad (1\ 3)H = \{(1\ 3), (1\ 2\ 3)\}, \quad \text{and} \quad (2\ 3)H = \{(2\ 3), (1\ 3\ 2)\}$$

in  $G/H$  are not the same as the three right cosets

$$H = \{(1), (1\ 2)\}, \quad H(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}, \quad \text{and} \quad H(2\ 3) = \{(2\ 3), (1\ 2\ 3)\}$$

in  $H\backslash G$ . We will prove that there exists a *quotient group*  $G/H$  if and only if  $G/H$  and  $H\backslash G$  are *not* different.

**4.12. Definition.** A subgroup  $H \subset G$  is called a *normal subgroup* of  $G$  if it has the following equivalent properties:

1. For every element  $g \in G$ , we have  $gH = Hg$ .
2. For every element  $g \in G$ , the subgroup  $gHg^{-1} = \{ghg^{-1} : h \in H\}$  is equal to  $H$ .

The equivalence of the two properties above can be seen by applying right multiplication by, respectively,  $g^{-1}$  and  $g$ . The second formulation is nicer because it provides a good way to think of normal subgroups: they are the subgroups that are mapped to themselves by all inner automorphisms  $\sigma_g \in \text{Inn}(G)$ .

**Exercise 10.** Show that in 4.12.2, it suffices to require that we have the *inclusion*  $gHg^{-1} \subset H$ .

In an abelian group, every subgroup is normal. It turns out that in some other groups, such as  $S_n$ , subgroups are rarely normal. We write  $H \triangleleft G$  to show that a subgroup  $H \subset G$  is normal in  $G$ .

**4.13. Proposition.** The kernel of a group homomorphism  $f : G \rightarrow G'$  is normal in  $G$ .

**Proof.** For  $h \in \ker(f)$  and  $g \in G$ , we have  $f(ghg^{-1}) = f(g)e'f(g)^{-1} = e' \in G'$ , so  $ghg^{-1} \in \ker(f)$ . By 4.12.2 (and Exercise 10), the kernel  $\ker(f)$  is now normal in  $G$ .

We can give an alternative proof, using 4.12.1, by observing that the fiber over an element  $f(g)$ , which we described as the *left* coset  $gN$  of  $N = \ker(f)$ , can also be described as the *right* coset  $Ng$  of  $N$ . □

It follows from 4.13 that the set  $G/H$  only “inherits” the structure of a group from  $G$  for normal subgroups  $H \triangleleft G$ . After all, we want the canonical map  $G \rightarrow G/H$  given by  $g \mapsto gH$  to be a homomorphism with kernel  $H$ .

**4.14. Theorem.** Let  $G$  be a group and  $N \triangleleft G$  be a normal subgroup of  $G$ . Then the binary operation

$$g_1N \cdot g_2N = g_1g_2N$$

defines the structure of a group on the set  $G/N$  of cosets of  $N$  in  $G$ . This makes the canonical map  $G \rightarrow G/N$  into a group homomorphism with kernel  $N$ .

**Proof.** We only need to check that the binary operation  $g_1N \cdot g_2N = g_1g_2N$  is well defined on  $G/N$ . This means that if we have  $g_1N = g'_1N$  and  $g_2N = g'_2N$ , we must also have  $g_1g_2N = g'_1g'_2N$ . The assumptions imply that we have  $g'_1 = g_1n_1$  and  $g'_2 = g_2n_2$  for some  $n_1, n_2 \in N$ , which gives

$$g'_1g'_2N = g_1n_1g_2n_2N = g_1g_2(g_2^{-1}n_1g_2)n_2N.$$

By the normality of  $N$ , we have  $g_2^{-1}n_1g_2 \in N$ . The desired result follows.

Now that we know that “coset multiplication” is well defined on  $G/N$ , the group axioms from 2.1 follow easily. The unit element in  $G/N$  is the coset  $eN = N$ , and the inverse of  $gN$  in  $G/N$  is  $g^{-1}N$ . The associativity for  $G/N$  is a direct consequence of the associativity of the multiplication on  $G$ .

The map  $G \rightarrow G/N$  is a homomorphism by the definition of the binary operation on  $G/N$ . The coset  $gN$  of  $N$  that contains  $g$  is only equal to  $N$  for  $g \in N$ , so the kernel of this homomorphism is  $N$ .  $\square$

It follows from 4.13 and 4.14 that the normal subgroups of a group  $G$  are exactly the subgroups of  $G$  that can serve as kernels of homomorphisms. Note that every subgroup  $H \subset G$  can serve as the image of a homomorphism: the inclusion map  $H \rightarrow G$  is a simple example.

## ► QUOTIENT GROUPS

The formation of the *quotient group* or *factor group*  $G/N$  of  $G$  by  $N$  is a fundamental construction also carried out in linear algebra (“*quotient spaces*”) and elsewhere in algebra. We say that we *quotient*  $G$  by  $N$  and call the quotient map  $G \rightarrow G/N$  the *canonical homomorphism*.

When calculating in  $G/N$ , we often write  $\bar{g}$  for the *residue class*  $gN$  of  $g$  modulo  $N$ . This notation is only useful when it is clear from the context modulo what normal subgroup the calculation is being done; if this is not the case, we also write  $g \bmod N$  for  $gN$ . For groups written additively, the residue class of  $g$  is denoted by  $\bar{g}$  or  $g + N$ . The element  $g$  is called a *representative* of the residue class  $gN$ . In general, there are many choices for such a representative. Maps on  $G/N$  are often defined by saying what happens to a representative  $g$  of  $gN$ . It is important always to verify that the given definition is independent of the choice of representative. If this is the case, then the map is *well defined*. We came across this phenomenon in the proof of 4.14 but also already in the definition of multiplication modulo 8 in §1.

**4.15. Examples.** We can think of the elements of the quotient group  $G/N$  as elements of  $G$  for which we “forget” a “well-chosen” part of the information. If we let  $N = \{\pm 1\}$  be the sign group in  $G = \mathbf{R}^*$ , then  $G/N = \mathbf{R}^*/\{\pm 1\}$  is the group of real numbers where we ignore the sign. Only the absolute value of the number remains. More formally, the map  $\mathbf{R}^* \rightarrow \mathbf{R}^*$  given by  $x \mapsto |x|$  is a homomorphism with kernel  $\{\pm 1\}$  and image  $\mathbf{R}_{>0}$ , and the isomorphism theorem provides an isomorphism  $\mathbf{R}^*/\{\pm 1\} \cong \mathbf{R}_{>0}$ .

Likewise, we can view the quotient group  $\mathbf{R}^*/\mathbf{R}_{>0}$  as the group of real numbers “where the size does not matter.” Only the sign remains, and we have an isomorphism  $\mathbf{R}^*/\mathbf{R}_{>0} \cong \{\pm 1\}$ . We obtain it by applying 4.10 to the *sign map*  $\mathbf{R}^* \rightarrow \{\pm 1\}$  given by  $x \mapsto \text{sgn}(x)$ .

Now, take  $G = \mathbf{R}$ , the additive group of real numbers, and  $\mathbf{Z} \subset \mathbf{R}$ , the subgroup of integers. The quotient group  $\mathbf{R}/\mathbf{Z}$  consists of real numbers  $x$  whose “integral part is forgotten.” After all, the additive analog of 4.7 says that two real numbers  $x, y \in \mathbf{R}$  are in the same residue class in  $\mathbf{R}/\mathbf{Z}$  exactly when their difference  $y - x$  is an integer. Every residue class, which we now write additively as  $x + \mathbf{Z}$ , contains a unique representative  $x - [x]$  in the half-open unit interval  $[0, 1)$ . Here,  $[x]$  is the largest integer  $\leq x$ , also called the *entier* of  $x$ .

The situation with  $\mathbf{R}/\mathbf{Z}$  is somewhat reminiscent of the sizes of angles in plane geometry. The size of an angle is a real number, but in practice, angles that differ by a multiple of  $2\pi$  are often seen as equal. We can make this precise by viewing the size of an angle as an element of the “angle group”  $\mathbf{R}/2\pi\mathbf{Z}$ . This group is isomorphic to  $\mathbf{R}/\mathbf{Z}$  because the multiplication  $x \mapsto 2\pi x$  gives an isomorphism  $\mathbf{R}/\mathbf{Z} \xrightarrow{\sim} \mathbf{R}/2\pi\mathbf{Z}$ .

The “feeling of a circle” given by the angle group  $\mathbf{R}/2\pi\mathbf{Z}$  can be made precise using 4.10. By Euler’s formula

$$e^{ix} = \cos x + i \sin x,$$

the homomorphism  $f : \mathbf{R} \rightarrow \mathbf{C}^*$  given by  $e^{ix} = \cos x + i \sin x$  has kernel  $2\pi\mathbf{Z}$  and image the circle group  $\mathbf{T} = \{z \in \mathbf{C}^* : |z| = 1\}$  from 4.11. Theorem 4.10 now gives an isomorphism  $\mathbf{R}/2\pi\mathbf{Z} \xrightarrow{\sim} \mathbf{T}$ : the angle group “is” a circle group.

**Exercise 11.** Give an explicit isomorphism  $\mathbf{R}/\mathbf{Z} \xrightarrow{\sim} \mathbf{T}$ .

Another well-known example of a quotient group is the additive group  $\mathbf{Z}/n\mathbf{Z}$  of *integers modulo  $n$* , where  $n \geq 1$  is an arbitrary integer. We speak of “doing arithmetic modulo  $n$ .” As the notation suggests, we obtain  $\mathbf{Z}/n\mathbf{Z}$  by quotienting the additive group  $\mathbf{Z}$  by the subgroup  $n\mathbf{Z} = \{nx : x \in \mathbf{Z}\}$  of  $n$ -tuples. The case  $n = 60$  is, for example, popular with the Nederlandse Spoorwegen (Dutch Railways), where timetables essentially repeat every 60 minutes. The group  $\mathbf{Z}/n\mathbf{Z}$  is a cyclic group of order  $n$  generated by the residue class  $\bar{1}$ . It is isomorphic to the group  $C_n$  from 3.8. We will return in detail to arithmetic modulo  $n$  in §6. Indeed, the *multiplication* of residue classes also turns out to be interesting.

## EXERCISES.

In the exercises below, unless stated otherwise,  $G$  always denotes a group.

12. Show that for groups, “being isomorphic” is an equivalence relation.
13. Show that the map  $\mathbf{C}^* \rightarrow \text{GL}_2(\mathbf{R})$  given by  $a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$  is an injective group homomorphism.
14. Show that the map  $G \rightarrow G$  given by  $x \mapsto x^2$  is a homomorphism if and only if  $G$  is abelian.

15. Show that the map  $G \rightarrow G$  given by  $x \mapsto x^{-1}$  is a homomorphism if and only if  $G$  is abelian.
16. Let  $f : G \rightarrow G'$  be a homomorphism and  $x \in G$  be of finite order. Prove: the order of  $f(x)$  divides the order of  $x$ .
17. Show that for any two groups  $G_1$  and  $G_2$ , under the componentwise operation  $(g_1, g_2) \cdot (g'_1, g'_2) = (g_1g'_1, g_2g'_2)$ , the product set  $G = G_1 \times G_2$  becomes a group, the *direct product*.
18. Show that the direct product  $C_2 \times C_2$  is a Klein four-group and that  $C_2 \times C_3$  is a cyclic group of order 6.
19. Let  $S \subset G$  be a subset that generates  $G$  and  $f, g : G \rightarrow G'$  be two homomorphisms that agree on  $S$ . Prove:  $f = g$ .  
[“A homomorphism is fixed by its values on a set of generators of the group.”]
20. Does there exist an injective homomorphism  $D_6 \rightarrow S_5$ ?
21. Show that there is no injective homomorphism  $D_6 \rightarrow A_5$ .
22. Let  $G$  be a cyclic group generated by  $x \in G$ . Prove that  $G$  is isomorphic to  $\mathbf{Z}$  if  $x$  has infinite order and to  $\mathbf{Z}/n\mathbf{Z}$  if  $x$  has finite order  $n$ .
23. Let  $G$  be a cyclic group of order  $n$ . Prove that for every divisor  $d$  of  $n$ , the group  $G$  contains exactly one subgroup of order  $d$ .
24. Let  $G$  be a finite group of even order. Prove:  $G$  contains an element of order 2.  
[Hint: look at the orbits of the permutation  $G \rightarrow G$  given by  $x \mapsto x^{-1}$ .]
25. Show that every endomorphism  $f \in \text{End}(\mathbf{Z})$  is of the form  $x \mapsto kx$  for some  $k \in \mathbf{Z}$ . Conclude that  $f \leftrightarrow f(1)$  gives a bijection  $\text{End}(\mathbf{Z}) \leftrightarrow \mathbf{Z}$ . Is  $\text{End}(\mathbf{Z})$  a group under composition?
26. Show that  $\text{Aut}(\mathbf{Z})$  is isomorphic to the sign group  $\{\pm 1\}$ .
27. Let  $G$  and  $G'$  be isomorphic groups. Prove that the *number* of isomorphisms  $G \rightarrow G'$  is equal to the order of the group  $\text{Aut}(G)$ .
28. Do there exist a group  $G$  and an endomorphism  $G \rightarrow G$  that is injective but not surjective? Do there exist a group  $G$  and an endomorphism  $G \rightarrow G$  that is surjective but not injective? Can you take  $G$  to be finite in any of the examples?
29. Show that the center  $Z(S_n)$  of  $S_n$  is trivial for  $n \neq 2$ . What is  $Z(S_2)$ ?
30. Determine the center  $Z(D_n)$  of the dihedral group  $D_n$  for all  $n \geq 1$ .
31. Determine the center of the matrix group  $\text{GL}_2(\mathbf{R})$ .
32. Determine the centers of  $O_2(\mathbf{R})$  and  $I_2(\mathbf{R})$ .
33. Show that a group  $G$  of order  $\#G \leq 5$  is abelian.
34. Suppose that  $G/Z(G)$  is cyclic. Prove:  $G$  is abelian, and  $G/Z(G)$  is the trivial group.
35. Let  $V_4$  be the Klein four-group. Prove:  $\text{Aut}(V_4) \cong S_3$ . How does Exercise 1.14 follow from this?
36. Prove:  $\text{Aut}(S_3) = \text{Inn}(S_3) \cong S_3$ .

37. Let  $H_1$  and  $H_2$  be subgroups of  $G$ , and suppose that we have  $G = H_1 \cup H_2$ . Prove:  $G = H_1$  or  $G = H_2$ . Does a similar statement hold for the identity  $G = H_1 \cup H_2 \cup H_3$ ?
38. Let  $n > 1$  be an integer. Show that the canonical multiplication of residue classes in  $\mathbf{Z}/n\mathbf{Z}$  is *not* a group operation.
39. Let  $G$  be a set with a binary operation that satisfies axioms (G1) and (G2) from 2.1. Prove that the subset

$$G^* = \{g \in G : \text{there exists an } x \in G \text{ with } xg = gx = e\}$$

of  $G$  is a group under the given binary operation.

40. Show that the following examples of sets  $G$  satisfy the conditions in the previous exercise, and determine the corresponding group  $G^*$ :
1.  $G = \mathbf{R}$ , and the operation is multiplication;
  2.  $G = \mathbf{Z}$ , and the operation is multiplication;
  3.  $G = \mathbf{Z}/8\mathbf{Z}$ , and the operation is the canonical multiplication;
  4.  $X$  is a set,  $G$  consists of the maps  $X \rightarrow X$ , and the operation is composition;
  5.  $X$  is a group,  $G = \text{End}(X)$ , and the operation is composition.
41. Let  $A$  and  $B$  be abelian groups written additively. Prove that  $\text{Hom}(A, B)$  becomes a group if we define the sum  $f_1 + f_2$  of two homomorphisms by the formula  $(f_1 + f_2)(a) = f_1(a) + f_2(a)$ . Is the restriction to abelian groups  $A$  necessary? Is the restriction to abelian groups  $B$  necessary?
42. Let  $X$  be a set and  $A$  be an abelian group. Prove that the set  $\text{Map}(X, A)$  of  $A$ -valued functions on  $X$  is a group under the “sum of functions”  $(f_1 + f_2)(x) = f_1(x) + f_2(x)$ . Is the restriction to abelian groups necessary?
43. Let  $X$  be a set and  $P(X)$  the power set of  $X$ . Show that the symmetric difference  $A \Delta B = (A \cup B) \setminus (A \cap B)$  defines a group operation on  $P(X)$  and that  $P(X)$  is isomorphic to  $\text{Map}(X, \mathbf{Z}/2\mathbf{Z})$ .  
[Hint: first construct a bijection  $P(X) \rightarrow \text{Map}(X, \mathbf{Z}/2\mathbf{Z})$  and “transport the structure.” (This is an efficient way of doing Exercise 2.25.)]
44. Let  $G$  be a group and  $H \subset G$  be a subgroup. Show that the relation

$$g_1 \sim g_2 \iff g_2 g_1^{-1} \in H$$

is an equivalence relation on  $G$  and that the equivalence classes for this relation are the right cosets of  $H$  in  $G$ . Conclude that  $G$  is a disjoint union of right cosets of  $H$ .

45. Let  $G$  be a group and  $H \subset G$  be a subgroup. Show that the bijection  $G \rightarrow G$  given by  $x \mapsto x^{-1}$  induces a bijection  $G/H \rightarrow H \backslash G$ . Conclude that the index  $[G : H]$  of a subgroup can also be defined as the number of *right* cosets of  $H$  in  $G$ .
46. Show that every subgroup  $H \subset G$  of index 2 is a normal subgroup.
47. Suppose that every left coset of  $H$  in  $G$  is also a right coset of  $H$  in  $G$ . Prove that  $H$  is normal in  $G$ .
48. Show that the only left coset of  $O_2(\mathbf{R})$  in  $I_2(\mathbf{R})$  that is also a right coset is the class of  $O_2(\mathbf{R})$  itself.

49. Show that the subgroup  $T \subset I_2(\mathbf{R})$  of translations is a normal subgroup in  $I_2(\mathbf{R})$  and that  $I_2(\mathbf{R})/T$  is isomorphic to the orthogonal group  $O_2(\mathbf{R})$ .
50. Prove that for every point  $x \in \mathbf{R}^2$ , the *stabilizer*

$$\text{Stab}_x = \{\varphi \in I_2(\mathbf{R}) : \varphi(x) = x\} \subset I_2(\mathbf{R})$$

is a subgroup of  $I_2(\mathbf{R})$  that is conjugate to  $O_2(\mathbf{R})$ . Conclude that  $I_2(\mathbf{R})$  contains infinitely many different subgroups isomorphic to  $O_2(\mathbf{R})$ .

51. Show that the subgroups  $H_1 = \langle (1\ 2), (3\ 4) \rangle$  and  $H_2 = \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle$  of  $S_4$  are both isomorphic to  $V_4$ . Show that  $H_1$  is not normal in  $S_4$  but  $H_2$  is. What group of order 6 is  $S_4/H_2$ ?
52. Let  $n$  and  $k$  be positive numbers with  $k \leq n$  and  $H \subset S_n$  be the set of permutations that map the subset  $\{1, 2, 3, \dots, k\} \subset \{1, 2, 3, \dots, n\}$  to itself. Prove:  $H$  is a subgroup of  $S_n$  of index  $\binom{n}{k}$ .  
[There are also other ways to prove that the binomial coefficient  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$  is an integer...]
53. A subgroup  $H \subset G$  is called *characteristic* if we have  $\sigma[H] = H$  for all  $\sigma \in \text{Aut}(G)$ . Show that characteristic subgroups are normal, and give an example of a non-characteristic normal subgroup.
54. Show that the center  $Z(G)$  is a characteristic subgroup of  $G$ .
55. Show that the subgroup  $\text{Inn}(G)$  of inner automorphisms is normal in the group  $\text{Aut}(G)$  of all automorphisms.  
[Non-inner automorphisms are called *outer* automorphisms. We define the quotient  $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$ . (This is not the “group of outer automorphisms”!)]
56. Let  $A$  be an *abelian* group. The *torsion subgroup*  $A^{\text{tor}}$  of  $A$  is the set of elements of finite order in  $A$ . Prove that  $A^{\text{tor}}$  is a subgroup of  $A$  and that  $A/A^{\text{tor}}$  contains no elements of finite order other than the unit element.  
[The assumption that  $A$  is abelian is essential; see Exercise 2.36.]
57. Determine  $A^{\text{tor}}$  for  $A = \mathbf{Q}$ ,  $\mathbf{Q}/\mathbf{Z}$ , and  $\mathbf{R}^*$ . Prove:  $(\mathbf{C}^*)^{\text{tor}} \cong \mathbf{Q}/\mathbf{Z}$ .
58. Let  $H_1$  and  $H_2$  be subgroups of a finite group  $G$  with  $H_1 \subset H_2 \subset G$ . Prove:  $H_1$  is a subgroup of  $H_2$ , and we have

$$[G : H_1] = [G : H_2][H_2 : H_1].$$

\*Is this also true if  $H_1$  has finite index in an infinite group  $G$ ?

59. Let  $N_1$  and  $N_2$  be normal subgroups of  $G$  with  $N_1 \subset N_2 \subset G$ . Prove that the canonical map  $G/N_1 \rightarrow G/N_2$  is a surjective homomorphism with kernel

$$N_2/N_1 = \{n_2N_1 : n_2 \in N_2\}.$$

Conclude that there is a canonical isomorphism

$$(G/N_1)/(N_2/N_1) \xrightarrow{\sim} G/N_2.$$

[This is also called “quotienting step-by-step”: we first quotient  $G$  by the small normal subgroup  $N_1$ , then quotient  $G/N_1$  by the image of the large normal subgroup  $N_2$  in  $G/N_1$ .]

- \*60. Let  $H_1$  and  $H_2$  be subgroups of finite index in  $G$ . Prove that  $H_1 \cap H_2$  is a subgroup of finite index in  $G$ . Is  $[G : (H_1 \cap H_2)]$  necessarily a divisor of  $[G : H_1] \cdot [G : H_2]$ ?

## 5 GROUP ACTIONS

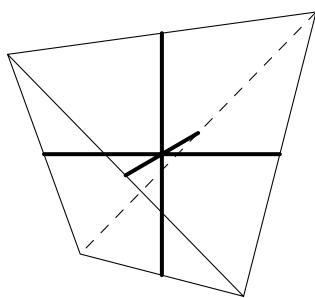
Many groups we have encountered so far have the property that they permute an “associated” set  $X$ . For the permutation group  $S(X)$  in §2, this is precisely the definition of the group; for the various groups of maps in §3 such as  $I_2(\mathbf{R})$  and  $GL_2(\mathbf{R})$ , we had  $X = \mathbf{R}^2$ . In geometry and algebra, an object  $X$  is often assigned a “symmetry group,” which “acts on  $X$ .”

### ► CUBIC AND TETRAHEDRAL GROUPS

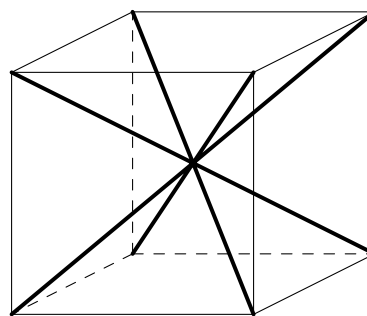
For plane figures, we defined the symmetry group in 3.7. This definition is easily generalized to symmetry groups  $\text{Sym}(X)$  of solid objects  $X \subset \mathbf{R}^3$ . If we take  $X$  to be a tetrahedron, then  $T = \text{Sym}(X)$  is a subgroup of  $S(X)$ . In §1, we saw that we do not need to look at the action on the whole tetrahedron  $X$ : since a symmetry is fixed by its action on the four vertices, there is an “inclusion”  $T \subset S_4$ , which turns out to be a group isomorphism. This establishes the “structure” of the tetrahedral group  $T$ :  $T$  is isomorphic to the permutation group  $S_4$ .

Similarly, we can view the group  $K$  of symmetries of the cube as a subgroup of  $S_8$ . After all, every symmetry in  $K$  is fixed by its action on the cube’s eight vertices. Since there are many ways to number a cube’s vertices, there is no fixed inclusion  $K \subset S_8$ . Each choice of numbering leads to an injective group homomorphism  $K \rightarrow S_8$ . Instead of injective group homomorphisms, we generally say *embeddings* of  $K$  into  $S_8$ . Note that such an embedding is nothing but an isomorphism from  $K$  to a subgroup of  $S_8$ . Since not all permutations of the eight vertices can be realized by symmetries in  $K$ , the embeddings  $K \rightarrow S_8$  themselves are not isomorphisms: the image is not the whole group  $S_8$ . Therefore, the “structure” and even the order of  $K$  are not immediately clear.

For both the tetrahedral group  $T$  and the cubic group  $K$ , we can study the action of the symmetries on other parts of the tetrahedron and cube than the vertices.



$$T \longrightarrow S_3$$



$$K \longrightarrow S_4$$

For example, if we look at the action of the tetrahedral group  $T \cong S_4$  on the three line segments connecting the midpoints of “opposite” edges, then by choosing a numbering, we obtain a “geometric homomorphism”  $S_4 \rightarrow S_3$ . Note that it is not obvious a priori whether such a homomorphism exists. For the cubic group  $K$ , we can study the action on the four space diagonals of the cube. After we choose a numbering, this gives rise to a homomorphism  $K \rightarrow S_4$ .

The resulting homomorphisms  $T \rightarrow S_3$  and  $K \rightarrow S_4$  are not injective. In the first case, this is obvious from the cardinalities: we cannot map the group  $T$  of order 24 injectively to a group of order 6. In the second case, we can easily determine the kernel: the symmetries of the cube that preserve the space diagonals are the identity and the point reflection in the center of the cube.

For the tetrahedron, the reflections in the planes through a “connecting line segment” and one of the corresponding edges give the three 2-cycles in  $S_3$ , and for the cube, we can interchange two space diagonals by reflecting in the plane through the other two space diagonals. Since  $S_3$  and  $S_4$  are generated by their 2-cycles by 1.5, it follows that the homomorphisms  $T \rightarrow S_3$  and  $K \rightarrow S_4$  are surjective.

**Exercise 1.** Determine which cubic symmetries the 3-cycles and 4-cycles in  $S_4$  give.

For the tetrahedral group  $T$ , the kernel  $N$  of the surjection  $T \rightarrow S_3$  consists of the identity and three half turns about the connecting line segments drawn in the figure. If we view  $T$  as  $S_4$ , then the kernel is the normal subgroup  $\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong V_4$  of  $S_4$ . “Geometrically,” we thus obtain an isomorphism

$$T/N = S_4/V_4 \xrightarrow{\sim} S_3.$$

For the cubic group  $K$ , the existence of a surjective homomorphism  $K \rightarrow S_4$  with kernel  $\{\pm 1\}$  generated by the point reflection  $-1$  in the center gives much information: we have  $K/\{\pm 1\} \cong S_4$  by the isomorphism theorem 4.10 and, in particular,  $\#K = 2 \cdot 24 = 48$ . If we define the *sign* of a solid symmetry through the determinant, as we did after 3.9, then the subgroup  $K^+ \subset K$  of cubic symmetries with sign  $+1$  is a group of order 24 that maps injectively to  $S_4$ . Conversely, the isomorphism

$$K^+ \xrightarrow{\sim} S_4$$

gives a “geometric interpretation” of  $S_4$  as the *rotation group of the cube* (cf. Exercise 2.65).

As in the examples above, in general, an *action* of a group on a set is nothing but a homomorphism  $G \rightarrow S(X)$ .

**5.1. Definition.** An operation or action of a group  $G$  on a set  $X$  is a homomorphism  $\phi : G \rightarrow S(X)$ .

If  $G$  acts on  $X$ , we say that  $X$  is a  $G$ -set. If  $\phi$  is injective, the action is called *faithful*. For  $\phi(g)(x)$ , we prefer to write  $g \circ x$ ,  $g(x)$ , or even  $gx$  for short. By the homomorphism property, we have  $g_1 g_2 \circ x = g_1 \circ (g_2 \circ x)$  for  $g_1, g_2 \in G$ , and the unit element  $e \in G$  acts as the identity on  $X$ .

**Exercise 2.** Show that a map  $G \times X \rightarrow X$ , denoted by  $(g, x) \mapsto g \circ x$ , gives an action of  $G$  on  $X$  if and only if it satisfies the following two conditions:

- (W1)  $e \circ x = x$  for all  $x \in X$ ;
- (W2)  $gh \circ x = g \circ (h \circ x)$  for all  $g, h \in G$  and  $x \in X$ .

In some situations, it is more natural to let a group  $G$  act “from the right” on the set  $X$  and consider maps  $X \times G \rightarrow X$  that satisfy  $x \circ (gh) = (x \circ g) \circ h$ . Unlike the action in 5.1, also called a *left action* of  $G$  on  $X$ , such a right action corresponds not to a homomorphism  $G \rightarrow S(X)$  but to an *anti-homomorphism*  $G \rightarrow S(X)$ . See Exercises 19 and 20 for details.

► ORBIT, STABILIZER, FIXED POINT

The notions of “orbit” and “stabilizer” are very natural in the context of group actions.

**5.2. Definition.** *Let  $G$  be a group that acts on  $X$ . The stabilizer or isotropy group of a point  $x \in X$  in  $G$  is the subgroup*

$$G_x = \{g \in G : gx = x\} \subset G,$$

and the orbit of  $x$  under  $G$  is the subset

$$Gx = \{gx : g \in G\} \subset X.$$

It is easy to see that the stabilizer  $G_x$  is a subgroup of  $G$ . The kernel of the action  $\phi : G \rightarrow S(X)$  in 5.1 is equal to the intersection  $\bigcap_{x \in X} G_x$  of all stabilizers.

The number of elements in the orbit  $Gx$ , which can be infinite for infinite groups  $G$ , is called the *length* of the orbit of  $x$ . If there exists an  $x \in X$  with  $Gx = X$ , then the action of  $G$  on  $X$  is called *transitive*.

If we have  $gx = x$  for  $g \in G$  and  $x \in X$ , then  $x$  is called a *fixed point* of  $g$ . If  $x$  is a common fixed point of all  $g \in G$ , then  $x$  is called a fixed point for the action of  $G$  on  $X$ . The fixed points for the action of  $G$  on  $X$  are the points  $x \in X$  for which the orbit  $Gx = \{x\}$  has length 1. The set of fixed points is often denoted by  $X^G$ . If  $X^G$  is the empty set, the action of  $G$  on  $X$  is called *fixed-point-free*.

The natural action of  $I_2(\mathbf{R})$  on  $\mathbf{R}^2$  is transitive and fixed-point-free. The stabilizer of the origin is the orthogonal group  $O_2(\mathbf{R})$ . The stabilizers of the other points are subgroups conjugate to  $O_2(\mathbf{R})$  (see Exercise 4.50).

Generally, the stabilizer of a point  $gx$  in the orbit of  $x$  is equal to  $gG_xg^{-1}$  and therefore conjugate to  $G_x$ . This follows easily from the equivalences

$$\tilde{g}gx = gx \iff g^{-1}\tilde{g}gx = x \iff g^{-1}\tilde{g}g \in G_x \iff \tilde{g} \in gG_xg^{-1}.$$

This is another one of the many situations in which conjugation automorphisms occur.

The length of the orbit  $Gx$  of  $x$  can be deduced from the size of the stabilizer  $G_x$  of  $x$ , as follows.

**5.3. Theorem.** *Let  $X$  be a  $G$ -set and  $x \in X$ . The map  $g \mapsto gx$  induces a bijection*

$$G/G_x \longleftrightarrow Gx$$

between the set of left cosets of  $G_x$  in  $G$  and the orbit of  $x$ . In particular, the length of the orbit  $Gx$  is equal to the index  $[G : G_x]$ .

**Proof.** Analogously to the situation in 4.7, we have equivalences

$$gx = hx \iff h^{-1}gx = x \iff h^{-1}g \in G_x \iff gG_x = hG_x,$$

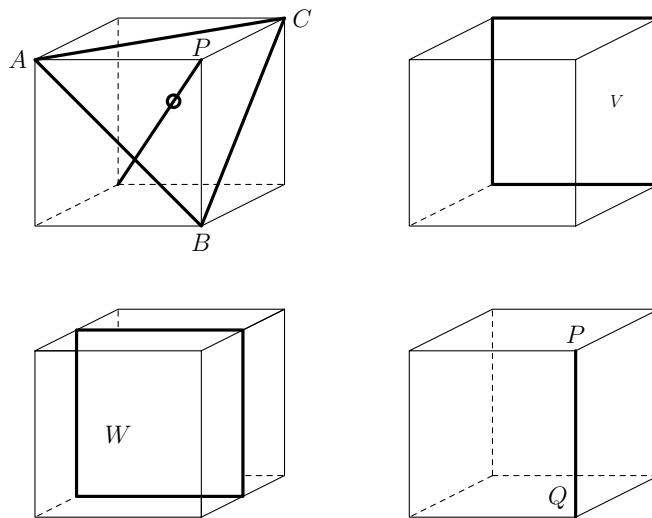
so the map  $g \mapsto gx$  sends left cosets of  $G_x$  injectively to elements of  $Gx$ . The surjectivity is clear from the definition of  $Gx$ .  $\square$

For any action of a finite group  $G$  on a set  $X$ , Theorem 5.3 gives us the useful identity

$$\#Gx \cdot \#G_x = \#G.$$

In words, for every point, the product of its orbit length and the order of its stabilizer is the group order. This allows us to determine the orders of all sorts of symmetry groups.

**5.4. Example.** Take the group  $K$  of symmetries of the cube. There are various ways to determine the order of  $K$ .



For a vertex  $P$  of the cube, the orbit of  $P$  consists of the cube's eight vertices. An element of the stabilizer  $K_P$  of  $P$  is fixed by its action on the three “adjacent” vertices  $A$ ,  $B$ , and  $C$ . A sketch immediately shows that  $K_P \cong D_3 \cong S_3$  is the symmetry group of the equilateral triangle  $ABC$ . It follows that the cubic group has order  $8 \cdot 6 = 48$ . If instead of  $P$ , we take the face  $V$  in the back, then we see that the orbit of  $V$  has length 6 and the stabilizer  $K_V$  is the group  $D_4$  of symmetries of the square  $V$ . Again, the product of the orbit length and the order of the stabilizer is equal to  $6 \cdot 8 = 48$ . For the “central plane”  $W$  in the cube, the orbit has length 3, and the stabilizer  $K_W$  has order 16. After all,  $K_W$  consists of  $K_V$  and the composition of the elements of  $K_V$  with the reflection in the plane through  $W$ . Finally, if we take an edge  $PQ$ , then the orbit has length 12, and the stabilizer  $K_{PQ} \cong V_4$  is the group generated by the reflections in the perpendicular bisector of  $PQ$  and in the plane through  $PQ$  and the space diagonal from  $P$ .

**Exercise 3.** What points on the faces have an orbit of length 48 under the action of  $K$ ?

If the orbits of two elements  $x, y \in X$  have a non-empty intersection, there exist  $g_1, g_2 \in G$  such that  $g_1x = g_2y$ . The orbit of  $x$  equals  $Gx = Gg_1x = Gg_2y = Gy$ , so the orbits coincide. Two  $G$ -orbits are apparently either disjoint or equal.

**Exercise 4.** Show that the orbits of  $X$  under  $G$  are the equivalence classes in  $X$  for the equivalence relation  $x \sim y \iff x = gy$  for some  $g \in G$ .

We conclude that under the action of  $G$ , the set  $X$  splits up into orbits.

**5.5. Theorem.** *A  $G$ -set  $X$  is a disjoint union of orbits.* □

In the case of a transitive action, there is only one orbit. For a fixed-point-free action, there are no orbits of length 1. The set of orbits of  $X$  under the action of  $G$  is called the *orbit space* or *quotient* of  $X$  under the action of  $G$  and is denoted by  $G \backslash X$ .

**5.6. Example.** For the action of the orthogonal group  $G = O_2(\mathbf{R})$  on the plane  $\mathbf{R}^2$ , the origin  $O$  is a fixed point. For  $x \neq O$ , the orbit  $Gx$  is a circle about the origin through  $x$ , and the stabilizer  $G_x$  is a group with two elements generated by the reflection  $\sigma_{\ell_x}$  in the line  $\ell_x$  through  $O$  and  $x$ . Indeed,  $\mathbf{R}^2$  is the disjoint union of  $O$  and the circles about  $O$ . For  $x \neq O$ , the stabilizer  $G_x$  is not a normal subgroup of  $G$ ; the cosets in  $G/G_x$  are of the form  $\rho G_x$  for a rotation  $\rho \in G$ , and the correspondence  $\rho G_x \leftrightarrow \rho x$  gives the bijection from 5.3. The action of  $O_2(\mathbf{R})$  on  $\mathbf{R}^2$  is neither transitive nor fixed-point-free.

**Exercise 5.** Show that the natural action of  $O_2(\mathbf{R})$  on  $\mathbf{R}^2 \setminus \{O\}$  is not transitive but that the stabilizers of the points are all conjugate. Is the action fixed-point-free?

#### ► ORBIT DECOMPOSITION FORMULA

For a group  $G$  that acts on a finite set  $X$ , there is a formula to count the *number* of orbits under the action. This *orbit decomposition formula*, often attributed to the Englishman William Burnside (1852–1927), goes back to work of the Frenchman Augustin-Louis Cauchy (1789–1857) and the German Georg Ferdinand Frobenius (1849–1917). The formula uses the *permutation character* associated with the action. This is the integer function  $\chi : G \rightarrow \mathbf{Z}$  that sends an element  $g \in G$  to the number

$$\chi(g) = \#\{x \in X : gx = x\}$$

of fixed points of  $g$  in  $X$ .

**5.7. Orbit decomposition formula.** *Let  $G$  be a finite group that acts on a finite set  $X$  and  $\chi$  be the corresponding permutation character. Then the number of  $G$ -orbits in  $X$  is equal to*

$$\#(G \backslash X) = \frac{1}{\#G} \sum_{g \in G} \chi(g).$$

**Proof.** We can write the number of  $G$ -orbits of  $X$  as a sum over the elements of  $X$ , where every  $x \in X$  has “weight”  $\frac{1}{\#G_x}$ . Using 5.3, we then obtain

$$\#(G \backslash X) = \sum_{x \in X} \frac{1}{\#G_x} = \frac{1}{\#G} \sum_{x \in X} \#G_x.$$

The number of elements  $\#G_x$  of the stabilizer of  $x$  can be written as  $\sum_{g \in G} \delta_{g,x}$ , where we take  $\delta_{g,x}$  equal to 1 if  $gx = x$  and equal to 0 if  $gx \neq x$ . By changing the order of summation, we obtain

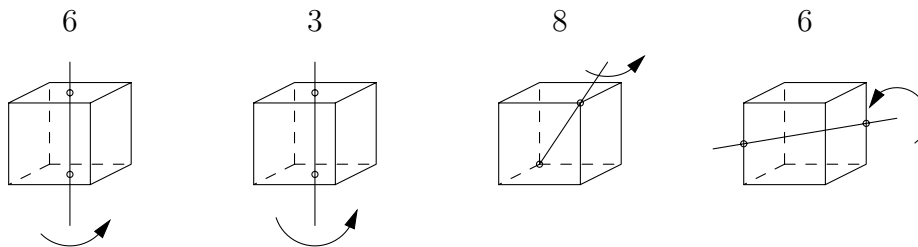
$$\frac{1}{\#G} \sum_{x \in X} \sum_{g \in G} \delta_{g,x} = \frac{1}{\#G} \sum_{g \in G} \sum_{x \in X} \delta_{g,x} = \frac{1}{\#G} \sum_{g \in G} \chi(g)$$

for the number of  $G$ -orbits. □

In words, the orbit decomposition formula says that the number of orbits is equal to the *average* number of fixed points per group element. It is particularly useful in combinatorics for counting numbers of configurations in situations where symmetry plays a role.

### ► COMBINATORICAL APPLICATIONS

A *Dutch cube* is a cube whose six faces are each red, white, or blue. Since there are three possible colors for each face, there are  $3^6 = 729$  ways to color the cube. The set  $X$  of 729 cubes obtained this way contains fewer than 729 “truly different” cubes. After all, many of these cubes can be transformed into one another through rotations. To know how many different Dutch cubes exist, we must calculate the number of *orbits* in  $X$  under the action of the rotation group  $K^+$  of the cube. As we saw before 5.1, the group  $K^+$  is isomorphic to  $S_4$ .



In addition to the identity  $\text{id} \in K^+$ , which leaves all 729 elements of  $X$  invariant, there exist four types of rotations of the cube. There are two quarter turns about each of the three central axes parallel to the edges. A Dutch cube that is invariant under one of these six quarter turns has the property that the four faces that are interchanged cyclically all have the same color. Such a cube has at most three different colors, so for each quarter turn, we find  $3^3 = 27$  invariant cubes in  $X$ .

The three half turns about the axes mentioned above leave two faces of a cube in place and interchange the other four in two pairs of opposite faces. For a cube invariant under this, these pairs of opposite faces have the same color. This leaves four colors to choose, and we find  $3^4 = 81$  invariant cubes in  $X$  for each of these three elements in  $K^+$ .

The eight rotations by  $\pm 2\pi/3$  about one of the four space diagonals interchange the six faces in two 3-cycles. Per element, this gives  $3^2 = 9$  invariant cubes in  $X$ .

Finally, we have the six half turns about the lines that connect the midpoint of an edge and the midpoint of the diametrically opposite edge. These interchange the faces in three pairs, so we find  $3^3 = 27$  invariant cubes in  $X$ .

The orbit decomposition formula now gives

$$\#(K^+ \setminus X) = \frac{1}{24}(1 \cdot 729 + 6 \cdot 27 + 3 \cdot 81 + 8 \cdot 9 + 6 \cdot 27) = 57$$

orbits for the action of  $K^+$  on  $X$ . This is the number of distinct Dutch cubes.

**Exercise 6.** Show that if we use  $n$  different colors, the number of distinct cubes is equal to

$$\frac{n^2}{24}(n^4 + 3n^2 + 12n + 8).$$

See Exercises 16–18 for similar problems involving other symmetry groups.

### ► REGULAR ACTION

In addition to the more geometric examples of group actions on sets we have already mentioned, there are “abstract actions” we can define for all groups and use to analyze the structure of finite groups. The remainder of this section gives an idea of some of the possibilities. In §9, we will discuss such methods in detail.

The most direct example of an abstract group action is the *regular action* of a group on itself by left multiplication. We can use it to view *every* group as a subgroup of a suitably chosen permutation group.

**5.8. Cayley’s theorem.** *Let  $G$  be a group and  $S(G)$  be the permutation group on the set  $G$ . For  $g \in G$ , denote by  $\lambda_g : G \rightarrow G$  the left multiplication  $x \mapsto gx$ . Then*

$$\begin{aligned} f : G &\longrightarrow S(G) \\ g &\longmapsto \lambda_g \end{aligned}$$

*is an embedding, and  $G$  is isomorphic to a subgroup of  $S(G)$ .*

**Proof.** After (2.3), we saw that for every  $g \in G$ , the map  $\lambda_g$  is a bijection  $G \rightarrow G$ . For elements  $g_1, g_2$ , and  $x$  in  $G$ , we have

$$\lambda_{g_1 g_2}(x) = g_1 g_2 x = \lambda_{g_1}(g_2 x) = \lambda_{g_1}(\lambda_{g_2}(x)) = (\lambda_{g_1} \lambda_{g_2})(x),$$

so  $f$  is a homomorphism. It follows from  $\lambda_g(e) = g$  that  $\lambda_{g_1}$  and  $\lambda_{g_2}$  are different for  $g_1 \neq g_2$ , so  $f$  is injective, and  $G$  is isomorphic to the subgroup  $f[G] \subset S(G)$ .  $\square$

Theorem 5.8, named after the Englishman Arthur Cayley (1821–1895), is mainly of theoretical interest. The theorem expresses that group elements can be viewed as permutations, namely from  $G$  to itself. In practice, the group  $S(G)$  is usually too large for explicit computations, and the choice in Cayley’s theorem is not very “efficient.” For example, we can embed the dihedral group  $D_5$  of order 10 in the permutation group  $S_5$  of order 120 by viewing its action on the five vertices of a regular pentagon. Cayley’s theorem gives an embedding in a group of order  $10! = 3628800$ .

