2. Abstract Algebra

In the book *Discrete Mathematics and Discret Models* we investigated a number of different mathematical operations, and thereby found that several of them had unexpected similarities. Compare for instance the calculation rules of set theory and of propositional logic, or divisor graphs and subset graphs, and you find remarkable similarities. These similarities can be used, by taking the common properties to make general analyses that can be applied in all the different situations. In this chapter we are going to look closer on a number of common structures.

This chapter may by the way be somewhat heavy reading, since its character is that of a dictionary covering concepts in abstract algebra, with a lot of definitions and few applications. The applications will appear in later chapters. We suggest that you skim this chapter once so that you know what it is about, and then return to it when a concept reappears later in the book.

Highlights from this chapter

- A *group* is an abstract structure consisting of *a set* G (of elements corresponding to numbers) and *an operation* $*$ that satisfies the group axioms:

  1. closedness: if x and y are group elements in G then $x * y$ is an element in G as well; you never leave the group.
  2. associativity: it always holds that $(x * y) * z = x * (y * z)$; because of this you don't need to put in parentheses, but can write $x*y*z$.
  3. identity: there is an element I in the group G which has the property that $I*x = x$ and $x*I = x$ for all group elements x in G; an identity element thus leaves the other elements unchanged.
  4. inverse: each group element x in G has an inverse, that is to say, an element x^{-1} with the property that $x*x^{-1} = I$ and $x^{-1}*x = I$.

- A *subgroup* is a group that is a subset of another group (with the same operation).
- *Lagrange's theorem* for finite groups states that the size of a subgroup is always a divisor of the size of the group.
- Using *power notation* one writes $g * g = g^2$, etcetera. A group is *cyclic* if there is an element g which generates the whole group, that is to say, $G = \{\ldots, g^{-2}, g^{-1}, g^0, g^1, g^2, \ldots\}$.
- An *Abelian group* is a group where the commutative law holds, that is to say, where $x * y = y * x$ for all group elements x and y.
- The groups G and H are *isomorphic* if there exists a bijection $\phi : G \longrightarrow H$ between the groups such that calculations in one of the groups correspond to calculations in the other one.

- A *lattice* is a partial order where each pair of elements, say x and y, has a unique least upper bound $x \vee y$ and a unique greatest lower bound $x \wedge y$.

2.1 Groups

In this section we will study similarities between different operations defined on different sets. Let's start by looking at *addition of integers*, which among other things has the following properties:

1. The calculations are **closed**, that is, the sum of two integers is an integer. (This is not as obvious as it sounds – for instance the quotient of two integers is not necessarily an integer.)
2. The operation is **associative**, that is, $a + (b + c) = (a + b) + c$.
3. The number zero has the very special property that it doesn't happen anything if you use it: $a + 0 = 0 + a = a$ holds for all integers a.
4. For each integer a you can find another integer (namely $-a$) such that the sum of the two numbers is zero.

Now compare these properties to what we find when studying *multiplication of positive real numbers*:

1. The calculations are closed, since the product of two positive real numbers is a positive real number as well.
2. The operation is associative, since $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. The number one has the very special property that it doesn't happen anything if you use it: $a \cdot 1 = 1 \cdot a = a$.
4. For each positive real number a you can find a positive real number (namely $^1/_a$) such that the product of the two numbers is one.

We can see obvious similarities between the two operations. To show that it doesn't even have to be *numbers* that we use in the calculations we finish by studying the operation **composition of functions** (denoted $\circ$) defined on the set of bijections on a given set A, for instance $A = \{a, b, c\}$. Remember that a bijection on A is a function $f : A \longrightarrow A$ such that each element in A is used as a function value exactly once. For instance,

$$f : \begin{array}{ccc} a & \mapsto & a \\ b & \mapsto & c \\ c & \mapsto & b \end{array} \qquad \text{and} \qquad g : \begin{array}{ccc} a & \mapsto & b \\ b & \mapsto & c \\ c & \mapsto & a \end{array}$$

are two different bijections on $A = \{a, b, c\}$. The composition $f \circ g$ is defined as the function that performs first g and then f, so that it for instance holds that $f \circ g(a) = f\big(g(a)\big) = f(b) = c$. For the operation $\circ$ we can check the properties above once more:

1. The operation is closed, since the composition of two bijections on A is a bijection on A.
2. The operation is associative, since $(f \circ g) \circ h$ has to be the same as $f \circ (g \circ h)$ since both map an arbitrary element x in A on $f\big(g(h(x))\big)$.