**Exercise 7.** Which embedding do we get for  $G = S_5$ ? Is it “efficient”?

If a subgroup  $H \subset G$  acts by left multiplication on  $G$ , then the orbit space  $H \backslash G$  is precisely the set of right cosets of  $H$  in  $G$ . Before 4.12, we already denoted this set by  $H \backslash G$ . So orbit spaces can be viewed as generalized sets of right cosets. For the regular action of a normal subgroup  $N$  on  $G$ , the orbit space  $N \backslash G = G/N$  “inherits” the structure of a group from  $G$ , as indicated in 4.14.

In geometry, it often happens that a group  $G$  of transformations acts on a given space  $X$ . Under suitable conditions on the action, the quotient  $G \backslash X$  “inherits” geometric properties from  $X$ , for example the notion of a distance. For  $X$  the plane and  $G$  a suitable group of isometries, we can obtain nice examples such as cylinders and tori; see Exercises 25 and 27.

We get a useful variant of the action in 5.8 by letting  $G$  act not on itself but on the set  $G/H$  of left cosets of a subgroup  $H$  in  $G$ . The *regular action* of  $G$  on  $G/H$  is now given by  $g \circ xH = gxH$ .

**5.9. Theorem.** *The regular action  $G \rightarrow S(G/H)$  of  $G$  on  $G/H$  is a homomorphism with kernel  $\bigcap_{x \in G} xHx^{-1}$ .*

**Proof.** It is easy to check that left multiplication by  $g$  permutes the left cosets of  $H$  and that the given map is an action. If we have  $gxH = xH$  for a coset  $xH$ , then we have  $x^{-1}gx \in H$  and  $g \in xHx^{-1}$ . It follows that  $g$  fixes all cosets if and only if it is an element of  $\bigcap_{x \in G} xHx^{-1}$ .  $\square$

**Exercise 8.** Show that  $N = \bigcap_{x \in G} xHx^{-1}$  is the largest normal subgroup of  $G$  that is contained in  $H$ .

The regular action of  $G$  on  $G/H$  in 5.9 is an example of a transitive action. The stabilizer of  $H \in G/H$  is the subgroup  $H$  itself, and in this case, the bijection in 5.3 is the identity. The stabilizers of the other cosets  $xH \in G/H$  are the conjugate subgroups  $xHx^{-1}$ .

For a normal subgroup  $N$ , the regular action of  $G$  on  $G/N$  is the composition of the canonical map  $G \rightarrow G/N$  with the regular action of  $G/N$  on itself, and from 5.9, we obtain a new proof of Theorem 4.14. In general, 5.9 gives a normal subgroup  $N \subset H$  in  $G$ .

As an application of 5.9, we generalize the result from Exercise 4.46 that every subgroup of index 2 is normal.

**5.10. Theorem.** *Let  $G \neq 1$  be a finite group and  $p$  be the smallest prime divisor of  $\#G$ . Then every subgroup  $H \subset G$  of index  $p$  is normal in  $G$ .*

**Proof.** Let us show that the kernel  $N$  of the map  $f$  in 5.9 is equal to  $H$ . Then  $H$  is normal by 4.13. Since  $S(G/H)$  is isomorphic to the permutation group  $S_p$ , the order of  $G/N \cong f[G] \subset S(G/H)$  is a divisor of the group order  $p!$  of  $S(G/H)$ . We have  $N \subset H \subset G$ , so  $[G : N] = p \cdot [H : N]$  is a divisor of both  $p!$  and  $\#G$ . Hence  $[H : N]$  is a divisor of both  $(p-1)!$  and  $\#G$ . Since  $(p-1)!$  and  $\#G$  have no common divisors by assumption, we find that  $[H : N] = 1$  and  $H = N$ .  $\square$

## ► CONJUGATION ACTION

A second standard example of an abstract group action is the *conjugation action* mentioned before. In 4.11, we saw that for every group element  $g \in G$ , the conjugation map  $\sigma_g : x \mapsto gxg^{-1}$  is a bijection of  $G$  and that the map  $g \mapsto \sigma_g$  is a homomorphism  $G \rightarrow \text{Aut}(G) \subset S(G)$  with kernel  $Z(G)$ , the center of  $G$ . In particular, this is an action of  $G$  on itself. There is specific terminology for orbits and stabilizers for this action. The stabilizer of  $x \in G$  under conjugation is called the *normalizer*

$$N_x = \{g \in G : gxg^{-1} = x\}$$

of the element  $x$ . It is the subgroup consisting of the elements that commute with  $x$ . The orbits under conjugation in  $G$  are called the *conjugacy classes* of  $G$ . For finite groups, the cardinality  $[G : N_x]$  of a conjugacy class divides the group order. The fixed points for the conjugation action are the elements of the center  $Z(G)$  of  $G$ .

**5.11. Example.** Determining the conjugacy classes for the symmetric group  $S_n$  is relatively straightforward. After all, for arbitrary  $\sigma, \tau \in S_n$ , to obtain the conjugate  $\tau\sigma\tau^{-1}$  of  $\sigma$ , we need (Exercise 2.46) to replace each cycle  $(x_1 x_2 \cdots x_k)$  in the disjoint cycle decomposition of  $\sigma$  with  $(\tau(x_1) \tau(x_2) \cdots \tau(x_k))$ . Elements in  $S_n$  are therefore conjugate exactly when their *cycle types*, defined before 2.7, correspond.

The group  $S_3$  of order 6 contains the unit element, two 3-cycles, and three 2-cycles; this gives three conjugacy classes of orders 1, 2, and 3, respectively. For larger  $n$ , we get a slightly more elaborate count. If we first note that the number of  $k$ -cycles in  $S_n$  is equal to  $\binom{n}{k} \cdot (k-1)!$ , then in specific cases, it is relatively easy to compute the number of elements of a given cycle type. For example, for  $n = 4$  and  $n = 5$ , we find the following numbers of elements in each of the conjugacy classes. Note that these numbers indeed divide the group orders  $\#S_4 = 24$  and  $\#S_5 = 120$ .

	(1)	(12)	(123)	(1234)	(12)(34)	(12345)	(12)(345)
$S_4$ :	1	6	8	6	3	–	–
$S_5$ :	1	10	20	30	15	24	20

We already came across the group  $S_4$  as the rotation group  $K^+$  of the cube. The five conjugacy classes in  $S_4$  are exactly the five “types” of rotations of the cube.

**Exercise 9.** Determine the sizes of all conjugacy classes in the alternating groups  $A_4$  and  $A_5$ .

Every group also acts by conjugation on the set of its subgroups. The orbit under conjugation of a subgroup  $H \subset G$  consists of the set of subgroups  $\{gHg^{-1} : g \in G\}$  conjugate to  $H$ . Since every conjugation gives an automorphism of  $G$ , all these subgroups are isomorphic to  $H$ . They also all have the same index in  $G$ . The fixed points for this conjugation action are precisely the normal subgroups of  $G$ . The stabilizer of a subgroup  $H \subset G$  under conjugation is called the *normalizer*

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

of  $H$  in  $G$ . We have  $H \triangleleft N_G(H)$ , and  $N_G(H)$  is the largest subgroup of  $G$  in which  $H$  is normal. For  $H \triangleleft G$ , we have  $N_G(H) = G$ , and for arbitrary  $H$ , the number of subgroups in  $G$  conjugate to  $H$  is equal to the index  $[G : N_G(H)]$  by 5.3.

**Exercise 10.** Show that a subgroup of finite index has only finitely many conjugates.

► CAUCHY’S THEOREM

When  $X$  is finite, we can write the order of  $X$  as the sum of the lengths of the orbits under  $G$ . Using the formula in 5.3 for the length of an orbit, this gives

$$\#X = \sum_{Gx \in G \backslash X} [G : G_x].$$

The stabilizer  $G_x$  in this formula depends on the choice of the *representative*  $x$  in each orbit, but the index  $[G : G_x]$  does not. After all, for different choices of  $x$  within an orbit, the stabilizers are conjugate, and conjugate subgroups have the same index in  $G$ . Instead of summing over orbits, we can also sum over the elements in a *system of representatives* for the  $G$ -orbits of  $X$ : this is a subset of  $X$  that contains exactly one element from every  $G$ -orbit. If  $\mathcal{B}$  is such a system of representatives, then we have  $X^G \subset \mathcal{B}$  because every fixed point is the unique representative of its  $G$ -orbit. We can therefore rewrite the previous formula as

$$(5.12) \quad \#X = \#X^G + \sum_{x \in \mathcal{B} \backslash X^G} [G : G_x].$$

As an application of this, we prove a fundamental theorem of Cauchy on finite groups. The proof is a generalization of a simpler argument that only works for  $p = 2$  (Exercise 4.24).

**5.13. Cauchy’s theorem.** *Let  $G$  be a finite group and  $p$  be a prime divisor of  $\#G$ . Then  $G$  contains an element of order  $p$ .*

**Proof.** Let  $X \subset G^p$  be the set of  $p$ -tuples  $(g_1, g_2, \dots, g_p) \in G^p$  for which we have  $g_1 g_2 g_3 \dots g_p = e$ . Conjugating  $g_1 g_2 g_3 \dots g_p$  by  $g_p$  shows that we then also have the equality  $g_p g_1 g_2 g_3 \dots g_{p-1} = e$ , so we can “shift” the  $p$ -tuples in  $X$  cyclically. This defines an action of the cyclic group  $\mathbf{Z}/p\mathbf{Z}$  on  $X$  given by

$$\bar{k} \cdot (g_1, g_2, \dots, g_p) = (g_{p-k+1}, g_{p-k+2}, \dots, g_{p-1}, g_p, g_1, \dots, g_{p-k}) \quad (1 \leq k \leq p).$$

By 5.3, the length of every orbit under this action is a divisor of  $\#(\mathbf{Z}/p\mathbf{Z}) = p$ , hence equal to 1 or  $p$ . The orbits of length 1 come from the fixed points under the shift, which are the constant sequences  $(x, x, \dots, x) \in X$ . By the product condition on  $X$ , there is exactly one such sequence for every element  $x \in G$  with  $x^p = e$ .

The number of elements of  $X$  is equal to  $(\#G)^{p-1}$ . After all, we can choose  $p - 1$  coordinates freely, and the product then fixes the last coordinate. Since the order of  $X$  is a  $p$ -tuple and all orbits have length 1 or  $p$ , we see (using 5.12 if necessary) that the number  $\#X^G$  of orbits of length 1 is a multiple of  $p$ . This means that the number of constant sequences  $(x, x, \dots, x) \in X$  is divisible by  $p$ . So, in addition to the trivial sequence  $(e, e, \dots, e)$ , there are other constant sequences in  $X^G$ , which correspond to elements of order  $p$  in  $G$ .  $\square$

More generally, it follows from 5.12 that if  $G$  is a  $p$ -group, that is, a finite group  $G$  whose order is a power of a prime  $p$ , then for every finite  $G$ -set  $X$ , the congruence

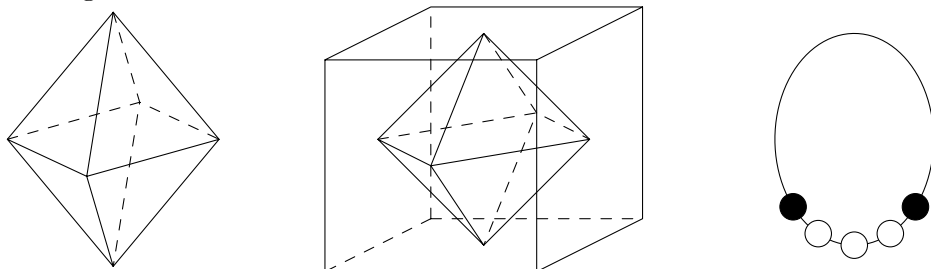
$$(5.14) \quad \#X \equiv \#X^G \pmod{p}$$

holds. Indeed, as in the proof of 5.13, all orbits outside of  $X^G$  have length divisible by  $p$ .

In 10.6 and 10.8, we will use 5.14 to show that every group  $G$  of order divisible by  $p^k$  contains a subgroup  $H$  of order  $p^k$ . For  $k = 1$ , this is Cauchy's theorem because a subgroup of order  $p$  is of the form  $\langle x \rangle$  with  $x$  of order  $p$ . In the case where  $p^k$  is the highest power of  $p$  that divides  $\#G$ , a subgroup  $H \subset G$  of order  $p^k$  is called a *Sylow  $p$ -subgroup* of  $G$ . For  $k > 1$ , such a subgroup need not be *cyclic*. Exercise 57 shows why Sylow  $p$ -subgroups always exist.

## EXERCISES.

11. Let  $\phi, \phi' : K \rightarrow S_8$  be two embeddings of the cubic group in  $S_8$  obtained by numbering the cube's vertices in two different ways. Prove:  $\phi = \sigma \circ \phi'$  for an inner automorphism  $\sigma \in \text{Inn}(S_8)$ .
12. Show that the formula  $r \circ z = z + r$  for  $r \in \mathbf{R}$  and  $z \in \mathbf{C}$  gives an action of the additive group  $G = \mathbf{R}$  of real numbers on the set  $X = \mathbf{C}$  of complex numbers. Describe the orbits under this action.
13. Repeat the previous exercise for  $r \circ z = e^{ir}z$ .
14. An *octahedron* is the solid figure bounded by eight equilateral triangles. Let  $\text{Oct}$  be the symmetry group of the octahedron. Determine the orders of the stabilizers of a vertex and of a face in  $\text{Oct}$  and the order of  $\text{Oct}$  itself.
15. Show that the six centers of the faces of a cube form the vertices of an octahedron. Deduce that we have an isomorphism  $K \xrightarrow{\sim} \text{Oct}$ .
16. Define a Dutch octahedron, and determine the number of “truly different” Dutch octahedra. How large does this number become if we view an octahedron and its mirror image as being “the same”?



17. An *orange necklace* consists of five spherical beads on a closed necklace, each red, white, blue, or orange. The beads can move freely along the necklace. Determine the number of different orange necklaces.
18. A *magical octagon* is obtained by soldering eight colored rods of equal length onto a regular octagon. How many truly different magical octagons can we make if the rods are available in ten different colors?
19. A group map  $f : G \rightarrow G'$  is called an *anti-homomorphism* if for any two elements  $x, y \in G$ , we have the identity  $f(xy) = f(y)f(x)$ .
  - a. Give an example of an anti-homomorphism that is *not* a homomorphism.
  - b. Do the statements in 4.2 and 4.3 hold for anti-homomorphisms?
  - c. Prove:  $f$  is an anti-homomorphism  $\iff f^* : x \mapsto f(x^{-1})$  is a homomorphism.
20. A *right action* of a group  $G$  on a set  $X$  is an anti-homomorphism  $\phi : G \rightarrow S(X)$ . In this case, we denote  $\phi(g)(x)$  by  $x \circ g$ .
  - a. Prove that a map  $X \times G \rightarrow X$ , denoted by  $(x, g) \mapsto x \circ g$ , gives a right action if and only if it satisfies the following two conditions:
    - (RW1)  $x \circ e = x$  for all  $x \in X$ ;
    - (RW2)  $x \circ gh = (x \circ g) \circ h$  for all  $g, h \in G$  and  $x \in X$ .
  - b. Prove that for every right action  $X \times G \rightarrow X$ , the map  $G \times X \rightarrow X$  given by  $(g, x) \mapsto x \circ g^{-1}$  is a (left) action.

21. Show that the *modular group*<sup>15</sup>  $\mathrm{SL}_2(\mathbf{Z})$  of integer matrices with determinant 1 acts on the complex upper half-plane  $\mathcal{H} = \{z : \Im(z) > 0\}$  by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az + b}{cz + d}.$$

Determine the isotropy groups of  $z = i$ ,  $z = 2i$ , and  $z = \zeta_3$  (the third root of unity in  $\mathcal{H}$ ). Is the action transitive?

22. Show that a matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$  has no fixed points on the complex upper half-plane  $\mathcal{H}$  if its trace has absolute value  $|a + d| > 2$ .
23. Let  $F = \mathrm{Map}(\mathcal{H}, \mathbf{C})$  be the set of complex-valued functions on  $\mathcal{H}$ . For  $f \in F$  and  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z})$ , define the function  $f \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  on  $\mathcal{H}$  by  $(f \circ \begin{pmatrix} a & b \\ c & d \end{pmatrix})(z) = f(\frac{az+b}{cz+d})$ . Prove that this gives a right action of  $\mathrm{SL}_2(\mathbf{Z})$  on  $F$ .  
[The fixed points under this action are called the *modular functions*.]
24. Show that for every  $G$ -set  $X$ , the set  $\mathrm{Map}(X, \mathbf{C})$  of complex-valued functions on  $X$  has a natural right action on  $G$ .
25. Define the natural action of  $\mathbf{Z}$  by translation on the complex plane  $\mathbf{C}$  by  $k \circ z = z + k$ , and let  $\Omega$  be the orbit space. The *distance* between two orbits  $B_1, B_2 \in \Omega$  is  $d(B_1, B_2) = \min\{|z_1 - z_2| : z_1 \in B_1, z_2 \in B_2\}$ .

- Show that  $\Omega$  can be identified with the quotient group  $\mathbf{C}/\mathbf{Z}$ .
- Show that for every  $z_0 \in \mathbf{C}$ , the canonical map  $\pi : \mathbf{C} \rightarrow \Omega$  given by  $z \mapsto \mathbf{Z} + z$  is injective and distance preserving on a disk of center  $z_0$ . Conclude that the group  $\Omega$  “locally looks like the plane.” [The map  $\pi$  is called a *local isometry*.]
- Explain why the group  $\Omega$  “is topologically a cylinder.”  
[*Topology*<sup>16</sup> makes this question more precise:  $\mathbf{C}/\mathbf{Z}$  is *homeomorphic* to the cylinder.]

26. State and make the analog of the previous exercise with  $\mathbf{Z}$  replaced by the group  $\mathbf{Z}[i] = \{a + bi \in \mathbf{C} : a, b \in \mathbf{Z}\}$  of *Gaussian integers*.  
[The orbit space is the surface of an inner tube, called a *torus*.]
27. Let  $X$  be a set. Show that a subset  $Y \subset X$  is *stable* under  $G$  (that is, we have  $gy \in Y$  for  $g \in G$  and  $y \in Y$ ) if and only if  $Y$  is a union of orbits. Conclude that a subgroup  $H \subset G$  is normal if and only if  $H$  is a union of conjugacy classes.
28. Show that the only normal subgroups of the alternating group  $A_5$  are the trivial ones  $N = 1$  and  $N = A_5$ .
29. Let  $G$  be a finite group that acts transitively on a set  $X$ , and let  $N$  be a normal subgroup of  $G$ . Prove that all orbits of  $X$  under  $N$  have the same length. Show that the condition that  $N$  is normal cannot be left out.
30. For  $G$ -sets  $X$  and  $Y$ , we denote by  $\mathrm{Map}(X, Y)$  the set of maps from  $X$  to  $Y$ . Prove that  $\mathrm{Map}(X, Y)$  becomes a  $G$ -set through the definition

$$(gf)(x) = gf(g^{-1}x) \quad (g \in G, f \in \mathrm{Map}(X, Y), x \in X).$$

31. A map  $f : X \rightarrow Y$  of  $G$ -sets is called  *$G$ -equivariant* if it satisfies  $f(gx) = g(f(x))$  for  $g \in G$  and  $x \in X$ . Prove that the fixed points of  $G$  in  $\mathrm{Map}(X, Y)$  are exactly the  $G$ -equivariant maps from  $X$  to  $Y$ .

32. Define the notion of an isomorphism for  $G$ -sets, and show that the bijection  $G/G_x \iff Gx$  given in 5.3 is an isomorphism of  $G$ -sets.
33. Let  $G$  be a finite group. Prove that there exists an  $n$  for which  $G$  is isomorphic to a subgroup of  $\text{GL}_n(\mathbf{R})$ .
34. Let  $G$  be a finite group of order  $n$  and  $G \rightarrow S(G) \cong S_n$  be the Cayley map from 5.8. Prove that the image of an element  $g \in G$  of order  $k$  is a product of  $n/k$  disjoint  $k$ -cycles in  $S(G)$ . When does the image of  $G$  in  $S(G)$  contain odd permutations?
35. Let  $G$  be a finite group of order  $2u$  with  $u$  odd. Prove that the elements of odd order form a subgroup of order  $u$  in  $G$ . [Hint: use the previous exercise.]
36. Show that the elements of odd order do not form a subgroup in  $S_n$  for  $n > 3$ .
37. Let  $G$  be a finite group of order  $2^n u$  with  $u$  odd, and suppose that  $G$  contains an element of order  $2^n$ . Prove that the elements of odd order form a subgroup of index  $2^n$  in  $G$ .
38. Let  $H \subset D_{10}$  be the subset of elements of odd order in  $D_{10}$ . Is  $H$  a subgroup? If so, determine the index  $[D_{10} : H]$ .
39. Prove that every group of order 6 is isomorphic to  $C_6$  or  $S_3$ .
40. Let  $I(n)$  be the number of isomorphism classes of groups of order  $n$ . Show that  $I(n)$  is finite for all  $n \geq 1$ , and calculate  $I(n)$  for  $n \leq 7$ .
41. Show that the number  $I(n)$  in the previous exercise satisfies  $I(n) \leq ((n-1)!)^{n-1}$ . \*Can you find a better upper bound?<sup>17</sup>
42. Let  $\mathcal{C}$  be a system of representatives for the conjugacy classes of  $G$ , and denote the normalizer of  $x \in G$  by  $N_x$ . Prove the *class formula*
- $$\#G = \#Z(G) + \sum_{x \in \mathcal{C} \setminus Z(G)} [G : N_x].$$
43. Let  $G$  be a finite group with exactly two conjugacy classes. Prove that  $G$  is the cyclic group of order 2.  
[There exist infinite groups with exactly two conjugacy classes.<sup>18</sup>]
- \*44. Let  $n \geq 1$  be an integer. Prove that (up to isomorphisms) there are only *finitely* many finite groups with exactly  $n$  conjugacy classes.  
[Hint: use the New Year's puzzle at the end of §1.]
45. Let  $G$  be a group with order a prime power  $p^k > 1$ . Prove:  $Z(G) \neq 1$ .
46. Let  $p$  be a prime. Prove that every group of order  $p^2$  is abelian.
47. Suppose that  $G$  contains a subgroup  $H$  of finite index  $[G : H] > 1$ . Prove that  $G$  contains a normal subgroup  $N$  of finite index  $[G : N] > 1$ .
48. Let  $H \subset \mathbf{R}$  be a subgroup of finite index in the additive group  $\mathbf{R}$  of real numbers. Prove:  $H = \mathbf{R}$ . Does the analogous statement hold for subgroups of the additive group  $\mathbf{Q}$  of rational numbers?
49. Let  $G$  be a finite group that acts transitively on a set  $X$  with  $\#X > 1$ . Prove: there is an element  $g \in G$  that does not fix any elements of  $X$ , that is, such that  $gx \neq x$  for all  $x \in X$ .

50. Let  $\mathcal{C}$  be a set of representatives for the conjugacy classes of a finite group  $G$ . Prove that  $G$  is generated by  $\mathcal{C}$ .
51. Determine the normalizers of  $H = \langle (1\ 2\ 3) \rangle$  in  $A_4$  and in  $S_4$ .
52. Determine the normalizers of  $H = \langle (1\ 2\ 3\ 4\ 5) \rangle$  in  $A_5$  and in  $S_5$ .
53. Let  $C$  be the conjugacy class of an even permutation  $\sigma \in S_n$ . Prove that  $C$  is a conjugacy class in  $A_n$  if the normalizer of  $\sigma$  in  $S_n$  contains an odd permutation and that it is a union of two conjugacy classes in  $A_n$  of the same order if this is not the case.
- \*54. Suppose that the element  $\sigma \in A_n$  in the previous exercise has a disjoint cycle decomposition corresponding to the partition  $n = a_1 + a_2 + \dots + a_t$ . Prove:  $C$  is a conjugacy class in  $A_n$  if and only if two  $a_i$  are equal or at least one of the  $a_i$  is even.
55. Let  $G$  be a finite group and  $p$  be a prime that divides the order of  $G$ . Let  $t$  be the number of elements of order  $p$  in  $G$  and  $h$  be the number of subgroups of order  $p$  in  $G$ . Prove:  $t = h(p - 1)$ , and  $h - 1$  is divisible by  $p$ .
- \*56. Show that every subgroup of  $S_n$  can be generated by at most  $n - 1$  elements. [Hint: use induction on  $n$  to prove the *stronger* statement that  $n - t$  elements suffice, with  $t$  the number of orbits of  $\{1, 2, 3, \dots, n\}$  under the action of the subgroup.]
57. Let  $G$  be a group of order  $n = p^k m$  with  $p$  prime and  $p \nmid m$ . A *Sylow  $p$ -subgroup* of  $G$  is a subgroup  $H \subset G$  of order  $p^k$ . To prove that such an  $H$  exists, take  $X$  equal to the collection of *subsets* of  $G$  of cardinality  $p^k$ , and let  $G$  act on  $X$  by left multiplication:  $gV = \{gv : v \in V\}$  for  $g \in G$  and  $V \in X$ .
- Prove:  $\#X = \binom{n}{p^k} \equiv m \pmod{p}$ .
  - Prove that there exists a  $V \in X$  for which the length of the orbit  $GV$  is relatively prime to  $p$ .
  - Show that the stabilizer  $H = G_V$  of a set  $V$  as in part b is a Sylow  $p$ -subgroup of  $G$ .
58. Let  $p \geq 3$  be a prime and  $n$  be a positive integer.
- Show that the edges of a regular  $p$ -gon can be colored in  $(n^p + (p - 1)n)/p$  truly different ways if every edge is given one of  $n$  possible colors.
  - Conclude that  $n^p - n$  is divisible by  $p$ . (Compare with Theorem 6.18.)
59. Let  $G$  be a finite group and  $H$  be a subgroup of  $G$ . Can the number of conjugacy classes of  $H$  be greater than that of  $G$ ?

## 6 INTEGERS

In this section, we study mathematical objects that are so fundamental that they are found in all developed cultures: *integers*. We obtain the set  $\mathbf{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$  of integers by adding negative numbers to the set  $\mathbf{N} = \{0, 1, 2, \dots\}$  of non-negative or *natural* numbers. Some do not view 0 as a natural number, and the number 0 is not natural in that, like the negative numbers, it was invented later than the positive numbers and was not used yet by, for example, ancient Greeks. We will not discuss the axiomatic descriptions<sup>19</sup> of  $\mathbf{N}$  given by the Italian Peano (1858–1932). Such axioms are used in logic to formalize the intuitively clear properties of the natural numbers, including the proof method of *complete induction* we have used and the fact that every non-empty set of positive numbers contains a *smallest element*.

The extension of  $\mathbf{N}$  to  $\mathbf{Z}$  needs no justification for anyone who has ever seen a ledger or thermometer; from the point of view of group theory, we can say that  $\mathbf{Z}$ , unlike  $\mathbf{N}$ , is a *group* under addition. It is an *infinite cyclic group* with generator 1 (or  $-1$ ). Every cyclic group generated by an element  $x$  of infinite order is isomorphic to  $\mathbf{Z}$  under the bijection  $x^k \leftrightarrow k$ .

Every finite cyclic group is a quotient of  $\mathbf{Z}$ . After all, if  $G = \langle x \rangle$  is generated by an element  $x$  of order  $n$ , then the map  $\mathbf{Z} \rightarrow G$  given by  $k \mapsto x^k$  is surjective with kernel  $n\mathbf{Z} = \{nk : k \in \mathbf{Z}\}$ . The isomorphism theorem gives  $G \cong \mathbf{Z}/n\mathbf{Z}$ . This is the “additive notation” for the cyclic group  $C_n$  from 3.8.

### ► DIVISION WITH REMAINDER

The cyclic groups  $\mathbf{Z}/n\mathbf{Z}$  of *residue classes modulo  $n$*  are the only quotients of  $\mathbf{Z}$ . The proof of this relies on the useful notion of *division with remainder*.

**6.1. Division with remainder.** *Let  $a$  and  $b > 0$  be natural numbers. Then there exist natural numbers  $q$  and  $r$  with*

$$a = qb + r \quad \text{and} \quad 0 \leq r < b.$$

**Proof.** The set  $S = \{a, a - b, a - 2b, a - 3b, \dots\}$  contains natural numbers, such as  $a \in S$ , and therefore a *smallest* natural number  $r = a - qb$ . The number  $r - b \in S$  is less than  $r$ , hence negative. This gives  $0 \leq r < b$ , as desired.  $\square$

**Exercise 1.** State and prove an analogous theorem for integers  $a$  and  $b \neq 0$ .

What 6.1 says is nothing but the well-known fact that we can subtract  $b$  from  $a$  “as often as possible.” The number  $r$  in 6.1 is called the *remainder* of  $a$  when dividing by  $b$ . For  $b = n$ , Theorem 6.1 shows that we can denote the elements of  $\mathbf{Z}/n\mathbf{Z}$  by  $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$ . An equality  $\bar{x} = \bar{y} \in \mathbf{Z}/n\mathbf{Z}$  for  $x, y \in \mathbf{Z}$  is called a *congruence* and has been denoted by  $x \equiv y \pmod{n}$  since Gauss (1777–1855).

**6.2. Corollary.** *Every subgroup of  $\mathbf{Z}$  is of the form  $n\mathbf{Z}$  for a natural number  $n$ .*

**Proof.** Let  $H \subset \mathbf{Z}$  be a subgroup. If  $H$  is the trivial group, we have  $n = 0$ . If  $H$  is non-trivial, then  $H$  contains positive numbers; after all, for  $x \in H$ , we have  $-x \in H$ .

Let  $n$  be the smallest positive number in  $H$ . Then we have  $H \supset n\mathbf{Z}$ , and we will show that equality holds. For  $a \in H$  arbitrary, we write  $a = qn + r$  as in 6.1. Then  $r = a - qn$  is a non-negative number less than  $n$ , and as the difference of elements in  $H$ , it is contained in  $H$ . It follows that  $r = 0$  and  $a = qn \in n\mathbf{Z}$ , so  $H = n\mathbf{Z}$ .  $\square$

### ► GCD AND LCM

Using 6.2, we can express divisibility properties of integers in terms of subgroups of  $\mathbf{Z}$ . We write  $a\mathbf{Z} + b\mathbf{Z}$  for the subgroup of  $\mathbf{Z}$  generated by  $a$  and  $b$ . It consists of the elements  $xa + yb$  with  $x, y \in \mathbf{Z}$ .

**6.3. Definition.** For integers  $a$  and  $b$ , we use the following terminology:

1. If we have  $a\mathbf{Z} \supset b\mathbf{Z}$ , then  $a$  is called a divisor of  $b$  and  $b$  a multiple of  $a$ .
2. If we have  $a\mathbf{Z} + b\mathbf{Z} = \mathbf{Z}$ , then  $a$  and  $b$  are said to be relatively prime or coprime.
3. The non-negative generators of  $a\mathbf{Z} + b\mathbf{Z}$  and  $a\mathbf{Z} \cap b\mathbf{Z}$  are called the greatest common divisor  $\text{GCD}(a, b)$  and the least common multiple  $\text{LCM}(a, b)$  of  $a$  and  $b$ .

Note that 6.3.1 is equivalent to another common formulation: a number  $a$  divides  $b$  if there exists an  $x \in \mathbf{Z}$  with  $ax = b$ . We denote “ $a$  divides  $b$ ” by  $a \mid b$ . We see that 0 is divisible by every number  $a$  because the trivial subgroup  $0\mathbf{Z}$  is contained in every subgroup  $a\mathbf{Z}$  of  $\mathbf{Z}$ . A number  $b \neq 0$  has only finitely many divisors because every divisor  $a \mid b$  satisfies  $|a| \leq |b|$ .

A number  $d \geq 0$  with  $d\mathbf{Z} = a\mathbf{Z} + b\mathbf{Z}$  is a divisor of both  $a$  and  $b$ . Conversely, for every common divisor  $n$  of  $a$  and  $b$ , we have the inclusion  $n\mathbf{Z} \supset a\mathbf{Z} + b\mathbf{Z} = d\mathbf{Z}$ , so  $n$  divides  $d$ . Thus, except in the case  $d = 0 = \text{GCD}(0, 0)$ ,  $d$  is indeed the *greatest* common divisor. Analog remarks explain the name of the least common multiple.

It follows from the definition of  $\text{GCD}(a, b)$  that there exist numbers  $x, y \in \mathbf{Z}$  with

$$(6.4) \quad xa + yb = \text{GCD}(a, b).$$

In particular,  $a$  and  $b$  are relatively prime if and only if the equation  $xa + yb = 1$  has an integer solution. In 6.13 and 6.14, we will indicate how to quickly calculate the numbers  $x, y$ , and  $\text{GCD}(a, b)$  given  $a$  and  $b$ .

**Exercise 2.** Define the numbers  $\text{GCD}(a_1, a_2, \dots, a_n)$  and  $\text{LCM}(a_1, a_2, \dots, a_n)$  for  $n \geq 2$ .

### ► PRIME NUMBERS

The *trivial divisors* of a number  $a \neq 0$  are the divisors  $\pm 1$  and  $\pm a$ . A number  $a > 1$  that has only trivial divisors is called a *prime number* or *prime* for short. A number  $a > 1$  that is not prime is called *composite*. By definition, 1 is not prime, and the set of prime numbers  $\mathcal{P}$  looks as follows:

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \dots\}.$$

Many elementary questions concerning  $\mathcal{P}$  remain unsolved.<sup>20</sup> A positive result is the following classical theorem of Euclid<sup>21</sup> ( $\pm 300$  BCE).

**6.5. Theorem.** *There are infinitely many primes.*

**Proof.** Suppose that  $\mathcal{P} = \{p_1, p_2, p_3, \dots, p_n\}$  is finite, and let  $p$  be the smallest divisor  $> 1$  of  $N = p_1 p_2 p_3 \dots p_n + 1$ . Then  $p$  is prime because every divisor of  $p$  is also a divisor of  $N$ . By our assumption, we have  $p = p_i \in \mathcal{P}$  for some  $i$ . Now,  $p = p_i$  is a divisor of  $N$  and of  $p_1 p_2 p_3 \dots p_n$ , hence also of  $N - p_1 p_2 p_3 \dots p_n = 1$ . This gives a contradiction.  $\square$

**Exercise 3.** Are the numbers  $p_1 p_2 p_3 \dots p_n + 1$ , with  $p_1, p_2, \dots, p_n$  the first  $n$  prime numbers, all prime?

A prime in  $\mathbf{Z}$  is defined by an *irreducibility property*: there are no non-trivial divisors. The following *prime property* of prime numbers is much more useful.

**6.6. Lemma.** *Let  $a$  and  $b$  be integers and  $p$  be a prime. Then we have  $p \mid ab \implies p \mid a$  or  $p \mid b$ .*

**Proof.** Suppose that  $p$  is a divisor of  $ab$  but not of  $b$ . Then  $\text{GCD}(p, b)$  is a positive divisor of  $p$  that is not equal to  $p$ , so we have  $\text{GCD}(p, b) = 1$ . As in 6.4, there exist  $x, y \in \mathbf{Z}$  with  $xp + yb = 1$ . Now, write  $a = (xp + yb)a = axp + yab$ ; then  $p$  divides both  $axp$  and  $yab$ , and therefore  $a$ .  $\square$

**Exercise 4.** Let  $a$  and  $b$  be relatively prime, and let  $c$  be divisible by  $a$  and  $b$ . Prove:  $ab \mid c$ .

It easily follows by induction from 6.5 that a prime  $p$  that divides a product  $a_1 a_2 \dots a_n$  must divide at least one of the numbers  $a_i$ .

#### ► UNIQUE PRIME FACTORIZATION

The primes are the “multiplicative building blocks” of the integers, as follows.

**6.7. Unique Factorization.** *Every positive number  $n$  can be factored uniquely as a product*

$$n = \prod_{p \in \mathcal{P}} p^{n_p}$$

*of primes. The exponents  $n_p$  are natural numbers that are non-zero for only finitely many primes  $p$ .*

**Proof.** We first use induction to prove that every integer  $n \geq 1$  has a decomposition in prime numbers. For  $n = 1$ , we can take the empty product. Let  $n > 1$  be arbitrary, and assume that all numbers less than  $n$  are products of prime numbers. If  $n$  has only trivial divisors, then  $n$  is prime, and we are done. If  $n$  has a non-trivial divisor  $n_1 > 1$ , we can write  $n = n_1 n_2$ . By the induction hypothesis,  $n_1$  and  $n_2$  both have a decomposition, and by combining them, we obtain a decomposition of  $n$ . This proves the *existence* of a prime factor decomposition for all  $n$ .

We still need to show that decompositions are unique. Suppose that we have two decompositions

$$p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$$

of a number in prime factors. We want to prove that the primes in both decompositions are the same, up to the order. We carry out the proof by induction on the length  $s$  of the first decomposition. For  $s = 0$ , there is nothing to prove. For  $s \geq 1$ , the prime  $p_1$

is a divisor of  $q_1 q_2 \dots q_t$ , so we have  $p_1 \mid q_i$  for some  $i$ . Since  $q_i$  is prime, this implies that we have  $p_1 = q_i$ . If we divide out the factors  $p_1$  and  $q_i$  in the equality above, we obtain two equal decompositions with  $s - 1$  prime factors on the left and  $t - 1$  on the right. By the induction hypothesis, we have  $s - 1 = t - 1$ , and the factors are equal up to their orders. This therefore also holds for the original decompositions. This proves the *uniqueness* of the decomposition.  $\square$

The exponent  $n_p$  of  $p$  in the factorization of  $n$  is also called the *order* of  $n$  at  $p$  and denoted by  $\text{ord}_p(n)$ . The function  $\text{ord}_p : \mathbf{Z}_{>0} \rightarrow \mathbf{Z}_{\geq 0}$  satisfies the “homomorphism-type” property  $\text{ord}_p(xy) = \text{ord}_p(x) + \text{ord}_p(y)$  for  $x, y \in \mathbf{Z}_{>0}$ .

**Exercise 5.** Show that there exists a unique homomorphism  $\text{ord}_p : \mathbf{Q}^* \rightarrow \mathbf{Z}$  whose restriction to  $\mathbf{Z}_{>0}$  is equal to the function we just defined.

Finding the *prime factor decomposition* or *factorization* in 6.7 is more or less elementary. An effective but often time-consuming way to decompose a number  $n > 1$  consists of simply trying out (“*trial division*”)  $d = 2, 3, 4, \dots$  as divisors of  $n$ . The smallest divisor  $p > 1$  of  $n$  is a prime number. If we have  $p < n$ , we write  $n = p \cdot m$  and then decompose  $m$ . When  $p = n$ , the number  $n$  is itself prime.

**Exercise 6.** Prove that a number  $n > 1$  is prime if it has no divisors  $d$  with  $1 < d \leq \sqrt{n}$ .

## ► RINGS

Theorem 6.7 is not a group-theoretic theorem for  $\mathbf{Z}$ . It concerns the *multiplication* in  $\mathbf{Z}$ , and we already saw in §4 that  $\mathbf{Z}$  is not a multiplicative group because not all elements have an inverse. Since in a multiplicative group, all elements are one another’s divisors, divisibility is only important in multiplicative structures that are *not* groups. To axiomatize the combination of the “additive structure” and “multiplicative structure” on  $\mathbf{Z}$ , we leave the framework of group theory, which has become too narrow, and introduce the notion of a *ring*.

**6.8. Definition.** A *ring* is an abelian group  $A$ , written additively, endowed with a binary operation  $A \times A \rightarrow A$  written multiplicatively that satisfies the following three conditions:

(R1)  $A$  contains a unit element 1 for the multiplication.

(R2) For any three elements  $a, b, c \in A$ , we have the associative property

$$a(bc) = (ab)c.$$

(R3) For any three elements  $a, b, c \in A$ , we have the distributive properties

$$a(b + c) = ab + ac \quad \text{and} \quad (a + b)c = ac + bc.$$

If we, moreover, have  $ab = ba$  for all  $a, b \in A$ , then  $A$  is called a *commutative ring*.

The additive group underlying a ring  $A$  is taken to be abelian by definition. This is not a restriction because this property follows from the other ring axioms (Exercise 50). Conditions (R1) and (R2) are equal to conditions (G1) and (G2) in 2.1. However, we do not require that every element of  $A$  has a multiplicative inverse, and the multiplicative structure of a ring is therefore less “nice” than we are used to for groups. The set of *units* or *invertible elements*

$$A^* = \{a \in A : \text{there exists an } a^\dagger \in A \text{ with } aa^\dagger = a^\dagger a = 1\}$$

in  $A$  does satisfy (Exercise 7) the group axioms under multiplication and is called the *group of units* of  $A$ . For  $\mathbf{Z}$ , the group of units  $\mathbf{Z}^* = \{\pm 1\}$  is significantly smaller than  $\mathbf{Z}$ .

**Exercise 7.** Show that the product of two units in a ring  $A$  is a unit.

Commutative rings  $A$  for which we have  $A^* = A \setminus \{0\}$  are called *fields*. In a field, every element different from 0 is a unit. The best-known examples of fields are  $\mathbf{Q}$ ,  $\mathbf{R}$ , and  $\mathbf{C}$ .

The choice of the general ring axioms is motivated, in part, by the existence of the ring of integers  $\mathbf{Z}$ ; this ring is the “standard example” of a commutative ring. Other well-known examples of commutative rings are the rings  $\mathbf{R}[X]$  and  $\mathbf{C}[X]$  of polynomials with coefficients in  $\mathbf{R}$  or  $\mathbf{C}$ . These polynomials are added and multiplied as in analysis, and it is well known that the ring axioms apply. We will come back to this in detail in the course Algebra 2.

**Exercise 8.** Define the polynomial ring  $A[X]$  over an arbitrary commutative ring  $A$ , and verify that  $A[X]$  is a commutative ring.

### ► THE RING $\mathbf{Z}/n\mathbf{Z}$

We already saw in §1 that we can also multiply modulo  $n$ ; formally, this finding means that the group  $\mathbf{Z}/n\mathbf{Z}$  of residue classes modulo  $n$  “is” a ring, just like  $\mathbf{Z}$ .

**6.9. Theorem.** *Let  $n$  be an integer and  $\pi : \mathbf{Z} \rightarrow \mathbf{Z}/n\mathbf{Z}$  be the canonical group homomorphism. Then the multiplication  $\pi(x)\pi(y) = \pi(xy)$  makes the group  $\mathbf{Z}/n\mathbf{Z}$  into a ring.*

**Proof.** We have to show that the natural multiplication on  $\mathbf{Z}/n\mathbf{Z}$  is well defined; all ring properties then follow from those for  $\mathbf{Z}$ . If  $x \equiv x' \pmod{n}$  and  $y \equiv y' \pmod{n}$ , we have

$$(6.10) \quad xy - x'y' = x(y - y') + (x - x')y'.$$

The right-hand side is an element of  $n\mathbf{Z}$ ; after all,  $x - x'$  and  $y - y'$  are elements of  $n\mathbf{Z}$ . So we have  $xy \equiv x'y' \pmod{n}$ , as desired.  $\square$

A map  $f : A \rightarrow A'$  between rings is called a *ring homomorphism* if it is a homomorphism of the additive groups that moreover satisfies

- (1)  $f(1_A) = 1_{A'}$ ;
- (2)  $f(xy) = f(x)f(y)$  for  $x, y \in A$ .

If  $f$  is also bijective, then  $f$  is called a *ring isomorphism*.

**Exercise 9.** Give an example to show that, unlike in the case of groups, condition (1) does not follow from condition (2).

Theorem 6.9 is the “ring equivalent” of 4.14 for  $G = \mathbf{Z}$ . It says that for the given product on  $\mathbf{Z}/n\mathbf{Z}$ , the quotient map  $\pi : \mathbf{Z} \rightarrow \mathbf{Z}/n\mathbf{Z}$  is a ring homomorphism.

For  $n \neq 0$ , the *residue class ring*  $\mathbf{Z}/n\mathbf{Z}$  is a finite ring with  $|n|$  elements. Its group of units  $(\mathbf{Z}/n\mathbf{Z})^*$  is the group of *invertible residue classes modulo  $n$* . A residue class  $\bar{a} \in \mathbf{Z}/n\mathbf{Z}$  is invertible if there is an element  $\bar{x} \in \mathbf{Z}/n\mathbf{Z}$  such that  $\bar{a}\bar{x} = \bar{1}$ , which means that the equation  $ax = 1 + ny$  admits an integer solution. Right after (6.4), we noted that this is possible exactly when  $a$  and  $n$  are relatively prime, so we have

$$(6.11) \quad (\mathbf{Z}/n\mathbf{Z})^* = \{\bar{a} \in \mathbf{Z}/n\mathbf{Z} : \text{GCD}(a, n) = 1\}.$$

The order of the group  $(\mathbf{Z}/n\mathbf{Z})^*$  is denoted by  $\varphi(n)$ , and the function  $\varphi : \mathbf{Z}_{\geq 1} \rightarrow \mathbf{Z}$  is called *Euler’s  $\varphi$ -function*.

**Exercise 10.** Calculate  $\varphi(n)$  for  $n \leq 20$ .

If *all* residue classes different from  $\bar{0}$  are units in  $\mathbf{Z}/n\mathbf{Z}$ , then  $n$  is relatively prime to all numbers  $1, 2, 3, \dots, n-1$ , which means that  $n$  is prime.

**6.12. Theorem.** *The ring  $\mathbf{Z}/n\mathbf{Z}$  is a field if and only if  $n$  is prime.*

The finite fields  $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$  for the primes  $p$  resemble the more familiar fields  $\mathbf{R}$  and  $\mathbf{C}$  in several ways. For example, many theorems from linear algebra about matrices, determinants, and dimensions hold over arbitrary base fields, so that we can also work over  $\mathbf{F}_p$  instead of  $\mathbf{R}$  or  $\mathbf{C}$ . However, linear algebra over  $\mathbf{F}_p$  misses the natural notion of a distance, which depends on the positivity of an inner product  $\langle x, x \rangle$ . There are no positive or negative numbers in  $\mathbf{F}_p$ , and we also cannot speak of “large” or “small” elements in the sense of an absolute value. On the other hand, all finite-dimensional vector spaces over  $\mathbf{F}_p$  have only finitely many elements, so that we can often use *counting arguments*, which in turn is not possible for  $\mathbf{R}$  or  $\mathbf{C}$ . In this setting, we have what are also called *finite geometries*.

Over  $\mathbf{F}_p$ , there are only finitely many matrices of a given dimension, which means that the groups  $\text{GL}_n(\mathbf{F}_p)$  of invertible  $n \times n$  matrices with coefficients in  $\mathbf{F}_p$  are all finite. Such *finite groups of Lie type* are ubiquitous.

**Exercise 11.** Show that  $\text{GL}_2(\mathbf{F}_2)$  is isomorphic to  $S_3$ .

For composite numbers  $n$ , the rings  $\mathbf{Z}/n\mathbf{Z}$  behave differently from the fields  $\mathbf{R}$  and  $\mathbf{C}$  in many aspects. An identity such as  $\bar{2} \cdot \bar{2} = \bar{0} \in \mathbf{Z}/4\mathbf{Z}$  shows that a product of elements different from zero can be zero and that a linear equation such as  $\bar{2} \cdot \bar{x} = \bar{0} \in \mathbf{Z}/4\mathbf{Z}$  can have two different solutions  $\bar{x} = \bar{2}$  and  $\bar{x} = \bar{0}$ . In fact, we already saw something like this in §1: the quadratic equation  $\bar{x}^2 = \bar{1}$  has *four* solutions  $\bar{1}, \bar{3}, \bar{5},$  and  $\bar{7}$  in  $\mathbf{Z}/8\mathbf{Z}$ . This shows that “well-known facts” about the numbers of zeros of polynomials are not always true if we do arithmetic with coefficients in arbitrary commutative rings.

► ARITHMETIC MODULO  $n$

When doing arithmetic in the group  $(\mathbf{Z}/n\mathbf{Z})^*$ , it is convenient to have a way to determine inverses explicitly. This means that we must find a way to calculate GCDs and solve equation (6.4) explicitly.

**6.13. Euclidean algorithm.** For integers  $a$  and  $b$ , define the sequence of non-negative integers  $r_0, r_1, r_2, \dots$  by  $r_0 = |a|$ ,  $r_1 = |b|$ , and

$$r_{i+1} = (\text{remainder of } r_{i-1} \text{ when dividing by } r_i) \quad \text{if } r_i \neq 0.$$

Then there is an index  $k > 0$  with  $r_k = 0$ , and we have  $\text{GCD}(a, b) = r_{k-1}$ .

**Proof.** Since the numbers in the sequence  $r_1, r_2, \dots$  keep decreasing but never become negative, we must have  $r_k = 0$  for some  $k > 0$ . We then have  $r_{k-1} = \text{GCD}(r_{k-1}, 0) = \text{GCD}(r_{k-1}, r_k)$ , and since  $\text{GCD}(a, b) = \text{GCD}(r_0, r_1)$  clearly holds, it now suffices to prove the equalities  $\text{GCD}(r_0, r_1) = \text{GCD}(r_1, r_2) = \dots = \text{GCD}(r_{k-1}, r_k)$ .

The equalities mentioned here say that for natural numbers  $a$  and  $b \neq 0$  and the remainder  $r$  of  $a$  when dividing by  $b$ , we always have  $\text{GCD}(a, b) = \text{GCD}(b, r)$ . This is equivalent to the equality

$$a\mathbf{Z} + b\mathbf{Z} = b\mathbf{Z} + r\mathbf{Z}$$

of subgroups of  $\mathbf{Z}$ . To prove this, note that  $a = qb + r$  is contained in the right-hand side and  $r = a - qb$  is contained in the left-hand side.  $\square$

The *extended Euclidean algorithm* is a calculation as in 6.13 that gives not only the GCD of  $a$  and  $b$  but also a solution of equation (6.4). For this, we choose  $x_0 = \pm 1$  and  $y_0 = 0$ , as well as  $x_1 = 0$  and  $y_1 = \pm 1$ , such that the equations

$$\begin{aligned} x_0a + y_0b &= r_0 (= |a|), \\ x_1a + y_1b &= r_1 (= |b|) \end{aligned}$$

hold. The division with remainder in 6.13 gives us numbers  $q_i$  that satisfy  $r_{i-1} = q_i r_i + r_{i+1}$ . This means that from the two equations above, we can deduce a sequence of equations

$$x_i a + y_i b = r_i \quad \text{for } i = 0, 1, 2, \dots$$

in which the  $(i + 1)$ -st equation arises by subtracting the  $i$ -th equation  $q_i$  times from the  $(i - 1)$ -st. In other words, like  $r_i$ , the numbers  $x_i$  and  $y_i$  satisfy the relations  $x_{i-1} = q_i x_i + x_{i+1}$  and  $y_{i-1} = q_i y_i + y_{i+1}$ . If  $k$  is the index in 6.13 for which  $r_k = 0$  holds, then  $x_{k-1}a + y_{k-1}b = r_{k-1} = \text{GCD}(a, b)$  gives a solution of (6.4).

**Exercise 12.** Prove: if  $a$  and  $b$  are positive, we have  $x_i y_{i+1} - x_{i+1} y_i = (-1)^i$  for  $i = 0, 1, \dots, k - 1$ .

Calculating GCDs with the Euclidean algorithm is usually more efficient than the calculation in Exercise 20 using prime factorization. The underlying idea is applicable in other situations as well, and variants of the algorithm therefore appear in numerous computer implementations.

**6.14. Example.** For  $b = 12345$  and  $a = 56789$ , we find successively

$$\begin{array}{rcl}
 1 \cdot 56789 - & 0 \cdot 12345 = & 56789 \\
 -0 \cdot 56789 + & 1 \cdot 12345 = & 12345 \quad (q_1 = 4) \\
 1 \cdot 56789 - & 4 \cdot 12345 = & 7409 \quad (q_2 = 1) \\
 -1 \cdot 56789 + & 5 \cdot 12345 = & 4936 \quad (q_3 = 1) \\
 2 \cdot 56789 - & 9 \cdot 12345 = & 2473 \quad (q_4 = 1) \\
 -3 \cdot 56789 + & 14 \cdot 12345 = & 2463 \quad (q_5 = 1) \\
 5 \cdot 56789 - & 23 \cdot 12345 = & 10 \quad (q_6 = 246) \\
 -1233 \cdot 56789 + & 5672 \cdot 12345 = & 3 \quad (q_7 = 3) \\
 3704 \cdot 56789 - & 17039 \cdot 12345 = & 1.
 \end{array}$$

This calculation shows that 12345 and 56789 are relatively prime and tells us how to write their GCD as a “linear combination” of 12345 and 56789. The choice of a sign “ $-0$ ” at the beginning emphasizes the alternating character of the signs of  $x_i$  and  $y_i$ .

If we only want to determine the GCD, it suffices to carry out only the calculations on the right-hand side of the equalities in 6.13. The given calculation is also called an “extended GCD calculation.” If the GCD of  $a$  and  $b$  is equal to 1, then the “final values”  $x_{k-1}$  and  $y_{k-1}$  give the inverses of  $a$  modulo  $b$  and of  $b$  modulo  $a$ . (If we only need one of the inverses, we can leave out the “superfluous” column throughout the calculation.) In our example, we obtain

$$\begin{aligned}
 \overline{56789}^{-1} &= \overline{3704} \in (\mathbf{Z}/12345\mathbf{Z})^*, \\
 \overline{12345}^{-1} &= \overline{-17039} = \overline{39750} \in (\mathbf{Z}/56789\mathbf{Z})^*.
 \end{aligned}$$

Note that our calculation gives  $\gcd(12345, 56789) = 1$  but gives *no* information on the prime factors of either number.

**Exercise 13.** Determine the GCD of  $a =$  your phone number (without area code) and  $b =$  your date of birth (in the format YYMMDD, so write 920301 for March 1, 1992), and determine  $x, y \in \mathbf{Z}$  for which  $xa + yb$  is equal to this GCD.

To understand the structure of the ring  $\mathbf{Z}/n\mathbf{Z}$  and its group of units  $(\mathbf{Z}/n\mathbf{Z})^*$ , there is a classic theorem for “decomposing” the ring  $\mathbf{Z}/n\mathbf{Z}$  as a product of rings. A *product*  $A_1 \times A_2$  of rings  $A_1$  and  $A_2$  is defined in the obvious way, as it is for groups (Exercise 4.17): addition and multiplication are defined coordinatewise on the product set  $A_1 \times A_2$  as

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \quad \text{and} \quad (x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2).$$

It is easy to check that this gives the structure of a ring on  $A_1 \times A_2$ . Products of more than two rings are defined likewise.

**6.15. Chinese remainder theorem.** *Let  $m$  and  $n$  be relatively prime integers. Then the canonical map*

$$\begin{aligned}
 \psi : \quad \mathbf{Z}/mn\mathbf{Z} &\xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z} \\
 (x \bmod mn) &\longmapsto (x \bmod m, x \bmod n)
 \end{aligned}$$

is a ring isomorphism. The map  $\psi$  induces an isomorphism of the groups of units

$$\psi_* : (\mathbf{Z}/mn\mathbf{Z})^* \xrightarrow{\sim} (\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*,$$

and Euler's  $\varphi$ -function satisfies  $\varphi(mn) = \varphi(m)\varphi(n)$ .

**Proof.** First note that  $\psi$  is a well-defined ring homomorphism: if  $x, x' \in \mathbf{Z}$  satisfy  $x \equiv x' \pmod{mn}$ , then we have  $(x \pmod{m}, x \pmod{n}) = (x' \pmod{m}, x' \pmod{n})$ .

Since  $m$  and  $n$  are relatively prime, there exist  $r, s \in \mathbf{Z}$  with  $rm + sn = 1$ . The map  $\psi$  sends the residue classes of  $rm = 1 - sn$  and  $sn = 1 - rm$  to  $(\bar{0}, \bar{1})$  and  $(\bar{1}, \bar{0})$ , respectively. These elements generate the additive group  $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ , so  $\psi$  is surjective. Since  $\mathbf{Z}/mn\mathbf{Z}$  and  $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$  both have  $mn$  elements,  $\psi$  is also injective. We conclude that  $\psi$  is a ring isomorphism.

Under  $\psi$ , the group  $(\mathbf{Z}/mn\mathbf{Z})^*$  is mapped isomorphically onto the group of units of  $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ , which is equal to  $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$ . Comparing the orders gives the relation  $\varphi(mn) = \varphi(m)\varphi(n)$ .  $\square$

The proof of 6.15 shows how a solution of the equation  $rm + sn = 1$  can be used to find an element  $x \in \mathbf{Z}$  with  $\psi(x) = (a \pmod{m}, b \pmod{n})$ . After all, since  $\psi(sn) = (\bar{1}, \bar{0})$  and  $\psi(rm) = (\bar{0}, \bar{1})$ , we have  $\psi(asn + brm) = (\bar{a}, \bar{0}) + (\bar{0}, \bar{b}) = (\bar{a}, \bar{b})$ .

**Exercise 14.** Determine a number  $x \in \mathbf{Z}$  that satisfies the congruences  $x \equiv 12 \pmod{34}$  and  $x \equiv 45 \pmod{67}$ .

By repeatedly applying 6.15, we can deduce from the prime factorization of  $n$  a “decomposition” of the ring  $\mathbf{Z}/n\mathbf{Z}$  in rings of the form  $\mathbf{Z}/p^k\mathbf{Z}$  with  $p$  a prime.

**6.16. Corollary.** For every positive integer  $n$ , there is a natural ring isomorphism

$$\mathbf{Z}/n\mathbf{Z} \xrightarrow{\sim} \prod_{p|n} (\mathbf{Z}/p^{\text{ord}_p(n)}\mathbf{Z}).$$

Consequently, Euler's  $\varphi$ -function satisfies

$$\varphi(n) = \prod_{p|n} \varphi(p^{\text{ord}_p(n)}) = \prod_{p|n} (p-1)p^{\text{ord}_p(n)-1} = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

**Proof.** The first statement follows by repeatedly applying 6.15. By comparing the orders of the groups of units, we obtain  $\varphi(n) = \prod_{p|n} \varphi(p^{\text{ord}_p(n)})$ . By (6.11), the invertible residue classes  $\bar{a} \in \mathbf{Z}/p^k\mathbf{Z}$  for  $k \geq 1$  are the residue classes with  $p \nmid a$ . There are  $\frac{1}{p} \cdot p^k$  residue classes  $\bar{a}$  with  $p \mid a$ , which gives  $\varphi(p^k) = (1 - \frac{1}{p}) \cdot p^k = (p-1)p^{k-1}$ .  $\square$

#### ► EULER'S THEOREM AND FERMAT'S LITTLE THEOREM

In 4.9, we deduced from Lagrange's theorem that the order of an element of a finite group always divides the group order. If we apply this to the group  $(\mathbf{Z}/n\mathbf{Z})^*$ , we find a theorem discovered by Euler around 1750.

**6.17. Theorem.** For  $a$  and  $n \geq 1$  relatively prime, we have  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .  $\square$

The case where  $n$  is prime had already been studied by Fermat (1601–1665), who formulated the following specific case of 6.17 around 1640.

**6.18. Fermat’s little theorem.** *For  $p$  a prime and  $a$  an integer, we have*

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

**Proof.** For  $a \equiv 0 \pmod{p}$ , the statement is clear. For  $a \not\equiv 0 \pmod{p}$ , the integer  $a$  is relatively prime to  $p$ , and we have  $\bar{a}^{p-1} = \bar{1} \in (\mathbf{Z}/p\mathbf{Z})^*$  by 6.17. Multiplying by  $\bar{a}$  on both sides gives the desired result.  $\square$

The name of theorem 6.18 is meant to distinguish it from Fermat’s “great” or “last” theorem, which says that for  $n > 2$ , the equation  $x^n + y^n = z^n$  has no integer solutions other than the trivial ones with  $xyz = 0$ . This last theorem was proved in 1995 by the British mathematician Andrew Wiles.<sup>22</sup> The proof is considered a milestone in twentieth-century number theory.

The rings  $\mathbf{Z}/n\mathbf{Z}$  can often be used to prove that equations have no solutions in  $\mathbf{Z}$ . We saw this in (1.2) for the equation  $3x^2 + 2 = y^2$  and in Exercise 1.26 for the equation  $55x^3 + 3 = y^3$ . For given  $n$ , the solvability in  $\mathbf{Z}/n\mathbf{Z}$  can be determined in finitely many steps, and if we use the ring structure of  $\mathbf{Z}/n\mathbf{Z}$  efficiently, this calculation is often straightforward. In most cases, because of 6.16, the integer  $n$  is taken to be a prime or a power thereof. A difficult question here is what can be concluded from the fact that an equation has solutions modulo all prime powers. In some cases, it is possible to infer from the existence of all these so-called “local solutions” that a “global solution” exists in  $\mathbf{Z}$ . For example, already in 1785, the Frenchman Legendre (1752–1833) found that for any three pairwise relatively prime positive integers  $a, b, c$ , the quadratic equation

$$ax^2 + by^2 = cz^2$$

has an integer solution  $(x, y, z) \neq 0$  if and only if this is the case modulo all primes  $p$ . The situation is significantly more complicated for higher-degree equations, and here, substantial progress was not made until the 20th century. The obstructions that occur here against the so-called *local-global principle* have given rise to several as yet unsolved problems in number theory.<sup>23</sup>

## EXERCISES.

15. Let  $a$  and  $b$  be integers with  $d = \text{GCD}(a, b) \neq 0$ . Prove:  $a/d$  and  $b/d$  are relatively prime.
16. Show that the “quotient”  $q$  and the remainder  $r$  in 6.1 are uniquely determined by  $a$  and  $b$ .
17. Let  $b > 1$  be an integer. Prove that every positive integer  $a$  has a unique representation

$$a = c_t b^t + c_{t-1} b^{t-1} + \dots + c_1 b + c_0$$

with  $t$  a non-negative number that depends on  $a$ , “digits”  $c_i \in \{0, 1, 2, \dots, b-1\}$ , and  $c_t \neq 0$ . [This is called the representation in the  $b$ -adic number system.]

18. Prove that every integer  $a \neq 0$  has a unique representation

$$a = 3^t c_t + 3^{t-1} c_{t-1} + \dots + 3c_1 + c_0$$

with  $t$  a non-negative number that depends on  $a$ , “digits”  $c_i \in \{-1, 0, 1\}$ , and  $c_t \neq 0$ . Do the same for the representations

$$a = 2^t c_t + 2^{t-1} c_{t-1} + \dots + 2c_1 + c_0$$

with “digits”  $c_i \in \{-1, 0, 1\}$  that satisfy  $c_t \neq 0$  and  $c_i c_{i+1} = 0$  for  $i = 0, 1, \dots, t-1$ .

19. The sequence 1, 1, 2, 3, 5, 8, 13, ... of *Fibonacci numbers* is defined recursively by  $x_1 = x_2 = 1$  and  $x_{n+2} = x_{n+1} + x_n$  for  $n \geq 1$ . Prove that two consecutive Fibonacci numbers are relatively prime. Do we also always have  $\text{GCD}(x_n, x_{n+2}) = 1$ ?
20. Show that the GCD and LCM of the numbers  $a = \prod_{p \in \mathcal{P}} p^{m_p}$  and  $b = \prod_{p \in \mathcal{P}} p^{n_p}$  are equal to, respectively,

$$\prod_{p \in \mathcal{P}} p^{\min(m_p, n_p)} \quad \text{and} \quad \prod_{p \in \mathcal{P}} p^{\max(m_p, n_p)}.$$

Conclude that for integers  $a$  and  $b$ , we have  $|ab| = \text{GCD}(a, b) \cdot \text{LCM}(a, b)$ .

21. Can we calculate  $\text{LCM}(a, b)$  without factoring  $a$  and  $b$  explicitly?
22. Calculate the GCD and the LCM of  $a = 10000010$  and  $b = 10000020$ .
23. Show that every rational number  $q \in \mathbf{Q}^*$  can be written uniquely as  $\varepsilon \prod_{p \in \mathcal{P}} p^{n_p}$  with  $\varepsilon \in \{\pm 1\}$  and numbers  $n_p \in \mathbf{Z}$  that are non-zero for only finitely many  $p$ .
24. Show that there exist infinitely many primes  $p \equiv 3 \pmod{4}$ .  
[Hint: imitate Euclid’s proof of 6.5.]
25. Let  $n$  be an integer of the form  $n = x^2 + 1$  with  $x \in \mathbf{Z}$  and  $p$  be an odd prime divisor of  $n$ . Prove:  $p \equiv 1 \pmod{4}$ .
26. Show that there exist infinitely many primes  $p \equiv 1 \pmod{4}$ .
27. Show that there exist infinitely many primes  $p \equiv 2 \pmod{3}$  and also that there exist<sup>24</sup> infinitely many primes  $p \equiv 1 \pmod{3}$ .
28. Let  $a > 1$  and  $k > 1$  be numbers such that  $a^k - 1$  is prime. Prove:  $a = 2$ , and  $k$  is prime. Are all numbers of the form  $2^p - 1$  with  $p$  prime themselves prime?  
[Primes of the form  $2^p - 1$  are called *Mersenne primes*.<sup>25</sup>]

29. Let  $a$  and  $b \neq 0$  be natural numbers and  $r$  be the remainder of  $a$  when dividing by  $b$ . Prove that for every integer  $t > 1$ , the remainder of  $t^a - 1$  when dividing by  $t^b - 1$  is equal to  $t^r - 1$ . Conclude that  $\text{GCD}(t^a - 1, t^b - 1) = t^{\text{GCD}(a,b)} - 1$ .
30. Let  $k \geq 1$  be an integer such that  $2^k + 1$  is prime. Prove:  $k = 2^n$  for some  $n$ . Are all numbers of the form  $2^{2^n} + 1$  prime?  
[The number  $F_n = 2^{2^n} + 1$  is called the  $n$ -th *Fermat number*.<sup>26</sup>]
31. Let  $n$  be positive and  $p$  be a prime divisor of  $F_n = 2^{2^n} + 1$ . Prove that  $\bar{2} \in (\mathbf{Z}/F_n\mathbf{Z})^*$  is an element of order  $2^{n+1}$ . Deduce that  $p \equiv 1 \pmod{2^{n+1}}$ .
32. Take  $n > 1$  and  $p$  and  $F_n$  as in the previous exercise, and define  $u = 2^{2^{n-2}} \pmod{F_n}$ . Prove that  $u$  has order 8 in  $(\mathbf{Z}/F_n\mathbf{Z})^*$  and that  $u - u^3$  has order  $2^{n+2}$ . Deduce that  $p \equiv 1 \pmod{2^{n+2}}$ .  
[For  $n = 5$ , it follows that  $p \equiv 1 \pmod{128}$ . The two smallest values are  $p = 257$  and  $p = 641$ .]
33. For all  $n \geq 1$ , determine the order of  $F_{n-1} \pmod{F_n}$  in  $(\mathbf{Z}/F_n\mathbf{Z})^*$ .
34. Let  $p$  be a prime and  $q$  be a prime divisor of the Mersenne number  $M_p = 2^p - 1$ . Prove:  $q \equiv 1 \pmod{p}$ .  
[Example:  $M_{11} = 2047 = 23 \cdot 89$  only has prime divisors that are  $1 \pmod{11}$ .]
35. Prove that every integer  $a$  satisfies the congruence  $a^{13} \equiv a \pmod{2730}$ .
36. Show that for every element  $x \in (\mathbf{Z}/7161\mathbf{Z})^*$ , the order of  $x$  is a divisor of 30. Does there exist an element  $x \in (\mathbf{Z}/7161\mathbf{Z})^*$  of order 30?
37. Prove:  $\varphi(5186) = \varphi(5187) = \varphi(5188)$ . Do we have  $\lim_{n \rightarrow \infty} \varphi(n) = \infty$ ?
38. Determine all  $n > 0$  with  $\varphi(n) = 8$ . Do likewise for  $\varphi(n) = 14$ .
39. Let  $m, n > 0$  satisfy  $\frac{\varphi(m)}{m} = \frac{\varphi(n)}{n}$ . Prove that  $m$  and  $n$  have the same prime divisors.
40. Determine all  $n > 0$  such that  $\frac{n}{\varphi(n)}$  is an integer.
41. Determine an integer  $x$  that satisfies the congruences

$$\begin{aligned}x &\equiv 1 \pmod{7}, \\x &\equiv 5 \pmod{11}, \\x &\equiv 1 \pmod{13}.\end{aligned}$$

To what extent is your answer uniquely determined?

42. Let  $G$  be cyclic of order  $n$ . Show that the number of elements of  $G$  that generate the group is equal to  $\varphi(n)$ . Deduce that  $\text{Aut}(G) \cong (\mathbf{Z}/n\mathbf{Z})^*$ .
43. Show that for every divisor  $d \mid n$ , a cyclic group of order  $n$  contains exactly  $\varphi(d)$  elements of order  $d$ . Use this to prove *Gauss's formula*:  $\sum_{d \mid n} \varphi(d) = n$ .
44. Determine for which primes  $p < 20$  the group  $(\mathbf{Z}/p\mathbf{Z})^*$  is cyclic.
45. Let  $p$  be a prime. Prove that the binomial coefficients  $\binom{p}{i}$  for  $1 \leq i \leq p-1$  are divisible by  $p$ , and deduce the congruence  $(x+y)^p \equiv x^p + y^p \pmod{p}$  for  $x, y \in \mathbf{Z}$ . Now, take  $y = 1$ , and prove the congruence  $x^p \equiv x \pmod{p}$  from 6.18 by induction on  $x$ .
46. Determine the smallest composite number  $n$  that satisfies the congruence  $2^n \equiv 2 \pmod{n}$ .  
[Anyone who can program will be done quickly...]

47. Show that  $\text{GL}_n(\mathbf{F}_p)$  is a group of order  $(p^n - 1)(p^n - p)(p^n - p^2) \dots (p^n - p^{n-1})$ .
48. (Exercise 2.22 without a star) Show that the subgroup  $G \subset \text{GL}_3(\mathbf{F}_3)$  given by

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{F}_3 \right\}$$

is a non-abelian group of order 27 and that  $x^3 = \text{id}$  holds for all  $x \in G$ .

49. Let  $m$  and  $n$  be positive numbers with  $d = \text{GCD}(m, n)$  and  $k = \text{LCM}(m, n)$ . Prove that the rings  $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$  and  $\mathbf{Z}/d\mathbf{Z} \times \mathbf{Z}/k\mathbf{Z}$  are isomorphic.
50. Show that the fact that the additive group of a ring  $R$  is abelian follows from the ring axioms (R1)–(R3).  
[Hint: look at  $(1+1)(a+b)$ .]
51. Let  $A$  be a ring and  $H \subset A$  be a subgroup of the additive group of  $A$ . Show that  $A/H$  can be made into a ring and the quotient map  $\pi : A \rightarrow A/H$  into a ring homomorphism if  $H$  satisfies the property

$$(*) \quad \text{for } a \in A \text{ and } h \in H, \text{ we have } ah \in H \text{ and } ha \in H.$$

[Hint: look at (6.10). The subgroups in question are called *ideals* of  $A$ .]

52. State and prove the analog of the isomorphism theorem 4.10 for rings.
53. Let  $A = \mathbf{R}[X]$  be the ring of polynomials with coefficients in  $\mathbf{R}$ . Prove:  $A^* = \mathbf{R}^*$ .
54. Let  $A = (\mathbf{Z}/4\mathbf{Z})[X]$  be the ring of polynomials with coefficients in  $\mathbf{Z}/4\mathbf{Z}$ . Prove: for all  $f \in A$ , we have  $1 + 2f \in A^*$ . Conclude that  $A^*$  is an infinite group and therefore not equal to  $(\mathbf{Z}/4\mathbf{Z})^*$ .
55. Show that for elements  $x$  and  $y$  in a field, we have  $xy = 0 \Rightarrow x = 0$  or  $y = 0$ .
- \*56. Let  $A = K[X]$  be the polynomial ring over a field  $K$ . Let  $f, g \in A$  be polynomials with  $g \neq 0$ . Prove that there exist polynomials  $q, r \in A$  with

$$f = qg + r \quad \text{and} \quad r = 0 \quad \text{or} \quad \deg(r) < \deg(g).$$

Deduce from this that for any two polynomials  $a, b \in A$ , there exists a polynomial  $d \in A$  such that  $aA + bA = \{ax + by : x, y \in A\}$  is equal to  $dA = \{dx : x \in A\}$ .

- \*57. Let  $K$  be a field. A non-constant polynomial  $f \in A = K[X]$  is called *irreducible* if it cannot be written as a product of two non-constant polynomials. Prove that an irreducible polynomial  $p \in A$  has the *prime property*:  $p \mid ab \Rightarrow p \mid a$  or  $p \mid b$ . The divisibility of polynomials is defined in the usual way.
- \*58. Let  $K$  be a field. Prove that every non-constant polynomial  $f \in K[X]$  can be written as a product of irreducible polynomials and that this product is unique up to the order of the factors and multiplication by constants.
59. Let  $n \in \mathbf{Z}$  be a square, and suppose that the last four digits of  $n$  in decimal notation are equal. Prove that  $n$  ends in four zeros. Does the same hold with “four” replaced by “three” both times?
60. Show that for every  $m \in \mathbf{Z}_{>0}$ , the equation  $\varphi(n) = m!$  has a solution  $n \in \mathbf{Z}_{>0}$ .

## 7 FACTORIZATION AND CRYPTOGRAPHY.

This section, which has a slightly different character than the other sections in these course notes, gives some applications of Euler's theorem 6.17 and Fermat's little theorem 6.18. These applications use the existence of computer equipment to quickly carry out elementary operations on large numbers. Some of the exercises assume that the reader has access to a somewhat advanced computation program such as Maple, Mathematica, Magma, or SAGE to routinely do calculations with large integers or modulo a number  $n$ .

### ► PRIMALITY OF LARGE NUMBERS

We begin by applying Fermat's little theorem to recognizing large primes. This skill will come in handy later.

Theorem 6.18 implies that if a number  $n$  is prime, then for all positive numbers  $a < n$ , we have the congruence  $a^{n-1} \equiv 1 \pmod{n}$ . This congruence can be tested "quickly" *without* first computing the often indecipherably large number  $a^{n-1}$ . Namely, we can use the binary notation for the exponent  $n - 1$ , writing it as a sum  $n - 1 = \sum_{k=0}^N c_k 2^k$  with digits  $c_k \in \{0, 1\}$ . We can calculate the powers  $\bar{a}^{2^k}$  for  $k = 0, 1, \dots, N$  by *repeatedly squaring*  $\bar{a}$ . Since the answer can be reduced modulo  $n$  after every squaring, no numbers greater than  $n^2$  occur in this process. The binary representation of  $n - 1$  shows which powers  $\bar{a}^{2^k}$  must be multiplied to obtain  $\bar{a}^{n-1}$ . These are no more than  $N + 1$  powers, and we can reduce modulo  $n$  after every multiplication. We conclude that we need at most  $2N + 2$  multiplications modulo  $n$ . Since  $N$  is not greater than  $2 \log n$ , the number of multiplications grows only logarithmically with  $n$ . In *complexity theory*, a subject on the boundary of mathematics and computer science that studies the behavior of algorithms, calculations whose "time" is bounded by a polynomial expression in the length of the input are said to be of *polynomial time*, or *polynomial* for short. This notion corresponds reasonably well to "efficient in practice." Testing a "Fermat congruence," for which the order of size of the length of the input  $(a, n)$  (in decimal or binary representation) is  $\log n$ , is polynomial in this terminology.

**7.1. Example.** Let us test whether  $n = 250093$  is prime. The number has no very small prime factors, so we check whether  $3^{250092} \equiv 1 \pmod{n}$  holds. To do this, we write the exponent 250092 as the 18-digit binary number

$$250092 = 111101000011101100_2.$$

By repeatedly squaring  $3 \pmod{250093}$ , we find the powers  $3^{2^k} \pmod{250093}$  for  $k = 0, 1, 2, \dots, 17$ . We need the ten values corresponding to  $k = 2, 3, 5, 6, 7, 12, 14, 15, 16$ , and 17. These are the residue classes of, respectively,

$$81, \quad 6561, \quad 174643, \quad 85634, \quad 205103, \quad 39836, \quad 49857, \quad 46122, \quad 197919, \quad 114064.$$

We multiply these, reducing the outcome modulo  $n$  after each multiplication. The result is  $187705 \pmod{250093}$ . We conclude that  $n$  is not prime. However, this does not give a factor of  $n$ .

**Exercise 1.** Verify that  $3^{250092}$  has more than 100 000 decimals.

If for a number  $n$ , we find that for a few randomly chosen values of  $a$ , we have  $\bar{a}^{n-1} \equiv 1 \pmod{n}$ , then this is a strong indication that  $n$  is prime. However, this does not give a *proof* that  $n$  is prime. More importantly, there are composite numbers  $n$ , the so-called *Carmichael numbers*, for which the Fermat congruence  $a^n \equiv a \pmod{n}$  from 6.18 holds for all  $a \in \mathbf{Z}$ . For such  $n$ , we have  $\bar{a}^{n-1} = \bar{1}$  for all  $\bar{a} \in (\mathbf{Z}/n\mathbf{Z})^*$ . Carmichael numbers are quite rare, but it has been known since 1992 that there are infinitely many.<sup>27</sup>

**Exercise 2.** Verify that  $n = 3 \cdot 11 \cdot 17 = 561$  and  $1729 = 7 \cdot 13 \cdot 19$  are Carmichael numbers.

Aside from the problems with any inverse of 6.18, testing any congruence for *all*  $a \pmod{n}$  is as much work as trying all divisors of  $n$  and therefore not practical. So we can often use the Fermat congruence to prove that certain numbers are composite but seldom that they are prime. To prove that a number  $p$  is prime, we need to show that  $(\mathbf{Z}/p\mathbf{Z})^*$  has order  $p - 1$  and not only that there are many elements in  $(\mathbf{Z}/p\mathbf{Z})^*$  whose order divides  $p - 1$ . So in practice, often variants of the Fermat congruence are applied that lead to what is also called a *pseudoprime test*. For these slightly more subtle congruences, it has been proved that if  $n$  is not prime, then for at least half of all  $a < n$ , the test congruence does *not* hold. This gives a *probabilistic method* to test the primality of  $n$ . After all, if  $n$  is composite, the probability of finding  $k$  different values of  $a$  in a row that satisfy the congruence is less than  $2^{-k}$ . For example, for  $k = 10$ , the probability that a composite  $n$  passes the test is less than 1 in 1000. To be sure, take  $k = 50$ ; the probability of a mistake caused by an error in the hardware is usually greater than the probability of 50 consecutive unfortunate choices for  $a$ . However, the probability for such algorithms is never 0.

There are primality tests that require a little more time but give a true *primality proof* for  $n$  if  $n$  is prime. Whether this can be done in polynomial time has long remained open. It was not until 2002 that the Indian computer scientists Agrawal, Kayal, and Saxena found a deterministic method, called the AKS-primality test using their initials, which they proved to be polynomial. Older methods, which use relatively advanced mathematics such as *elliptic curves* and *cyclotomic fields*, were already fast enough that the primality of numbers with several thousand digits could be proved using them.<sup>28</sup>

Large primes are not only easy to recognize; they are also easy to *make* in practice. Indeed, there is the following quantitative version of Euclid's theorem 6.5.

**7.2. Prime theorem.** Let  $\pi(x)$  be the number of primes less than  $x \in \mathbf{R}$ . Then we have

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log x}{x} = 1.$$

This famous theorem, already conjectured by Gauss before 1800, was only proved in 1896, by the French mathematician Hadamard (1865–1963) and the Belgian mathematician de la Vallée-Poussin (1866–1962). The proof applies complex-analytic arguments to the *Riemann zeta function*, which for  $s > 1$  is defined by  $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$  and has a natural continuation to  $\mathbf{C} \setminus \{1\}$ . This is beyond the scope of this course.<sup>29</sup>

The prime number theorem is often written as  $\pi(x) \sim x/\log x$ , where the symbol  $\sim$  means that the quotient of the two functions approaches 1 as  $x \rightarrow \infty$ . Based on this theorem, we expect that in the neighborhood of a large number  $x$ , approximately 1 in  $\log x$  numbers is prime. For  $x = 10^{100}$ , this is 1 in  $100 \log(10) \approx 230$ . There is no theorem that guarantees that prime numbers are not occasionally unexpectedly far apart; hence it may happen, in principle, that after  $10^{100}$ , there is a large “gap” in the prime numbers. In practice, however, there are never any problems. For example, the first ten primes after  $10^{100}$  are the numbers  $10^{100} + k$  with  $k = 267, 949, 1243, 1293, 1983, 2773, 2809, 2911, 2967, \text{ and } 3469$ , which lie at intervals ranging from 790 to 36. We summarize the above in the following informal way.

**7.3. Fact.** *Large primes are easy to make.*

► LARGE NUMBER FACTORIZATION

The fact that we can easily determine whether a large number is prime does not mean that if the number is composite, we can easily decompose it in factors. For instance, the number in Example 7.1 has decomposition  $250093 = 449 \cdot 557$ , but that does not follow from our “compositeness proof.” In this case, the prime divisors are so small that they can easily be found using the method of *trial division* outlined after 6.7. However, this method is not polynomial in the sense of complexity theory; for numbers without small prime factors, it is *exponential*. Indeed, in the worst case, all divisors  $d \leq \sqrt{n}$  of  $n$  must be tested. In practice, trial division is therefore often completely unfeasible. For example, if we have a number  $n$  with 100 digits that is a product of two approximately equally sized primes and a fast computer that can test a trillion divisors per second, this method takes roughly  $10^{50}/10^{12} = 10^{38}$  seconds. To get an idea of what such large numbers represent, note that there are about  $3 \cdot 10^7$  seconds in a year; on average, a human life lasts well over  $2 \cdot 10^9$  seconds; and the estimated age of the universe is around  $10^{18}$  seconds. This shows that trial division for numbers without small prime factors has no practical value.

The cryptographic application of Euler’s theorem we will now give is, in a sense, a negative application. It relies on the fact that we *cannot*, for the time being, factor properly and will cease to exist upon the discovery of an efficient factorization algorithm.

**7.4. Carpenter’s wisdom.** *The decomposition of large integers is difficult.*

In more mathematical terms, the wisdom above means that the best algorithms we currently have to factor numbers  $n$  have a running time that is far from polynomial for “many”  $n$ . In practical terms, this means that no one can factor composite numbers with a few hundred digits without “easy” prime factors. Easy prime factors are factors  $p$  that are sufficiently small to be quickly found by trial division or other exponential methods.

► CRYPTOGRAPHY

*Cryptography* owes its existence to the fact that there is a need to send messages in such

a way that anyone other than the recipient cannot understand the message if it somehow falls into wrong hands. In other words, the message must be sent in *code*, and no one except the recipient must be able to decrypt it. The oldest applications of cryptography are military, but nowadays, it is applied in far more areas. Modern communication techniques such as mobile telephony, online banking, and online shopping require the large-scale routine encryption of information sent through more or less public channels. The *RSA cryptosystem*, named after its discoverers Rivest, Shamir, and Adleman, who proposed the method in 1976, is a standard method for this. It is an example of a *public key cryptosystem*. This means that, unlike in more traditional cryptosystems, the key and the method for encoding messages are public. This has the advantage, which is undoubtedly extremely practical in many modern applications, that there is *no* need for a secret key to be agreed upon in advance between the sender and recipient, with all the security problems that entails. The amazing thing is that even with this apparent lack of secrets, information can *still* be sent that is virtually unreadable to third parties.

► THE RSA CRYPTOSYSTEM

In the RSA system, we assume that the message to be sent consists of one or more numbers of a fixed size, say 300 digits. For “letter messages,” the words can, for example, be “digitized” as numbers by using a simple substitution ( $a = 01$ ,  $b = 02$ ,  $c = 03$ , through space = 27; there is even room for 100 characters) and cutting up the resulting long number into blocks with 300 digits. Someone who wants to receive messages not readable by anyone else chooses two numbers that are made public, for example by publishing them on a personal website. The first number is the personal *modulus*  $n$ . This is a number  $n > 10^{300}$  that the recipient makes by multiplying two large primes of, say, 150 digits each. The factorization  $n = pq$  is kept secret, and unless the choice of  $p$  and  $q$  is extremely awkward, with the current state of affairs, this means that no one else can find the values of  $p$  and  $q$ .

**Exercise 3.** Why is the choice  $n = (10^{150} + 67)(10^{150} + 427)$ , the product of the two smallest primes with 151 digits, not safe? More generally, is it wise to choose two consecutive primes?

The second number the recipient discloses is the *public exponent*. This is a number  $e > 1$  whose most important property is that it is relatively prime to  $(p - 1)(q - 1)$ . This can be, for example, the smallest prime that does not divide  $(p - 1)(q - 1)$ , but in principle, every other number for which the Euclidean algorithm shows that it is relatively prime to  $(p - 1)(q - 1)$  is good.<sup>30</sup> We now use the following corollary of Euler’s theorem 6.17.

**7.5. Theorem.** *Let  $n = pq$  be a product of two distinct primes  $p$  and  $q$ , and let  $e > 1$  be a number that is relatively prime to  $(p - 1)(q - 1)$ . Then there exists a number  $f > 0$  with  $ef \equiv 1 \pmod{(p - 1)(q - 1)}$ , and for such an  $f$ , we have*

$$a^{ef} \equiv a \pmod{n}$$

for all  $a \in \mathbf{Z}$ .

**Proof.** Since  $e$  is invertible modulo  $(p-1)(q-1)$ , there exist positive numbers  $f$  with the stated property. For such  $f$ , we can write  $ef = 1 + r(p-1)(q-1)$  with  $r \in \mathbf{Z}$ . By 6.16, we have  $\varphi(pq) = (p-1)(q-1)$ . Using 6.17 applied to  $n = pq$ , we now obtain  $a^{ef} = a \cdot a^{r(p-1)(q-1)} \equiv a \pmod{n}$  for all  $a$  that are relatively prime to  $n = pq$ . If  $a$  is divisible by  $p$  or  $q$ , then it easily follows from the proof of 6.18 that the congruence also holds.  $\square$

**Exercise 4.** Show that 7.5 also holds if we require  $ef \equiv 1 \pmod{\text{LCM}(p-1, q-1)}$ .

To send a secret message  $N$  with 300 digits to a recipient with modulus  $n$  and public exponent  $e$ , we compute the number  $N^e \pmod{n}$ . As we have already seen, this can be done efficiently by repeatedly squaring modulo  $n$ , and it is never necessary to compute a large number like  $N^e$ . For the system to work, no one other than the recipient must be able to deduce the value of  $N \pmod{n}$  from that of  $N^e \pmod{n}$ . (Note that once we have  $N \pmod{n}$ , we also have  $N$  itself because we chose  $0 < N < n$ .) This relies on the fact that in practice, the only known way to deduce the value of  $N \pmod{n}$  from the value of  $N^e$  consists in determining an “inverse exponent”  $f$  as in Theorem 7.5. Indeed, using the inverse exponent  $f$ , we can recover the original message  $N < n$  through a second exponentiation:  $(N^e)^f \equiv N \pmod{n}$ . Other possible methods, such as trying out exponents, cost way too much time.

Finding the inverse exponent  $f$  in 7.5 consists in finding the inverse of  $e$  modulo  $(p-1)(q-1)$ , and no one can do this other than the recipient, who knows the values of  $p$  and  $q$ . Even the message’s sender, who knows not only  $N^e$  but also  $N$ , cannot find the inverse exponent  $f$ . So the recipient can guarantee the “unreadability” of all received messages by choosing the values of  $p$  and  $q$  wisely and keeping the “secret exponent”  $f$  secret.

**Exercise 5.** Show how to determine the factors  $p$  and  $q$  from  $n = pq$  and  $m = (p-1)(q-1)$ . Factor  $250093 = pq$  using the value  $249088 = (p-1)(q-1)$ .

**7.6. Example.** Suppose that we want to send the message “OK” to a recipient with public exponent 23 and (unrealistically small) modulus 250093. We digitize the message as indicated as 1511 and calculate  $1511^{23} \equiv 141886 \pmod{250093}$ . The number 141886 is now sent. The recipient, who has the factorization  $250093 = 449 \cdot 557$ , knows the inverse of 23 modulo  $448 \cdot 556 = 249088$ , which is  $f = 129959$ . The calculation  $141886^{129959} \equiv 1511 \pmod{250093}$  is easily obtained and gives the original message  $1511 = \text{OK}$ .

**Exercise 6.** Suppose that the recipient has public modulus 1111 and exponent 29. Decode the sent message 607.

## ► DIGITAL SIGNATURES

There is a refinement of the *RSA protocol* described above where the sender  $A$  also *proves* the message was sent by  $A$  and not by an impostor posing as  $A$ . Imagine the situation where the recipient  $B$  is a bank and  $A$  is someone who sends payment orders. The bank would then like to see a “digital signature” from  $A$  under those orders.