3. The identity function Id is defined by $\mathrm{Id}(x) = x$ for all x in A. Id is clearly a bijection on A with the very special property that $f \circ \mathrm{Id} = \mathrm{Id} \circ f = f$ (since $f\big(\mathrm{Id}(x)\big) = f(x)$ and $\mathrm{Id}\big(f(x)\big) = f(x)$ for all x).
4. For each bijection f you can find a bijection (namely the inverse f^{-1}) such that the composition of the two bijections is the identity function.

Apparently all these three mathematical structures had very large similarities. To isolate the similarities, the general concept *group* has been introduced, meaning all calculation structures having the above properties.

Definition 2.1: ***Group*** A **group** is a set G with an operation $*$ that satisfies the four **group axioms**:

1. **Closedness**: if you take two elements in G you get an element in G, that is to say,
$$\forall x \forall y \big[x \in G \wedge y \in G \;\rightarrow\; (x * y) \in G\big].$$
2. **Associativity**: It doesn't matter how we group a calculation including three objects, that is to say,
$$\forall x \forall y \forall z \big[x \in G \wedge y \in G \wedge z \in G \;\rightarrow\; (x * y) * z = x * (y * z)\big].$$
3. **Identity**: There is an element I in G that doesn't affect the others, that is to say,
$$\exists I \big[I \in G \;\wedge\; \forall y (y \in G \;\rightarrow\; I * y = y * I = y)\big].$$
Instead of identity one sometimes says **unit** or **neutral element.**
4. **Inverses**: For each element in G we can find some element in G that carry us to the identity I, that is to say,
$$\forall x [x \in G \;\rightarrow\; \exists y (y \in G \wedge x * y = I)].$$

The group is usually denoted $\langle G, * \rangle$. (If the operation is clear from the context, simply "the group G" is used.) If we let S_A denote the set of all bijections on the set A, we have thus already seen three examples of groups: $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{R}_+, \cdot \rangle$, and $\langle S_A, \circ \rangle$.

S_A is usually called the **symmetric group** on the set A. It's a very important group to which we'll return several times both in this chapter and in chapter 5. ■

Exercise 2.1 Determine whether the following structures are groups. Check all the axioms, even if you find that one of the first ones doesn't hold!

(a) $\langle \mathbb{Z}, - \rangle$, that is to say, the integers under subtraction.

(b) $\langle \mathbb{Q}, \cdot \rangle$, that is to say, the rational numbers under multiplication.

(c) $\langle \mathcal{P}(\mathbb{N}), \cup \rangle$, that is to say, the power set of $\mathbb{N}$ under union.

(d) $\langle \mathbb{Z}_2, + \rangle$, that is to say, addition modulo 2.

(e) The solution set of a homogeonous linear system of equations $\mathsf{A}\mathbf{x} = \mathbf{0}$ under vector addition.

Exercise 2.2 What does the smallest group imaginable look like?

Exercise 2.3: ***Important!***

(a) Show that there is only one identity element in a group. (Hint: assume that you have two of them, and show that they are identical.)

(b) Show that every group element has only one inverse.

2.1.1 Abelian Groups

Out of the three examples of groups that we studied initially, two have another interesting property in common: the **commutative** rules $a + b = b + a$ and $a \cdot b = b \cdot a$ hold! Composition of functions, on the other hand, is not a commutative operation.

If the operation is commutative the group is called an **Abelian group**, after the most distinguished Nordic mathematician, the Norwegian Niels Henrik Abel.

The smallest non-Abelian group has the size 6, and is precisely the group $\langle S_A, \circ\rangle$ that we studied above. There we defined two group elements f and g, and you can easily check for yourself that

$$f \circ g : \quad \begin{array}{ccc} a & \mapsto & c \\ b & \mapsto & b \\ c & \mapsto & a \end{array} \qquad \text{but} \qquad g \circ f : \quad \begin{array}{ccc} a & \mapsto & b \\ b & \mapsto & a \\ c & \mapsto & c \end{array}$$

so $f \circ g \neq g \circ f$.