For this refinement, we need not only the public exponent  $e_B$  and modulus  $n_B$  of the recipient  $B$  but also similar values  $e_A$  and  $n_A$  chosen by  $A$ . Here  $B$  is the only person

who can decompose  $n_B$ , and  $A$  is the only person who can decompose  $n_A$ . Suppose that we want to send a message  $N < n_A < n_B$ . To digitize a secret message  $N$ , person  $A$  first replaces  $N$  with a number  $M < n_A$  satisfying  $M \equiv N^{f_A} \pmod{n_A}$ . Here  $f_A$  is  $A$ 's secret exponent, known to no one else than  $A$ . The sender  $A$  now transmits  $M$  as before. This means that  $A$  sends the value  $M^{e_B} \pmod{n_B}$  to  $B$ . Person  $B$  can raise this to the power of their own secret exponent to deduce the value of  $M$  and thus knows the number  $N^{f_A} \pmod{n_A}$ . To now obtain the original message,  $B$  takes the public exponent  $e_A$  and calculates the  $e_A$ -th power of  $N^{f_A} \pmod{n_A}$  modulo the modulus  $n_A$ . This is  $N^{e_A f_A} = N \pmod{n_A}$ , which gives  $N$ . Moreover,  $B$  now knows that the message comes from  $A$  because no one other than  $A$  can raise the message to the power of the secret exponent  $f_A$  modulo  $n_A$ .

**Exercise 7.** Is the assumption  $n_A < n_B$  essential?

### ► SAFETY OF RSA

The safety of the RSA protocol relies on the assumption that no one can factor a well-chosen 300-digit modulus without additional knowledge. When the RSA system was introduced, in 1976, Rivest included an encoded message as a challenge. He used the “secure” 129-digit number

$$\text{RSA}_{129} = 1143816257578888676692357799761466120102182967212423625625618429 \backslash \\ 35706935245733897830597123563958705058989075147599290026879543541$$

and said that he expected that the many millions of years of computer time needed to factor this number would make this code practically unbreakable. Making predictions turns out to be difficult here; the methods for decomposing large numbers have drastically improved in the last 50 years.

In 1994, the number was factored using a method known as the *quadratic sieve*, giving

$$\text{RSA}_{129} = 3490529510847650949147849619903898133417764638493387843990820577 \cdot \\ 32769132993266709549961988190834461413177642967992942539798288533.$$

This method uses many thousands of “auxiliary factorizations” contributed by computer owners via email. Using the “number field sieve” developed in the early 1990s, in 1996, the next “RSA challenge,” the 130-digit RSA key  $\text{RSA}_{130}$ , was cracked.<sup>31</sup> The number field sieve is a slightly more complicated algorithm that uses the arithmetic of number fields. The optimization took some time, but it is now the method that sets all records. In December 2009, a milestone was reached when the first 768-bit key (232 decimal digits) was cracked, and in 2020  $\text{RSA}_{250}$  was cracked with the number field sieve. The 1024-bit keys (309 decimal digits) initially used by banks have already been replaced by 2048-bit keys.

The quantum computer<sup>32</sup>, which does not yet exist in a serious form, but for which Peter Shor showed in 1994 that it can in principle factor numbers in polynomial

time, has led to a transition in cryptography starting around 2015. One now prefers quantum resistant protocols that, unlike RSA, do not depend on the alleged difficulty of factoring integers.

► DISCRETE LOGARITHMS

If someday, an efficient factorization algorithm is found that renders RSA useless as a cryptosystem, there are various other public key cryptosystems that can still be used. What is needed to make such systems is a mathematical procedure that is easy to carry out in one direction but for which the “converse” is disproportionately more difficult. The multiplication of primes  $p$  and  $q$  to obtain a large number  $n$  is such a procedure for RSA since the converse, the decomposition of  $n$  in  $p$  and  $q$ , is not something we have a fast algorithm for.

In group theory, there is a similar problem that is entirely within the scope of these course notes, namely determining *discrete logarithms*. This appears to be a challenging problem in some groups, but as in the case of factorization, there is no *theorem* that a fast algorithm does not exist; perhaps we are clumsy, and a smart algorithm is just around the corner for whoever knows enough mathematics!

Let  $G$  be a cyclic group of order  $n$  and  $g$  be a generator of  $G$ . Then the isomorphism

$$\begin{aligned} f : \mathbf{Z}/n\mathbf{Z} &\xrightarrow{\sim} G \\ k &\longmapsto g^k \end{aligned}$$

is a map for which the input  $k$  has length  $\log n$  and the output  $g^a$  can be calculated in time polynomial in  $\log n$  for many groups  $G$ . The discrete logarithm problem in the group  $G$  consists in calculating the *inverse* of  $f$ . In other words, given an element  $h \in G$ , determine an exponent  $k = f^{-1}(h) \in \mathbf{Z}/n\mathbf{Z}$  such that we have  $g^k = h$ . The exponent  $k = f^{-1}(h)$  is called the *discrete logarithm* of  $h \in G$  to the base  $g$  and is written as

$$k = f^{-1}(h) = \log_g(h).$$

The difficulty in computing  $f^{-1}$  depends very much on the choice of  $G$ . For example, if  $G = \mathbf{Z}/n\mathbf{Z}$  and  $g = 1 \pmod n$ , then  $f$  is the identity, and there is no problem. If we take another generator  $x$  for the additive group  $G = \mathbf{Z}/n\mathbf{Z}$ , then the discrete logarithm problem for  $h \in \mathbf{Z}/n\mathbf{Z}$  is nothing but solving  $k$  from the equation  $kx = h$ . To do this, it suffices to multiply both sides by the *multiplicative* inverse  $x^{-1}$  of  $x$  modulo  $n$ ; this inverse can be calculated using the Euclidean algorithm, as in 6.14. In this case, the discrete logarithm problem can be solved in time polynomial in  $\log n$ .

**Exercise 8.** Let  $g_1$  and  $g_2$  be generators of  $G$ . Prove:  $\log_{g_2}(h) = \log_{g_1}(h) \log_{g_2}(g_1)$ .

An interesting choice for  $G$  is the multiplicative group  $G = (\mathbf{Z}/p\mathbf{Z})^*$  modulo a prime  $p$ ; this group has order  $n = p - 1$ .

**7.7. Theorem.** For a prime  $p$ , the group  $(\mathbf{Z}/p\mathbf{Z})^*$  is cyclic of order  $p - 1$ .

The proof of 7.7 relies on a fact that has more to do with rings than with groups. We will see it again in 12.3 and 12.4.

**7.8. Lemma.** Let  $f = X^n + a_{n-1}X^{n-1} + \dots + a_1X + a_0$  be a polynomial of degree  $n \geq 1$  with coefficients in  $\mathbf{Z}/p\mathbf{Z}$ . Then  $f$  has no more than  $n$  zeros in  $\mathbf{Z}/p\mathbf{Z}$ .

**Proof.** We carry out the proof by induction on the degree of  $f$ . For  $n = 1$  and  $f = X + a_0$ ,  $-a_0$  is the only zero: inverses in the additive group  $\mathbf{Z}/p\mathbf{Z}$  are unique!

Now, let  $f$  be of degree  $n > 1$  and  $x \in \mathbf{Z}/p\mathbf{Z}$  be a zero of  $f$ . Then we can write  $f$  as  $f = (X - x)g$  for a polynomial  $g$  of degree  $\leq n - 1$ . After all, since  $X^k - x^k$  is divisible by  $X - x$  for  $k \geq 1$ , we have, explicitly,

$$f(X) = f(X) - f(x) = \sum_{k=0}^n a_k(X^k - x^k) = (X - x) \cdot \sum_{k=1}^n a_k \sum_{j=0}^{k-1} x^{k-1-j} X^j.$$

If  $y \neq x$  is a second zero of  $f$  in  $\mathbf{Z}/p\mathbf{Z}$ , then we have  $(y - x)g(y) = 0$ . By the prime property 6.6, a product of two elements in  $\mathbf{Z}/p\mathbf{Z}$  is only 0 if one of the elements is. Since  $x - y \neq 0$ , we must have  $g(y) = 0$ , so the zeros of  $f$  different from  $x$  are the zeros of  $g$ . By the induction hypothesis,  $g$  has at most  $n - 1$  zeros, and we are done.  $\square$

Note that the assumption that  $p$  is prime is essential: in  $\mathbf{Z}/24\mathbf{Z}$ , the polynomial  $X^2 - 1$  has the *eight* zeros  $\pm 1, \pm 5, \pm 7, \pm 11$ .

**Proof of 7.7.** Recall (Exercise 6.43) that for every positive divisor  $d \mid n$ , a *cyclic* group of order  $n$  contains exactly  $\varphi(d)$  elements of order  $d$ , where  $\varphi$  is Euler's  $\varphi$  function. Summing over all  $d \mid n$  gives  $\sum_{d \mid n} \varphi(d) = \#C = n$ , *Gauss's formula*.

Let  $\psi(d)$  denote the number of elements of order  $d$  in  $(\mathbf{Z}/p\mathbf{Z})^*$ . If  $x \in (\mathbf{Z}/p\mathbf{Z})^*$  has order  $d$ , then the  $d$  different powers  $x, x^2, x^3, \dots, x^d = 1$  of  $x$  are zeros of  $X^d - 1$  in  $\mathbf{Z}/p\mathbf{Z}$ . By 7.8, there are no other zeros of  $X^d - 1$  in  $\mathbf{Z}/p\mathbf{Z}$ , so the elements of order  $d$  in  $(\mathbf{Z}/p\mathbf{Z})^*$  are exactly the  $\varphi(d)$  powers  $x^i$  of  $x$  with exponent  $i$  relatively prime to  $d$ . We conclude that  $\psi(d)$  is equal to  $\varphi(d)$  if  $(\mathbf{Z}/p\mathbf{Z})^*$  contains an element of order  $d$  and equal to 0 if that is not the case. We now have

$$p - 1 = \#(\mathbf{Z}/p\mathbf{Z})^* = \sum_{d \mid p-1} \psi(d) \leq \sum_{d \mid p-1} \varphi(d) = p - 1,$$

and it follows that  $\psi(d) = \varphi(d)$  for all  $d \mid p - 1$ . In particular, we have  $\psi(p - 1) = \varphi(p - 1) > 0$ , so  $(\mathbf{Z}/p\mathbf{Z})^*$  contains an element of order  $p - 1$  and is cyclic.  $\square$

See Exercise 16 for a proof of 7.7 that does not rely on Gauss's formula.

A number  $a \in \mathbf{Z}$  for which  $a \bmod p$  is a generator of  $(\mathbf{Z}/p\mathbf{Z})^*$  is called a *primitive root* modulo  $p$ . Note that a number  $a$  that is not divisible by  $p$  is a primitive root modulo  $p$  if and only if  $a^d \not\equiv 1 \pmod{p}$  holds for all divisors  $d < p - 1$  of  $p - 1$ .

**Exercise 9.** Show that  $a$  is a primitive root modulo  $p$  if  $p$  does not divide  $a$  and we have  $a^d \not\equiv 1 \pmod{p}$  for all exponents  $d = (p - 1)/\ell$ , with  $\ell$  running through the prime divisors of  $p - 1$ .

If  $p$  is a large prime and  $a$  is a primitive root modulo  $p$ , then for a given  $k$ , the isomorphism

$$(7.9) \quad f : \quad \mathbf{Z}/(p-1)\mathbf{Z} \xrightarrow{\sim} (\mathbf{Z}/p\mathbf{Z})^* \\ k \longmapsto a^k$$

can be calculated efficiently as in 7.1, by repeated squaring. However, determining the inverse of  $f$  is a difficult problem, underlying several cryptographic routines. There are better methods than simply trying all possible values of  $k$  for  $f^{-1}(b)$ , but these methods are still far too slow for large primes. As of 2019, the record stands at 240-digit primes.

There are several cyclic groups different from  $(\mathbf{Z}/p\mathbf{Z})^*$  in which it is possible to take powers “quickly” but in which determining discrete logarithms seems complicated. Cyclic groups generated by a point of large order on an *elliptic curve* over  $\mathbf{Z}/p\mathbf{Z}$  are already used in cryptography, and arithmetic algebraic geometry has more groups in store whose cryptographic merits are still being researched.

### ► DIFFIE–HELLMAN PROTOCOL

To conclude, we provide a protocol that allows two parties  $A$  and  $B$  to choose a *public* channel what *secret* key they will use to encode messages to each other. The obvious thought that such a thing is impossible turns out to be wrong, and the reason is of the same kind as in the case of RSA: calculating  $a^k \in (\mathbf{Z}/p\mathbf{Z})^*$  for given  $a \in (\mathbf{Z}/p\mathbf{Z})^*$  and  $k \in \mathbf{Z}$  is easy, but recovering  $k \in \mathbf{Z}/(p-1)\mathbf{Z}$  from  $a$  and  $a^k \in (\mathbf{Z}/p\mathbf{Z})^*$  is a discrete logarithm problem that is difficult to carry out in practice for large  $p$ . More precisely, we can do the first in polynomial time, whereas there are no known polynomial algorithms for the second. People therefore say that for large  $p$ , the isomorphism  $f$  in 7.9 is a *one-way function*.

The *Diffie–Hellman protocol* uses the “irreversibility” of 7.9 to allow  $A$  and  $B$  to choose a secret key over a public line. To do this, they agree on a large prime  $p$  and a primitive root  $g \bmod p$  “in public.” Next, each party chooses a strictly personal secret exponent. Party  $A$  chooses the exponent  $a$  and sends  $g^a$  to  $B$ . Likewise,  $B$  sends  $A$  the element  $g^b$ , where  $b$  is  $B$ ’s secret exponent. Now  $A$ , who knows  $a$  but not  $b$ , calculates the  $a$ -th power  $g^{ab}$  of the message  $g^b$  received from  $B$ . Likewise,  $B$ , who knows  $b$  but not  $a$ , calculates the  $b$ -th power  $g^{ab}$  of the message  $g^a$  received from  $A$ . We see that  $g^{ab}$  is an element that both  $A$  and  $B$  can easily calculate; this is chosen by  $A$  and  $B$  as the secret key.

An unsuspecting eavesdropper on the public channel *cannot* calculate the key  $g^{ab}$ . After all, this person knows  $p$  and  $g$  as well as the powers  $g^a$  and  $g^b$  but knows *neither* secret exponent  $a$  or  $b$ . These are the discrete logarithms of  $g^a$  and  $g^b$  to the base  $g$ , and the eavesdropper cannot calculate these if  $p$  is chosen sufficiently large. As long as large quantum computers do not exist, there is no efficient method to calculate  $g^{ab}$  from  $g$ ,  $g^a$  and  $g^b$  without first calculating  $a$  or  $b$ . This makes us confident that this so-called *Diffie–Hellman protocol* is still a safe method for choosing a secret key.

## EXERCISES.

10. Let  $n = n_0$  be a natural number, and for  $k \geq 0$  and  $n_k \neq 0$ , define integers  $r_k \in \{0, 1\}$  and  $n_{k+1} \in \mathbf{Z}$  inductively by setting  $n_k = 2n_{k+1} + r_k$ , where  $r_k \equiv n_k \pmod{2}$ . Calculate the numbers  $(r_k)_k$  for  $n_0 = 250092$ , and prove in general that the number sequence  $\dots r_2 r_1 r_0$  gives the binary representation of  $n$ .
11. Let  $a$  be an integer and  $p \nmid a$  be an odd prime. Prove:  $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ .
12. (*Pseudoprimality tests.*) Determine an odd number  $n$  that is composite and for which the congruences  $2^{(n-1)/2} \equiv \pm 1 \pmod{n}$  and  $3^{(n-1)/2} \equiv \pm 1 \pmod{n}$  are satisfied.  
[Try programming this pseudoprimality test. There are two solutions  $n < 10000$ .]
13. Decode the message 99099932142 sent to a recipient with public exponent 13 and modulus 246790125209.  
[Hint: the last prime year of the 20th century is used in the modulus...]
- \*14. (For the serious factorizer...) Here is one last message, encoded with exponent  $e = 31$  modulo  $n = 15241578753238836751577503665157706318489955952973821$ :
- $$7937693314177547247598946714302495358389154176115486.$$
15. Let  $A$  be an abelian group, and suppose that  $A$  contains elements of finite orders  $a$  and  $b$ . Prove that  $A$  contains an element of order  $\text{LCM}(a, b)$ .  
[Hint: first look at the case where  $a$  and  $b$  are relatively prime.]
16. Let  $A$  be an abelian group of order  $n$ . Define the *exponent* of  $A$  as the smallest positive number  $e$  such that  $a^e = 1$  holds for all  $a \in A$ .
- Prove: the number  $e$  is a divisor of  $n$  and is equal to  $n$  if and only if  $A$  is cyclic.
  - Deduce from 7.8 that the exponent of  $A = (\mathbf{Z}/p\mathbf{Z})^*$  is equal to  $p - 1$  and that  $(\mathbf{Z}/p\mathbf{Z})^*$  is *therefore* cyclic.
17. Determine primitive roots modulo 11, 31, 41, and 71.
18. Determine the six smallest prime numbers  $p > 2$  for which  $5 \pmod{p}$  is a primitive root. What do you notice about the final digits of these primes?<sup>33</sup> \*Are there infinitely many primes  $p$  for which  $5 \pmod{p}$  is a primitive root?<sup>34</sup>
19. Show that 2 is a primitive root modulo 101, and calculate  $\log_2(3)$ ,  $\log_2(5)$ , and  $\log_2(7)$  in the group  $(\mathbf{Z}/101\mathbf{Z})^*$ .

## 8 QUOTIENTS AND PRODUCTS.

The construction of the quotient map  $G \rightarrow G/N$  in 4.14 allows us to do all kinds of “abstract group theory.” We begin with several general theorems on quotient groups that are direct consequences of the definitions and the isomorphism theorem 4.10.

### ► SUBGROUPS UNDER QUOTIENT MAPS

The quotient  $G/N$  of a group  $G$  modulo a normal subgroup  $N$  is, in principle, “simpler” than  $G$ ; after all, we have “forgotten” information. So we can describe the subgroups, normal subgroups, and quotients of  $G/N$  directly in terms of  $G$ .

**8.1. Theorem.** *The subgroups of the quotient group  $\overline{G} = G/N$  are of the form  $\overline{H} = H/N$ , with  $H \subset G$  a subgroup of  $G$  that contains  $N$ . For such  $H$ ,*

$$\begin{aligned} f : G/H &\longrightarrow \overline{G}/\overline{H} \\ gH &\longmapsto \overline{g}\overline{H} \end{aligned}$$

is a bijective map between the sets of left cosets. In particular, we have  $[G : H] = [\overline{G} : \overline{H}]$ , and  $H$  is normal in  $G$  if and only if  $\overline{H}$  is normal in  $\overline{G}$ . In the normal case,  $f$  is a group isomorphism.

**Proof.** If  $X \subset G/N$  is a subgroup and  $\pi : G \rightarrow G/N$  is the quotient map, then  $H = \pi^{-1}[X]$  is a subgroup of  $G$  that contains  $N = \ker \pi$ . Since  $\pi$  is surjective, we have  $X = \pi[H] = H/N$ , so  $X$  is of the required form.

For  $H \supset N$  as above,  $f : G/H \rightarrow \overline{G}/\overline{H}$  is well defined and surjective. If  $g_1, g_2 \in G$  satisfy  $\overline{g_1}\overline{H} = \overline{g_2}\overline{H}$ , then we have  $\overline{g_1} = \overline{g_2}\overline{h} = \overline{g_2h}$  and  $g_1 = g_2hn$  for some  $h \in H$  and  $n \in N \subset H$ . Since  $hn \in H$ , we have  $g_1H = g_2H$ , so  $f$  is also injective. The resulting bijection immediately gives the index equality  $[G : H] = [\overline{G} : \overline{H}]$ .

If  $H$  is normal in  $G$  or  $\overline{H}$  is normal in  $\overline{G}$ , then  $G/H$  and  $\overline{G}/\overline{H}$  inherit the structure of a group from  $G$ . In this case,  $f$  is an isomorphism.  $\square$

**Exercise 1.** For a normal subgroup  $H \supset N$  of  $G$ , deduce the isomorphism in 8.1 by applying the isomorphism theorem to the canonical map  $G/N \rightarrow G/H$ .

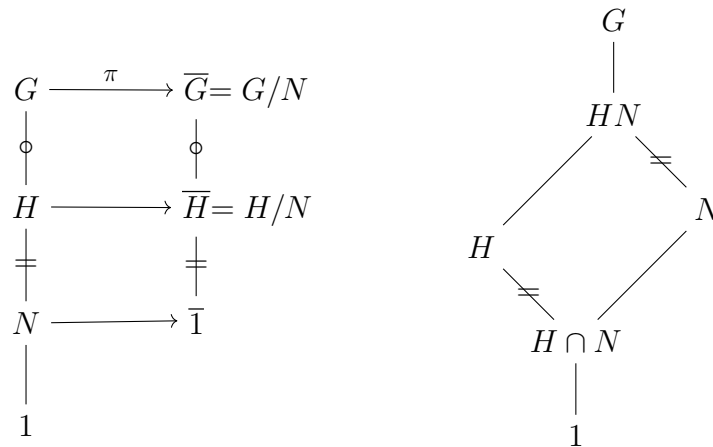
We can ask what happens to an arbitrary subgroup  $H \subset G$  under the quotient map  $\pi : G \rightarrow G/N$ . The image  $\pi[H]$  is the subgroup of  $G/N$  consisting of the residue classes  $hN$  with  $h \in H$ . By 8.1, this corresponds to a subgroup of  $G$  that contains  $N$ , namely  $HN = \{hn : h \in H, n \in N\}$ .

**8.2. Theorem.** *Let  $N \triangleleft G$  be a normal subgroup and  $H \subset G$  be a subgroup. Then there is a natural isomorphism*

$$H/(H \cap N) \xrightarrow{\sim} HN/N.$$

**Proof.** The restriction of the quotient map  $\pi : G \rightarrow G/N$  to  $H$  gives a homomorphism  $H \rightarrow G/N$  with kernel  $H \cap N$  and image  $HN/N$ . The isomorphism theorem 4.10 now gives an isomorphism  $H/(H \cap N) \xrightarrow{\sim} HN/N$ .  $\square$

We can visualize the statements of Theorems 8.1 and 8.2 using *diagrams* that show the various arrows and inclusions. The convention is that all inclusions are indicated by connecting lines going up straight or at an angle. In the diagrams below, the mark “=” indicates pairs of inclusions that lead to isomorphic quotients. The inclusions marked with “◦” are the subject of Theorem 8.1.



**8.3. Examples. 1.** Let  $a$  and  $b$  be positive integers, and take  $H = a\mathbf{Z}$  and  $N = b\mathbf{Z}$  in 8.2. By definition 6.3.3,  $H + N$  (the additive equivalent of  $HN$ ) and  $H \cap N$  are the subgroups of the additive group  $\mathbf{Z}$  generated by, respectively,  $\text{GCD}(a, b)$  and  $\text{LCM}(a, b)$ . The quotient groups  $a\mathbf{Z}/\text{LCM}(a, b)\mathbf{Z}$  and  $\text{GCD}(a, b)\mathbf{Z}/b\mathbf{Z}$  are isomorphic by 8.2. So their orders  $\text{LCM}(a, b)/a$  and  $b/\text{GCD}(a, b)$  are the same, leading to the equality

$$\text{GCD}(a, b) \cdot \text{LCM}(a, b) = ab$$

known from Exercise 6.20

**2.** The symmetric group  $G = S_4$  of order 24 has a normal subgroup  $N = V_4$  consisting of (1) and the three products of two disjoint 2-cycles. If we apply 8.2 to the non-normal subgroup  $H = S_3$  of permutations that fix the element 4, then we have  $H \cap N = 1$ , and we find an isomorphism  $S_3 \xrightarrow{\sim} S_3V_4/V_4$ . Since  $S_3$  has order 6 and  $V_4$  has order 4,  $S_3V_4$  has order 24 and is therefore equal to  $S_4$ . We obtain an isomorphism  $S_3 \xrightarrow{\sim} S_4/V_4$ . This is the inverse of the isomorphism  $S_4/V_4 \xrightarrow{\sim} S_3$  induced by the “tetrahedron homomorphism”  $T = S_4 \rightarrow S_3$  from §5.

The symmetric group  $S_3$  contains a normal subgroup  $A_3$  of index 2 and three non-normal subgroups of index 3. If we apply 8.1 to the quotient map  $\pi : S_4 \rightarrow S_4/V_4 \cong S_3$ , then it follows that  $S_4$  contains a normal subgroup of index 2 and three non-normal subgroups  $H_1, H_2, H_3 \subset S_4$  of index 3. The subgroup of index 2 is  $A_4$ . The three non-normal subgroups  $H_i$ , which have order 8, each contain  $V_4$  as a subgroup. Every subgroup of  $S_4$  generated by  $V_4$  and a 2-cycle is equal to one of the  $H_i$ .

**Exercise 2.** Show that the three subgroups  $H_i \subset S_4$  are isomorphic to  $D_4$  and are mapped to one another by inner automorphisms of  $S_4$ .

Example 8.3.2 shows that Theorems 8.1 and 8.2, which give relations between the groups  $G$  and  $G/N$ , allow us to transfer information in either direction. In the example

above, we first used a subgroup  $H = S_3$  of  $G = S_4$  to understand the quotient  $G/N = S_4/V_4$  and then our explicit knowledge of this quotient to find subgroups of  $S_4$  of order 8.

► **HOMOMORPHISM THEOREM**

The homomorphism theorem tells us when a homomorphism  $f : G \rightarrow G'$  factors through the quotient group  $G/N$ . By this, we mean that  $f$  can be written as a “product”  $f = \bar{f}\pi$  of the quotient map  $\pi : G \rightarrow G/N$  and a homomorphism  $\bar{f} : G/N \rightarrow G'$ . The existence of such a factorization implies that  $N$  is contained in  $\ker(f)$ .

**8.4. Homomorphism theorem.** *Let  $f : G \rightarrow G'$  be a homomorphism and  $N$  be a normal subgroup of  $G$  contained in  $\ker(f)$ . Then there exists a unique homomorphism  $\bar{f} : G/N \rightarrow G'$  such that  $f$  is the composition*

$$G \xrightarrow{\pi} G/N \xrightarrow{\bar{f}} G'$$

of the quotient map  $\pi : G \rightarrow G/N$  and  $\bar{f}$ .

**Proof.** A map  $\bar{f} : G/N \rightarrow G'$  with the stated property is necessarily given by  $gN \mapsto f(g)$ , so we must show that with this definition,  $\bar{f}$  is a well-defined homomorphism.

If  $g_1N = g_2N$ , then we have  $g_1 = g_2n$  for some  $n \in N \subset \ker(f)$ . Since  $f(n) = e'$ , we have  $f(g_1) = f(g_2n) = f(g_2)f(n) = f(g_2)$ , so  $\bar{f}$  is well defined. The homomorphism property of  $\bar{f}$  follows from that of  $f$ :

$$\bar{f}(g_1N \cdot g_2N) = \bar{f}(g_1g_2N) = f(g_1g_2) = f(g_1)f(g_2) = \bar{f}(g_1N)\bar{f}(g_2N). \quad \square$$

**Exercise 3.** Prove:  $\ker(\bar{f}) = \ker(f)/N$ . How does 4.10 follow from this?

In short, the characterization of the quotient map  $\pi : G \rightarrow G/N$  given by 8.4 is that all homomorphisms from  $G$  that are trivial on  $N$  go through the quotient  $G/N$ .

The homomorphism theorem 8.4 is often formulated as saying that there is a unique homomorphism  $\bar{f} : G/N \rightarrow G'$  for which the diagram

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ & \searrow \pi & \nearrow \bar{f} \\ & & G/N \end{array}$$

*commutes* or *is commutative*. In general, a diagram is said to be commutative if whenever there are two ways to follow the arrows of the diagram from one group to another, the corresponding homomorphism compositions are equal. For example, a square diagram

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ g \downarrow & & \downarrow h \\ G_3 & \xrightarrow{j} & G_4 \end{array}$$

is commutative when the compositions  $hf$  and  $jj$  give the *same* homomorphism  $G_1 \rightarrow G_4$ . So-called *commutative algebra*, a part of algebra we will be introduced to later, frequently expresses itself in terms of such diagrams.

► COMMUTATOR SUBGROUP

As an application of 8.4, we consider the case where  $N$  is the *commutator subgroup*  $[G, G] \subset G$ . By definition, this is the subgroup of  $G$  generated by all *commutators*

$$[x, y] = xyx^{-1}y^{-1}$$

of elements  $x, y \in G$ . The identity  $[\sigma(x), \sigma(y)] = \sigma([x, y])$  for  $\sigma \in \text{Aut}(G)$  shows that an automorphism of  $G$  permutes the commutators. So the commutator subgroup is invariant under automorphisms and is therefore a *characteristic subgroup* of  $G$ . Since  $[G, G]$  is, in particular, invariant under all inner automorphisms  $\sigma \in \text{Inn}(G)$ , it is a normal subgroup of  $G$ .

The quotient  $G_{\text{ab}} = G/[G, G]$  is called the *abelianization* of  $G$  or  $G$  *made abelian*. After all, by the definition of the commutator subgroup, for any two elements  $\bar{x}, \bar{y} \in G_{\text{ab}}$ , we have the relation  $\bar{x}\bar{y}\bar{x}^{-1}\bar{y}^{-1} = \bar{e}$ , and so  $\bar{x}\bar{y} = \bar{y}\bar{x}$ . The group  $G_{\text{ab}}$  is also called the *maximal abelian quotient* of  $G$ . If  $G$  itself is abelian, we have  $[G, G] = \{e\}$  and  $G_{\text{ab}} = G$ .

**Exercise 4.** Show that  $G/N$  is abelian if and only if we have  $N \supset [G, G]$ .

Every homomorphism  $f : G \rightarrow A$  to an *abelian* group  $A$  sends the commutators of  $G$  to the unit element  $e_A \in A$ :

$$f([x, y]) = f(xyx^{-1}y^{-1}) = f(x)f(y)f(x)^{-1}f(y)^{-1} = f(x)f(x)^{-1}f(y)f(y)^{-1} = e_A.$$

It follows that  $[G, G]$  is contained in  $\ker(f)$ , and 8.4 gives the following statement.

**8.5. Theorem.** *Let  $f : G \rightarrow A$  be a homomorphism to an abelian group  $A$ . Then there exists a homomorphism  $f_{\text{ab}} : G_{\text{ab}} = G/[G, G] \rightarrow A$  such that  $f$  is the composition*

$$G \xrightarrow{\pi} G_{\text{ab}} \xrightarrow{f_{\text{ab}}} A$$

of the canonical map  $\pi : G \rightarrow G_{\text{ab}}$  and  $f_{\text{ab}}$ . □

It follows from 8.5 that giving a homomorphism  $G \rightarrow A$  to an abelian group is “the same” as giving a homomorphism  $G_{\text{ab}} \rightarrow A$ : the map  $f_{\text{ab}} \mapsto f_{\text{ab}}\pi$  gives a bijection  $\text{Hom}(G_{\text{ab}}, A) \iff \text{Hom}(G, A)$ .

**8.6. Corollary.** *Every homomorphism  $f : S_n \rightarrow A$  to an abelian group  $A$  is the composition*

$$S_n \xrightarrow{\varepsilon} \{\pm 1\} \xrightarrow{\bar{f}} A$$

of the sign map  $\varepsilon$  and a homomorphism  $\bar{f} : \{\pm 1\} \rightarrow A$ .

**Proof.** By 8.5, it suffices to prove that the alternating group  $A_n = \ker \varepsilon$  is equal to the commutator subgroup of  $S_n$ . Since every commutator  $xyx^{-1}y^{-1}$  in  $S_n$  is an even permutation, we have  $[S_n, S_n] \subset A_n$ . For the other inclusion, by 2.10, it suffices to write every 3-cycle as a commutator. For  $n \leq 2$ , there is nothing to prove; for  $n \geq 3$ , the identity

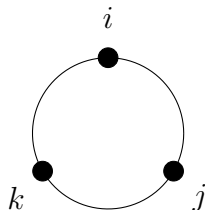
$$[(a\ b), (a\ c)] = (a\ b)(a\ c)(a\ b)(a\ c) = (a\ b\ c)$$

shows that every 3-cycle is a commutator. This gives  $A_n = [S_n, S_n]$ .  $\square$

**8.7. Example.** Hamilton’s *quaternion group*  $Q$ , named after the Irishman William Rowan Hamilton (1805–1865), consists of the eight elements  $\pm 1, \pm i, \pm j$ , and  $\pm k$  and has a group structure given by the identities

$$i^2 = j^2 = k^2 = ijk = -1 \quad \text{and} \quad (-1)^2 = 1.$$

The rule that can be deduced from this for the elements  $i, j$ , and  $k$  of order 4 is that the product of two consecutive ones in “clockwise” direction on the circle below equals the third. So,  $jk = i$  and  $ki = j$ . Going counterclockwise gives the opposite results:  $kj = -i$  and  $ik = -j$ .



The element  $-1$ , which is a power of both  $i$  and  $j$ , commutes with all elements of  $Q = \langle i, j \rangle$ . It is a generator of the center  $Z(Q) = \{\pm 1\}$  of  $Q$ .

The commutator subgroup  $[Q, Q]$  is also equal to  $\{\pm 1\}$  because any two non-commuting elements of  $Q$  have commutator  $-1$ . In the quotient group  $Q/[Q, Q]$ , the three non-trivial elements  $\bar{i}, \bar{j}$ , and  $\bar{k}$  each have order 2, and the product of two of them is equal to the third. Apparently, the abelianization  $Q^{\text{ab}}$  of the quaternion group is isomorphic to the Klein four-group  $V_4$ .

**\*Exercise 5.** Show that  $Q$  has exactly 24 different automorphisms. What group is  $\text{Aut}(Q)$ ?

In addition to the already known vector addition, the 4-dimensional real vector space  $\mathbf{H} = \mathbf{R} \cdot 1 + \mathbf{R} \cdot i + \mathbf{R} \cdot j + \mathbf{R} \cdot k$  admits a natural *non-commutative* ring structure. Multiplication in Hamilton’s *quaternion algebra*, which contains the field of complex numbers  $\mathbf{C} = \mathbf{R} \cdot 1 + \mathbf{R} \cdot i$  as a subring, is done by systematically applying the distributive property (R3) from 6.8 and the multiplication rules for  $i, j$ , and  $k$ :

$$\begin{aligned} (a + bi + cj + dk) \cdot (a' + b'i + c'j + d'k) = \\ (aa' - bb' - cc' - dd') + (ab' + a'b + cd' - c'd)i + \\ (ac' + a'c + db' - d'b)j + (ad' + a'd + bc' - b'c)k. \end{aligned}$$

We will not discuss this ring further in these course notes.

► DIRECT PRODUCT

The previous theorem in this section illustrates the well-known group-theoretic fact that a group  $G$  can often be studied through its quotients  $G/N$  for suitable normal subgroups  $N \triangleleft G$ . In most cases,  $N$  and  $G/N$  are both “smaller” and therefore “easier” to study than  $G$  itself. In the remainder of this section, we study the important question to what extent  $G$  can be “reconstructed” from a normal subgroup  $N$  and the corresponding quotient  $G/N$ . Sometimes,  $G$  can be recovered as the “product” of  $N$  and  $G/N$ . Let us first consider general products of groups.

The simplest way to make a product group from two groups  $G_1$  and  $G_2$  is by constructing the *direct product*  $G_1 \times G_2$ . We already came across this construction in the Chinese remainder theorem 6.15. This shows that forming products is possible not only for groups but also for other *categories* of objects.

As a set, the group  $G_1 \times G_2$  is the Cartesian product

$$G_1 \times G_2 = \{(x_1, x_2) : x_1 \in G_1, x_2 \in G_2\},$$

and we take coordinate-wise multiplication

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2)$$

as the binary operation. This gives a group with unit element  $(e_1, e_2)$ . The inverse of  $(x_1, x_2)$  is the element  $(x_1^{-1}, x_2^{-1})$ . We can define products

$$\prod_{i=1}^n G_i = G_1 \times G_2 \times \dots \times G_n$$

of  $n$  groups likewise: take the Cartesian product of the sets and carry out the group operations coordinate-wise. The *projection*  $\pi_i : G_1 \times G_2 \times \dots \times G_n \rightarrow G_i$  onto the  $i$ -th coordinate is a surjective group homomorphism for all  $i$ . The  $n$ -tuple product of a group with itself is often denoted by  $G^n$ . For example, the product  $C_2^2 = C_2 \times C_2$  of the cyclic group of order 2 with itself is an abelian group of order 4 in which all elements satisfy  $x^2 = e$ . We know from §1 that this means that  $C_2 \times C_2$  is isomorphic to the Klein four-group  $V_4$ .

For abelian groups  $A_1$  and  $A_2$  denoted additively, the direct product is called the *direct sum* and denoted by  $A_1 \oplus A_2$ . The additive group of the vector space  $\mathbf{R}^n$  is a direct sum of  $n$  copies of the additive group  $\mathbf{R}$ . Every choice of a basis in a real vector space  $V$  of dimension  $n$  is in fact the choice of an isomorphism  $\mathbf{R}^n \xrightarrow{\sim} V$ . Thus, a vector space can be isomorphic to a direct sum of 1-dimensional subspaces in many ways.

The product group  $G_1 \times G_2$  contains subgroups  $G_1 \times 1$  and  $1 \times G_2$  that are isomorphic to  $G_1$  and  $G_2$  and are often identified with  $G_1$  and  $G_2$ . So to write a group  $G$  as a product of smaller groups, we must find subgroups  $H_1, H_2 \subset G$  for which there is an isomorphism  $H_1 \times H_2 \xrightarrow{\sim} G$  given by “multiplying coordinates”:  $(x, y) \mapsto xy$ . For example, if  $G = V_4 = \{e, a, b, c\}$  is the Klein four-group, then  $H_1 = \langle a \rangle$  and  $H_2 = \langle b \rangle$  are cyclic subgroups of order 2, and we can make the isomorphism  $C_2 \times C_2 \xrightarrow{\sim} V_4$  explicit by defining

$$\langle a \rangle \times \langle b \rangle \xrightarrow{\sim} V_4$$

by  $(x, y) \mapsto xy$ . More generally, the following theorem helps us establish that a group can be obtained as a direct product of two subgroups.

**8.8. Theorem.** *Let  $H_1$  and  $H_2$  be subgroups of  $G$  for which we have*

1.  $H_1 \cap H_2 = 1$ ;
2.  $H_1H_2 = \{h_1h_2 : h_1 \in H_1 \text{ and } h_2 \in H_2\} = G$ ;
3. for  $h_1 \in H_1$  and  $h_2 \in H_2$ , we have  $h_1h_2 = h_2h_1$ .

*Then the map  $(h_1, h_2) \mapsto h_1h_2$  defines a group isomorphism*

$$H_1 \times H_2 \xrightarrow{\sim} G.$$

*There are surjections  $\pi_1 : G \rightarrow H_1$  and  $\pi_2 : G \rightarrow H_2$  with  $\ker \pi_1 = H_2$  and  $\ker \pi_2 = H_1$ .*

**Proof.** Let  $f : H_1 \times H_2 \rightarrow G$  be the indicated map. Property (3) implies that  $f$  is a homomorphism:

$$f((h_1, h_2)(\tilde{h}_1, \tilde{h}_2)) = f(h_1\tilde{h}_1, h_2\tilde{h}_2) = h_1\tilde{h}_1 \cdot h_2\tilde{h}_2 = h_1h_2 \cdot \tilde{h}_1\tilde{h}_2 = f((h_1, h_2))f((\tilde{h}_1, \tilde{h}_2)).$$

For  $(h_1, h_2) \in \ker(f)$ , we have  $h_1h_2 = e$ , so  $h_1 = h_2^{-1} \in H_1 \cap H_2 = 1$ . This gives  $(h_1, h_2) = (e, e)$ , and  $f$  is injective by 4.4. By (2),  $f$  is also surjective, hence an isomorphism. The mentioned surjections are the “projections onto the coordinates” given by  $\pi_1 : h_1h_2 \mapsto h_1$  and  $\pi_2 : h_1h_2 \mapsto h_2$ .  $\square$

**Exercise 6.** Show that we can replace condition (3) in Theorem 8.8 with “ $H_1$  and  $H_2$  are normal in  $G$ .”

**Exercise 7.** Generalize 8.8 to isomorphisms  $H_1 \times H_2 \times \dots \times H_n \xrightarrow{\sim} G$ .

**8.9. Examples. 1.** The multiplicative group  $\mathbf{R}^*$  contains a sign subgroup  $\{\pm 1\}$  and a subgroup  $\mathbf{R}_{>0}$  of positive real numbers that satisfy the conditions in 8.8. This gives an isomorphism  $\{\pm 1\} \times \mathbf{R}_{>0} \xrightarrow{\sim} \mathbf{R}^*$ .

**2.** Likewise, the multiplicative group of complex numbers  $\mathbf{C}^*$  can be obtained as a product  $\mathbf{C}^* \cong \mathbf{T} \times \mathbf{R}_{>0}$  of the circle group  $\mathbf{T} = \{z \in \mathbf{C}^* : |z| = 1\}$  and  $\mathbf{R}_{>0}$ . The isomorphism for  $\mathbf{R}^*$  is obtained from this by restriction.

**3.** The group  $K$  of symmetries of the cube has a subgroup  $K^+$  of rotation symmetries and a subgroup  $\langle -1 \rangle$  generated by the central point reflection  $-1$ . We already saw in §5 that these subgroups of  $K$  satisfy conditions 8.8.1 and 8.8.2. To see that they also satisfy 8.8.3, we view the rotation symmetries as linear maps  $\mathbf{R}^3 \rightarrow \mathbf{R}^3$  by taking the center of the cube as the origin in  $\mathbf{R}^3$ . The central point reflection is then given by the scalar multiplication by  $-1$ , which commutes with *all* linear maps. So for the cubic group, we have

$$K \cong \langle -1 \rangle \times K^+ \cong C_2 \times S_4.$$

**4.** Let  $A$  be an abelian group of order  $mn$ , with  $m, n \in \mathbf{Z}_{>0}$  relatively prime numbers. Since  $A$  is abelian,

$$A_m = \{a \in A : a^m = 1\} \quad \text{and} \quad A_n = \{a \in A : a^n = 1\}$$

are subgroups of  $A$ . We have  $A_m \cap A_n = 1$  because an element whose order divides both  $m$  and  $n$  has order  $\text{GCD}(m, n) = 1$ . If we choose  $x, y \in \mathbf{Z}$  such that  $nx + my = 1$ , then an element  $a \in A$  can be written as  $a = a^{nx+my} = a^{nx} \cdot a^{my}$ . We now have  $a^{nx} \in A_m$  because  $(a^{nx})^m = a^{mnx} = 1$  and, likewise,  $a^{my} \in A_n$ . It follows that  $A_m$  and  $A_n$  satisfy the conditions of Theorem 8.8, and we obtain  $A \cong A_m \times A_n$ . Since the order of  $A_m$  is relatively prime to  $n$  (why?) and that of  $A_n$  is relatively prime to  $m$ , comparing orders gives  $\#A_m = m$  and  $\#A_n = n$ .

If we repeatedly apply the “decomposition” of  $A$  in Example 8.9.4, we find that every finite abelian group of order  $n = \prod_p p^{n_p}$  is the product of abelian groups of orders  $p^{n_p}$ . In terms of the Sylow  $p$ -subgroups introduced at the end of §5, the conclusion is as follows.

**8.10. Theorem.** *Every finite abelian group is the direct product of its Sylow  $p$ -subgroups.*  $\square$

### ► SEMI-DIRECT PRODUCT

The subgroups  $H_1$  and  $H_2$  in 8.8 are both normal in  $G$  because they are the kernels of the projection maps  $\pi_1$  and  $\pi_2$ . Roughly speaking, Theorem 8.8 boils down to the fact that if we have natural isomorphisms  $H_1 \xrightarrow{\sim} G/H_2$  and  $H_2 \xrightarrow{\sim} G/H_1$ , then the group  $G$  is a direct product of  $H_1$  and  $H_2$ .

In many situations, the condition that  $H_1$  and  $H_2$  are both normal in  $G$  is not satisfied, and only one of the two groups is the quotient of  $G$  modulo the other. In this asymmetric situation, we have a normal subgroup  $N \subset G$  and a subgroup  $H \subset G$  for which the natural map  $H \rightarrow G/N$  is an isomorphism. In this case, we can describe  $G$  as the *semi-direct product* of  $N$  and  $H$ .

At first glance, the definition of the semi-direct product looks somewhat complicated, so we will first look at the example of the group  $I_2(\mathbf{R})$  of *plane isometries* from §3. This group contains a subgroup  $T$  of translations and an orthogonal subgroup  $O_2(\mathbf{R})$  of linear isometries. The identity is the only element of the intersection of these subgroups, and we proved in 3.3.1 that every element  $\varphi \in I_2(\mathbf{R})$  can be written uniquely as a product  $\varphi = \tau\psi$  of a translation  $\tau$  and an orthogonal map  $\psi$ . Conditions (1) and (2) of 8.8 are now satisfied, but (3) is not. For while taking the linear component from 3.9 induces a “projection map”  $L : I_2(\mathbf{R}) \rightarrow O_2(\mathbf{R})$  with kernel  $T$ , the situation is not symmetric in  $T$  and  $O_2(\mathbf{R})$  because it follows from 3.10 that  $T$  is normal in  $I_2$ , whereas  $O_2(\mathbf{R})$  is not. That means that the correspondence  $\tau\psi \leftrightarrow (\tau, \psi)$  gives a bijection

$$I_2(\mathbf{R}) \leftrightarrow T \times O_2(\mathbf{R}),$$

but the group operation on  $I_2(\mathbf{R})$  does *not* correspond to the group operation on the direct product. To see what the “right” group operation  $T \times O_2(\mathbf{R})$  is, we take a closer look at the relation

$$\psi\tau_x\psi^{-1} = \tau_{\psi(x)}$$

given in (3.10). This relation says that if we identify  $T$  with  $\mathbf{R}^2$  in the obvious way, then the *conjugation action* of  $O_2(\mathbf{R})$  on  $T = \mathbf{R}^2$  is the “same” as the *natural action*

of  $O_2(\mathbf{R})$  on  $\mathbf{R}^2$ . With this knowledge, we can explicitly take products of translations and orthogonal maps:

$$(8.11) \quad \tau_{x_1}\psi_1 \cdot \tau_{x_2}\psi_2 = \tau_{x_1}(\psi_1\tau_{x_2}\psi_1^{-1}) \cdot \psi_1\psi_2 = \tau_{x_1}\tau_{\psi_1(x_2)} \cdot \psi_1\psi_2.$$

So the multiplication on the “orthogonal component” is the usual multiplication, but the multiplication on the “translation component” is not. The presence of a non-trivial conjugation action of  $O_2(\mathbf{R})$  on  $T$  makes the group operation 8.11 on  $T \times O_2(\mathbf{R})$  into an example of *semi-direct multiplication*.

In general, we can make semi-direct products by letting a group  $H$  “act” on a group  $N$ . By this, we mean that for every element  $h \in H$ , we have an automorphism  $\sigma_h \in \text{Aut}(N)$  and that, as in the case of conjugation actions, we have the identity  $\sigma_{h_1}\sigma_{h_2} = \sigma_{h_1h_2}$ . The latter simply means that the map  $\sigma : H \rightarrow \text{Aut}(N)$  given by  $h \mapsto \sigma_h$  is a group homomorphism. This can be expressed evocatively by using the “exponential notation”  $\sigma_h(n) = {}^h n$  with rule  ${}^{h_1}({}^{h_2}n) = {}^{h_1h_2}n$ .

**8.12. Proposition.** *Let  $N$  and  $H$  be groups and  $\sigma : H \rightarrow \text{Aut}(N)$  be a homomorphism, and write  $\sigma(h)(n) = {}^h n$ . Then the operation*

$$(n_1, h_1)(n_2, h_2) = (n_1 {}^{h_1}n_2, h_1h_2)$$

*defines a group action on the product set  $N \times H$ .*

**Proof.** The definition is chosen to imitate exactly what occurs for  $I_2(\mathbf{R})$ . If we view  $N$  and  $H$  as subsets of  $N \times H$  through  $n \mapsto (n, e_H)$  and  $h \mapsto (e_N, h)$ , then the given operation induces the “usual” multiplication on  $N$  and  $H$ , and every group element can be written as a product  $(n, h) = (n, e_H)(e_N, h) = nh$ . The automorphism  $\sigma(h) \in \text{Aut}(N)$  is now literally the conjugation by  $h$ :

$$hnh^{-1} = (e_N, h)(n, e_H)(e_N, h^{-1}) = ({}^h n, e_H) = {}^h n = \sigma(h)(n).$$

This means that we can multiply products of the form  $nh$  by first concatenating them and then moving all  $h$  to the right using the “conjugation trick” (8.11). The unit element is  $e = (e_N, e_H)$ , and it follows from  $(nh)^{-1} = h^{-1}n^{-1} = {}^{h^{-1}}(n^{-1})h^{-1}$  that the inverse of  $(n, h)$  is  $({}^{h^{-1}}(n^{-1}), h^{-1})$ . The reader can check the associative property as an exercise.  $\square$

The group obtained in 8.12 is called the *semi-direct product* of  $N$  and  $H$  with respect to the map  $\sigma$  and is denoted by  $N \rtimes_{\sigma} H$  or  $N \rtimes H$  for short. If  $\sigma : H \rightarrow \text{Aut}(N)$  is the trivial homomorphism, then we always have  ${}^h n = n$ , and the semi-direct product is nothing but the direct product.

As in the proof of 8.12, we view  $N$  and  $H$  as subgroups of  $N \rtimes H$ . The subgroup  $N$ , which is invariant under conjugation with elements of both  $N$  and  $H$ , is normal in  $N \rtimes H$ . The symbol  $\rtimes$ , which is related to the symbol  $\triangleleft$ , expresses this fact. The analog of 8.8 for semi-direct products reads as follows.

**8.13. Theorem.** Let  $N$  and  $H$  be subgroups of  $G$  for which we have

1.  $N \cap H = 1$ ;
2.  $NH = \{nh : n \in N \text{ and } h \in H\} = G$ ;
3.  $N$  is normal in  $G$ .

If  $\sigma : H \rightarrow \text{Aut}(N)$  is the map that describes the conjugation action of  $H$  on  $N$ , then the map  $(n, h) \mapsto nh$  defines a group isomorphism

$$N \rtimes_{\sigma} H \xrightarrow{\sim} G.$$

The map  $nh \mapsto h$  gives a surjection  $G \rightarrow H$  with kernel  $N$ .

**Proof.** The semi-direct product is defined precisely so that the map in question is a homomorphism. It is injective by (1) and surjective by (2), hence an isomorphism. It follows from 8.12 that the projection onto the  $H$ -component is a surjective homomorphism; its kernel is clearly  $N$ .  $\square$

**Exercise 8.** Show that  $H$  in 8.13 is only normal in  $G$  if  $\sigma$  is trivial and that in that case,  $G$  is the direct product of  $N$  and  $H$ .

Theorem 8.13 is much more generally applicable than 8.8 because we only require “ $G/N = H$ ” and not also “ $G/H = N$ .” However, because of this, the obtained product  $N \rtimes_{\sigma} H$  is not “symmetric” in  $N$  and  $H$ .

**8.14. Examples. 1.** The *affine group*  $\text{Aff}(\mathbf{R})$  is the subgroup of  $S(\mathbf{R})$  consisting of the bijections

$$\{x \mapsto ax + b : a \in \mathbf{R}^*, b \in \mathbf{R}\}.$$

We obtain subgroups  $H = \mathbf{R}^*$  and  $N = \mathbf{R}$  by letting  $a \in \mathbf{R}^*$  and  $b \in \mathbf{R}$  correspond to, respectively, the maps  $\sigma_a : x \mapsto ax$  and  $\tau_b : x \mapsto x + b$ . The intersection of the two subgroups contains only the identity, and every affine map is the unique composition of a multiplication  $x \mapsto ax$  and a translation  $x \mapsto x + b$ . The subgroup  $\mathbf{R}$  of translations is normal, and the conjugation action of  $\mathbf{R}^*$  on  $\mathbf{R}$  in  $\text{Aff}(\mathbf{R})$  is the natural multiplication:

$$(\sigma_a \tau_b \sigma_a^{-1})(x) = a(a^{-1}x + b) = x + ab = \tau_{ab}(x).$$

We conclude that  $\text{Aff}(\mathbf{R})$  is a semi-direct product  $\mathbf{R} \rtimes \mathbf{R}^*$  with respect to the map  $\mathbf{R}^* \rightarrow \text{Aut}(\mathbf{R})$  given by  $a \mapsto \sigma_a$ .

**2.** The dihedral group  $D_n$  contains a normal subgroup  $N = C_n$  of index 2, generated by a rotation  $\rho$  of order  $n$ , and a subgroup  $H = C_2 = \langle \sigma \rangle$  of order 2 generated by a reflection. Every element is a unique product of an element of  $C_n$  and an element of  $C_2$ , and by (3.6), the conjugation action of the non-trivial element  $\sigma \in C_2$  on  $C_n$  is described by the identity  $\sigma \rho \sigma = \rho^{-1}$ . This means that the corresponding map  $C_2 \rightarrow \text{Aut}(C_n)$  sends the generator of  $C_2$  to the automorphism of  $C_n$  that inverts all elements. We find that

$$D_n \cong C_n \rtimes C_2$$

is a semi-direct product of a cyclic group of order  $n$  and a group of order 2 that acts by *inversion*. More generally, for every abelian group  $A$ , we can construct a *generalized dihedral group*  $A \rtimes C_2$  by letting  $C_2$  act on  $A$  by inversion.

**3.** In 8.3.2, we saw that the symmetry group  $S_4$  contains a normal subgroup  $N = V_4$  and a subgroup  $H = S_3$  that satisfy the conditions of 8.13. The conjugation action  $\sigma : S_3 \rightarrow \text{Aut}(V_4)$  of  $S_3$  on  $V_4$  is (cf. Exercise 4.35) an isomorphism. The obtained isomorphism

$$S_4 \cong V_4 \rtimes S_3 \cong V_4 \rtimes \text{Aut}(V_4)$$

shows that  $S_4$  can be constructed from  $V_4$  by taking the semi-direct product of  $V_4$  and its automorphism group.

**4.** For every group  $G$ , we can form the product  $G \rtimes \text{Aut}(G)$  with respect to the natural action of  $\text{Aut}(G)$  on  $G$ .

For the cyclic group  $G = \mathbf{Z}/n\mathbf{Z}$ , we have

$$(8.15) \quad \text{Aut}(G) = (\mathbf{Z}/n\mathbf{Z})^*.$$

After all, an element  $\sigma \in \text{Aut}(\mathbf{Z}/n\mathbf{Z})$  with  $\sigma(\bar{1}) = \bar{a}$  is given by  $\sigma(\bar{x}) = \bar{a}\bar{x}$ . The map  $\sigma$  is only an automorphism for  $\bar{a} \in (\mathbf{Z}/n\mathbf{Z})^*$ ; this gives the identification  $\text{Aut}(\mathbf{Z}/n\mathbf{Z}) = (\mathbf{Z}/n\mathbf{Z})^*$ . The semi-direct product  $G \rtimes \text{Aut}(G) = \mathbf{Z}/n\mathbf{Z} \rtimes (\mathbf{Z}/n\mathbf{Z})^*$ , which is the analog of 8.14.1 for the ring  $\mathbf{Z}/n\mathbf{Z}$  instead of  $\mathbf{R}$ , is called the *affine group*  $\text{Aff}(\mathbf{Z}/n\mathbf{Z})$  over  $\mathbf{Z}/n\mathbf{Z}$ .

**Exercise 9.** Prove: there are isomorphisms  $\text{Aff}(\mathbf{Z}/3\mathbf{Z}) \cong S_3$  and  $\text{Aff}(\mathbf{Z}/4\mathbf{Z}) \cong D_4$ .

## EXERCISES.

10. Let  $f : G \rightarrow G'$  be a homomorphism and  $N' \triangleleft G'$  be a normal subgroup. Prove:  $N = f^{-1}[N']$  is normal in  $G$ . Also show that a surjective homomorphism  $f$  induces an isomorphism  $G/N \xrightarrow{\sim} G'/N'$ .
11. Determine all subgroups of  $A_4$ , and check which are normal.
12. Give an example of a group  $G$  with subgroups  $H_1$  and  $H_2$  for which we have  $H_1 \triangleleft H_2$  and  $H_2 \triangleleft G$  but *not*  $H_1 \triangleleft G$ .
13. Let  $D_n$  be the dihedral group of order  $2n$  from §3 and  $\rho \in D_n$  be a rotation of order  $n$ . Prove that  $[D_n, D_n]$  is generated by  $\rho^2$ , and deduce that

$$(D_n)_{\text{ab}} \cong \begin{cases} \{\pm 1\} & \text{if } n \text{ odd is,} \\ V_4 & \text{if } n \text{ even is.} \end{cases}$$

14. Determine the subgroups of  $D_n$  of index 2 for  $n \geq 1$ .
15. Determine the numbers of elements of  $\text{Hom}(S_n, \mathbf{C})$ ,  $\text{Hom}(S_n, \mathbf{C}^*)$ , and  $\text{Hom}(D_n, \mathbf{C}^*)$  for  $n \geq 1$ .
16. Let  $A$  be an abelian group written additively and  $n \geq 2$  be an integer. Give an explicit bijection between  $\text{Hom}(S_n, A)$  and the 2-torsion subgroup  $A[2] = \{a \in A : 2a = 0\}$  of  $A$ .
17. Let  $G$  be a group and  $N \subset G$  be the subgroup generated by  $S = \{g^2 : g \in G\}$ . Prove:  $N$  is normal in  $G$ , and  $G/N$  is abelian.
18. Calculate the commutator  $[(1\ 2\ 3), (1\ 4\ 5)] \in A_5$ , and prove that for  $n \geq 5$ , the commutator subgroup  $[A_n, A_n]$  is equal to  $A_n$ .
19. Determine  $[A_n, A_n]$  for  $n \leq 4$ .
20. Determine the number of elements of  $\text{Hom}(A_n, \mathbf{C}^*)$  for  $n \geq 1$ .
21. Let  $f : G \rightarrow G'$  be a homomorphism. Prove that there exists a homomorphism  $f_{\text{ab}} : G_{\text{ab}} \rightarrow G'_{\text{ab}}$  such that the diagram

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow & & \downarrow \\ G_{\text{ab}} & \xrightarrow{f_{\text{ab}}} & G'_{\text{ab}} \end{array}$$

with natural vertical arrows commutes.

[The abelianization of a group is said to be *functorial*: not only the groups but also the maps between them can be made abelian.]

22. Let  $H_1$  and  $H_2$  be finite subgroups of  $G$  with  $H_1 \cap H_2 = 1$ . Prove that the number of elements of the set  $H_1H_2 = \{h_1h_2 : h_1 \in H_1 \text{ and } h_2 \in H_2\}$  is equal to  $\#H_1 \cdot \#H_2$ . Show that  $H_1H_2$  is a subgroup of  $G$  if  $G$  is abelian, and give a non-abelian example where this is not the case.
23. Let  $N_1$  and  $N_2$  be normal subgroups of  $G$  with  $N_1 \cap N_2 = 1$ . Prove: for  $n_1 \in N_1$  and  $n_2 \in N_2$ , we have  $n_1n_2 = n_2n_1$ . Deduce that  $G$  contains a subgroup isomorphic to  $N_1 \times N_2$ .

24. Let  $N_1$  and  $N_2$  be as in the previous exercise. Prove that  $G/N_1 \times G/N_2$  contains a subgroup isomorphic to  $G$ .
25. Show that there is a natural bijection  $\text{Hom}(X, G_1 \times G_2) \leftrightarrow \text{Hom}(X, G_1) \times \text{Hom}(X, G_2)$  for any three groups  $G_1, G_2, X$ . Does something similar hold for  $\text{Hom}(G_1 \times G_2, X)$ ?
26. Let  $\text{SL}_3(\mathbf{R})$  be the group of matrices with determinant 1 in  $\text{GL}_3(\mathbf{R})$ . Prove: there is an isomorphism

$$\mathbf{R}^* \times \text{SL}_3(\mathbf{R}) \xrightarrow{\sim} \text{GL}_3(\mathbf{R}).$$

Does the dimension 3 matter?

27. Determine the center  $Z(K)$  of the cubic group.
28. Give an example of a group  $G$  with
- isomorphic normal subgroups  $N_1$  and  $N_2$  for which  $G/N_1$  and  $G/N_2$  are not isomorphic,
  - non-isomorphic normal subgroups  $N_1$  and  $N_2$  for which  $G/N_1$  and  $G/N_2$  are isomorphic.
29. Show that for  $n > 2$ , there exists an injective homomorphism  $D_n \rightarrow \text{Aff}(\mathbf{Z}/n\mathbf{Z})$  and that this is only an isomorphism for  $n \in \{3, 4, 6\}$ .
30. Show that the affine group  $\text{Aff}(\mathbf{R})$  is isomorphic to the matrix group

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} : a \in \mathbf{R}^*, b \in \mathbf{R} \right\} \subset \text{GL}_2(\mathbf{R}).$$

31. Show that the matrix group  $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathbf{R}^*, b \in \mathbf{R} \right\} \subset \text{GL}_2(\mathbf{R})$  is isomorphic to a direct product  $\mathbf{R}^* \times \mathbf{R}$ .
- \*32. Show that  $\text{SL}_2(\mathbf{R})$  is generated by the matrices of the form  $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$  and  $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$  with  $x \in \mathbf{R}$ .
33. Determine  $[\text{GL}_2(\mathbf{R}), \text{GL}_2(\mathbf{R})]$ , and show that every homomorphism  $f : \text{GL}_2(\mathbf{R}) \rightarrow A$  to an abelian group  $A$  factors through the determinant map  $\det : \text{GL}_2(\mathbf{R}) \rightarrow \mathbf{R}^*$ .  
[Hint: calculate commutators such as  $\left[ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} \right]$ , and use the previous exercise.]
34. Show that for  $n \geq 3$ , the group  $S_n$  is isomorphic to a semi-direct product  $A_n \rtimes C_2$  and that the conjugation action  $\sigma : C_2 \rightarrow \text{Aut}(A_n)$  depends on the choice of the subgroup  $C_2 \subset S_n$ .
35. In a semi-direct product  $G = N \rtimes H$ , is every normal subgroup  $N' \triangleleft N$  also a normal subgroup of  $G$ ?
36. Let  $A$  be an abelian group and  $G = A \rtimes C_2$  be the corresponding generalized dihedral group from 8.14.2.
- Show that every subgroup  $H \subset A$  is normal in  $G$ .
  - Determine the center  $Z(G)$  of  $G$ .
  - Determine the abelianization  $G_{\text{ab}}$ .
37. (*Goursat's lemma*)<sup>35</sup> Let  $H \subset G_1 \times G_2$  be a subgroup, and assume that the images of  $H$  under the projections onto the coordinates equal  $G_1$  and  $G_2$ . Define

$$N_1 = \{g_1 \in G_1 : (g_1, e_2) \in H\} \quad \text{and} \quad N_2 = \{g_2 \in G_2 : (e_1, g_2) \in H\}.$$

Prove that  $N_1$  and  $N_2$  are normal in, respectively,  $G_1$  and  $G_2$  and that  $H$  is the “graph” of an isomorphism  $\phi : G_1/N_1 \xrightarrow{\sim} G_2/N_2$ , in other words, that

$$H = \{(g_1, g_2) \in G_1 \times G_2 : \phi(g_1N_1) = g_2N_2\}.$$

38. Prove that every subgroup of  $C_5 \times S_4$  is of the form  $1 \times H$  or  $C_5 \times H$  with  $H$  a subgroup of  $S_4$ .
39. Determine the numbers of subgroups of  $C_5 \times C_5$  and  $C_5 \times C_{25}$ .
40. Let  $f : S_m \rightarrow S_n$  be a homomorphism. Prove:  $f[A_m] \subset A_n$ .
41. Let  $G^n$  be the  $n$ -tuple product of  $G$  with itself, and let  $C_n$  act on  $G^n$  by cyclic shifting as in the proof of 5.13. Show that this leads to a semi-direct product  $G^n \rtimes C_n$ , the *wreath product*  $G \wr C_n$  of  $G$  and  $C_n$ . What group is  $C_2 \wr C_2$ ?

## 9 ABELIAN GROUPS

The product constructions in §8 allow us to construct groups as (semi-)direct products of smaller groups. It is more difficult to recognize that a given group  $G$  is “built up” from smaller groups in this way. The problem comes down to finding a normal subgroup  $N \triangleleft G$  and a “complement”  $H \cong G/N$  in  $G$  to which Theorem 8.13 applies. A technique that can be used for this is the so-called *splitting of exact sequences*. This technique,<sup>36</sup> which is primarily a matter of efficient language use, will also prove helpful in the context of modules and vector spaces.

This section focuses mainly on the simpler case of *abelian* groups. For *finitely generated* abelian groups, we will prove a complete structure theorem, 9.11. For non-abelian groups, finding normal subgroups is a more complex problem we will deal with in §10.

### ► EXACT SEQUENCES

Given group homomorphisms  $f : A \rightarrow B$  and  $g : B \rightarrow C$ , we say that the sequence

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is *exact* (at  $B$ ) if we have  $\text{im } f = \ker g$ : the image of  $f$  is the kernel of  $g$ . Longer sequences of groups and homomorphisms such as

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} A_3 \xrightarrow{f_3} A_4 \xrightarrow{f_4} A_5$$

are called exact if we have  $\text{im } f_i = \ker f_{i+1}$  for  $i = 1, 2, 3$ . If  $A = 1$  is the trivial group, then the exactness of the sequence  $1 \rightarrow B \xrightarrow{g} C$  simply means that  $\ker g$  consists of only the unit element. By 4.4,  $g$  is then *injective*. Likewise, the exactness of the sequence  $A \xrightarrow{f} B \rightarrow 1$  means that the homomorphism is  $f$  *surjective*. Note that we do not need to specify the homomorphisms to and from the trivial group—there is no choice. A *short exact sequence* is an exact sequence of the form

$$(9.1) \quad 1 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 1.$$

If the maps  $f$  and  $g$  are clear from the context, they are often not denoted in the sequence. By the isomorphism theorem 4.10, the homomorphism  $g$  in (9.1) induces an isomorphism  $B/f[A] \cong C$ . The group  $B$  is also called an *extension* of  $C$  by  $A$ . The injection  $f$  is often viewed as an inclusion that makes  $A$  into a subgroup of  $B$ , in which case the notation  $B/A \cong C$  is often used for short. Note that  $B$  is finite if and only if  $A$  and  $C$  are and that in that case, we have  $\#B = \#A \cdot \#C$ .

Instead of groups and group homomorphisms, we can also consider the above for vector spaces and linear maps. The zero space, denoted by  $0$  for short, then plays the role of the trivial group. Much from this section is strongly reminiscent of what we have in linear algebra. That is not so surprising because we will see in §16 that vector spaces and abelian groups are special examples of *modules* over a ring.

If  $G$  is a group and  $N \triangleleft G$  is normal, then the quotient map  $\pi : G \rightarrow G/N$  fits into a short exact sequence

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} G/N \longrightarrow 1.$$

Let us try to express the structure of  $G$  in that of the smaller groups  $N$  and  $G/N$ . For suitable choices of  $N$ , we can sometimes obtain an isomorphism  $G \cong N \times G/N$ , which “splits”  $G$  into two smaller groups.

The general problem we are confronted with is, given a short exact sequence as in (9.1), determining the structure of  $B$  from those of  $A$  and  $C$ . This is not always possible. For example, if  $G$  has a normal subgroup  $N$  of order 2 for which  $G/N$  is isomorphic to the Klein four-group  $V_4 \cong C_2 \times C_2$ , then  $G$  is a group of order 8 that fits into a short exact sequence

$$1 \longrightarrow C_2 \longrightarrow G \longrightarrow V_4 \longrightarrow 1.$$

Even if we know that  $G$  is abelian, this does not fix the isomorphism class of  $G$ : both  $C_2 \times V_4 = C_2 \times C_2 \times C_2$  and  $C_4 \times C_2$  fit into such a sequence. So there exist “truly different” extensions of  $V_4$  by  $C_2$ .

**Exercise 1.** Show that the dihedral group  $D_4$  and the quaternion group  $Q$  also fit into this sequence.

### ► SPLITTING EXACT SEQUENCES

All groups in the remainder of this section will be abelian. To better highlight the analogies with linear algebra, we will write these groups additively as much as possible. So we write  $kx$  for the sum of  $k \in \mathbf{Z}$  elements  $x$  (for  $k < 0$ , we take  $|k|$  elements  $-x$ ) and denote the trivial group by 0. In this additive context, we usually write  $A \oplus C$  instead of  $A \times C$ . The direct sum  $A \oplus C$  of two abelian groups  $A$  and  $C$  fits naturally into a short exact sequence

$$0 \longrightarrow A \xrightarrow{\varepsilon_A} A \oplus C \xrightarrow{\pi_C} C \longrightarrow 0.$$

Here  $\varepsilon_A$  is the embedding  $a \mapsto (a, 0)$  into the first coordinate, and  $\pi_C$  is the projection  $(a, c) \mapsto c$  onto the second coordinate. We can now use the terminology of commutative diagrams introduced in §8 to say when the sequence (9.1) is “in fact” the simple sequence above.

**9.2. Definition.** A short exact sequence  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  of abelian groups splits (or is split) if there exists a homomorphism  $\phi : B \rightarrow A \oplus C$  such that the diagram of groups and homomorphisms

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow \text{id}_A & & \downarrow \phi & & \downarrow \text{id}_C & & \\ 0 & \longrightarrow & A & \xrightarrow{\varepsilon_A} & A \oplus C & \xrightarrow{\pi_C} & C & \longrightarrow & 0 \end{array}$$

commutes.

In 9.2, we do not require that  $\phi$  is an isomorphism because this is automatically the case. After all, for  $b \in \ker \phi$ , we have  $g(b) = \pi_C(\phi(b)) = 0$ , so by the exactness, we have  $b = f(a)$  with  $a \in A$ . It follows from  $(0, 0) = \phi(b) = \phi(f(a)) = (a, 0)$  that  $a = 0$ , so  $b = 0$ , and  $\phi$  is injective. The image of  $\phi$  contains the subgroup  $(\phi \circ f)[A] = \varepsilon_A[A] = A \oplus 0$ . Moreover, by the surjectivity of  $g = \pi_C \circ \phi$ , for every  $c \in C$ , there is an element  $(a, c) \in \text{im}(\phi)$ . Consequently, we have  $\text{im}(\phi) = A \oplus C$ , so  $\phi$  is an isomorphism.

Arguments of the type above fall into the category of “diagram chasing.” They are common in commutative algebra. See also Exercise 9.9.5.

The fundamental question is now how to see whether an exact sequence splits.

**9.3. Theorem.** For a short exact sequence  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  of abelian groups, the following statements are equivalent:

1. There exists a homomorphism  $p : B \rightarrow A$  such that  $p \circ f = \text{id}_A$ .
2. There exists a homomorphism  $s : C \rightarrow B$  such that  $g \circ s = \text{id}_C$ .
3. The exact sequence splits.

The homomorphisms  $p$  and  $s$ , which as a rule are not unique, are also called a *retraction* of the injection  $f$  and a *section* of the surjection  $g$ . They “split” the extension  $B$  of  $C$  by  $A$ .

**Proof of 9.3.** Let  $\phi : B \xrightarrow{\sim} A \oplus C$  be a splitting of the extension. Then the composition with the projection onto the first coordinate gives a homomorphism  $p : B \rightarrow A$  for which  $p \circ f$  is the identity on  $A$ . Likewise, the composition of the natural embedding  $C \rightarrow A \oplus C$  with  $\phi^{-1}$  gives a section  $C \rightarrow B$  of  $g$ . This shows that (1) and (2) are implied by (3).

Given a retraction  $p$  of  $f$  as in (1), we define a homomorphism  $\phi : B \rightarrow A \oplus C$  by setting  $\phi(b) = (p(b), g(b))$ . Then  $B$  and  $\phi$  fit into the commutative diagram in 9.2, so  $\phi$  is an isomorphism, and the sequence splits.

Finally, let a section  $s$  of  $g$  as in (2) be given. For  $b \in B$ ,  $b$  and  $(s \circ g)(b)$  have the same image under  $g$ , so we have  $b - (s \circ g)(b) \in \ker g = \text{im } f$ . The map  $p : B \rightarrow A$  that sends  $b \in B$  to the element  $a \in A$  with  $f(a) = b - (s \circ g)(b)$  is now a homomorphism. For  $b \in \text{im } f$ , we have  $(s \circ g)(b) = s(0) = 0$ , so we have  $p(f(a)) = a$ , and  $p$  is a retraction of  $f$  as in (1). As above, it follows that the sequence splits.  $\square$

**Exercise 2.** Show that the map  $(a, c) \mapsto f(a) + s(c)$  gives an isomorphism  $A \oplus C \xrightarrow{\sim} B$  for every section  $s$  of  $g$ .

In the typical case where  $C$  is *cyclic*, 9.3 gives the following result.

**9.4. Lemma.** Let  $C$  be a cyclic group with generator  $c$ . Then the exact sequence of abelian groups

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

splits if and only if one of the following conditions is satisfied:

1. The generator  $c$  has infinite order.

2. The generator  $c$  has finite order  $n$ , and the fiber  $g^{-1}(c)$  over  $c$  contains an element of order  $n$ .

**Proof.** By 9.3, the sequence splits if and only if there exists a section  $s : C = \langle c \rangle \rightarrow B$  of  $g$ . Such a section is fixed by the choice of an element  $b = s(c) \in B$ , and the question is whether a suitable  $b$  exists.

If  $c$  has finite order  $n$ , not every element  $b$  in the fiber  $g^{-1}(c)$  above  $c$  gives a section  $s$  with  $s(c) = b$ . After all, for such a section, we have  $nb = s(nc) = s(0) = 0 \in B$ , so the order of  $b$  divides  $n$ . Since the orders of the elements in the fiber over  $c$  are always multiples of the order of  $c$  itself (Exercise 4.16), a section can only exist if there exists an element  $b \in g^{-1}(c)$  of order exactly  $n$ . For such an element  $b$  of order  $n$ , we indeed obtain a section by setting  $s(kc) = kb$ . Conclusion: the sequence splits if and only if  $g^{-1}(c)$  contains an element of order  $n$ .

For  $c$  of infinite order, we have  $C \cong \mathbf{Z}$ , and the constraint mentioned above disappears: every element  $b \in g^{-1}(c) \subset B$  gives a section  $s$  of  $g$  with  $s(c) = b$ , and the sequence splits.  $\square$

**Exercise 3.** Show that every short exact sequence of abelian groups  $0 \rightarrow A \rightarrow B \rightarrow \mathbf{Z}^n \rightarrow 0$  splits.

We can easily generalize 9.4 to the case where  $C$  is a direct sum of cyclic groups. The sequence splits if and only if we can “lift” each of the generators of these cyclic parts to an element of the corresponding fiber with the same order. Generators of infinite order can always be lifted as in the previous exercise; for generators of finite order, the problem may arise that the orders of *all* elements of the fiber are too large. The sequence then does not split.

**9.5. Example.** The natural homomorphism  $g : \mathbf{Z}/6\mathbf{Z} \rightarrow \mathbf{Z}/3\mathbf{Z}$  given by  $g(x \bmod 6) = x \bmod 3$  is surjective with kernel  $\{0 \bmod 6, 3 \bmod 6\} \cong \mathbf{Z}/2\mathbf{Z}$  of order 2. To obtain a section  $s : \mathbf{Z}/3\mathbf{Z} \rightarrow \mathbf{Z}/6\mathbf{Z}$  of  $g$ , we must designate an image  $s(1 \bmod 3) \in \mathbf{Z}/6\mathbf{Z}$ . The elements of the fiber  $g^{-1}(1 \bmod 3) = \{1 \bmod 6, 4 \bmod 6\}$  have order, respectively, 6 and 3. So only  $4 \bmod 6$  qualifies as the image of  $1 \bmod 3$ , and the corresponding section  $s : \mathbf{Z}/3\mathbf{Z} \rightarrow \mathbf{Z}/6\mathbf{Z}$  given by  $s(x \bmod 3) = 4x \bmod 6$  gives a splitting of the exact sequence

$$0 \rightarrow \mathbf{Z}/2\mathbf{Z} \rightarrow \mathbf{Z}/6\mathbf{Z} \xrightarrow{g} \mathbf{Z}/3\mathbf{Z} \rightarrow 0.$$

The resulting isomorphism  $\mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$  is a special case of 6.15.

In the analogous situation with  $g : \mathbf{Z}/8\mathbf{Z} \rightarrow \mathbf{Z}/4\mathbf{Z}$  given by  $g(x \bmod 8) = x \bmod 4$ , the fiber  $g^{-1}(1 \bmod 4) = \{1 \bmod 8, 5 \bmod 8\}$  above  $1 \bmod 4$  contains two elements of order 8, so *no* element of the desired order 4. In this case,  $g$  has no section, and since  $\ker(g) = \{0 \bmod 8, 4 \bmod 8\} \cong \mathbf{Z}/2\mathbf{Z}$ , we obtain a sequence

$$0 \rightarrow \mathbf{Z}/2\mathbf{Z} \rightarrow \mathbf{Z}/8\mathbf{Z} \xrightarrow{g} \mathbf{Z}/4\mathbf{Z} \rightarrow 0$$

that *does not* split. The group  $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$  is indeed not cyclic of order 8.

**9.6. Lemma.** A short exact sequence  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$  of finite abelian groups splits if the orders of  $A$  and  $C$  are relatively prime.

**Proof.** By 6.4 and the assumption, a multiple  $m$  of  $\#A$  exists for which we have  $m \equiv 1 \pmod{\#C}$ . Take  $c \in C$ , and choose an arbitrary element  $b \in g^{-1}(c)$  in the fiber of  $g$  over  $c$ . We claim that  $mb$  is also an element in the fiber over  $c$  and that it is independent of the choice of the element  $b \in g^{-1}(c)$ . For the first statement, we note that we have  $g(mb) - g(b) = (m - 1)g(b) = (m - 1)c = 0$  because  $m - 1$  is divisible by the order of  $C$ . For the second, we choose two elements  $b, b' \in g^{-1}(c)$ . Then we have  $b - b' \in \ker(g) = f[A]$ , and since the  $m$ -tuple of any element in  $f[A]$  is the zero element, we have  $m(b - b') = 0$  and, therefore,  $mb = mb'$ .

Now that we know that the  $m$ -tuple  $mb$  of an arbitrary element  $b \in g^{-1}(c)$  gives a unique element in  $g^{-1}(c)$ , it follows immediately that the map  $s : C \rightarrow B$  given by  $s(c) = mb$  is a homomorphism. After all, for  $b_1$  and  $b_2$  in the fibers over, respectively,  $c_1$  and  $c_2$ , the sum  $b_1 + b_2$  is in the fiber over  $c_1 + c_2$ . This gives  $s(c_1) + s(c_2) = mb_1 + mb_2 = m(b_1 + b_2) = s(c_1 + c_2)$ .

We conclude that  $s$  is a section of  $g$ , and by 9.3, the sequence splits.  $\square$

### ► FREE ABELIAN GROUPS

As in 2.8, we say that a subset  $S$  of an abelian group  $A$  *generates* the group  $A$  if every element  $x \in A$  can be written as a sum  $x = \sum_{s \in S} c_s s$  with numbers  $c_s \in \mathbf{Z}$  that are different from 0 for only finitely many  $s$ . Such a representation is generally not unique. If all  $x \in A$  can be written uniquely as such a sum, then  $A$  is called a *free abelian group* and  $S$  a *basis* of  $A$ . In such a case, the uniqueness of the representation of  $x = 0$  means that the elements of a basis  $S$  are *linearly independent*; that is, we have  $\sum_{s \in S} c_s s = 0$  if and only if  $c_s = 0$  holds for all  $s \in S$ . The cardinality of a basis of  $A$  is called the *free rank* or *rank*, for short, of  $A$ . It can be infinite. For  $S = \emptyset$ ,  $A = 0$  is the trivial group of rank 0.

**Exercise 4.** Show that the set  $\mathcal{P}$  of primes forms a basis of the multiplicative group  $\mathbf{Q}_{>0}$  of positive rational numbers.

For a free abelian group  $A$  with *finite* basis  $S = \{s_1, s_2, \dots, s_n\}$  of cardinality  $n$ , the map

$$\begin{aligned} \mathbf{Z}^n &\longrightarrow A \\ (c_i)_{i=1}^n &\longmapsto \sum_{i=1}^n c_i s_i \end{aligned}$$

is an isomorphism. The induced isomorphism  $A/2A \cong (\mathbf{Z}/2\mathbf{Z})^n$  shows that  $A/2A$  has order  $2^n$ , and we conclude that the rank of  $A$  apparently does not depend on the choice of a basis of  $A$ .

The given definitions strongly resemble similar ones from linear algebra. For example, the rank of an abelian group is the analog of the dimension of a vector space. The important difference is that here, the “scalars” lie in the ring  $\mathbf{Z}$  and not in a field. The theory of abelian groups, which can be referred to as “linear algebra over  $\mathbf{Z}$ ,” therefore differs somewhat from “classic” linear algebra. For example, our argument for the rank’s independence of the choice of a basis does not work for the dimension of vector spaces. Moreover, not every abelian group has a basis.

**Exercise 5.** Show that a free abelian group contains no elements  $x \neq 0$  of finite order.

An abelian group  $A$  is called *finitely generated* if there exists a finite subset  $S \subset A$  that generates  $A$ . If  $S = \{s_1, s_2, \dots, s_n\}$  is such a subset, then the map  $\mathbf{Z}^n \rightarrow A$  given above is surjective but not necessarily injective. By the isomorphism theorem 4.10, there is an isomorphism  $A \cong \mathbf{Z}^n/H$  for some  $H \subset \mathbf{Z}^n$ . So the finitely generated abelian groups are all of the form  $\mathbf{Z}^n/H$  for some  $n \geq 0$  and  $H \subset \mathbf{Z}^n$ . Note that every quotient of a finitely generated abelian group is again finitely generated.

All proofs of the structure theorem 9.11 for finite abelian groups in some way use the explicit knowledge of the subgroups of  $\mathbf{Z}^n$ . A rather direct proof is given in Exercises 9.42–43. We follow a slightly different path giving us some interesting intermediary results.

**9.7. Theorem.** *Every subgroup  $A \subset \mathbf{Z}^n$  is free of rank  $k \leq n$ .*

**Proof.** We apply induction on  $n$ . For  $n = 0$ , the group  $A = 0 = \mathbf{Z}^0$  is free of rank 0. Suppose that the theorem is proved for subgroups of  $\mathbf{Z}^{n-1}$ , and consider the projection  $\pi : \mathbf{Z}^n \rightarrow \mathbf{Z}$  onto the last coordinate. This gives a short exact sequence

$$0 \longrightarrow A \cap \ker \pi \longrightarrow A \xrightarrow{\pi} \pi[A] \longrightarrow 0.$$

By the induction hypothesis, the subgroup  $A' = A \cap \ker \pi$  of  $\ker \pi \cong \mathbf{Z}^{n-1}$  is free of rank  $k' \leq n - 1$ . We now have two cases. In the case  $\pi[A] = 0$ , it follows immediately that  $A = A'$  is free of rank  $\leq n - 1$ . In the other case,  $\pi[A]$  is a non-trivial subgroup of  $\mathbf{Z}$ , so as in 6.2, it is of the form  $\pi[A] = m\mathbf{Z} \cong \mathbf{Z}$ . By 9.4, the extension  $A$  of  $\pi[A] \cong \mathbf{Z}$  by  $A'$  is split; it follows that  $A \cong A' \oplus \mathbf{Z}$  is free of rank  $k' + 1 \leq n$ .  $\square$

**9.8. Example.** We use the method of 9.7 to determine a basis of the subgroup  $A \subset \mathbf{Z}^3$  given by

$$A = \{(x, y, z) \in \mathbf{Z}^3 : 4x + y + 3z \equiv 0 \pmod{6}\}.$$

For the projection  $\pi : A \rightarrow \mathbf{Z}$  onto the  $z$ -coordinate, we have  $\pi(a) = 1$  for the element  $a = (1, -1, 1) \in A$ . This gives  $A = A' \oplus \langle a \rangle$  with  $A' = \{(x, y, 0) \in \mathbf{Z}^3 : 4x + y \equiv 0 \pmod{6}\}$ . We can view  $A'$  as a subgroup of  $\mathbf{Z}^2$ . The projection  $\pi' : A' \rightarrow \mathbf{Z}$  onto the  $y$ -coordinate is *not* surjective:  $y$  must clearly be even. We have  $\pi'[A'] = 2\mathbf{Z}$  because  $\pi'(a') = 2$  holds for  $a' = (1, 2, 0) \in A'$ . Consequently,  $A' = \ker \pi' \oplus \langle a' \rangle$ , and  $\ker \pi' = \{(x, 0, 0) \in \mathbf{Z}^3 : 4x \equiv 0 \pmod{6}\}$  is generated by  $(3, 0, 0)$ . We see that  $A$  is free of rank 3, and if we write the elements of  $\mathbf{Z}^3$  as column vectors, we have

$$A = \mathbf{Z} \cdot \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix} \oplus \mathbf{Z} \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} \oplus \mathbf{Z} \cdot \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}.$$

The resulting “upper triangular form” of the basis with respect to the standard basis of  $\mathbf{Z}^3$  makes it easy to express an element of  $A$  in this basis.

**Exercise 6.** Determine the index of  $A$  in  $\mathbf{Z}^3$  in the example above.

**9.9. Corollary.** *Let  $A$  be a finitely generated abelian group in which every element  $a \neq 0$  has infinite order. Then  $A$  is free of finite rank.*

**Proof.** Let  $S \subset A$  be a finite set of generators and  $S' \subset S$  be a subset of linearly independent elements that is the largest possible. Then the subgroup  $F \subset A$  generated by  $S'$  is a free abelian group with basis  $S'$ . The maximality of  $S'$  implies that for every element  $s \in S \setminus S'$ , there exists a positive number  $m_s \in \mathbf{Z}$  with  $m_s s \in F$ . Let  $m \geq 1$  be a common multiple of the numbers  $m_s$  for  $s \in S \setminus S'$ . Then multiplication by  $m$  is a homomorphism  $A \rightarrow A$  whose image lies in  $F$ . By the assumption, this homomorphism is injective. It follows that  $A \cong mA \subset F$  is isomorphic to a subgroup of a free group of finite rank. By 9.7,  $A$  is then also free of finite rank.  $\square$

Using a variant of the proof of 9.9, we can prove that discrete subgroups of  $\mathbf{R}^n$  are always free of finite rank. A subgroup  $A \subset \mathbf{R}^n$  is called *discrete* if every bounded subset of  $\mathbf{R}^n$  contains only finitely many elements of  $A$ . Such subgroups are also called *lattices* in  $\mathbf{R}^n$ .

**9.10. Theorem.** *A discrete subgroup  $A \subset \mathbf{R}^n$  is free of rank  $k \leq n$ .*

**Proof.** From linear algebra, we know that a maximal subset  $S \subset A$  of elements linearly independent over  $\mathbf{R}$  cannot contain more than  $n$  elements. Let  $S = \{s_1, s_2, \dots, s_k\}$  be such a subset, with  $k \leq n$ . Then every element  $x \in A$  can be written as  $x = \sum_{i=1}^k r_i s_i$  with  $r_i \in \mathbf{R}$ . Let us prove that the free subgroup  $A_0 \subset A$  generated by  $S$  has *finite* index in  $A$ .

Every real number is the sum of an integer and an element  $\lambda \in [0, 1)$ , so every element of  $A$  can be written as the sum of an element of  $A_0$  and an element of the set

$$F = \left\{ \sum_{i=1}^k r_i s_i : 0 \leq r_i < 1 \right\}.$$

Since  $F$  is a bounded set in  $\mathbf{R}^n$ , it contains only finitely many elements of  $A$ , so there are only finitely many cosets of  $A_0$  in  $A$ . The index  $m = [A : A_0]$  is therefore finite. Multiplication by  $m$  is now a homomorphism that sends  $A$  injectively to the free group  $A_0$  of rank  $k$ . It follows, again from 9.7, that  $A$  itself is free of finite rank, and this rank is at most  $k \leq n$ .  $\square$

**Exercise 7.** Show that  $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Z}\}$  is a subgroup of  $\mathbf{R}$  that is free of rank 2.

### ► STRUCTURE THEOREM

We introduce some terminology to formulate the structure theorem for finitely generated abelian groups.