2.1.2 Subgroups

A group $\langle G, *\rangle$ consists as stated of a set G and an operation $*$. Among all the subsets of G some of them will be groups in their own right under the same operation. Such a group $\langle H, *\rangle$, where H is a subset of G, is called a **subgroup** of $\langle G, *\rangle$.

Example 2.1 The positive real numbers $\mathbb{R}_+$ under multiplication are a group. The positive rational numbers $\mathbb{Q}_+$, which form a subset of $\mathbb{R}_+$, are a group under multiplication as well. Check:

1. The set is closed, since ${}^{a}\!/_{b} \cdot {}^{c}\!/_{d} = {}^{ac}\!/_{bd}$, which is a rational number.

2. The operation is associative, since we are discussing normal multiplication.

3. There is a neutral element, the rational number 1, with the property that ${}^{a}\!/_{b} \cdot 1 = 1 \cdot {}^{a}\!/_{b} = {}^{a}\!/_{b}$.

4. To each number ${}^{a}\!/_{b}$ we can find a number ${}^{b}\!/_{a}$ with the property that ${}^{a}\!/_{b} \cdot {}^{b}\!/_{a} = {}^{b}\!/_{a} \cdot {}^{a}\!/_{b} = 1$, so there are inverses.

Thus $\langle \mathbb{Q}_+, \cdot\rangle$ is a subgroup of $\langle \mathbb{R}_+, \cdot\rangle$. ■

Exercise 2.4: ***Important!*** Actually, it ought to be possible to take advantage of the fact that you already know that $\langle G, *\rangle$ is a group when you check whether $\langle H, *\rangle$ is a group. How many of the four test we did when we were checking that $\langle \mathbb{Q}_+, \cdot\rangle$ is a group were in fact necessary?

Exercise 2.5

(a) Are the positive integers a subgroup of $\langle \mathbb{R}_+, \cdot\rangle$?

(b) Are the odd numbers a subgroup of $\langle \mathbb{Z}, +\rangle$?

(c) Are the even numbers a subgroup of $\langle \mathbb{Z}, +\rangle$?

2.1.3 Finite Groups

In this book we'll mainly have reason to study **finite groups**, that is, groups where the set is of finite size.

Some typical finite groups are:

- $\langle \mathbb{Z}_n, + \rangle$ for an arbitrary integer n. This group has n elements.
- $\langle \mathbb{Z}_p \setminus \{0\}, \cdot \rangle$ for an arbitrary prime p. This group has $p - 1$ elements.
- The symmetric group $\langle S_A, \circ \rangle$ for an arbitrary set A. If $|A| = n$, this group has $n!$ elements.

For finite groups you can describe the whole group by writing down its **group table**, that is to say, the counterpart of a multiplication table for the operation in question.

Example 2.2 The group tables of $\langle \mathbb{Z}_4, + \rangle$ and $\langle \mathbb{Z}_5 \setminus \{0\}, \cdot \rangle$ are respectively

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

and

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

■

Note that a group table will always be a **Latin square**, that is to say, in each row and column each group element appears exactly once.

Exercise 2.6 Verify that

(a) $\langle \mathbb{Z}_n, + \rangle$ is a group for an arbitrary integer n,

(b) $\langle \mathbb{Z}_p \setminus \{0\}, \cdot \rangle$ is a group for an arbitrary prime p,

(c) $\langle \mathbb{Z}_n \setminus \{0\}, \cdot \rangle$ *isn't* a group if n isn't prime,

(d) $\langle S_A, \circ \rangle$ has $n!$ elements if $|A| = n$ *

Exercise 2.7: *Important!* Show that every group table is a Latin square.

Exercise 2.8 On the set $A = \{a, b\}$ the symmetric group S_A has two elements: the identity function Id and the bijection f that maps a on b and vice versa. Write down the group table for $\langle S_A, \circ \rangle$.