An abelian group  $A$  in which every element  $a \neq 0$  has infinite order is called *torsion-free*. An element of  $A$  of finite order is called a *torsion element* of  $A$ . If we have  $ma = 0 \in A$  for  $m \in \mathbf{Z}$ , then  $a$  is *annihilated* by  $m$ . We say that a number  $m \in \mathbf{Z}$  annihilates the group  $A$  if we have  $ma = 0$  for all  $a \in A$ . The torsion elements of  $A$  form the *torsion subgroup*  $A^{\text{tor}} \subset A$ , and  $A$  is torsion-free if we have  $A^{\text{tor}} = 0$ . More generally, the quotient  $A/A^{\text{tor}}$  is always torsion-free. After all, an element  $a \in A$  for which  $ma$  is a torsion element for some  $m > 0$  is itself also torsion.

**Exercise 8.** Show that the elements of finite order in a non-abelian group do not, in general, form a subgroup.

An abelian group  $A$  is called a *torsion group* if we have  $A^{\text{tor}} = A$ . Finite abelian groups are always torsion. The additive group  $\mathbf{Q}/\mathbf{Z}$  is an example of an infinite torsion group.

A finitely generated torsion group is finite. After all, a surjection  $\mathbf{Z}^n \rightarrow A$  that maps the “standard basis” of  $\mathbf{Z}^n$  onto elements annihilated by  $m$  leads to a surjective map  $(\mathbf{Z}/m\mathbf{Z})^n \twoheadrightarrow A$  from a finite group to  $A$ .

**9.11. Theorem.** *Every finitely generated abelian group  $A$  is a direct sum of cyclic groups. There exist an  $r \geq 0$  and an isomorphism*

$$A \cong A^{\text{tor}} \oplus \mathbf{Z}^r.$$

The torsion subgroup  $A^{\text{tor}}$  of  $A$  is finite and isomorphic to the direct sum of its Sylow  $p$ -subgroups  $A(p)$ . For every prime  $p$ , there is an isomorphism

$$A(p) \xrightarrow{\sim} \mathbf{Z}/p^{k_1}\mathbf{Z} \oplus \mathbf{Z}/p^{k_2}\mathbf{Z} \oplus \dots \oplus \mathbf{Z}/p^{k_m}\mathbf{Z},$$

where the integers  $m \geq 0$  and  $k_1 \geq k_2 \geq \dots \geq k_m > 0$  are uniquely determined by  $p$ .

The number  $r$  in 9.11, which is 0 exactly when  $A$  is finite, is called the *free rank* of  $A$ .

**Proof.** Consider the exact sequence  $0 \rightarrow A^{\text{tor}} \rightarrow A \rightarrow A/A^{\text{tor}} \rightarrow 0$ . The group  $A/A^{\text{tor}}$  is torsion-free, and as a quotient of  $A$ , it is finitely generated, so by 9.9, it is isomorphic to  $\mathbf{Z}^r$  for some  $r \geq 0$ . After 9.4 (in Exercise 3), we already saw that such an exact sequence splits, and we obtain an isomorphism  $A \cong A^{\text{tor}} \oplus \mathbf{Z}^r$ . As a quotient of  $A$ , the group  $A^{\text{tor}} \cong A/\mathbf{Z}^r$  is finitely generated. Since it is also torsion, it is finite. By 8.10,  $A^{\text{tor}}$  is now isomorphic to the sum of its Sylow  $p$ -subgroups  $A(p)$ .

To prove the structure theorem for the Sylow  $p$ -subgroups  $A(p)$ , which are finite abelian  $p$ -groups, we use induction on the order of  $A(p)$ . For  $A(p)$  of order 1 or  $p$ , there is nothing to prove.

Now, suppose that every abelian  $p$ -group of order less than  $\#A(p)$  is a sum of cyclic  $p$ -groups, and choose an element  $x \in A(p)$  that has *maximal* order  $p^{k_1}$  in  $A(p)$ . Every element of  $A(p)$  then has order  $p^k$  with  $k \leq k_1$ . We consider the exact sequence

$$0 \longrightarrow \langle x \rangle \longrightarrow A(p) \xrightarrow{g} A(p)/\langle x \rangle \longrightarrow 0.$$

By the induction hypothesis, we have  $A(p)/\langle x \rangle \cong \mathbf{Z}/p^{k_2}\mathbf{Z} \oplus \mathbf{Z}/p^{k_3}\mathbf{Z} \oplus \dots \oplus \mathbf{Z}/p^{k_m}\mathbf{Z}$  for integers  $k_i \leq k_1$ , and it suffices to show that the sequence splits. We want to construct a section  $s$  of  $g$ ; this means that for every one of the generators  $y_2, y_3, \dots, y_m$  of the cyclic components of  $A(p)/\langle x \rangle$ , we must specify an element  $s(y_i) \in g^{-1}(y_i)$  of order  $p^{k_i}$ .

First take an arbitrary element  $x_i \in g^{-1}(y_i)$ . Let us show that, once we subtract a suitable multiple of  $x$ , this element has order  $p^{k_i}$ . Since  $p^{k_i}x_i$  is an element of  $\ker g = \langle x \rangle$ , there exists a number  $n_i$  with  $p^{k_i}x_i = n_i x$ . Since  $A(p)$  is annihilated by  $p^{k_1}$ , we have

$$(p^{k_1 - k_i} n_i) x = p^{k_1} x_i = 0.$$

It follows that  $p^{k_1}$  is a divisor of  $p^{k_1 - k_i} n_i$ , in other words, that  $n_i$  is divisible by  $p^{k_i}$ . If we write  $n_i = p^{k_i} u_i$ , then we have  $p^{k_i}(x_i - u_i x) = 0$ , and we conclude that  $x_i - u_i x \in g^{-1}(y_i)$

has the desired order  $p^{k_i}$ . This show that there exists a section and that our sequence splits.

The uniqueness of  $m$  and of the exponent  $k_i$  also follows by induction on the order of  $A(p)$ . For  $A(p) = 1$ , we have  $m = 0$ , and there is nothing to prove. For  $A(p) \neq 1$ , given a set of exponents  $k_i$  for  $A$ , we can deduce a set of exponents for the subgroup  $pA(p) \subsetneq A(p)$  by replacing  $k_i$  with  $k_i - 1$  and leaving it out if we have  $k_i - 1 = 0$ . By the induction hypothesis, the exponents of  $pA(p)$  are uniquely determined, so the exponents  $k_i \geq 2$  of  $A(p)$  also are. To obtain the uniqueness of *all*  $k_i$ , it now suffices to observe that the *number* of exponents  $m$  of  $A(p)$  is uniquely determined by  $A$ . After all, the given representation leads to an isomorphism  $A(p)/pA(p) \cong (\mathbf{Z}/p\mathbf{Z})^m$ , and the order  $p^m$  of  $A^{\text{tor}}/pA^{\text{tor}}$  only depends on  $A$ .  $\square$

**9.12. Corollary.** *Every finite abelian group  $A$  has a unique representation*

$$A \cong \mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_2\mathbf{Z} \oplus \dots \oplus \mathbf{Z}/d_t\mathbf{Z},$$

with numbers  $d_i \geq 2$  that satisfy the divisibility relations  $d_t \mid d_{t-1} \mid \dots \mid d_2 \mid d_1$ .

**Proof.** For every  $p$  that divides the order of  $A$ , write the Sylow  $p$ -subgroup  $A(p)$  as a direct sum of cyclic  $p$ -groups with orders  $p^{k_{1,p}} \geq p^{k_{2,p}} \geq \dots \geq p^{k_{m,p}}$  as in 9.11. By taking  $k_{i,p} = 0$  where necessary, we may assume that for every prime  $p$ , the number of exponents  $m$  is equal to a fixed number  $t$  and that there is a prime  $p$  with  $k_{t,p} \neq 0$ . Now take  $d_i = \prod_p p^{k_{i,p}}$  for  $i = 1, 2, \dots, t$ . Then we have  $\mathbf{Z}/d_i\mathbf{Z} \cong \prod_p \mathbf{Z}/p^{k_{i,p}}\mathbf{Z}$  by 6.16. The product over the  $i$  gives

$$\prod_{i=1}^t \mathbf{Z}/d_i\mathbf{Z} \cong \prod_p \prod_{i=1}^t \mathbf{Z}/p^{k_{i,p}}\mathbf{Z} \cong \prod_p A(p) \cong A.$$

We leave the proof of the uniqueness of the  $d_i$  to the reader as an exercise.  $\square$

**9.13. Corollary.** *An abelian group of square-free order is cyclic.*

The numbers  $d_i$  in 9.12 are called the *elementary divisors* of  $A$ . The greatest elementary divisor  $d_1$  of  $A \neq 1$  is the maximal order of an element of  $A$  and is called the *exponent* of  $A$ ; it is the smallest positive number that annihilates  $A$ . The trivial group has exponent 1. The exponent of  $A$  divides the order of  $A$  and is equal to  $\#A$  exactly when  $A$  is cyclic. If the exponent of  $A$  is a prime  $p$ , then  $A$  is a direct sum of cyclic groups of order  $p$  and  $A$  is called an *elementary abelian  $p$ -group*.

The number  $t$  in 9.12 is the minimal number of elements needed to generate  $A$ . After all, for every prime divisor  $p \mid d_t$ , the quotient  $A/pA \cong (\mathbf{Z}/p\mathbf{Z})^t$  is a vector space of dimension  $t$  over  $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ , and this cannot be generated by fewer than  $t$  elements. If for a prime  $p$ , we define the  *$p$ -rank* of a finite abelian group  $A$  as the dimension of the vector space  $A/pA$  over the field  $\mathbf{Z}/p\mathbf{Z}$ , then  $t$  is the maximum over all primes  $p$  of the  $p$ -rank of  $A$ .

**Exercise 9.** Show that  $A$  is cyclic if and only if all its Sylow  $p$ -subgroups are.

► THE GROUP  $(\mathbf{Z}/n\mathbf{Z})^*$

A common finite abelian group is the group  $(\mathbf{Z}/n\mathbf{Z})^*$  of invertible residue classes modulo  $n$  from 6.11. By restricting the ring isomorphism 6.16 to the group of units of  $\mathbf{Z}/n\mathbf{Z}$ , we obtain a group isomorphism

$$(\mathbf{Z}/n\mathbf{Z})^* \xrightarrow{\sim} \prod_p (\mathbf{Z}/p^{\text{ord}_p(n)}\mathbf{Z})^*.$$

To write  $(\mathbf{Z}/n\mathbf{Z})^*$  as a sum (or product) of cyclic groups, it suffices to do so for every group  $(\mathbf{Z}/p^k\mathbf{Z})^*$  with  $p$  prime and  $k \geq 1$ . For  $k = 1$ , we know from 7.7 that  $(\mathbf{Z}/p\mathbf{Z})^*$  is cyclic.

**9.14. Lemma.** *Let  $p$  be an odd prime and  $k \geq 2$  be an integer. Then we have the following:*

1. *The order of  $\overline{1+p} \in (\mathbf{Z}/p^k\mathbf{Z})^*$  is  $p^{k-1}$ .*
2. *The order of  $\overline{5} \in (\mathbf{Z}/2^k\mathbf{Z})^*$  is  $2^{k-2}$ .*

**Proof.** We use induction on  $s$  to prove the equality

$$\text{ord}_p[(1+p)^{p^s} - 1] = s + 1$$

for  $p$  odd and  $s \geq 0$ . For  $s = 0$ , the equality is correct. Suppose that it is correct for  $s = n - 1 \geq 0$ , and write  $(1+p)^{p^{n-1}} = 1 + up^n$  with  $p \nmid u$ . Then for  $s = n \geq 1$ , we have

$$(1+p)^{p^n} = (1+up^n)^p = 1 + p \cdot up^n + \left(\sum_{i=2}^{p-1} \binom{p}{i} u^i p^{in}\right) + u^p p^{pn}$$

by Newton's binomial theorem. The binomial coefficients in the indexed sum are divisible by  $p$ , so all terms of this sum contain at least  $2n + 1 \geq n + 2$  factors  $p$ . Moreover, the last term  $p^{pn}$  contains  $pn \geq n + 2$  factors  $p$ —here we use the assumption  $p \neq 2$ . We conclude that  $(1+p)^{p^n} - 1$  is congruent to  $up^{n+1} \pmod{p^{n+2}}$ ; this gives the desired equality for  $s = n$ . The proved equality shows that for odd  $p$ , the  $p^{k-1}$ -th power of  $\overline{1+p}$  in  $(\mathbf{Z}/p^k\mathbf{Z})^*$  is the unit element, whereas the  $p^{k-2}$ -th power is not. The order of  $\overline{1+p}$  is then equal to  $p^{k-1}$ , as stated in (1).

The proof of (2) is analogous to that of (1) and is left to the reader. Proving the equality  $\text{ord}_2[5^{2^s} - 1] = s + 2$  for  $s \geq 0$  concludes the proof.  $\square$

**9.15. Theorem.** *Let  $p$  be an odd prime and  $k > 0$  be an integer.*

1. *The group  $(\mathbf{Z}/p^k\mathbf{Z})^*$  is cyclic of order  $p^{k-1}(p-1)$ .*
2. *The group  $(\mathbf{Z}/2^k\mathbf{Z})^*$  is cyclic of order  $2^{k-1}$  for  $k \leq 2$ , and for  $k \geq 3$ , we have*

$$(\mathbf{Z}/2^k\mathbf{Z})^* = \langle \overline{5} \rangle \times \langle \overline{-1} \rangle \cong \mathbf{Z}/2^{k-2}\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

**Proof.** The canonical map  $(\mathbf{Z}/p^k\mathbf{Z})^* \rightarrow (\mathbf{Z}/p\mathbf{Z})^*$  is surjective, and the kernel is a subgroup of  $(\mathbf{Z}/p^k\mathbf{Z})^*$  of order  $p^{k-1}$  that contains  $\overline{1+p}$ . It follows from 9.14 that for odd  $p$ ,  $\overline{1+p}$  generates the kernel, which gives a natural exact sequence

$$1 \longrightarrow \langle \overline{1+p} \rangle \longrightarrow (\mathbf{Z}/p^k\mathbf{Z})^* \longrightarrow (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow 1.$$

The group  $(\mathbf{Z}/p\mathbf{Z})^*$  is cyclic of order  $p-1$  by 7.7, and since  $p-1$  and  $p^{k-1}$  are relatively prime, the sequence splits by 9.6. As a product of two cyclic groups of relatively prime orders,  $(\mathbf{Z}/p^k\mathbf{Z})^*$  is also cyclic by 6.15. This proves (1).

It is clear that  $(\mathbf{Z}/2^k\mathbf{Z})^*$  is cyclic for  $k \leq 2$ . For  $k \geq 3$ , we can imitate the proof of (1), but in this explicit case, we can also apply 8.8 to the subgroups  $H_1 = \langle \bar{5} \rangle$  and  $H_2 = \langle \bar{-1} \rangle$ . By 9.14.2,  $H_1 \cong \mathbf{Z}/2^{k-2}\mathbf{Z}$  is a cyclic subgroup of index 2 in  $(\mathbf{Z}/2^k\mathbf{Z})^*$ . Since all powers of 5 are congruent to 1 mod 4, we have  $-1 \notin H_1$ , and  $H_2 \cong \mathbf{Z}/2\mathbf{Z}$  satisfies  $H_1 \cap H_2 = 1$ . An application of 8.8 now gives the desired isomorphism  $(\mathbf{Z}/2^k\mathbf{Z})^* = \langle \bar{5} \rangle \times \langle \bar{-1} \rangle \cong \mathbf{Z}/2^{k-2}\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ .  $\square$

## EXERCISES.

10. Consider the following commutative diagram of abelian groups whose rows are short exact sequences:

$$\begin{array}{ccccccccc}
 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & 0 \\
 & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\
 0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 & \longrightarrow & 0.
 \end{array}$$

Prove that  $\beta$  is injective (resp. surjective) if  $\alpha$  and  $\gamma$  are. Conclude that  $\beta$  is an isomorphism if  $\alpha$  and  $\gamma$  are.

11. Show that *every* short exact sequence of vector spaces over a field  $K$  splits.
12. Determine all isomorphism types of abelian groups of order 16. What types can be obtained as extensions of  $C_4$  by  $C_4$ ? And what types can be obtained as extensions of  $V_4$  by  $V_4$ ?
13. Let  $f : A \rightarrow B$  be an injective homomorphism to an abelian group  $B$  and  $p$  be a retraction of  $f$ . Prove:  $B \cong \text{im } f \oplus \ker p$ . What is the corresponding statement for a surjective homomorphism  $g : A \rightarrow B$  with section  $s$ ?
14. Let  $C$  be a finitely generated abelian group with the property that every short exact sequence  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  splits. Prove that  $C$  is a free group. [Compare with 9.4.]
15. Show that the additive group  $\mathbf{R}$  of real numbers is torsion-free but not free.
16. Are the abelian groups  $\mathbf{Q}$ ,  $\mathbf{R}$ , and  $\mathbf{Q}/\mathbf{Z}$  finitely generated? Are they torsion-free? Answer the same questions for the multiplicative groups  $\mathbf{Q}^*$  and  $\mathbf{R}^*$ .
17. An abelian group  $A$  is called *divisible* if for all  $a \in A$  and  $k \in \mathbf{Z}_{>0}$ , there exists an element  $x \in A$  with  $kx = a$ . Prove: a divisible group  $A \neq 0$  is not free.
18. Prove: a subgroup of a finitely generated abelian group is finitely generated.
- \*19. Let  $G \subset \text{GL}_2(\mathbf{Q})$  be the group generated by  $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$  and  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . Prove that the subgroup  $H = \{g \in G : \det(g) = 1\} \subset G$  is abelian and *not* finitely generated.
20. Determine a basis of the group  $A = \{(x, y, z) \in \mathbf{Z}^3 : x + 2y + 3z \equiv 0 \pmod{6}\} \subset \mathbf{Z}^3$ . Show that the group  $B \subset \mathbf{Z}^3$  generated by  $v_1 = (4, -5, 2)$ ,  $v_2 = (-1, 2, -1)$ , and  $v_3 = (1, 7, -5)$  is a subgroup of  $A$ , and determine the structures of  $\mathbf{Z}^3/B$  and  $A/B$ .
21. Answer the same question as above, now with  $v_1 = (4, -5, 8)$ ,  $v_2 = (-1, 2, -1)$ , and  $v_3 = (1, 7, -5)$ .
22. Let  $A \subset \mathbf{Z}^4$  be the kernel of the homomorphism

$$\begin{aligned}
 \mathbf{Z}^4 &\longrightarrow \mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z} \\
 (w, x, y, z) &\longmapsto (w + x - 5z, w - y + z \pmod{4}, -w + 3y - z \pmod{6}).
 \end{aligned}$$

Determine a basis of  $A$  and the structure of  $\mathbf{Z}^4/A$ .

23. Let  $A$  be an abelian group of order  $n$  and  $m > 0$  be a divisor of  $n$ . Prove that  $A$  contains a subgroup  $H_m$  of order  $m$ . Prove that the subgroup  $H_m \subset A$  is uniquely determined by  $m$  for all divisors  $m \mid n$  if and only if  $A$  is cyclic.
24. Show that an exact sequence  $R : 0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  of finite abelian groups leads to an exact sequence  $R_p : 0 \rightarrow A(p) \rightarrow B(p) \rightarrow C(p) \rightarrow 0$  of Sylow  $p$ -subgroups for every prime  $p$  and that  $R$  splits if and only if this is the case for all  $R_p$ .
25. Show that every short exact sequence  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  of abelian groups leads to an exact sequence  $0 \rightarrow A^{\text{tor}} \rightarrow B^{\text{tor}} \rightarrow C^{\text{tor}}$  but that the map  $B^{\text{tor}} \rightarrow C^{\text{tor}}$  is not necessarily surjective. Verify that the sequence  $0 \rightarrow A/A^{\text{tor}} \rightarrow B/B^{\text{tor}} \rightarrow C/C^{\text{tor}} \rightarrow 0$  is a short exact sequence if and only if  $B^{\text{tor}} \rightarrow C^{\text{tor}}$  is surjective.
26. For a finite abelian group  $A$  and a prime power  $p^k$ , define the  $p^k$ -rank of  $A$  as the number of cyclic groups of order divisible by  $p^k$  in a decomposition of  $A$  as a product of cyclic groups. Show that this rank does not depend on the chosen decomposition and that for  $k = 1$ , it gives the  $p$ -rank defined in the text. Is this also true if we replace  $p^k$  with an arbitrary positive number?
27. Show that finite abelian groups that contain the same numbers of elements of order  $k$  for every  $k \geq 1$  are isomorphic. [This is not true in general for finite groups; see Exercise 6.45.]
28. Suppose that  $A$  and  $B$  are finitely generated abelian groups and that for every  $k \geq 1$ , the orders of  $A/kA$  and  $B/kB$  are equal. Are  $A$  and  $B$  necessarily isomorphic?
29. Let  $A$  be a finitely generated abelian group with subgroup  $H$ , and suppose that for every prime  $p$ , the canonical map  $H \rightarrow A/pA$  is surjective. Prove:  $H = A$ . Show that this is not true for arbitrary abelian groups  $A$ .
30. Show that a finite abelian group is cyclic if and only if there is no prime  $p$  for which it contains a subgroup isomorphic to  $\mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$  and that a finitely generated abelian group  $A$  is cyclic if and only if  $A/pA$  is cyclic for all primes  $p$ .
31. Show that the number of isomorphism classes of abelian groups of order  $q^m$  for  $q$  prime is equal to  $p(m)$ , where  $p$  is the partition function. Deduce that the number of isomorphism classes of abelian groups of order  $n = \prod_q q^{k_q}$  is equal to  $\prod_q p(k_q)$ .
32. Let  $S \subset \mathbf{R}$  be a finite set with  $1 \in S$  and  $H \subset \mathbf{R}$  be the additive subgroup generated by  $S$ . Prove:  $H$  is discrete in  $\mathbf{R} \iff S \subset \mathbf{Q}$ .
33. Let  $p$  be an odd prime, and suppose that  $x - 1$  has exactly  $k \geq 1$  factors  $p$ . Prove that  $x^{p^s} - 1$  has exactly  $k + s$  factors  $p$ . Show that for  $k \geq 2$ , this is also true for  $p = 2$ .
34. Let  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  be a short exact sequence of finitely generated abelian groups. Show that we have the equality  $r(A) + r(C) = r(B)$  for the free ranks of these groups. Also show that if  $B$  is finite and  $p$  is prime, the inequality

$$r_p(A) + r_p(C) \geq r_p(B)$$

holds for the  $p$ -ranks. Give an example where this inequality is strict.

35. Determine the elementary divisors of  $(\mathbf{Z}/n\mathbf{Z})^*$  for  $n = 720, 1000$ , and  $17000$ .
36. Determine the zeros of the polynomial  $X^2 - 1$  in  $\mathbf{Z}/n\mathbf{Z}$  for  $n = 720, 1000$ , and  $17000$ .

37. Let  $p$  be a prime and  $k \geq 1$  be an integer. Show that the canonical map  $(\mathbf{Z}/p^k\mathbf{Z})^* \rightarrow (\mathbf{Z}/p\mathbf{Z})^*$  has a section given by  $a \bmod p \mapsto a^{p^{k-1}} \bmod p^k$ . [Note that it is unclear a priori that this map is *well defined!*]
- \*38. Let  $A$  be a finitely generated abelian group and  $f : A \rightarrow A$  be a surjective homomorphism. Prove that  $f$  is an isomorphism. Does a similar statement hold for injective homomorphisms?
39. Let  $F$  be a free abelian group of finite rank and  $\pi : F \rightarrow \mathbf{Z}$  be a surjective homomorphism. Prove that  $F$  has a basis in which  $\pi$  is the projection onto the last coordinate.
40. Let  $F$  be a free abelian group of finite rank and  $H \neq 0$  be a subgroup. Let  $\pi : F \rightarrow \mathbf{Z}$  be a surjective homomorphism with  $\pi[H] \neq 0$  for which the index  $a = [\mathbf{Z} : \pi[H]] > 0$  is minimal. Prove: there exist a splitting  $F = F' \oplus \langle x \rangle$  and a subgroup  $H' \subset aF'$  with  $H = H' \oplus \langle ax \rangle$ .
41. Let  $F$  be a free abelian group of rank  $n$  and  $H$  be a subgroup. Prove that there exist a basis  $x_1, x_2, \dots, x_n$  of  $F$  and integers  $d_i$  such that  $d_1x_1, d_2x_2, \dots, d_nx_n$  is a basis of  $H$  and  $d_1 \mid d_2 \mid d_3 \mid \dots \mid d_n$ . Deduce Corollary 9.12 from this.
42. Let  $M$  be an  $n \times n$  matrix with integer coefficients. Prove that there exist matrices  $A, B \in \mathrm{SL}_n(\mathbf{Z})$  for which  $AMB$  is a diagonal matrix. [Hint: use the previous exercise.]
43. Let  $A \subset \mathbf{Z}^n$  be the subgroup generated by the columns of the matrix  $M = (c_{ij})_{i,j=1}^n$ . Prove that  $A$  has finite index in  $\mathbf{Z}^n$  exactly when  $M$  is non-singular and that in that case, the index  $[\mathbf{Z}^n : A]$  is equal to  $|\det(M)|$ .
44. Determine the structure of  $\mathbf{Z}^3/A$  if  $A$  is generated by the columns of the matrix

$$M = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}.$$

45. Let  $S$  be a (not necessarily finite) set. An abelian group  $F \supset S$  is called the *free abelian group on the set  $S$*  if every (set-theoretic) map  $S \rightarrow X$  to an abelian group  $X$  has a *unique* extension to a homomorphism  $F \rightarrow X$ . Show that  $F$  exists and is uniquely determined up to isomorphisms.
46. Consider a (not necessarily finite) collection of abelian groups  $A_i$  ( $i \in I$ ). An abelian group  $D$  endowed with homomorphisms  $f_i : A_i \rightarrow D$  for all  $i \in I$  is called the *direct sum* of the groups  $A_i$ , denoted by  $D = \bigoplus_{i \in I} A_i$ , if for every collection of homomorphisms  $g_i : A_i \rightarrow X$  to an abelian group  $X$ , there exists a unique homomorphism  $g : D \rightarrow X$  with  $g \circ f_i = g_i$  for all  $i \in I$ . Show that  $D$  exists and is uniquely determined up to isomorphisms. What is the relation to the previous exercise?
47. For  $A = \mathbf{Q}^*$  and  $p$  prime, define the subgroup  $A_p \subset A$  by  $A_p = \{p^k : k \in \mathbf{Z}\}$ . Prove that  $A$  is the direct sum of  $A^{\mathrm{tor}} = \langle -1 \rangle$  and the subgroups  $A_p$  for the primes  $p$ .
48. Consider a (not necessarily finite) collection of abelian groups  $A_i$  ( $i \in I$ ). An abelian group  $P$  endowed with homomorphisms  $f_i : P \rightarrow A_i$  for all  $i \in I$  is called the *direct product* of the groups  $A_i$ , denoted by  $P = \prod_{i \in I} A_i$ , if for every collection of homomorphisms  $g_i : X \rightarrow A_i$  from an abelian group  $X$ , there exists a unique homomorphism  $g : X \rightarrow P$  with  $f_i \circ g = g_i$  for all  $i \in I$ . Show that  $P$  exists and is uniquely determined up to isomorphisms.<sup>37</sup>

49. Let  $I$  be a set and  $A$  be an abelian group. Show that the set  $A^I$  of maps  $f : I \rightarrow A$  becomes an abelian group under the “coordinate-wise addition”  $(f_1 + f_2)(i) = f_1(i) + f_2(i)$  and that this group is isomorphic to the product group  $\prod_{i \in I} A$  in the sense of the previous exercise.
50. Show that the direct sum of finitely many abelian groups is isomorphic to the direct product of these groups but that this is not the case for an infinite collection of (non-trivial) abelian groups.
51. Given homomorphisms of abelian groups  $f_i : A \rightarrow B_i$  for  $i = 1, 2$ , we define the *fibred sum*  $B_1 \oplus_A B_2$  of  $B_1$  and  $B_2$  over  $A$  as  $(B_1 \oplus B_2) / \langle f_1(a), -f_2(a) : a \in A \rangle$ . Likewise, for homomorphisms of abelian groups  $g_i : B_i \rightarrow C$  for  $i = 1, 2$ , we define the *fibred product*  $B_1 \times_C B_2$  of  $B_1$  and  $B_2$  over  $C$  as  $\{(b_1, b_2) \in B_1 \times B_2 : g_1(b_1) = g_2(b_2)\}$ . Show that these are abelian groups for which the diagrams

$$\begin{array}{ccc}
 A & \xrightarrow{f_1} & B_1 \\
 \downarrow f_2 & & \downarrow \text{id} \times 0 \\
 B_2 & \xrightarrow{0 \times \text{id}} & B_1 \oplus_A B_2
 \end{array}
 \quad \text{and} \quad
 \begin{array}{ccc}
 B_1 \times_C B_2 & \xrightarrow{\pi_2} & B_2 \\
 \downarrow \pi_1 & & \downarrow g_2 \\
 B_1 & \xrightarrow{g_1} & C
 \end{array}$$

commute. \*Can you state “universal properties” as in Exercises 45 and 46 that characterize fibred sums and products?

**\*Homologic algebra.** In the following exercises, we consider *abelian extensions*  $E$  of an abelian group  $C$  by an abelian group  $A$ . Two extensions  $0 \rightarrow A \rightarrow E \rightarrow C \rightarrow 0$  and  $0 \rightarrow A \rightarrow E' \rightarrow C \rightarrow 0$  are called isomorphic if they fit into a commutative diagram of the form

$$\begin{array}{ccccccc}
 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & C & \longrightarrow & 0 \\
 & & \downarrow \text{id}_A & & \downarrow f & & \downarrow \text{id}_C & & \\
 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & C & \longrightarrow & 0.
 \end{array}$$

We denote the set of isomorphism classes of extensions of  $C$  by  $A$  by  $\text{Ext}(C, A)$ . If the arrows are clear, we often say “the extension  $E \in \text{Ext}(C, A)$ ” for short. In the exercises below, we show that the set  $\text{Ext}(C, A)$  itself has the structure of a group.

52. Give an example of non-isomorphic extensions  $E, E' \in \text{Ext}(C, A)$  for which  $E$  and  $E'$  are isomorphic as abelian groups.
53. For  $E \in \text{Ext}(C, A_1)$  and a group homomorphism  $\phi : A_1 \rightarrow A_2$ , we define  $\phi_* E$  to be the fibred sum  $A_2 \oplus_{A_1} E$ . Show that this leads to a natural map  $\phi_* : \text{Ext}(C, A_1) \rightarrow \text{Ext}(C, A_2)$ .
54. For  $E \in \text{Ext}(C_2, A)$  and a group homomorphism  $\phi : C_1 \rightarrow C_2$ , we define  $\phi^* E$  to be the fibred product  $E \times_{A_2} C_1$ . Show that this leads to a natural map  $\phi^* : \text{Ext}(C_2, A) \rightarrow \text{Ext}(C_1, A)$ .

55. Given two extensions  $E_1, E_2 \in \text{Ext}(C, A)$ , we define the *Baer sum*  $E_1 + E_2 \in \text{Ext}(C, A)$  by mapping the sum  $E_1 \oplus E_2 \in \text{Ext}(C \oplus C, A \oplus A)$  (whose definition is clear) to  $\text{Ext}(C, A)$  via the maps

$$\text{Ext}(C \oplus C, A \oplus A) \xrightarrow{\Delta^*} \text{Ext}(C, A \oplus A) \xrightarrow{\nabla^*} \text{Ext}(C, A).$$

Here  $\Delta : C \rightarrow C \oplus C$  is the “diagonal embedding”  $c \mapsto (c, c)$ , and  $\nabla : A \oplus A \rightarrow A$  is the “addition”  $(a, a') \mapsto a + a'$ . Show that  $\text{Ext}(C, A)$  becomes an abelian group for this addition with the split extension  $0 \rightarrow A \rightarrow A \oplus C \rightarrow C \rightarrow 0$  as its unit element.

56. Let  $p$  be a prime. Show that  $\text{Ext}(C_p, C_p)$  has order  $p$ .
57. Let  $p$  be an odd prime. Prove:
- If  $a, b \in \{2, 3, \dots, p-1\}$  satisfy  $ab \equiv 1 \pmod{p}$ , then either the order of  $(a \pmod{p^2})$  or the order of  $(b \pmod{p^2})$  in  $(\mathbf{Z}/p^2\mathbf{Z})^*$  is divisible by  $p$ .
  - There is a primitive root modulo  $p^2$  in  $\{2, 3, \dots, p-1\}$ .

## 10 FINITE GROUPS

In the previous section, we saw that finite abelian groups can be “split” into sums of cyclic groups. In this section, we try to analyze arbitrary finite groups  $G$  in a similar way. For non-abelian groups, we encounter the problem that although we can easily point out non-trivial subgroups, these are often not *normal*. The Sylow theorems in this section can frequently be used to create normal subgroups. If we have a normal subgroup  $N \triangleleft G$ , the situation is often still considerably more complicated than in the abelian case. For split sequences, we generally get a splitting of  $G$  as a *semi-direct product* rather than a direct product.

For numbers  $n$  with few divisors, we can “unravel” groups of order  $n$  as products of simple groups and construct a list of all isomorphism types of groups of order  $n$ . For highly divisible numbers  $n$ , such an explicit classification, the fundamental *classification problem* of finite group theory, is impossible.

### ► NON-ABELIAN EXACT SEQUENCES

We begin with the non-abelian analog of 9.2.

**10.1. Definition.** A short exact sequence  $1 \rightarrow N \rightarrow G \xrightarrow{g} H \rightarrow 1$  of groups is said to split or be split if there exists a section  $s : H \rightarrow G$  with  $g \circ s = \text{id}_H$ .

If  $G$  is abelian, then  $N$  and  $H$  also are, and by 9.3, the definition is equivalent to 9.2.

If the sequence in 10.1 splits, we can view  $H$  as a subgroup of  $G$  through the injection  $s$ . We then have  $N \cap H = 1$  and  $G = \{nh : n \in N, h \in H\}$ . So Theorem 8.13 applies, and  $G$  is the semi-direct product of  $N$  and  $H$ . Conversely, in a semi-direct product, the projection  $\pi_H : N \rtimes H \rightarrow H$  onto the  $H$ -coordinate is a surjection with kernel  $N$  that leads to a short exact sequence as in 10.1. Semi-direct products and split short exact sequences are therefore “the same” in the following sense.

**10.2. Theorem.** Let  $N$  and  $H$  be groups and  $\sigma : H \rightarrow \text{Aut}(N)$  be a homomorphism. Then the semi-direct product  $N \rtimes_\sigma H$  fits into a short exact sequence

$$1 \rightarrow N \rightarrow N \rtimes_\sigma H \xrightarrow{\pi_H} H \rightarrow 1$$

that is split by the natural section  $h \mapsto (1_N, h)$  of  $\pi_H$ .

Conversely, in a short exact sequence of groups

$$1 \rightarrow N \rightarrow G \xrightarrow{g} H \rightarrow 1,$$

every section  $s : H \rightarrow G$  of  $g$  leads to an isomorphism  $N \rtimes_\sigma H \xrightarrow{\sim} G$  given by  $(n, h) \mapsto ns(h)$ . Here  $\sigma : H \rightarrow \text{Aut}(N)$  is the conjugation action induced by  $s$ :  $\sigma(h)(n) = s(h)ns(h)^{-1}$ .  $\square$

The splitting of an exact sequence  $1 \rightarrow N \rightarrow G \rightarrow G/N \rightarrow 1$  amounts to finding a subgroup  $H \subset G$  with  $N \cap H = 1$  and  $G = NH$ . Such a subgroup  $H$  is also called a *complement* of  $N$  in  $G$ . For such a complement, the natural isomorphism

$G/N = NH/N \xrightarrow{\sim} H/(H \cap N) = H \subset G$  gives an associated section. We already saw in the abelian case that not every normal subgroup  $N \triangleleft G$  has a complement. A complement is, moreover, not necessarily unique.

**Exercise 1.** Show that for a normal subgroup  $N$  of a finite group  $G$ , a subgroup  $H \subset G$  with  $N \cap H = 1$  is a complement of  $N$  if and only if  $H$  has order  $[G : N]$ .

**10.3. Example. 1.** We saw in 8.14.2 that the subgroup  $C_n$  of rotations in the dihedral group  $D_n$  is a normal subgroup of index 2, and to the split exact sequence

$$1 \rightarrow C_n \longrightarrow D_n \xrightarrow{\det} \langle -1 \rangle \rightarrow 1$$

corresponds the semi-direct product  $D_n = C_n \rtimes \langle \sigma \rangle$  from 8.14.2. Every map  $s : \langle -1 \rangle \rightarrow D_n$  that sends  $-1$  to a reflection  $\sigma \in D_n$  gives a section, and for every choice of  $\sigma$ ,  $-1$  acts on  $D_n$  by inversion (compare with Exercise 11).

**2.** For  $n \geq 2$ , the kernel  $A_n$  of the sign map  $\varepsilon : S_n \rightarrow \langle -1 \rangle$  is a normal subgroup of index 2 of the symmetric group  $S_n$ . The exact sequence

$$1 \rightarrow A_n \longrightarrow S_n \xrightarrow{\varepsilon} \langle -1 \rangle \rightarrow 1$$

splits because every homomorphism  $s : \langle -1 \rangle \rightarrow S_n$  that sends  $-1$  to a 2-cycle is a section of the sign map. More generally, every odd element of order 2 in  $S_n$  generates a complement of  $A_n$ . Here, we also have a semi-direct product  $S_n \cong A_n \rtimes \langle -1 \rangle$ , but in contrast to the previous example, the action of  $-1$  on  $A_n$  for  $n$  not too small now does depend on the choice of the section  $s$ . Apparently, completely different actions of  $H$  on  $N$  can lead to isomorphic semi-direct products. See Exercise 14 for an amusing example of this phenomenon.

**3.** By 8.3.2, the symmetric group  $S_4$  fits into a split exact sequence

$$1 \rightarrow V_4 \longrightarrow S_4 \longrightarrow S_3 \rightarrow 1$$

induced by the tetrahedron homomorphism from §5. We see that the extension is split by viewing  $S_3$  as the stabilizer of a point in  $S_4$ . The resulting action  $S_3 \rightarrow \text{Aut}(V_4)$  permutes the non-trivial elements of  $V_4$  and is an isomorphism.

**4.** On the group  $I_2(\mathbf{R})$  of isometries of the plane, the “linear component” homomorphism  $L$  from 3.9 leads to an exact sequence

$$1 \longrightarrow T \longrightarrow I_2(\mathbf{R}) \xrightarrow{L} O_2(\mathbf{R}) \longrightarrow 1.$$

We see that this sequence splits by viewing  $O_2(\mathbf{R})$  as a subgroup of  $I_2(\mathbf{R})$  in the usual way; this gives the semi-direct product we already know from 8.11.

### ► CLASSIFICATION FOR SIMPLE GROUP ORDERS

The classification problem for groups of order  $n$  is easy if  $n = p$  is prime: the only group of order  $p$  is the cyclic group  $C_p$ . For the product  $n = pq$  of two primes  $p \leq q$ , by Cauchy’s theorem 5.13, there is a cyclic subgroup  $C_q \subset G$  of order  $q$  and index  $p$ . By 5.10,  $C_q$  is normal in  $G$ , so we have an exact sequence

$$1 \rightarrow C_q \longrightarrow G \longrightarrow C_p \longrightarrow 1.$$

For  $p \neq q$ , this sequence splits. After all, by 5.13,  $G$  then contains a subgroup of order  $p$  that is mapped isomorphically onto  $C_p$ ; the inverse of this isomorphism gives a section. For  $p = q$ , the sequence does not split in the case where  $G$  contains elements of order  $p^2$  and therefore is cyclic. In the case of a split sequence, we find  $G = C_q \rtimes_{\phi} C_p$  for a map

$$\phi : C_p \longrightarrow \text{Aut}(C_q) \cong (\mathbf{Z}/q\mathbf{Z})^* \cong C_{q-1}.$$

Here, we use the isomorphisms from 8.15 and 7.7. If  $p$  does *not* divide  $q - 1$ , then  $\phi$  is trivial, and we have  $G = C_p \times C_q$ , which is an abelian group that is cyclic for  $q \neq p$  by the Chinese remainder theorem 6.15. If  $p$  divides  $q - 1$ , then  $\text{Aut}(C_q)$  contains a unique cyclic subgroup of order  $p$ , and a non-trivial action  $\phi$  identifies  $C_p$  with this subgroup. This completes the proof of the following result.

**10.4. Theorem.** *Let  $p$  and  $q$  be primes with  $p < q$ .*

1. *Every group of order  $p^2$  is abelian and isomorphic to  $C_p \times C_p$  or  $C_{p^2}$ .*
2. *For  $p \nmid q - 1$ , every group of order  $pq$  is cyclic.*
3. *For  $p \mid q - 1$ , every group of order  $pq$  is isomorphic to  $C_{pq}$  or the semi-direct product  $C_q \rtimes C_p$  of  $C_q$  and the cyclic subgroup  $C_p \subset \text{Aut}(C_q)$ .  $\square$*

For  $p = 2$ , the non-abelian group  $C_q \rtimes C_2$  is the dihedral group  $D_q$  from 10.3.1.

**10.5. Theorem.** *There are exactly five isomorphism classes of groups of order 8. The abelian groups are  $C_2 \times C_2 \times C_2$ ,  $C_4 \times C_2$ , and  $C_8$ ; the non-abelian groups are the dihedral group  $D_4$  and the quaternion group  $Q$ .*

**Proof.** For  $G$  of order 8, the possible orders of the elements of  $G$  are 1, 2, 4, and 8. If  $G$  contains an element of order 8, we have  $G \cong C_8$ . If  $a^2 = 1$  for all  $a \in G$ , then  $G$  is an elementary abelian 2-group, and we find  $G \cong C_2 \times C_2 \times C_2$ . From now on, assume that  $G$  contains an element  $a$  of order 4 and no element of order 8. The cyclic subgroup  $C_4 = \langle a \rangle$  has index 2 in  $G$  and is therefore normal. We obtain an exact sequence  $1 \rightarrow C_4 \rightarrow G \rightarrow C_2 \rightarrow 1$ .

We first look at the case where this sequence splits. Then there is an element  $b$  of order 2 in  $G$  that is not in  $C_4 = \langle a \rangle$ , and we have  $G = C_4 \rtimes C_2$ , where the non-trivial element  $b \in C_2$  acts on  $C_4$  by conjugation. Since  $\text{Aut}(C_4) \cong (\mathbf{Z}/4\mathbf{Z})^*$  consists of the identity and inversion, this gives us two groups: the abelian direct product  $C_4 \times C_2$  and the non-abelian dihedral group  $D_4$ .

Finally, assume that the sequence does not split. This means that every element  $b$  in the fiber  $G \setminus \langle a \rangle$  has order 4. Choose such a  $b$ . Then we have  $b^2 \in \langle a \rangle$ , and since  $b^2$  has order 2, we have  $b^2 = a^2 = a^{-2}$  and  $a^2 b^2 = 1$ . The elements  $a$  and  $b$  do not commute because, otherwise,  $ab \notin \langle a \rangle$  would have order 2. Since  $bab^{-1} \in \langle a \rangle$  has order 4, we apparently have  $bab^{-1} = a^{-1}$ . The structure of  $G = \langle a, b \rangle$  is now fixed by the fact that  $a$  and  $b$  have order 4 and satisfy the relations  $b^2 = a^2$  and  $bab^{-1} = a^{-1}$ . In more traditional notation, we write  $a = i$  and  $b = j$  and have  $i^2 = j^2 = -1$ . Note that  $-1$  commutes with  $i$  and  $j$  and therefore with all elements of the group. If we also write  $ij = k$ , we obtain the representation of the quaternion group  $Q$  from 8.7.  $\square$

**Exercise 2.** Determine the number of subgroups of order 2 and 4 of each of the groups in 10.5.

► SYLOW  $p$ -SUBGROUPS

So far, Cauchy’s theorem 5.13 has been our main tool for constructing subgroups of an abstract finite group  $G$ . We now give an important strengthening that was proved in the 1870s by the Norwegian L. Sylow (1832–1918). Among other things, this strengthening says that for every prime power  $p^i$  that divides the order of a finite group  $G$ , there is a subgroup  $H \subset G$  of order  $p^i$ . Such a subgroup is called a  $p$ -subgroup of  $G$ .

**Exercise 3.** Show that the group  $A_4$  of order 12 does not have a subgroup of order 6.

For a given prime  $p$ , we can write the order of a finite group  $G$  as  $\#G = p^k m$  with  $p \nmid m$ . A subgroup  $H$  of  $G$  is called a *Sylow  $p$ -subgroup* of  $G$  if  $H$  has order  $p^k$ . Such an  $H$  is a “maximal  $p$ -subgroup” of  $G$  and is only non-trivial if  $p$  divides the group order. It does not have to be normal in  $G$ . Sylow  $p$ -subgroups are made by beginning with a subgroup of prime order obtained from 5.13 and extending it step by step. For this, we use the following lemma.

**10.6. Lemma.** *Let  $H$  be a  $p$ -subgroup of a finite group  $G$ . Then we have*

$$[N_G(H) : H] \equiv [G : H] \pmod{p}.$$

**Proof.** Let  $H$  act regularly on  $X = G/H$  by left multiplication. A coset  $xH$  is invariant under multiplication by  $H$  if we have  $hxH = xH$  for  $h \in H$ , that is,  $hx \in xH$  and  $h \in xHx^{-1}$  for all  $h \in H$ . This means exactly that  $xHx^{-1} = H$ , so we have  $x \in N_G(H)$  and  $X^H = N_G(H)/H$ . By 5.14, we have  $\#X^H \equiv \#X \pmod{p}$ , and since the orders of  $X^H = N_G(H)/H$  and  $X = G/H$  are equal to, respectively,  $[N_G(H) : H]$  and  $[G : H]$ , this is the congruence we wanted to prove.  $\square$

**10.7. Theorem.** *Let  $G$  be a finite group and  $p$  be a prime. Then  $G$  has a Sylow  $p$ -subgroup. Every  $p$ -subgroup of  $G$  is contained in a Sylow  $p$ -subgroup of  $G$ .*

**Proof.** We take  $p \mid \#G$ ; otherwise, the theorem is trivial. By Cauchy’s theorem,  $G$  then contains a  $p$ -subgroup of order  $p$ , and it suffices to prove the second statement, which, after all, implies that such a subgroup of order  $p$  is contained in a Sylow  $p$ -subgroup of  $G$ .

Let  $H \subset G$  be an arbitrary  $p$ -subgroup. If  $[G : H]$  is not divisible by  $p$ , then by 4.8,  $\#H$  contains the same number of factors  $p$  as  $\#G$ , and  $H$  itself is a Sylow  $p$ -subgroup of  $G$ . If  $[G : H]$  is divisible by  $p$ , we will show that there exists a subgroup  $H' \supset H$  of  $G$  that contains  $H$  as a subgroup of index  $p$ . Then  $H'$  is a larger  $p$ -subgroup of  $G$ , and by repeating the argument as often as necessary, we obtain a Sylow  $p$ -subgroup  $P \supset H$ .

For the construction of  $H'$ , we note that if  $[G : H]$  is divisible by  $p$ , then the order of the group  $N_G(H)/H$  is also divisible by  $p$  by 10.6. Then there exists a subgroup of  $N_G(H)/H$  of order  $p$ , and according to 8.1, this can be written as  $H'/H$  for a subgroup  $H' \supset H$  of  $G$ . This gives  $[H' : H] = \#(H'/H) = p$ .  $\square$

The set of Sylow  $p$ -subgroups of  $G$  is denoted by  $\text{Syl}_p(G)$ . We have the following useful theorem for the order  $n_p$  of  $\text{Syl}_p(G)$ .

**10.8. Sylow’s theorem.** *Let  $G$  be a finite group of order  $p^k m$  with  $p \nmid m$  prime. Then the number  $n_p$  of Sylow  $p$ -subgroups of  $G$  is a divisor of  $m$ , and we have  $n_p \equiv 1 \pmod{p}$ . All Sylow  $p$ -subgroups of  $G$  are conjugate in  $G$ .*

**Proof.** We first prove that any two Sylow  $p$ -subgroups  $P$  and  $P'$  of  $G$  are conjugate. Take the set  $X$  of subgroups conjugate to  $P'$ , and let  $G$  act on  $X$  by conjugation. The number of subgroups conjugate to  $P'$ , which is equal to  $\#X = [G : N_G(P')]$ , divides  $[G : P'] = m$  and therefore is not a  $p$ -tuple. If we apply 5.14 for the conjugation action of  $P$  on  $X$ , we obtain  $\#X^P \equiv \#X \not\equiv 0 \pmod{p}$ . In particular,  $X^P$  is not empty, so there is at least one subgroup  $P''$  conjugate to  $P'$  that is fixed under conjugation by elements of  $P$ . We claim that  $P = P''$ , so that  $P$  and  $P'$  are indeed conjugate. To prove this, we consider the normalizer  $N_G(P'')$  of  $P''$ . This contains  $N = P''$  as a normal subgroup and  $H = P$  as a subgroup. Theorem 8.2 gives us an isomorphism

$$P/(P \cap P'') \xrightarrow{\sim} PP''/P''.$$

On the left, we have a  $p$ -group; on the right, a group whose order divides  $[G : P''] = m$ . Both groups are therefore trivial, which means that we have  $P = P''$ .

Now that we know that all Sylow  $p$ -subgroups of  $G$  are conjugate, we have  $X = \text{Syl}_p(G)$ , and the given argument shows that  $P'' = P$  is the *only* fixed point for the conjugation action of  $P$  on  $X$ . We therefore have  $n_p = \#X \equiv \#X^P = 1 \pmod{p}$ .  $\square$

**10.9. Corollary.** *A normal  $p$ -subgroup  $N \triangleleft G$  is contained in every Sylow  $p$ -subgroup of  $G$ . For a normal Sylow  $p$ -subgroup  $P \triangleleft G$ , we have  $\text{Syl}_p(G) = \{P\}$ .*

**Proof.** There exists a Sylow  $p$ -subgroup  $P \supset N$  by 10.7. Every other Sylow  $p$ -subgroup is of the form  $gPg^{-1}$  by 10.8 and therefore contains  $gNg^{-1} = N$ . The second statement follows easily.  $\square$

**10.10. Corollary.** *Suppose that all Sylow subgroups of  $G$  are normal. Then  $G$  is isomorphic to the direct product of its Sylow subgroups.*

**Proof.** Since the Sylow  $p$ -subgroups  $N_p \triangleleft G$  for different primes  $p$  are normal subgroups of relatively prime order, we have  $N_p \cap N_{p'} = 1$  for  $p \neq p'$ . This implies that an element  $n \in N_p$  always commutes with an element  $n' \in N_{p'}$ . After all, the commutator  $[n, n'] = n(n'n^{-1}n'^{-1}) = (nn'n^{-1})n'^{-1}$  is in  $N_p$  by the first representation and in  $N_{p'}$  by the second. It follows that  $[n, n'] = e$ . The map

$$\prod_{p \mid \#G} N_p \longrightarrow G$$

from the product of the Sylow subgroups to  $G$  given by multiplying the coordinates is now a homomorphism that sends every “component”  $N_p \subset \prod_{p \mid \#G} N_p$  injectively to  $G$ . The order of the image, which is divisible by  $\#N_p$  for all  $p \mid \#G$ , is equal to  $\#G$ , so the map is surjective. Since the orders on the two sides are equal, the map is an isomorphism.  $\square$

A finite group  $G$  with the property that all its Sylow subgroups are normal is called *nilpotent*. Note that finite *abelian* groups are always nilpotent. For non-abelian groups, nilpotence is a strong requirement.

**10.11. Example.** Let us determine the Sylow  $p$ -subgroups of  $S_4$  and  $S_5$ . For this, we use the conjugacy classes determined in 5.11.

For the group  $S_4$  of order  $24 = 2^3 \cdot 3$ , it follows from 10.8 that we have  $n_2 \in \{1, 3\}$  and  $n_3 \in \{1, 4\}$ . Each of the eight 3-cycles in  $S_4$  is contained in a Sylow 3-subgroup, which has order 3 and therefore contains two 3-cycles; consequently, we have  $n_3 = 4$ . The 16 elements of  $S_4$  that are not 3-cycles each have order 1, 2, or 4 and are contained in a Sylow 2-subgroup, which has order 8. This implies  $n_2 > 1$  and therefore  $n_2 = 3$ .

To give the Sylow 2-subgroups of  $S_4$  explicitly, we note that the subgroup

$$V_4 = \{(1), (12)(34), (13)(24), (14)(23)\} \triangleleft S_4$$

is normal in  $S_4$ , and so by 10.9, it is contained in every Sylow 2-subgroup. If we add an arbitrary element of order 2 or 4 outside  $V_4$ , for example (12), we obtain a Sylow 2-subgroup of order 8:

$$P = \langle V_4, (12) \rangle = V_4 \cup \{(12), (34), (1324), (1423)\}.$$

The group  $P$  is generated by  $\rho = (1324)$  and  $\sigma = (12)$ , which satisfy the relation  $\sigma\rho = \rho^{-1}\sigma$ , so we have  $P \cong D_4$ . If in the above, we replace (12) with (13) or (14), we obtain groups  $P'$  and  $P''$  conjugate to  $P$ . We have  $\text{Syl}_2(S_4) = \{P, P', P''\}$ . Note that we already came across this in 8.3.2.

For the group  $S_5$  of order  $120 = 2^3 \cdot 3 \cdot 5$ , we obtain  $n_2 \in \{1, 3, 5, 15\}$ ,  $n_3 \in \{1, 4, 10, 40\}$ , and  $n_5 \in \{1, 6\}$ . Since there are 24 different 5-cycles in  $S_5$ , it is immediately clear that we have  $n_5 = 6$ , with four non-trivial powers of a 5-cycle in each Sylow 5-subgroup. Likewise, we obtain  $n_3 = 10$  from the 20 different 3-cycles in  $S_5$ . For the Sylow 2-subgroups, which do not have prime order and therefore are not necessarily pairwise disjoint, we cannot deduce  $n_2$  directly from the numbers of elements of 2-power order. However, since there are  $1 + 10 + 30 + 15 = 56$  elements of order 1, 2, or 4 and a Sylow 2-subgroup has order 8, we have  $n_2 > 7$ , and so  $n_2 = 15$ . We obtain these 15 groups by embedding  $S_4$  in  $S_5$  in one of the five obvious ways and then taking one of the three Sylow 2-subgroups of  $S_4$ .

### ► CONSTRUCTION OF NORMAL SUBGROUPS

We can often use the Sylow theorems to make normal subgroups in groups of which we only know the order. Sometimes, we can prove directly that there is a prime divisor  $p \mid \#G$  with  $n_p = 1$ ; other times, we can make normal subgroups by letting  $G$  act by conjugation on suitable sets  $\text{Syl}_p(G)$ .

**10.12. Example. 1.** Let  $G$  be a group of order  $42 = 2 \cdot 3 \cdot 7$ . Then  $n_7 \equiv 1 \pmod{7}$  divides 6. It follows that  $n_7 = 1$ , so  $G$  has a normal subgroup of order 7.

**2.** Let  $G$  be a group of order  $30 = 2 \cdot 3 \cdot 5$ . Then we have  $n_5 \in \{1, 6\}$  and  $n_3 \in \{1, 10\}$ . If we have  $n_5 = 6$ , then  $G$  has exactly  $6 \times 4 = 24$  elements of order 5, and we find  $n_3 = 1$  “for lack of space.” So  $G$  has a normal subgroup of order 3 or 5.

**3.** Let  $G$  be a group of order  $300 = 2^2 \cdot 3 \cdot 5^2$ . Then we have  $n_5 \in \{1, 6\}$ . In the case  $n_5 = 1$ , the group  $G$  has a normal subgroup of order 25. In the case  $n_5 = 6$ , we can let  $G$

act by conjugation on  $\text{Syl}_5(G)$ . This gives a transitive action  $\phi : G \rightarrow S(\text{Syl}_5(G)) \cong S_6$ . The kernel  $N$  of this homomorphism is a normal subgroup  $N \neq G$ . If  $H$  is the stabilizer of a subgroup of  $\text{Syl}_5(G)$ , then  $H$  has index 6 in  $G$  by the transitivity of the action. Since  $N \subset H$ , the order of  $N$  is a divisor of  $300/6 = 50$ . Since  $\#G = 300 = 2^2 \cdot 3 \cdot 5^2$  does not divide  $6! = 720 = 2^4 \cdot 3^2 \cdot 5$ , the order of  $N$  is divisible by 5. So  $G$  has an  $N$  of order 5, 10, 25, or 50.

Having found a normal subgroup  $N \triangleleft G$ , we can try to “construct”  $G$  from  $N$  and  $G/N$  using 10.2. For this, in addition to  $N$ , we need to know  $\text{Aut}(N)$ . This is straightforward for cyclic  $N$  (8.15) and for elementary abelian  $N$  (Exercise 43). If the group order  $n$  is a product of only a few primes, it is often possible to give a complete classification of the isomorphism types of groups of order  $n$  in this way.

**10.13. Theorem.** *There are exactly five isomorphism classes of groups of order 12. The abelian groups are  $C_6 \times C_2$  and  $C_{12}$ ; the non-abelian groups are the alternating group on four letters  $A_4$ , the dihedral group  $D_6$ , and the semi-direct product  $C_3 \rtimes_{\phi} C_4$  with respect to the unique surjection  $\phi : C_4 \rightarrow \text{Aut}(C_3)$ .*

**Proof.** Let  $G$  be of order 12. Then the number of Sylow 3-subgroups  $n_3(G)$  is equal to 1 or 4. In the first case, we have  $G = N_3 \rtimes H_4$  for a normal Sylow 3-subgroup  $N_3 \subset G$  and a Sylow 2-subgroup  $H_4$  we can take as its complement. In the second case, there are eight elements of order 3 in  $G$ , and the other four elements form a normal Sylow 2-subgroup  $N_4 \subset G$ . This case gives  $G = N_4 \rtimes C_3$  for a Sylow 3-subgroup  $C_3$ .

First assume  $G = N_4 \rtimes C_3$ . If  $N_4 = C_4$  is cyclic, then  $\text{Aut}(N_4) \cong (\mathbf{Z}/4\mathbf{Z})^*$  has order 2 and  $C_3$  can only act trivially. In this case,  $G = C_4 \times C_3 \cong C_{12}$  is cyclic. If  $N_4 = V_4$  is the Klein four-group, then  $\text{Aut}(V_4) \cong S_3$  has a unique subgroup of order 3. In this case, in addition to the direct product  $G \cong V_4 \times C_3 \cong C_6 \times C_2$ , we can also make the semi-direct product  $G \cong V_4 \rtimes C_3 \cong A_4$ . This is the subgroup of index 2 in the group  $S_4 = V_4 \rtimes S_3$  from 10.3.3.

Next, assume  $G = N_3 \rtimes_{\phi} H_4$  for an action  $\phi : H_4 \rightarrow \text{Aut}(N_3) \cong (\mathbf{Z}/3\mathbf{Z})^*$ . If this product is direct, we obtain one of the abelian groups from the previous paragraph, so take  $\phi$  non-trivial. If  $H_4$  is cyclic, this determines  $\phi$  uniquely: the generator of  $H_4 = C_4$  acts by inversion on  $N_3 = C_3$ , and we find the non-abelian group  $G \cong C_3 \rtimes C_4$ . If  $H_4 = V_4$  is the Klein four-group, we can write  $H_4 = \langle x \rangle \times \langle y \rangle$  for an element  $x$  that commutes with  $C_3$  and an element  $y$  that acts on  $C_3$  by inversion. Since  $x$  is its own inverse, we can also say that  $y$  acts by inversion on  $C_3 \times \langle x \rangle \cong C_6$ ; this gives  $G \cong C_6 \rtimes C_2 = D_6$ .  $\square$

**Exercise 4.** Which group in 10.13 is isomorphic to  $S_3 \times C_2$ ?

Using the results obtained so far, we know the isomorphism types of all groups of order  $n \leq 15$ . They are listed in the “table of small groups” given after this section. For the number of isomorphism types  $I(n)$  for order  $n \leq 32$ , we have the following table:

$n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16*
$I(n)$	1	1	1	2	1	2	1	5	2	1	1	5	1	2	1	14
$n$	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32*
$I(n)$	1	5	1	5	2	2	1	15	2	2	5	4	1	4	1	51

We refer to the exercises for the determination of  $I(n)$  for the values  $17 \leq n \leq 31$  that are not covered by 10.4. The determination of  $I(n)$  for the orders marked with a star is beyond the scope of these course notes.

The list shows that for prime powers  $p^n$ , the number  $I(p^n)$  grows rapidly with  $n$ . The values  $I(2^n)$  were calculated by hand for  $n \leq 6$ ; for the recent calculation of values such as  $I(2^7) = I(128) = 2328$  and  $I(2^8) = I(256) = 56092$ , computers were used. For these types of statements, verifying the correctness of a proof is a problem in itself. In 1997, the value 10 494 213 was found for  $I(2^9) = I(512)$ , and  $I(2^{10}) = I(1024) = 49 487 365 422$  was calculated at the beginning of this century.<sup>38</sup> Currently, the precise value of  $I(2048) \approx 1.77 \cdot 10^{15}$  is not known.

### ► SOLVABLE GROUPS

For arbitrary finite groups, we have no guarantee that the group can be “built step by step” from smaller groups. However, this approach does work well for so-called *solvable groups*.

**10.14. Definition.** A finite group  $G$  is called *solvable* if there exists a chain of subgroups

$$G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_k = 1$$

of  $G$  for which  $H_{i+1}$  is always normal in  $H_i$  and  $H_i/H_{i+1}$  is cyclic of prime order.

The historical reason for this name is a connection to solving polynomial equations by extracting roots, which we will encounter later in *Galois theory*. The *solvability chain* in 10.14 is not always unique.

**Exercise 5.** Show that  $S_3$  has a unique solvability chain but  $C_6$  does not.

Cauchy’s theorem 5.13 gives rise to cyclic subgroups of prime order. If there are no problems with normality, for example because the group in question is abelian, this inductively leads to solvability.

**10.15. Proposition.** Finite abelian groups are solvable.

**Proof.** The proof is by induction on the group order. For  $G = 1$ , there is nothing to prove. For non-trivial  $G$ , by Cauchy’s theorem, there exists an element  $x \in G$  of prime order. The subgroup  $H = \langle x \rangle$  is normal in  $G$  because  $G$  is abelian, and the quotient group  $G/H$  is solvable by the induction hypothesis. Write the corresponding chain of subgroups as  $G/H = M_0 \supset M_1 \supset M_2 \supset \dots \supset M_k = H/H = 1$ . By 8.1, we have  $M_i = H_i/H$  for subgroups  $H_i \supset H$  of  $G$ , and the quotients  $H_i/H_{i+1} \cong M_i/M_{i+1}$  are cyclic of prime order. The chain

$$G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_k = H \supset 1$$

now shows that  $G$  is solvable.  $\square$

Note that 10.15 also follows directly from the structure theorem 9.11. However, the given proof is interesting because the abelian property of  $G$  is only used to guarantee the normality of the subgroup  $H = \langle x \rangle$ .

**Exercise 6.** Show that  $A_4$  has no normal subgroups of prime order.

A normal subgroup of prime order always exists if  $G$  is a  $p$ -group, that is, a finite group  $G$  whose order is a power of a prime  $p$ .

**10.16. Lemma.** *Let  $G$  be a finite  $p$ -group. Then we have  $Z(G) \neq 1$ .*

**Proof.** We let  $G$  act on itself by conjugation. The fixed points under this action are the elements of the center of  $G$ , and congruence 5.14 gives  $\#Z(G) \equiv \#G \equiv 0 \pmod{p}$ . So the order of  $Z(G)$  is divisible by  $p$ .  $\square$

For an element  $x \in Z(G)$ , the subgroup  $H = \langle x \rangle$  is conjugation-invariant and therefore normal in  $G$ . For a  $p$ -group  $G$ , the proof of 10.15 therefore remains valid with as only modification that for the generator  $x$  of  $H$ , we take an element of  $Z(G)$  of order  $p$ .

**10.17. Theorem.** *Every finite  $p$ -group is solvable.*  $\square$

For the 2-group  $D_4 = \langle \rho, \sigma \rangle$  of order 8, there are several solvability chains. The chain  $D_4 \supset \langle \rho \rangle \supset Z(D_4) = \langle \rho^2 \rangle \supset 1$  consists of normal subgroups of  $D_4$ ; the chain  $D_4 \supset \langle \rho^2, \sigma \rangle \supset \langle \sigma \rangle \supset 1$  contains a non-normal subgroup of order 2.

**Exercise 7.** Show that every  $p$ -group admits a solvability chain consisting of normal subgroups.

## ► SIMPLE GROUPS

The strategy of analyzing  $G$  through its normal subgroups only has a chance of success if  $G$  has a non-trivial normal subgroup. For most small groups that are not of prime order, it is not too difficult to prove that they contain a non-trivial normal subgroup. This leads to the following well-known theorem, whose proof we leave to the reader as an exercise.

**10.18. Theorem.** *Every group of order  $n < 60$  is solvable.*  $\square$

The alternating group  $A_5$  of order  $60 = 2^2 \cdot 3 \cdot 5$  is not solvable. Indeed, it follows easily from 5.11 that the class formula from Exercise 5.42 for  $A_5$  is given by  $60 = 1 + 15 + 20 + 12 + 12$ . Every normal subgroup  $N \triangleleft A_5$  is a union of conjugacy classes that contains the class of the unit element (of order 1). Since, additionally, the order of  $N$  is a divisor of 60, we easily see that only the trivial cases  $N = 1$  and  $N = A_5$  can occur.

This argument shows that  $A_5$  not only has no solvability chain but also has no non-trivial normal subgroups. A group  $G \neq 1$  with this property is called a *simple group*. Every finite group  $G$  admits a chain

$$G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_k = 1$$

for which  $H_{i+1}$  is always normal in  $H_i$  and the quotient  $H_i/H_{i+1}$  is simple. If  $G$  is trivial or simple, this statement is immediately clear. For  $G \neq 1$  not simple, we take a non-trivial normal subgroup  $N \triangleleft G$  and use induction to make a chain for  $G$  from a chain for  $N$  and the inverse image of a chain for  $G/N$  under  $G \rightarrow G/N$ . Any finite group can therefore be constructed from a chain having “simple steps,” and the solvable groups are exactly those for which only cyclic prime steps are required. In somewhat physics-like terminology, we can state that the simple groups are the “elementary building blocks” of finite group theory.

**Exercise 8.** Show that an abelian simple group is cyclic of prime order.

Non-abelian simple groups are relatively rare. The first example after  $A_5$  of a non-abelian simple group is the group  $\mathrm{SL}_2(\mathbf{F}_7)/\{\pm 1\}$ , which has order 168. The *classification of finite simple groups* undertaken in the 1950s has been one of the biggest projects in group theory. This classification says that, in addition to several known infinite families of simple groups, such as the groups of prime order and the alternating groups  $A_n$  for  $n \geq 5$ , there exist exactly 26 finite simple groups. The last of these 26 so-called *sporadic simple groups* were only found around 1970 and have exotic names such as *monster* and *baby monster*. The proof of the correctness of the classification, which counts many thousands of pages, is spread over hundreds of papers, some of which remain unpublished. To improve the status of this “proof,” a “revision project” has been started that aims to publish a new and complete proof.<sup>39</sup>

#### EXERCISES.

9. Suppose that a semi-direct product  $N \rtimes_{\phi} H$  is abelian. Prove that  $N$  and  $H$  are abelian and that the map  $\phi : H \rightarrow \mathrm{Aut}(N)$  is trivial.
10. Let  $1 \rightarrow N \xrightarrow{f} G \rightarrow H \rightarrow 1$  be an exact sequence of groups, and suppose that  $f$  admits a section  $p : G \rightarrow N$ . Prove that  $G$  is isomorphic to  $N \times H$ .
11. Let  $1 \rightarrow A \rightarrow G \rightarrow H \rightarrow 1$  be an extension with  $A$  abelian, and suppose that the extension splits. Show that the conjugation action  $H \rightarrow \mathrm{Aut}(A)$  does not depend on the choice of the section  $s : H \rightarrow G$ . [Compare with 4.4.]
12. Show that in the previous exercise, there is also a natural conjugation action  $H \rightarrow \mathrm{Aut}(A)$  if the extension does *not* split. Describe this action for  $A = \langle i \rangle \subset G = Q$  and  $H = Q/A \cong \mathbf{Z}/2\mathbf{Z}$ .
13. Show that for every exact sequence  $1 \rightarrow N \rightarrow G \rightarrow H \rightarrow 1$ , there is an induced homomorphism  $H \rightarrow \mathrm{Out}(N)$ , where  $\mathrm{Out}(N)$  is as in Exercise 4.55.
14. Let  $G$  be a group and  $\phi : G \rightarrow \mathrm{Aut}(G)$  be the conjugation action of  $G$  on itself. Prove that the semi-direct product  $G \rtimes_{\phi} G$  is isomorphic to the direct product  $G \times G$ . [Hint: choose a “better” section  $G \rightarrow G \rtimes_{\phi} G$  to see that this is less unlikely than it seems at first sight.]
15. Let  $p$  be a prime. Prove that  $C_p \times C_p$  and  $C_{p^2}$  are the only groups of order  $p^2$  up to isomorphism.

16. Let  $G$  be a non-abelian group of order  $p^3$  with  $p$  prime. Prove that  $Z(G) = [G, G]$  has order  $p$  and that there is an isomorphism  $G/Z(G) \cong \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$ .
17. Prove that the dihedral group  $D_n$  is solvable for  $n \geq 1$ .
18. Let  $G$  be a finite group and  $N \triangleleft G$  be a normal subgroup. Prove that  $G$  is solvable if and only if  $N$  and  $G/N$  are.
19. Let  $A$  be an abelian group of order  $n$ . Prove that for every divisor  $m$  of  $n$ , there is a subgroup  $B \subset A$  of order  $m$ .
20. Let  $p$  be a prime. Show that the conjugation action of  $G$  on  $X = \text{Syl}_p(G)$  is transitive. What is the kernel of the corresponding map  $G \rightarrow S(X)$ ?
21. Show that the regular action of  $G$  on the set  $X = G/P$  with  $P \in \text{Syl}_p(G)$  is transitive. What is the kernel of the corresponding map  $G \rightarrow S(X)$ ? Are  $\text{Syl}_p(G)$  and  $G/P$  isomorphic as  $G$ -sets?
22. For the primes  $p$  that divide the group order, determine the number of Sylow  $p$ -subgroups of  $A_4$  and their structure. Do the same for  $A_5$ .
23. For every divisor  $d$  of 24, determine the number of subgroups of  $S_4$  of order  $d$ . Which of these subgroups are normal?
24. Let  $\mathcal{C}$  be the conjugacy class of  $(12)(34) \in S_n$ . Prove that for  $n \in \{4, 5\}$ , the map defined by  $x \mapsto N_x$  (the normalizer of  $x$ ) is a bijection  $\mathcal{C} \rightarrow \text{Syl}_2(S_n)$ .
25. Show that every group of order 200 contains a non-trivial normal subgroup.
26. Show that there are exactly four isomorphism classes of groups of order 30: the cyclic group  $C_{30}$  and the non-abelian groups  $D_{15}$ ,  $D_3 \times C_5$ , and  $D_5 \times C_3$ .
27. Let  $G$  be a group of order  $pq^n$  for  $p < q$  both prime and  $n \geq 1$ . Prove:  $G$  is solvable.<sup>40</sup> [*Burnside's theorem* says this is also the case for groups of order  $p^m q^n$ .]
28. Let  $G$  be a group of order  $2n$  with  $n$  odd. Prove that there is an isomorphism  $G \cong N \rtimes C_2$  for a normal subgroup  $N \triangleleft G$  of order  $n$ .
29. Let  $G$  be a group of even order, and suppose that the Sylow 2-subgroups of  $G$  are cyclic. Prove that  $G$  contains a normal subgroup of index 2.
30. Let  $p$  be a prime and  $G_p = \text{Aff}(\mathbf{Z}/p\mathbf{Z})$  be the affine group over  $\mathbf{Z}/p\mathbf{Z}$ . Prove that for every prime divisor  $q \mid p-1$ , the group  $G_p$  contains a unique subgroup of order  $pq$  and that this subgroup is not abelian.
31. Let  $p$  be a prime and  $H_p \subset \text{GL}_n(\mathbf{F}_p)$  be a Sylow  $p$ -subgroup. Prove:  $H_p$  is conjugate to the subgroup of upper triangular matrices of the form

$$\begin{pmatrix} 1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & 1 \end{pmatrix}.$$

32. Prove Theorem 10.18.

\*33. Let  $G$  be a simple group of order 60. We are going to prove that  $G$  is isomorphic to  $A_5$ .

- a. Let  $n > 1$  be the *minimal* index of a proper subgroup  $H \subsetneq G$ . Prove: we have  $n \geq 5$ , and we have  $G \cong A_5$  if  $n = 5$ .
- b. Prove:  $G$  has  $n_3 = 10$ ,  $n_5 = 6$ , and  $n_2 \in \{5, 15\}$ ; in the case  $n_2 = 5$ , we have  $G \cong A_5$ .
- c. Prove: any two distinct Sylow 2-groups  $H_2$  and  $H'_2$  in  $G$  have intersection  $H_2 \cap H'_2 = 1$ . Conclude that  $n_2 \neq 15$ , so  $G \cong A_5$  by part b. [Hint: look at the normalizer of  $H_2 \cap H'_2$ .]
- \*34. Prove that  $A_n$  is simple for  $n \geq 5$ .  
[Hint: Take  $N \triangleleft A_n$  non-trivial and  $n \geq 5$ . Then for every subgroup  $G_i = \{\sigma \in A_n : \sigma(i) = i\} \cong A_{n-1}$ , we have  $N \cap G_i = 1$ , and  $N$  has order  $n$ . The image of the Cayley map  $N \rightarrow S(N)$  is now a normal subgroup of the group  $\text{Alt}(N)$  of even permutations on the set  $N$ , and every even permutation of  $N$  that fixes the unit element is an automorphism.]
35. Let  $G$  be a group of order 255. Prove that  $G$  is cyclic.  
[So there is a big difference between  $I(255) = I(257) = 1$  and  $I(256)$ .]
- \*36. Let  $G$  be a finite group, and suppose that every *maximal* subgroup of  $G$  is abelian. Prove that  $G$  is solvable.  
[A subgroup  $H \subset G$  is called maximal if we have  $H \neq G$  and every subgroup  $H' \supsetneq H$  of  $G$  is equal to  $G$ .]
37. Let  $n$  be a positive integer. Prove that the following are equivalent:
- $I(n) = 1$ ;
  - $I(d) = 1$  for every divisor  $d$  of  $n$ ;
  - every group of order  $n$  is cyclic;
  - $n$  is relatively prime to  $\varphi(n)$ .
38. Determine all isomorphism classes of groups of orders 20 and 28. Generalize to order  $4p$  for  $p > 3$  prime.
39. Let  $G \neq 1$  be a group with  $\text{Aut}(G) = 1$ .
- Suppose that  $G$  is finite. Prove:  $\#G = 2$ .  
[Hint: first prove that  $G$  is abelian; then look at inversion.]
  - Show that the assumption in part a that  $G$  is finite is, in fact, unnecessary.
40. Let  $A$  be a finitely generated abelian group. Prove that  $\text{Aut}(A)$  is finite if and only if the free rank of  $A$  is not greater than 1.
41. Let  $G$  be a group of order  $n = pq^2$  with  $p < q$  prime. Prove: if  $p$  does not divide  $q^2 - 1$ , then  $G$  is abelian, and there are two isomorphism classes of groups of order  $pq^2$ . What is the smallest value of  $n$  that satisfies these conditions?
42. Show that every automorphism of the additive group  $\mathbf{Q}$  is of the form  $x \mapsto ax$  with  $a \in \mathbf{Q}^*$ . Conclude:  $\text{Aut}(\mathbf{Q}) \cong \mathbf{Q}^*$ .
43. Show that for  $n \geq 1$  square-free and  $G = (\mathbf{Z}/n\mathbf{Z})^k$ , there is an isomorphism  $\text{Aut}(G) \cong \text{GL}_k(\mathbf{Z}/n\mathbf{Z})$ .
44. Show that  $\text{Aut}(C_2 \times C_4)$  has order 8. Which group from Theorem 10.5 is it?
45. Show that for  $n > 2$ , there is an isomorphism  $\text{Aut}(D_n) \cong \text{Aff}(\mathbf{Z}/n\mathbf{Z})$ , where  $\text{Aff}(\mathbf{Z}/n\mathbf{Z})$  is the affine group from 8.14.4.

46. Show that the wreath product  $C_p \wr C_2$  has order  $2p^2$ .
47. Let  $p$  be a prime and  $B_p \subset \text{GL}_3(\mathbf{F}_p)$  be the group of matrices of the form

$$M_{i,j,k} = \begin{pmatrix} 1 & i & j \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix} \quad \text{with } i, j, k \in \mathbf{F}_p.$$

Prove that  $B_p$  is a non-abelian group of order  $p^3$  and that  $B_p$  is the semi-direct product of  $N = \{M_{i,j,0} : i, j \in \mathbf{F}_p\} \subset B_p$  and  $H = \{M_{0,0,k} : k \in \mathbf{F}_p\} \subset B_p$ . Which group of order 8 is  $B_2$ ?

48. Let  $Q$  be the quaternion group,  $x \in Q$  be an element of order 4, and  $y \in Q$  be an element of  $Q \setminus \langle x \rangle$ . Prove that there is an automorphism  $\phi \in \text{Aut}(Q)$  such that  $\phi(i) = x$  and  $\phi(j) = y$  and that  $\text{Aut}(Q)$  has order 24.
49. Show that every automorphism of  $Q$  induces an automorphism of  $Q/Z(Q) \cong V_4$  and that this leads to an exact sequence  $1 \rightarrow K \rightarrow \text{Aut}(Q) \rightarrow \text{Aut}(Q/Z(Q)) \rightarrow 1$ . Prove that  $K$  is a group isomorphic to  $V_4$  and consists of the identity and the automorphisms of  $Q$  that send exactly two of the three elements  $i, j, k \in Q$  to their inverses. Deduce that there is an isomorphism  $\text{Aut}(Q) \cong S_4$ .
- \*50. Let  $V$  be the real 3-dimensional vector space with basis  $\{i, j, k\}$  and  $\text{Aut}(Q) \rightarrow \text{GL}(V)$  be the natural linear action of  $\text{Aut}(Q)$  on  $V$ . Prove that  $\text{Aut}(Q)$  permutes the four 1-dimensional vector spaces generated by each of the elements of the form  $i \pm j \pm k$  and that this leads to an isomorphism  $\text{Aut}(Q) \cong S_4$ .
51. Determine  $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$  for  $G = Q$  and for  $G = D_n$ .
52. Let  $N$  be an abelian group, and suppose that  $H_1$  and  $H_2$  are conjugate subgroups of  $\text{Aut}(N)$ . Prove that there is an isomorphism  $N \rtimes H_1 \cong N \rtimes H_2$ .
- \*53. Determine the isomorphism classes of the groups of order 24.  
[Hint: We have  $n_2 \in \{1, 3\}$  and  $n_3 \in \{1, 4\}$ . There are five groups with  $n_2 = n_3 = 1$  by 10.5. There are only two groups of order 8 with an automorphism of order 3, so two groups with  $n_2 = 1$  and  $n_3 = 4$ . There are seven groups with  $n_2 = 3$  and  $n_3 = 1$ . The only group with  $n_2 = 3$  and  $n_3 = 4$  is  $S_4$ . This last statement can be seen by considering the conjugation action of the group on its Sylow 3-subgroups.]
54. The group  $G = \text{GL}_2(\mathbf{F}_3)$  of order 48 has a quotient group  $\text{PSL}_2(\mathbf{F}_3) = G/\{\pm 1\}$  and a subgroup  $\text{SL}_2(\mathbf{F}_3)$  that each have order 24. Determine  $n_2$  and  $n_3$  for each of these groups, as well as their position in the list from the previous exercise.
55. Let  $p$  be a prime and  $G$  be an elementary abelian  $p$ -group of rank  $k$ . Prove:  $\text{Aut}(G)$  is isomorphic to the group  $\text{GL}_k(\mathbf{F}_p)$  of invertible  $k \times k$  matrices over  $\mathbf{F}_p$  and has order  $\prod_{i=0}^{k-1} (p^k - p^i)$ .
56. Let  $p$  be an odd prime and  $G$  be a non-abelian group of order  $2p^2$ . Prove:  $G$  is isomorphic to the dihedral group  $D_{p^2}$ , the direct product  $C_p \times D_p$ , or the semi-direct product  $(C_p \times C_p) \rtimes C_2$  with respect to the inversion action of  $C_2$  on  $C_p \times C_p$ . Conclude that  $I(2p^2) = 5$ .
57. Let  $p$  be an odd prime. Prove that there exists a non-abelian group of order  $p^3$  in which every element  $x \neq e$  has order  $p$ . \*Is this group uniquely determined up to isomorphism?

- \*58. Let  $p$  be an odd prime and  $G$  be a non-abelian group of order  $p^3$  that contains an element of order  $p^2$ . Prove:  $G$  is isomorphic to the semi-direct product  $C_{p^2} \rtimes C_p$  of  $C_{p^2}$  and the unique subgroup  $C_p \subset \text{Aut}(C_{p^2})$ .
59. Prove:  $I(p^3) = 5$  for every prime  $p$ .

## TABLE OF SMALL GROUPS

Order	Abelian	Non-abelian
1	$C_1$	
2	$C_2$	
3	$C_3$	
4	$C_4, V_4$	
5	$C_5$	
6	$C_6$	$D_3$
7	$C_7$	
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$	$D_4, Q$
9	$C_9, C_3 \times C_3$	
10	$C_{10}$	$D_5$
11	$C_{11}$	
12	$C_{12}, C_6 \times C_2$	$A_4, D_6, C_3 \rtimes_{\phi} C_4$
13	$C_{13}$	
14	$C_{14}$	$D_7$
15	$C_{15}$	

Notation:

- $A_n$ : the alternating group on  $n$  symbols
- $C_n$ : a cyclic group of order  $n$
- $D_n$ : the dihedral group of order  $2n$
- $Q$ : the quaternion group
- $V_4$ : the Klein four-group

Justification:

- Order 1: exercise
- Orders 2, 3, 5, 7, 11, 13: Exercise 4.8
- Orders 4 and 9: Theorem 10.4.1
- Orders 6, 10, and 14: Theorem 10.4.3
- Order 8: Theorem 10.5
- Order 12: Theorem 10.13
- Order 15: Theorem 10.4.2

## LITERATURE

De verwijzingen in dit deel van de syllabus geven een handvat om zelfstandig in een wiskundebibliotheek rond te neuzen zonder direct door de bomen het bos niet meer te zien. De hier verzamelde referenties variëren van populair-wetenschappelijke artikelen, zoals men die in tijdschriften als de *Mathematical Intelligencer* vindt, tot leerboeken en onderzoeksartikelen. Verwacht niet alles in één keer te begrijpen—er is meer wiskunde dan een mensenhoofd kan bevatten.

Nederlandstalige wiskunde van enig niveau is uiterst schaars, want Nederlanders drukken zich te pas en te onpas uit in het Engels. Iets oudere literatuur of boeken met grotere oplage zijn vaak in één van onze beide andere buurtalen, Duits en Frans, geschreven of vertaald. Voor wie meer Europees dan provinciaal georiënteerd is, kan dat geen groot bezwaar zijn. Zie eventueel de Europese pagina voor een paar lastige woorden.

1. Er is geen reden om het bij voorbaat eens te zijn met mijn definitie van algebra. Vorm een eigen oordeel door één van de vele boeken met de titel ‘Algebra’ van de plank te trekken en eens door te bladeren. Ik noem een aantal boeken die het inkijken meer dan waard zijn, nu en in de loop van je studie. Naarmate ons college vordert wordt waarschijnlijk duidelijker waar al deze boeken over gaan. Wie elk half jaar opnieuw kijkt kan zien hoe zijn kennis groeit.

- [M. Artin](#), *Algebra*, Prentice Hall, 1991. [Second edition 2011](#).

Een aardig modern boek, enigszins in de geest van deze tekst. Sla hoofdstuk 1 gewoon over. Online: een [MAA-review](#).

- [I. R. Shafarevich](#), *Basic notions of algebra*, Encyclopaedia of Mathematical Sciences 11, Springer, 2005.

Geen eerstejaars tekstboek, maar panoramisch geschreven. De standaardvolgorde ‘groepen-ringen-lichamen’ wordt in dit boek omgedraaid. Een goed medicijn voor wie denkt dat de wiskunde uit losse onderdelen bestaat die weinig met elkaar of de andere exacte wetenschappen te maken hebben. Online: een [MAA-review](#), en een [necrologie](#).

- [S. Lang](#), *Algebra*. Springer, revised 3rd edition, 2002.

Een standaardreferentie voor de moderne algebra die door velen gebruikt wordt. Iedere nieuwe editie is dikker dan de vorige—de laatste heeft ruim 900 bladzijden.

- [M. A. Armstrong](#), *Groups and symmetry*, Springer UTM, corrected 2nd printing, 1997.

Een leesbaar, niet te dik boekje dat ongeveer dezelfde onderwerpen behandelt als deze syllabus.

- [J. A. Gallian](#), *Contemporary Abstract Algebra*, CRC Press, 10th revised edition, 2020.

Een representant uit de Amerikaanse cultuur van ‘college texts’. Minder zwaar op de hand dan voorafgaande teksten, vol citaten, computerprogramma’s en biografieën van wiskundigen die een belangrijke bijdrage hebben geleverd aan het ontstaan van de moderne algebra. Om de paar jaar verschijnt er een ‘nieuwe’ editie.

- [B.L. van der Waerden](#), *Algebra*, Springer, 1930. [Diverse edities](#) sinds de eerste Duitse uitgave, ook in het Engels.

Het eerste moderne algebraboek, geschreven door de Nederlandse wiskundige die wat toen nog *Moderne Algebra* was leerde bij Emil Artin en Emmy Noether. Zeer de moeite waard.

2. Wie geïnteresseerd is in de geschiedenis van de wiskunde, of in de tragisch verlopen levens van een aantal grondleggers van de groepentheorie zoals Galois en Abel kan voor geromanitiseerde, enigszins oppervlakkige verhalen terecht bij Bell. Bondiger zijn de schetsjes in het ten zeerste aanbevolen geschiedenisboekje van Stillwell. Online is er de [St. Andrews MacTutor website](#).

Voor uitgebreidere biografische gegevens is er nog het laatstgenoemde standaardwerk, een uittreksel uit de *Dictionary of Scientific Biography*.

- E.T. Bell, *Men of mathematics*, Simon & Schuster, 1937. Diverse herdrukken.
- J. Stillwell, *Mathematics and its history*, Springer UTM, 1989.
- *Biographical dictionary of mathematicians*, 4 vols, Scribner's, New York, 1991.

3. In de negentiende eeuw werden permutaties ook wel ‘substituties’ genoemd. Wie oude wiskundeliteratuur leuk vindt kan eens kijken in Netto's boek, en het vervolgens vergelijken met de modernere tekst van Dixon en Mortimer.

- E. Netto, *Substitutionentheorie und ihre Anwendungen auf die Algebra*, Teubner, 1882. Er is een Engelse vertaling, herdrukt bij Chelsea.
- J. D. Dixon, B. Mortimer, *Permutation groups*, Springer, 1996.

4. De mededeling dat twee permutaties in  $S_n$  ‘al snel’ de hele groep (of in ieder geval  $A_n$ ) voortbrengen krijgt een precieze betekenis in onderstaand artikel.

- John D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110**, 199–205 (1969).

5. Sam Loyd's puzzeltje staat bekend als *Sam Loyd's Fifteen*. Onderstaand boek ging onder meer de geschiedenis na, en claimt dat de Amerikaanse postbeambte Noyes Chapman de eigenlijke uitvinder is.

- Jerry Slocum, Dic Sonneveld, *The 15 Puzzle*, Slocum Puzzle Foundation: 2006.

6. Over Rubik's kubus is veel geschreven, van oplosmethodes tot lijsten van ‘mooie patronen’. Bekijk in onderstaande referenties ‘van het eerste uur’ de literatuurverwijzingen, of kijk op [www.rubiks.com](http://www.rubiks.com).

- J. van de Craats, *De magische kubus van Rubik*, De Muiderkring, 1981.
- D. Hofstadter, *Metamagical Themas*, Scientific American **244**, 20–39 (1981).