2.1.4 Cyclic Groups

If we in a group $\langle G, * \rangle$ take an element $g \in G$ and pair it with itself we get $g * g$. Let's use normal power notation and denote this element g^2. In the same way we let g^{-2} denote $g^{-1} * g^{-1}$. Finally, we let g^0 mean the identity I. Now we can calculate using the normal power rules:

$$g^m * g^n = g^{m+n} \quad \text{for all integers } m, n.$$

For each element $g \in G$ we can now define the set of all its powers as $\langle g \rangle$:

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

It can be shown that $\langle g \rangle$ is a group as well, which because of this is called the **group generated by** g. The element g is called the **generator** of the group.

Theorem 2.1 For each element g in a group $\langle G, * \rangle$, $\langle g \rangle$ is a subgroup of G.

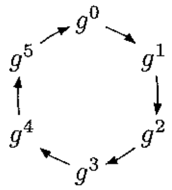
Proof. Arbitrary elements in $\langle g\rangle$ have the form g^n for integers n. Thus $\langle g\rangle$ is closed, since $g^n * g^m = g^{n+m}$ which belongs to $\langle g\rangle$. Furthermore, $\langle g\rangle$ has an identity, namely g^0. Finally each element in $\langle g\rangle$ has an inverse, since the inverse of g^n is g^{-n}, which belongs to $\langle g\rangle$. ■

A group generated by an element g is called a **cyclic group**. We'll soon see why.

Example 2.3 The group $\langle\mathbb{Z},+\rangle$ is cyclic, since it is generated by the element 1 (because every integer can be written as a sum of a large enough number of ones or minus ones). This group has as a matter of fact two generators, since -1 generates the whole of $\mathbb{Z}$ as well.

For each integer n, the group $\langle\mathbb{Z}_n,+\rangle$ is also a cyclic group. A group like that may have even more generators. For instance you can check that $\mathbb{Z}_8 = \langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle$. ■

If G is a finite group, of course the subgroup $\langle g\rangle$ will be finite as well (since it can at most be of the same size as G). The number of elements in the cyclic subgroup $\langle g\rangle$ is called the **order** of g.



From the form of the diagram you can see why the group is said to be "cyclic". If you start to list the powers g^0, g^1, g^2, ... you will, when $\langle g\rangle$ is finite, sooner or later get back to $g^0 = I$. This must as a matter of fact occur before any other element reappears (see exercise 2.10), so the order of the element g can also be expressed as the least positive power of g that is equal to the identity:

$$\text{order}(g) = \min\{m \in \mathbb{Z}_+ \mid g^m = I\}.$$

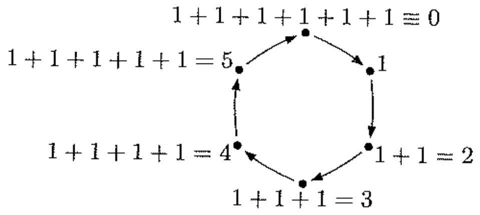
Example 2.4 We look at the orders of the different elements when adding in $\mathbb{Z}_6$. Zero is already zero, so we don't have to study it further, and the analysis can start at one:

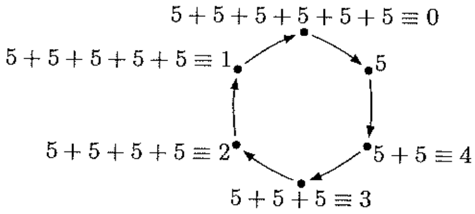
$$\begin{array}{lllll}
1+1=2 & 2+2=4 & 3+3=6 & 4+4=8\equiv 2 & 5+5\equiv 4 \\
2+1=3 & 4+2=6 & \quad\;\;\equiv 0 & 2+4=6 & 4+5\equiv 3 \\
3+1=4 & \quad\;\;\equiv 0 & & \quad\;\;\equiv 0 & 3+5\equiv 2 \\
4+1=5 & & & & 2+5\equiv 1 \\
5+1=6 & & & & 1+5\equiv 0 \\
\quad\;\;\equiv 0 & & & &
\end{array}$$

We thus find that the orders of the elements in the group $\langle\mathbb{Z}_6,+\rangle$ are

$$\begin{aligned}
\text{order}(0) &= 1\\
\text{order}(1) &= 6\\
\text{order}(2) &= 3\\
\text{order}(3) &= 2\\
\text{order}(4) &= 3\\
\text{order}(5) &= 6
\end{aligned}$$

1 and 5 are obviously the only generators of the group $\langle\mathbb{Z}_6,+\rangle$.





■

Exercise 2.9 Are you able to see what kind of numbers it was that appeared as orders of elements in $\mathbb{Z}_6$? Do you see any system concerning which order it is that belongs to which element?

Exercise 2.10 Show that if you list the powers and one element reappears (that is, $g^n = g^m$ for some integers $m < n$) then $g^{n-m} = g^0$, that is to say, the identity has already reappeared.

Exercise 2.11: ***Important!*** If a subset of a group is *finite*, how many tests are then needed to check whether it is a subgroup?

Exercise 2.12 The invertible elements in $\mathbb{Z}_8$ make up a group under multiplication. Check whether the group is cyclic.

Exercise 2.13 Carry out the same investigation for the invertible elements in $\mathbb{Z}_{10}$.

2.1.5 Cosets and Lagrange's Theorem

In the previous section we found that the group $\langle \mathbb{Z}_6, + \rangle$ had cyclic subgroups of the sizes 1, 2, 3, and 6. Note that every subgroup-size is a divisor of the size of the full group! This remarkable relationship will always hold and is called **Lagrange's theorem**.

Why do we say that Lagrange's theorem is remarkable? Well, we started by introducing groups as a comprehensive concept for all structures that satisfy four axioms. We have seen that there exists a large number of such different structures, and à priori they wouldn't need to have any other interesting properties in common except for exactly these four axioms. But by using the group axioms, you can prove nontrivial things that hold for all groups, such as for instance Lagrange's theorem.

The proof of Lagrange's theorem demands that we introduce the concept **coset** of a subgroup. This concept is easiest understood based on the example $\mathbb{Z}_6$.

Example 2.5: ***Cosets in*** $\mathbb{Z}_6$ The subgroups of $\langle \mathbb{Z}_6, + \rangle$ are $H_1 = \{0\}$, $H_2 = \{0, 3\}$, and $H_3 = \{0, 2, 4\}$ (and $\mathbb{Z}_6$ in itself). A coset of a subgroup is obtained by taking a number and adding it to all the elements in the subgroup. The subgroup H_1 has one element and six cosets:

$$H_1 + 0 = \{0\}, \qquad H_1 + 1 = \{1\},$$
$$H_1 + 2 = \{2\}, \qquad H_1 + 3 = \{3\},$$
$$H_1 + 4 = \{4\}, \qquad H_1 + 5 = \{5\}.$$

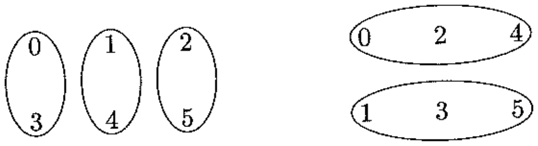
The subgroup H_2 has two elements and three cosets:

$$H_2 + 0 = H_2 + 3 = \{0, 3\}, \qquad H_2 + 1 = H_2 + 4 = \{1, 4\},$$
$$H_2 + 2 = H_2 + 5 = \{2, 5\}.$$

The subgroup H_3 has three elements and two cosets:

$$H_3 + 0 = H_3 + 2 = H_3 + 4 = \{0, 2, 4\},$$
$$H_3 + 1 = H_3 + 3 = H_3 + 5 = \{1, 3, 5\}.$$

Every time the number of elements in the subgroup times the number of cosets equal six, the size of the main group. The explanation is that each element in the group appears in exactly one coset!



■

Now we'll carry out the general argument. If H is a subgroup of $\langle G, *\rangle$, then for each $g \in G$ we define its (right) coset as

$$H * g = \{h * g \mid h \in H\}.$$

We will now prove that each element in the group appears in exactly one coset, that is to say, that if it appears in two cosets, then those cosets are identical (like $H_2 + 0$ and $H_2 + 3$ in the example above).

Theorem 2.2 If H is a subgroup of the group $\langle G, *\rangle$ and two of its cosets have an element in common, then these two cosets are identical.