7. De partitiefunctie  $p(n)$ , die al bestudeerd werd door Euler, groeit nogal snel met  $n$ . Er geldt

$$p(n) \approx e^{\pi\sqrt{2n/3}} / (4n\sqrt{3}).$$

Opgave 2.58 laat zien dat de waarden van  $p(n)$  de machtreekscoëfficiënten zijn van een eenvoudige *genererende functie*. Studie van deze functie, die in essentie een *modulaire vorm* is, heeft in deze eeuw geleid tot representaties van  $p(n)$  die de functie ook voor grote  $n$  berekenbaar maken. De waarden van  $p(n)$  voor zulke  $n$ , waarin niemand ooit enige bijzondere structuur met betrekking tot hun delers heeft gevonden, worden als test-input gebruikt voor *factorisatiealgoritmen* zoals genoemd in §7. Hoofdstuk XIX in de volgende klassieke referentie geeft enige details, hoofdstuk 7 in Grosswald is moderner.

- G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, 1938. Er zijn diverse verbeterde herdrukken.

- E. Grosswald, *Topics from the Theory of Numbers*, 2nd edition, Birkhäuser, 1984.
- 8.** Voor de maximale orde  $g(n)$  van een element in  $S_n$  in opgave 2.60 geldt voor grote  $n$  de relatie  $\log g(n) \approx \sqrt{n} \log n$ . Omdat je in essentie  $n$  als een som van een boel kleine priemgetallen wilt schrijven is het niet verwonderlijk dat Landau's boek een bewijs van dit resultaat geeft, in §61. Andere interessante eigenschappen van de functie  $g(n)$ , zoals het feit dat er willekeurig lange intervallen bestaan waarop  $g$  constant is, vind je in het artikel van Nicolas.
- E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, 1909. Heruitgave: Chelsea, New York, 1953.
  - J.-L. Nicolas, *Sur l'ordre maximum d'un élément dans le groupe  $S_n$  des permutations*, Acta Arithm. **14**, 315–332 (1967/68).
- 9.** De Sinterklaaslootjesobservatie in opgave 2.63 komt in veel varianten voor en gaat terug tot Montmort (1708). Lees hierover de pagina's 99–101 in onderstaand boek, dat veel interessant materiaal bevat voor wie van combinatorische problemen houdt.
- W. Feller, *An introduction to probability theory*, Wiley, 1950.
- 10.** Het bestaan van enantiomeren is van belang in scheikunde en biologie. Wie zelf wil weten waarom het al dan niet nuttig is om rechtsdraaiende yoghurt te eten raadplege zijn scheikundeboeken.
- 11.** Het Erlanger Programm van Felix Klein maakte de groep tot een centraal en unificerend wiskundig concept. Later ontwikkelde takken van meetkunde, zoals de algebraïsche meetkunde, passen niet direct binnen het programma van Klein.
- F. Klein, *Vergleichende Betrachtungen über neuere geometrische Forschungen*, Math. Annalen **43**, 63–100 (1893).
- Voor een 'historische evaluatie' van het Erlanger Programm, en algemener een goed historisch perspectief op wiskundige ideeën, is er een klassiek werk, in voordelige pocketeditie beschikbaar.
- M. Kline, *Mathematical thought from ancient to modern times*, Oxford University Press, 1972. Paperback edition, 1990.
- 12.** Voor wie zich wil vermaken met begrippen als oriëntatie, binnen en buiten en andere topologische concepten in het platte vlak is er een klassiek science fiction-achtig boekje, dat nu ook verfilmd is ([www.flatlandthemovie.com](http://www.flatlandthemovie.com)). Verkrijgbaar als Dover-pocket, maar ook in een recente geannoteerde editie. Zie voor een recensie <http://www.ams.org/notices/200210/rev-dewdney.pdf>.
- E. A. Abbott, *Flatland*, 1882. Heruitgave: *The annotated Flatland, a romance of many dimensions*, introduction and notes by Ian Stewart, The Perseus Press, 2002.
- 13.** De eindige ondergroepen van de rotatiegroep  $O_3^+(\mathbf{R})$  in 3 dimensies zijn, naast de groepen  $C_n$  en  $D_n$  die door realisaties van vlakke symmetrieën als ruimtelijke rotaties ontstaan, alleen de groep  $T^+ \cong A_4$  van rotaties van de tetraëder, de draaiingsgroep  $K^+$  van de kubus, en de groep  $\text{Icos}^+ \cong A_5$  van rotaties van een regelmatig twaalf- of twintigvlak. Zie hiervoor de onder referentie **1** genoemde boeken van Artin (stelling V.9.1) of Armstrong (hoofdstuk 19). Met een beetje extra werk krijgt men hieruit een beschrijving van alle eindige ondergroepen van de orthogonale groep  $O_3(\mathbf{R})$  in 3 dimensies, zie de pagina's 276–277 in onderstaand boek.

- H. S. M. Coxeter, *Introduction to Geometry*, Wiley, New York, 1969.

**14.** Het idee dat veel ‘standaardconstructies’ in de wiskunde op een soort universele manier beschreven kunnen worden heeft geleid tot het concept van categorieën. Veel resultaten in deze hoek staan te boek als ‘abstract nonsense’. Onze isomorfiestelling 4.10 en soortgelijke stellingen in §8 als de homomorfiestelling 8.4 zijn representatieve voorbeelden. Veel moderne algebraboeken hebben een paragraaf over categorieën. Wij besteden er een hoofdstuk aan in de syllabus Algebra 3. Het betreft meer een taalgebruik dan een theorie.

- P. J. Hilton, U. Stammbach, *A course in homological algebra*, Springer GTM 4, 1971.
- S. MacLane, *Categories for the working mathematician*, Springer GTM 5, 1971.

**15.** De actie van de modulaire groep  $SL_2(\mathbf{Z})$  op het complexe bovenhalfvlak is één van de fundamentele groepswerkingen in de algebra en de complexe analyse. Deze werking en zijn varianten geven aanleiding tot de theorie van *modulaire functies* en *modulaire vormen*. De rijke verbanden met getaltheorie, meetkunde en complexe analyse maken dit tot een centraal en intensief bestudeerd deel van de wiskunde. De populariteit ervan is nog eens toegenomen na het verschijnen van Wiles’ bewijs van de laatste stelling van Fermat – zie verwijzing 22. Hoofdstuk VII van Serre’s boekje geeft een compacte inleiding.

- J.-P. Serre, *A course in arithmetic*, Springer GTM 7, 1973. [Dit is de Engelse vertaling van *Cours d’arithmétique*, Presses Universitaires de France, 1970.]

**16.** De constructie van *quotiëntruïmtes* of *identificatieruïmtes* komt men in meetkunde en topologie tegen. Stillwell’s boekje, dat tevens een aardige inleiding bevat over overeenkomsten en verschillen tussen Euclidische, sferische en hyperbolische meetkunde, is toegankelijk en heeft veel plaatjes.

- J. Stillwell, *Geometry of surfaces*, Springer Universitext, 1992.

**17.** De beste gepubliceerde afchatting van de functie  $I(n)$  in opgave 5.40 schijnt  $I(n) < n^k$  met  $k = \text{cst} \cdot n^{2/3} \log n$  te zijn.

- P. X. Gallagher, *Counting finite groups of given order*, Math. Zeitschrift **102**, 236–237 (1967).

**18.** Het blijkt dat men groepen soms goed kan bestuderen door ze te laten werken op zogenaamde ‘bomen’. Zie hiervoor het onder 1 genoemde boek van Armstrong (Chapter 28), alsook onderstaand boek van Serre. Serre geeft een voorbeeld van een oneindige groep met precies twee conjugatieklassen in I.1.4.

- J.-P. Serre, *Trees*, Springer, 1980. [Dit is de Engelse vertaling van *Arbres, amalgames,  $SL_2$* , Astérisque **46** (1977).]

**19.** De axiomatische beschrijving van de natuurlijke getallen door Peano gaat uit van een ‘verzameling’  $\mathbf{N}$  van ‘natuurlijke getallen’ met een begrip ‘opvolger’. De axioma’s zeggen achtereenvolgens dat er een natuurlijk getal ‘0’ is, dat ieder natuurlijk getal een opvolger heeft, dat zo’n opvolger nooit 0 is, en dat getallen met dezelfde opvolger gelijk zijn. Tenslotte volgt het bekende *axioma van volledige inductie*. Zie het onder 11 genoemde boek van Kline of een logicaboek naar keuze.

**20.** Er zijn eindeloos veel open problemen met betrekking tot de elementaire eigenschappen van de gehele getallen.

- D. Shanks, *Solved and unsolved problems in number theory*, Chelsea, New York, 3rd edition, 1985.

**21.** De *Elementen* van Euclides vormden eeuwenlang de bijbel van de wiskunde, en na de echte bijbel de bestseller van de boekdrukkunst. De klemtoon op de tweede lettergreep in *Euclides* is ook al eeuwen oud – maar niet iedereen lijkt dat nog te weten.

Er zijn erg veel edities van de *Elementen*, onder meer een Dover-pocket in 3 delen met commentaar van Heath en een handzaam Duits deeltje van de Wissenschaftliche Buchgesellschaft. De boeken VII-IX behandelen getaltheorie, en wie zich niet door de meetkundige formuleringen van de wijs laat brengen vindt diverse stellingen uit §6 terug. Stelling 6.5 = IX, §20. 6.6 = VII, §30. Stelling 6.7 komt alleen als speciaal geval voor: IX, §14. Wie liever een klassieke stelling als de *stelling van Pythagoras* naslaat: I, §47. Zie voor meer informatie ook de desbetreffende paragraaf in het in **11** genoemde boek van Kline.

**22.** De beroemde laatste stelling van Fermat, die meer dan 350 jaar een open probleem is geweest, is uiteindelijk bewezen door Andrew Wiles. Er is veel publiciteit rond dit bewijs geweest, en de BBC maakte er een aardige documentaire over. De stelling werd aan het eind van de jaren tachtig door Ribet afgeleid uit een onbewezen vermoeden over *elliptische krommen* dat onder de naam Shimura-Taniyama-vermoeden bekend staat. Wiles' artikel, dat een belangrijk deel van dit vermoeden bewijst, sluit niet naadloos aan op dit college. De proceedings van de grote Boston-conferentie in 1995 over Wiles' bewijs bevatten aanvullende informatie en de eerste vereenvoudigingen van het bewijs.

- K. A. Ribet, *From the Taniyama-Shimura conjecture to Fermat's last theorem*, Ann. Fac. Sci. Toulouse Math. (5) 11 no. 1, 116–139 (1990).
- A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141**(3), 443–551 (1995).
- G. Cornell, J. H. Silverman, G. Stevens (eds), *Modular forms and Fermat's last theorem*, Springer, 1997.

**23.** Een gedegen uitleg van de werking van lokaal-globaal-principes behoort tot de *algebraïsche getaltheorie*. Er zijn tamelijk veel boeken over dit onderwerp. Hoofdstuk 3 uit onderstaand boek is redelijk elementair.

- H. E. Rose, *A course in number theory*, 2nd edition, Oxford, 1994.

**24.** De stelling van Dirichlet over priemrijen zegt dat voor  $n \geq 1$  en  $a \in (\mathbf{Z}/n\mathbf{Z})^*$  er oneindig veel priemgetallen  $p \equiv a \pmod{n}$  bestaan. Met andere woorden: in de rekenkundige rij  $a, a + n, a + 2n, \dots$  komen oneindig veel priemgetallen voor. De stelling werd in 1837 met methoden uit de complexe functietheorie bewezen door de Duitser Gustav Peter Lejeune Dirichlet (1805–1857).

- H. Davenport, *Multiplicative Number Theory*, 3rd edition, Springer GTM 74, 2000.

**25.** Mersenne-priemen zijn genoemd naar de Franse monnik Marin Mersenne (1588–1648). De lijst van Mersenne-priemen  $M_p = 2^p - 1$  is naar men vermoedt oneindig, maar dit is onbewezen. In oktober 2024 werd de 52<sup>e</sup> waarde van  $p$  gevonden waarvoor  $M_p$  priem is. Deze  $p = 136\,279\,841$  is de grootste bekende Mersenne-exponent, en correspondeert met een priemgetal van meer dan 41 miljoen decimale cijfers. Er is een Great Internet Mersenne Prime Search waaraan iedereen met een computer met 'ijdele tijd' deel kan nemen. Zie [www.mersenne.org](http://www.mersenne.org) voor de bijbehorende internet-site.

**26.** Fermat merkte op dat de getallen  $F_n = 2^{2^n} + 1$  priem zijn voor  $n = 0, 1, 2, 3, 4$ . Zijn optimistische gedachte dat dit voor alle  $n$  zo zou zijn bleek niet juist: er zijn geen getallen  $n > 4$  bekend waarvoor  $F_n$  priem is. De rij van getallen  $2^{2^n} + 1$  groeit dubbel-exponentieel in  $n$ , en het vermoeden is dat er slechts eindig veel priemgetallen bij zijn. Zie [www.prothsearch.net/fermat.html](http://www.prothsearch.net/fermat.html) voor een ‘statusoverzicht’, en Chris Caldwell’s *Prime Pages* (<http://primes.utm.edu>) voor allerlei andere informatie over priemgetallen.

**27.** In 1992 bewezen Alford, Granville en Pomerance dat er oneindig veel Carmichael-getallen bestaan. De voordracht van Pomerance op ons nationale KWG-congres van 1992 is uitgewerkt in het Nieuw Archief.

- C. Pomerance, *Carmichael numbers*, Nieuw Arch. Wisk. (4) 11, no. 3, 199–209 (1993).
- W. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math. **140**, 703–722 (1994)

**28.** Voor een enigszins algoritmische blik op primaliteit, factorisatie en de eigenschappen van pseudo-priemtests is het boek van Crandall en Pomerance de beste referentie. Het besteedt ook aandacht aan de toepassingen van elliptische krommen op primaliteit en factorisatie. Dunner en meer op de cryptografie gericht zijn de boeken van Koblitz en Buchmann.

Het overzichtsartikel van René Schoof over primaliteitstests in het recent verschenen MSRI-boek over algoritmische getaltheorie geeft niet alleen de AKS-primaliteitstest uit 2002, maar ook een beschrijving van de iets oudere, nog steeds zeer effectieve methoden. Ook het originele AKS-artikel is zeer leesbaar.

- R. Crandall, C. Pomerance, *Prime numbers—a computational perspective*, second edition, Springer, 2005.
- N. Koblitz, *A Course in Number Theory and Cryptography*, Springer GTM 114, 1987. Second edition 1994.
- J. Buchmann, *Einführung in die Kryptographie*, Springer, 1999. In diverse talen vertaald.
- M. Agrawal, N. Kayal, N. Saxena, *PRIMES is in P*, Annals of Math. **160**, 781–793 (2004). Online-versie: <http://annals.math.princeton.edu/wp-content/uploads/annals-v160-n2-p12.pdf>
- J. P. Buhler, P. Stevenhagen (eds), *Algorithmic number theory*, MSRI Publications vol. 44, Cambridge University Press, 2008. Webversie op mijn homepage.

**29.** Hoewel er zogenaamde ‘elementaire bewijzen’ van de priemgetalstelling bestaan, maken de meeste bewijzen gebruik van enige geavanceerde functietheorie of functionaalanalyse. Een bewijs van de eerste soort wordt in het onder **7** genoemde boek van Hardy en Wright gegeven. Voor de tweede soort is er meer keus.

- J. Korevaar, *On Newman’s quick way to the prime number theorem*, Math. Intelligencer **4**, no. 3, 108–115 (1982).
- W. Rudin, *Functional analysis*, McGraw-Hill, 1973.

**30.** De hier gegeven beschrijving van ‘textbook RSA’ gaat voorbij aan een aantal details dat belangrijk is om een daadwerkelijk veilig systeem te verkrijgen. Zo vermijdt men tegenwoordig in RSA-implementaties liever al te kleine publieke exponenten.

- D. Boneh, *Twenty years of attacks on the RSA cryptosystem*, Notices Amer. Math. Soc. **46**(2), 203–213 (1999).

**31.** De getallenlichamenzeef is op dit moment één van de meest effectieve methodes om grote getallen te factoriseren. Het onder **28** genoemde MSRI-boek heeft een overzichtsartikel van mijn hand, het Lenstra-boekje heeft meer details. De succesvolle toepassing op de factorisatie van het negende Fermat-getal  $F_9$  is ook goed gedocumenteerd.

- A. K. Lenstra, H. W. Lenstra, Jr. (eds), *The development of the number field sieve*, Springer Lecture Notes 1554, 1993.
- A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, J. M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61**, no. 203, 319–349 (1993).

**32.** Of en wanneer er ooit een quantumcomputer zal bestaan die getallen van meer dan 2 cijfers kan ontbinden is al sinds het artikel van Shor in 1994 een punt van discussie. Er wordt hard gewerkt aan de realisatie van dergelijke computers, onder meer aan de TU in Delft. Zie voor details bijvoorbeeld de Delfste website [Quantum computing](#).

**33.** Er blijkt een onverwacht verband te bestaan tussen  $5 \bmod p$  en  $p \bmod 5$ : de eerste is een kwadraat in  $(\mathbf{Z}/p\mathbf{Z})^*$  dan en slechts dan als de tweede een kwadraat is in  $(\mathbf{Z}/5\mathbf{Z})^*$ . Dit is een speciaal geval van de kwadratische reciprociteitswet, die wij in 26.4 zullen bewijzen. Deze wet werd in 1744 ontdekt door Euler en in 1796 bewezen door de 19-jarige Gauss. Er zijn bewijzen door ‘slim tellen’, zoals in het boek van Hardy en Wright uit **6**, en meer conceptuele bewijzen zoals het bewijs dat wij in §26 zullen geven.

**34.** Het is niet bekend of  $5 \bmod p$  een primitieve wortel is voor oneindig veel priemgetallen  $p$ . Een door de Duitser Emil Artin (1898–1962) uitgesproken vermoeden zegt dat dit wel zo is, en maakt precies hoeveel van zulke priemen men kan verwachten. Onder aanname van een onbewezen vermoeden, de zogenaamde gegeneraliseerde Riemann-hypothese voor de ligging van nulpunten van zeta-functies, kan men Artin’s vermoeden bewijzen.

- M. Ram Murty, *Artin’s conjecture for primitive roots*, Math. Intelligencer 10, no. 4, 59–67 (1988).

**35.** Goursat’s lemma, dat genoemd is naar de Fransman Edouard Jean-Baptiste Goursat (1858–1936), is bijzonder nuttig in de Galoistheorie. Niet iedereen die het lemma kent, kent het onder deze naam.

**36.** Het manipuleren van exacte rijtjes wordt meestal tot de *homologische algebra* gerekend. Naast het al in **14** genoemde boek van Hilton en Stammbach is er de herdruk van een klassiek boek van MacLane, één van de grondleggers van het vak.

- S. MacLane, *Homology*, Springer Classics in Mathematics, 1995.

**37.** Het karakteriseren van objecten als sommen en producten in deze en de twee voorafgaande opgaven door een zogenaamde *universele eigenschap* is een goede gewoonte uit de al onder **14** genoemde categorieëentheorie. Objecten met zo’n karakterisering zijn automatisch op isomorfie na uniek bepaald. Existentie is echter niet verzekerd!

**38.** Er zijn verschillende artikelen van Bettina Eick en co-auteurs waarin  $I(n)$  voor  $n < 2000$  wordt bepaald.

- H. U. Besche, B. Eick, E. A. O’Brien, *A millennium project: constructing small groups*, Internat. J. Algebra Comput. 12 (2002), no. 5, 623–644.

**39.** De eerste delen van het nu in boekvorm verschijnende bewijs van de classificatie van

eindige simpele groepen zijn inmiddels verschenen. Er is een overzichtsartikel naar aanleiding van het verschijnen van deel 1.

- R. Solomon, *On finite simple groups and their classification*, Notices of the Amer. Math. Soc. **42**(2), 231–239 (1995).

**40.** De zogenaamde  $p$ - $q$ -stelling van Burnside zegt algemener dat iedere groep van orde  $p^m q^n$  met  $p$  en  $q$  priem oplosbaar is. Er is meer groepentheorie voor een bewijs nodig dan deze syllabus bevat. Zie stelling 28.24 in Isaacs voor meer informatie.

- I. M. Isaacs, *Algebra, a graduate course*, Brooks-Cole, 1994.

**41.** Voor de existentie van precies zeven verschillende groepen van bandsymmetrieën, zie ook de artikelen in de Math Intelligencer

- H. McLeay, *A Closer Look at the Cast Ironwork of Australia*, Mathematical Intelligencer, **16**(4), 61–65 (1994).
- R. Wilson, I. Hargittai, M. Hargittai, *Stamp corner, One-dimensional space groups*, Mathematical Intelligencer, **18**(2), 78–79 (1996).

**42.** De volgende boeken bevatten informatie over kristallografische groepen, ook over het het door ons niet behandelde driedimensionale geval.

- I. R. Shafarevich, *Algebra I – Basic notions of algebra*, Encyclopaedia of Mathematical Sciences 11, Springer Verlag, 1990.
- H. S. M. Coxeter, *Introduction to Geometry*, Wiley, 1961.
- D. Hilbert & S. Cohn-Vossen, *Anschauliche Geometrie*, Springer Verlag,
- M. Artin, *Algebra*, Prentice Hall, 1991.

## THE GREEK ALPHABET

In mathematics, there is a great need for symbols to denote variables. In addition to a few single letters from non-European alphabets, such as the Hebrew aleph  $\aleph$ , the entire Greek alphabet is used by default.

A	$\alpha$	alpha	N	$\nu$	nu
B	$\beta$	beta	$\Xi$	$\xi$	xi
$\Gamma$	$\gamma$	gamma	O	$o$	omicron
$\delta$	$\delta$	delta	$\Pi$	$\pi, \varpi$	pi
E	$\epsilon, \varepsilon$	epsilon	P	$\rho, \varrho$	rho
Z	$\zeta$	zeta	$\sigma$	$\sigma, \varsigma$	sigma
H	$\eta$	eta	T	$\tau$	tau
$\Theta$	$\theta, \vartheta$	theta	$\Upsilon$	$\upsilon$	upsilon
I	$\iota$	iota	$\Phi$	$\phi, \varphi$	phi
K	$\kappa$	kappa	X	$\chi$	chi
$\Lambda$	$\lambda$	lambda	$\Psi$	$\psi$	psi
M	$\mu$	mu	$\Omega$	$\omega$	omega

## INDEX

- $b$ -adic number system, 81
- $p$ -group, **66**, 115, 116
- $p$ -rank, 116
- $p$ -subgroup, 127
- $\text{Aff}_2(\mathbf{R})$ , **39**, 41
- $A_n$ , **25**, 25
- $\text{Aut}(G)$ , **43**, 48
- $C_n$ , **35**, 36
- $D_4$ , 11, 12
- $D_n$ , **35**, 35, 36
- $\text{End}(G)$ , 42
- $G \cong G'$ , 42
- $G/H$ , 46
- $[G : H]$ , 46
- $G$ -equivariant, 68
- $G$ -set, **57**, 58, 134
- $G_x$ , 58
- $\text{Hom}(G, G')$ , 42
- $I_2(\mathbf{R})$ , **32**, 33, 101, 125
- $\text{Inn}(G)$ , 48
- $\text{Map}(X, A)$ , 53
- $\mathbf{N}$ , 71
- $N \triangleleft G$ , 49
- $O_2(\mathbf{R})$ , **32**, 33, 34, 101, 125
- $\text{Out}(G)$ , **54**, 133, 136
- $Q$ , 98
- $\mathbf{Q}^*$ ,  $\mathbf{R}^*$ ,  $\mathbf{C}^*$ , 43
- $S(X)$ , 19
- $\text{Sim}_2(\mathbf{R})$ , **39**, **41**
- $S_n$ , **19**, 21
- $\text{Syl}_p(G)$ , 127
- $\text{Sym}(F)$ , 35
- $V_4$ , 9
- $Z(G)$ , 48
- $\mathbf{Z}$ ,  $\mathbf{Q}$ ,  $\mathbf{R}$ ,  $\mathbf{C}$ , 43
- $\mathbf{Z}/n\mathbf{Z}$ , **51**, 71, 75
- $(\mathbf{Z}/n\mathbf{Z})^*$ , **76**, 77
- 15 puzzle, 26
  
- abelian group, **18**, 42, 43, 48, 49, 101, 108
- Abelian, N. H., 18
- abelianization, 106
- abelianization of a group, **97**
- abstract action, 62
- abstraction, 7, 43
- action, **29**, **57**, 101
- additive group, **43**, 43, 50, 51
- additive notation, **43**, 71, 74
- affine group, 41, **103**, 104, 134
- affine map, **39**, 41
- age of the universe, 86
  
- AKS-primaliteitstest, 144
- AKS-primality test, 85
- algebra, 7, 139
- alphabet, 40
- alternating group, 23, **25**, 64, 68, 70, 98
- angle, 31, 32
- angle group, **51**, 51
- annihilate, **114**, 116
- anti-homomorphism, **58**, 67
- area-preserving map, 44
- Artin's vermoeden, 145
- Artin, E., 145
- associativity, **17**, 18, 22, 74
- automorphism, **43**, 49, 58
  - inner, **48**, 67, 95, 97
  - outer, 54
- automorphism group, 43
- average, 34, 61
- axiom, 7, 71
- axioms, 17
  
- baby monster, 133
- basis, 112
- bijection, 5, 19, 20, 31–34, 46
- bijective, 13
- binary operation, 8, **17**, 74
- binomial coefficient, 54
- building block, 46, 73, 133
- Burnside, W., 60, 146
  
- canonical homomorphism, 48, 50
- canonical map, **46**, 50, 63
- cardinality, 45
- Carmichael numbers, 85
- carpenter's wisdom, 86
- Cartesian product, 99
- category, 42, 99
- Cauchy's theorem, **65**, 127
- Cauchy, A.-L., 65
  - theorem, 65
- Cauchy, A.-L., 60
- Cayley's theorem, 19, **62**, 69
- Cayley, A., 19, 62
  - theorem, 19, **62**
- center, **48**, 52, 64, 98, 106
- chain, 27
- characteristic subgroup, **54**, 97
- Chinese remainder theorem, **79**, 99, 126
- choice of a basis, 99
- choice of basis, 48
- choice of coordinates, 48

- circle, 18
- circle group, **47**, 51, 100
- class, 10
- class formula, **69**, 132
- classification problem, 124, 125
- closed, 9
- code, 87
- collinear, 32
- collinear, 32
- combinatorics, 61
- commutative algebra, **97**, 110
- commutative diagram, **96**, 119
- commutative ring, 74
- commutator, 27, **97**, 98
- commutator subgroup, **97**, 98
- commute, 12, **18**, 20, 27, 34, 48, 64
- complement, 124
- complex analysis, 85
- complex conjugation, 38
- complex number, 37, 38
- complex plane, 38
- complexity theory, 84
- composite number, **72**
- composite numbers, 76, 85
- compositeness proof, 86
- composition, 8, 9, 17, 34, 37, 42
- composition law, 17
- computer equipment, 84
- computer implementation, 77
- congruence, **32**, 71
- conjugacy class, **28**, 29, 64, 68–70, 129
- conjugate, **28**, 58, 64
- conjugate subgroup, 40, 58, 63
- conjugation, **28**, 29, 40, 48, 49, 58, 64, 65
  - complex, 38
- conjugation action, **64**, 101
- conjugation map, 43
- continuous map, 42
- contradiction
  - proof by, 5
- coordinate system, 31, 48
- coordinates, 31
- coprime, **72**
- coset, 46, 50
- cosets, **45**
- count, 64
- countably infinite, 28
- counting argument, 76
- cryptografie, 144
- cryptography, 86
- cryptosystem, 87
- crystallographic group, 14, **40**
- crystallography, 31
- cube, 56, 59, 61, 100
  - Dutch, 61
  - rotation group of the, **57**, 61, 64
  - Rubik's , **26**
  - the Rubik's, 30
- cubic group, 56, **57**, 100, 106
- cycle, **13**, 20, 21
  - length of a, 20
  - parity of a, 25
- cycle notation, **13**, 20, 21
- cycle type, **22**, 25, 28, 29, 64
- cyclic group, **23**, 37, 51, 52, 71, 90
- cyclic permutation, 20
- cyclic subgroup, 23, 35
- cyclotomic fields, 85
- cylinder, 63
- de la Vallée-Poussin, C., 85
- decomposition, 73
- determinant, 5, 30, 35, 37, 41, 42
- diagram, 95
  - commutative, 96
- diagram chasing, 110
- diamond pattern, 16
- Diffie–Hellman protocol, 92
- digital signature, 88
- digitized, 87
- dihedral group, **35**, 36, 62, 103, 105, 125, 126, 134
  - generalized, 103, 106
- dimension, 112
- direct product, **99**, 100, 103, 121, 124
- direct product , **52**
- direct sum, **99**, 121
- Dirichlet, G. P. L., 143
- discrete, 114
- discrete logarithm, 90
- disjoint cycle decomposition, **21**, 64, 69, 70
- disjoint cycle representation, **21**, 21
- disjoint cycles, 20
- disjoint union, 46
- distance, 31, **32**, 68, 76
- distributivity, 74
- divisibility, 72
- divisible group, 119
- division with remainder, **71**, 83
- divisor, 72
- doing arithmetic modulo  $n$ , 51
- Dutch cube, 61
- efficient, 62
- elementary abelian, **116**, 126
- elementary divisors, 116

- elliptic curve, 85, 92
- elliptic geometry, 31
- elliptische krommen, 143
- embedding, 56, 62
- empty product, 18, 20, 22
- enantiomer, 30
- enantiomeren, 141
- endomorphism, 42
- entier, 51
- equilateral triangle, 15
- equivalence class, 28, 46, 53, 60
- equivalence relation, 5, 29, 46, 51, 53, 60
- Erlanger Programm, 31, 32, 39, 141
- Euclid, 31, 72, 85
- Euclidean algorithm, 77
  - extended, 77
- Euclidean geometry, 31
- Euclidean space, 31
- Euclides
  - Elementen van, 143
  - klemtoon, 143
- Euler’s  $\varphi$ -function , 76
- Euler, L., 43, 79, 84, 87, 145
  - $\varphi$  function, 79, 91
  - $\varphi$ -function, 76, 79
  - formula, 45, 51
- even permutation, 24
- exact sequence, 108
- exactness, 108
- exercise
  - with a star, 5
- exercises, 5
- exotic symbols, 17, 43
- exp, 43
- exponent, 73, 74, 93, 116
- exponential algorithm, 86
- exponential map, 43, 45
- extension, 108, 110
- extensions, 109
  
- factor group, 50
- factorisatiealgoritmen, 140
- factorization, 73, 74
  - of a homomorphism, 96
- factorization algorithm, 86, 89
- faithful, 57
- Fermat congruence, 84
- Fermat number, 82
- Fermat, P.
  - last theorem, 80
  - little theorem, 80, 84
- Fermat, P. de
  - laatste stelling van, 142, 143
- Fermat, P. the, 80
- Fermat-getal, 144, 145
- fiber, 44, 45
- fibered product, 122
- fibered sum, 122
- Fibonacci numbers, 81
- field, 5, 8, 75, 76
  - finite, 76
- finite field, 76
- finite geometry, 76
- finite group, 18, 27
  - of Lie type, 76
- finite order, 18, 23, 28
- finite symmetry group, 36
- finitely generated, 23, 28, 108, 113
- fixed point, 29, 32, 33, 36, 38, 58, 64, 68
- fixed-point-free, 58, 60
- four-group
  - Klein, 10
- free abelian group, 112
- free group, 112, 113, 114
- free rank, 112, 115
- Frobenius, G. F., 60
- full tetrahedral group, 14
- function space, 7
- functorial, 105
- fundamental group, 5
  
- Galois theory, 8, 131
- Galois, E., 8
- Gauss’s formula, 82, 91
- Gauss, C. F., 145
  - formula, 82
- Gauss, C. F., 85
- Gauss, C. F., 68, 71
  - formula, 91
- Gaussian integers, 68
- GCD, 72
- general linear, 39
- generalized dihedral group, 103, 106
- generate, 13, 23, 23, 52, 112
- generator, 15, 23, 90
- genererende functie, 140
- geometry, 31
  - elliptic, 31
  - Euclidean, 31
  - Greek, 31
  - hyperbolic, 31
  - plane, 31, 38
- geschiedenis, 140
- glide reflection, 38

- Goursat’s lemma, **106**  
 Goursat, E. J-P., **145**  
 Goursat, E. J-P., **106**  
   lemma, **106**  
 greatest common divisor, **72**  
 Greek mathematics, **31, 71**  
 group, **5, 8, 17, 71**  
   abelian, **18, 43**  
   alternating, **23, 25**  
   cyclic, **23, 37, 51, 66, 71, 90**  
   divisible, **119**  
   finite, **18, 27**  
   finitely generated, **23**  
   simple, **132**  
   solvable, **131, 132**  
   symmetric, **19, 64**  
 group axioms, **17, 19**  
 group of units, **75, 76**  
 group order, **18, 23, 28**  
 group table, **27**  
 group theory, **5**
- Hadamard, J., **85**  
 Hamilton, W. R., **98**  
 homeomorphic, **68**  
 homologic algebra, **108, 122**  
 homologische algebra, **145**  
 homomorphism, **42**  
   bijective, **42**  
   canonical, **48**  
   image of, **44, 47**  
   injective, **44, 56**  
   trivial, **42**  
 homomorphism property, **43**  
 homomorphism theorem, **96**  
 human life, **86**  
 hyperbola, **9**  
 hyperbolic geometry, **31**
- ideal, **83**  
 identificatieruimtes, **142**  
 identity, **9, 17**  
 image, **44, 46, 47, 50**  
 index, **46, 53, 63**  
 induction, **5, 14, 20, 71**  
 infinite order, **18, 23, 28**  
 injection, **5**  
 injective, **45**  
 inner automorphism, **48, 49, 97**  
 inner product, **31, 39, 76**  
 integers, **71**  
 invariant, **31, 39, 41**  
 invariant point, **32, 33, 36**  
 inverse, **11, 17, 18, 43, 77, 78**  
 inverse exponent, **88**  
 inverse map, **19**  
 inversion, **25, 103**  
 invertible residue class, **76**  
 irreducibility, **73**  
 irreducible, **83**  
 isometrie, **32**  
 isometry, **33, 37, 101, 125**  
   sign of a, **42, 51**  
   sign of an, **37, 38, 44, 57**  
 isomorphic, **11, 42**  
 isomorphism, **11, 42**  
 isomorphism theorem, **44, 47, 48**  
 isotropy group, **58, 68**
- kernel, **44, 44–50**  
 Klein four-group, **9, 9, 15, 27, 40, 52, 57, 98, 99**  
 Klein, F., **31, 141**  
   four-group, **9, 9, 10, 15, 27, 40, 52, 57, 98, 99**  
 kubus  
   van Rubik, **140**  
 kwadratische reciprociteitswet, **145**
- Lagrange’s theorem, **46, 79**  
 Lagrange, J. L.  
   theorem, **79**  
 Lagrange, J. L., **45**  
   theorem of, **46**
- lattice, **114**  
 LCM, **72**  
 least common multiple, **29, 72**  
 ledger, **71**  
 left action, **58, 67**  
 left coset, **45, 45, 46, 49, 53, 58, 63**  
 left multiplication, **19, 25, 45, 62, 63**  
 Legendre, A.-M., **80**  
 lemma van Goursat, **145**  
 length, **58**  
 length of a cycle, **20**  
 Linear algebra, **31**  
 linear algebra, **5, 31, 39, 42, 48, 50, 108, 112, 114**  
 linear component, **37, 37, 42**  
 linear map, **5, 8, 32–34, 42**  
 linearly independent, **112**  
 locaal-globaal-principes, **143**  
 local isometry, **68**  
 local-global principle, **80**  
 log, **43**  
 logarithm, **43**  
 logic, **71**  
 magical octagon, **67**

- Magma, [84](#)
- Maple, [84](#)
- Mathematica, [84](#)
- Mathematical Intelligencer, [139](#)
- matrix, [5](#), [8](#), [48](#)
- matrix group, [7](#)
- matrix representation, [9](#)
- maximal abelian quotient, [97](#)
- Mersenne primes, [81](#)
- Mersenne, M., [143](#)
- modulaire functies, [142](#)
- modulaire vorm, [140](#)
- modulaire vormen, [142](#)
- modular group, [68](#)
- module, [108](#)
- modulo, [10](#), [50](#), [51](#), [76](#), [77](#)
- modulus, [87](#)
- monster, [133](#)
- morphism, [42](#)
- multiple, [72](#)
- multiplication in rings, [74](#)
- multiplication table, [10](#)
- multiplicative group, [43](#)
- multiplicative notation, [17](#), [43](#), [74](#)
- multiplicativity, [25](#), [35](#), [37](#)
  
- natural map, [46](#), [46](#)
- natural number, [71](#)
- Nederlandse Spoorwegen, [51](#)
- New Year's puzzle, [16](#), [69](#)
- nilpotent, [128](#)
- normal, [49](#)
- normal subgroup, [49](#), [49](#), [50](#), [53](#), [63](#), [108](#), [109](#), [124](#), [129](#)
- normalizer, [64](#), [64](#), [69](#), [134](#)
- Noyes Chapman, [140](#)
- number field sieve, [89](#)
- number theory, [9](#), [80](#)
  
- octahedron, [67](#)
- odd permutation, [24](#)
- one-way function, [92](#)
- operation, [57](#)
- opposite, [43](#)
- orange necklace, [67](#)
- orbit, [21](#), [29](#), [30](#), [58](#), [60](#)
- orbit decomposition formula, [60](#)
- orbit length, [59](#)
- orbit space, [60](#), [63](#)
- order, [8](#), [9](#), [11–13](#), [18](#), [18](#), [23](#), [46](#), [52](#), [65](#), [74](#)
- oriëntatie, [141](#)
- orientation, [35](#), [37](#), [38](#)
- origin, [31](#), [32](#)
  
- orthogonal group, [34](#), [35](#), [44](#), [60](#), [101](#)
- orthogonal map, [32](#), [33](#)
- outer, [54](#)
  
- parity, [24–26](#)
- parity argument, [15](#)
- partitiefunctie, [140](#)
- partition, [22](#)
- partition function, [29](#), [120](#)
- Peano, G., [71](#)
- periodic, [18](#)
- permutation, [7](#), [13](#), [13](#), [20](#), [21](#), [24](#), [62](#)
  - cyclic, [20](#)
  - even, [24](#), [25](#)
  - odd, [24](#), [25](#)
  - order of a, [29](#)
  - parity of a, [24](#)
  - sign of a, [23](#), [24–26](#), [30](#), [42](#), [44](#), [45](#), [125](#)
- permutation character, [60](#)
- permutation group, [17](#), [19](#), [31](#), [56](#), [62](#)
- permutation matrix, [30](#)
- $p$ -group, [66](#)
- $p$ -group, [115](#), [116](#), [132](#)
- plane, [31](#)
- plane figure, [35](#)
- plane geometry, [31](#), [32](#), [38](#), [51](#)
- plane isometry, [32](#), [101](#), [125](#)
- plane symmetries, [32](#), [33](#)
- point group, [40](#)
- polynomial, [75](#), [76](#), [83](#), [91](#)
- polynomial algorithm, [84](#)
- polynomial ring, [75](#), [83](#)
- polynomial-time algorithm, [84](#)
- postmarking machine, [12](#)
- power set, [27](#), [53](#)
- $p$ -rank, [116](#)
- primality proof, [85](#)
- primality test, [85](#)
- prime, [72](#), [90](#)
- prime divisor, [65](#)
- prime factor decomposition, [74](#)
- prime number, [72](#)
- prime order, [46](#), [65](#)
- prime property, [73](#), [83](#), [91](#)
- prime theorem, [85](#)
- primitive root, [91](#)
- probabilistic method, [85](#)
- product, [11](#), [13](#), [17](#), [43](#)
  - empty, [18](#), [20](#), [22](#)
- product group, [78](#)
- product of rings, [78](#)
- projection, [47](#), [99](#)

- pseudoprimality test, 93
- pseudoprime test, 85
- $p$ -subgroup, 127
- public exponent, 87
- public key cryptosystem, 87
  
- quadratic sieve, 89
- quadrilateral, 15
- quantum computer, 89
- quarter turn, 11
- quaternion group, 98, 126
- quotiëntruimte, 142
- quotient, 50, 60, 81
- quotient group, 50, 51, 94, 98
- quotient map, 50, 94
- quotient space, 50
- quotienting step-by-step, 54
  
- rank, 112
- reflection, 8, 11, 15, 32–35, 38
- regular  $n$ -gon, 15
- regular action, 62, 63
- rekenkundige rij, 143
- relatively prime, 72, 111
- remainder, 71
- repeatedly squaring, 84
- representative, 50, 65
- residue class, 10, 50, 71, 76
- residue class ring, 75, 76
- retraction, 110
- revision project, 133
- rhombus, 8, 9, 11, 35
- Riemann zeta function, 85
- Riemann-hypothese, 145
- right action, 58, 67, 68
- right axioms, 27
- right coset, 49, 53, 63
- right multiplication, 19
- ring, 5, 8, 74, 74, 90, 108
- ring homomorphism, 75
- ring isomorphism, 75
- rotation, 15, 32–38
- rotation group of the cube, 57, 61, 64
- RSA cryptosystem, 87
- RSA key, 89
- RSA protocol, 88, 89
- RSA-protocol
  - textbook RSA, 144
- Rubik’s cube, 26, 30
- Rubik’s kubus, 140
  
- SAGE, 84
- Sam Loyd, 140
  
- scalar multiplication, 31, 112
- secret exponent, 88
- Secret Santa, 30
- section, 110, 124
- semi-direct multiplication, 102
- semi-direct product, 101, 102, 103, 124, 125
- set theory, 19
- shift, 65
- Shimura-Taniyama-vermoeden, 143
- shoe-sock rule, 18, 23
- short exact sequence, 108, 108
  - split, 109
- sign
  - of a isometry, 42, 51
  - of a permutation, 23, 24–26, 30, 42, 44, 45, 125
  - of an isometry, 37, 38, 44, 57
- sign group, 44, 52, 100
- sign map
  - seesign, 24
- similarity, 39, 41
- simple, 132
- simple group, 133
  - sporadic, 133
- simplification by generalization, 14
- Sinterklaas, 30
- smallest prime divisor, 63
- solid geometry, 31, 37
- solid symmetry, 56
- solvability chain, 131, 132
- solvable, 131, 132
- sorting machine, 13
- space diagonal, 56, 59
- spatial symmetries, 14
- split, 110
- splitting, 108, 109, 124
- square, 11, 35
- square-free, 116
- stabilizer, 54, 58
- stable, 68
- standard basis, 31, 37
- stelling van Pythagoras, 143
- stereometry, 31, 37
- strong induction, 70
- structure, 7, 9, 42, 56, 74
- subgroup, 22, 23, 32, 34
  - characteristic, 54, 97
  - conjugate, 28, 40, 58, 63, 64
  - cyclic, 23
  - normal, 49, 49
  - trivial, 22
- substituties, 140

- sum, 43
- sum of functions, 53
- surface of an inner tube, 68
- surjection, 5
- swimming, 5
- Sylow  $p$ -subgroup, 66, 70, 101, 115, 116, 120, 127, 128
- Sylow, L., 127
  - theorem, 128
- symmetric difference, 15, 27, 53
- symmetric group, 19, 64
- symmetries, 11, 43
- symmetry, 8, 9, 15, 61
- symmetry group, 32, 35, 36, 40, 56, 59
  - finite, 36
- system of representatives, 65, 69
  
- taxonomists, 7
- tetrahedral group, 56, 57
- tetrahedron, 14, 30
- textbook RSA, 144
- thermometer, 71
- three-quarter turn, 11
- Topology, 68
- topology, 42
- torsion element, 18, 28, 114
- torsion group, 115
- torsion subgroup, 54, 114
- torsion-free, 113, 114
- torus, 63, 68
- transformation group, 31
- transitive, 58, 60
- translation, 32, 33, 38, 101
- translation subgroup, 40
- transport of structure, 46, 53
- transposition, 24–26
- transpositions, 13
- trial division, 74, 85, 86
- trivial divisor, 72
- trivial element, 9
- trivial group, 18, 20, 36, 48, 116
- trivial homomorphism, 42
- trivial subgroup, 22
- trivial symmetry, 9
  
- unique factorization, 73
- unit, 75
- unit element, 10, 17
- universale eigenschap, 145
- upper half-plane, 68
- upper triangular matrix, 134
  
- vector addition, 31
- vector space, 31, 99, 108
- visualize, 14
  
- well defined, 50, 75, 94, 96
- well-defined, 79
- Wiles, A. J., 80, 142, 143
- word in the plane, 40
- wreath product, 107, 136
  
- yoghurt, 141
  
- zero, 71, 76, 91
- zero element, 43