Proof. If we let x be an element that is included in both coset $H * g_1$ and $H * g_2$, we thus have to prove that $H * g_1 = H * g_2$. That x is included in both the cosets means that

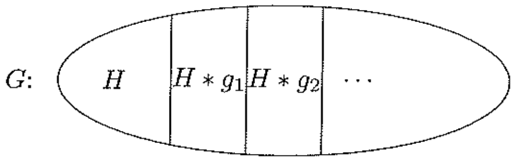
$$x = h_1 * g_1 = h_2 * g_2$$

for some elements h_1 and h_2 in the subgroup H. When multiplying both sides by h_1^{-1} we get the equality

$$g_1 = h_1^{-1} * h_2 * g_2.$$

Each element in $H * g_1$ can be written on the form $h * g_1$ for som $h \in H$, and by rewriting g_1 as $h_1^{-1} * h_2 * g_2$, $h * g_1$ can be written as $h * h_1^{-1} * h_2 * g_2$. Since H is a group and thus closed, $h * h_1^{-1} * h_2$ is an element h' of H as well. Thus we have written an arbitrary element in the coset $H * g_1$ on the form $h' * g_2$ and thereby it's an element of the coset $H * g_2$ as well. In the same way we get that all elements in $H * g_2$ belong to $H * g_1$ as well, and thus these two cosets are identical. ■

According to the theorem above we have a situation as in the following figure:



The group G is partitioned in disjoint cosets. Each coset is of course of the same size as the subgroup H. If g is finite then the number of elements in G thus equals the number of cosets times the number of elements in H. This proves Lagrange's theorem:

Theorem 2.3: ***Lagrange's Theorem*** If H is a subgroup of the finite group G then $|H|$ divides $|G|$. ∎

Exercise 2.14: ***Important!*** Prove that the order of an element in a finite group G will always be a divisor of $|G|$.

Exercise 2.15: ***Important!*** Galois introduced the concept **normal subgroup** for subgroups where the left cosets are identical to the right cosets. (The definition of **left coset** is like the definition of right coset, but with the multiplication in the opposite order.)

(a) Show that in Abelian groups all subgroups are normal.

(b) Let S_A be the symmetric group on the set $\{a, b, c\}$. Let

$$f: \begin{array}{ccc} a & \mapsto & a \\ b & \mapsto & c \\ c & \mapsto & b \end{array} \qquad \text{and} \qquad g: \begin{array}{ccc} a & \mapsto & b \\ b & \mapsto & c \\ c & \mapsto & a \end{array}$$

Show that $\langle g \rangle$ is a normal subgroup of S_A but that $\langle f \rangle$ isn't a normal subgroup of S_A.

(c) If H is a normal subgroup of G then G/H denotes the **quotient group** where the elements are all the cosets of H. Cosets are multiplied elment by element, that is,

$$(H * g_1) * (H * g_2) = \{h_1 * g_1 * h_2 * g_2 \mid h_1, h_2 \in H\}.$$

Show that the quotient group really is a group.

2.1.6 Group Isomorphisms

Let's study two different groups: addition in $\mathbb{Z}_6$ and multiplication of the invertible elements in $\mathbb{Z}_7$. We draw the group tables:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Both tables contain $6 \cdot 6 = 36$ elements, and no row or column contains the same element twice, but for the rest they look fairly different. The most obvious thing in the addition table is the diagonal structure: in each diagonal directed upwards to the right only one element is represented. Nothing like this holds in the multiplication table the way it is written here, but if we rearrange the rows and columns in the order 1, 3, 2, 6, 4, 5, the table will look like this:

$\cdot$	1	3	2	6	4	5
1	1	3	2	6	4	5
3	3	2	6	4	5	1
2	2	6	4	5	1	3
6	6	4	5	1	3	2
4	4	5	1	3	2	6
5	5	1	3	2	6	4

The multiplication table of $\mathbb{Z}_7 \setminus \{0\}$ now has in principle the same appearance as the addition table of $\mathbb{Z}_6$! You may say that these groups are fundamentally identical; the only difference is the notation used.

This phenomenon, that two apparently different things are identical in principle, is called **isomorphism** (a word that ought to be known from graph theory). The formal definition reads like this in group theory:

Definition 2.2: ***Isomorphic groups*** Two groups $\langle G_1, * \rangle$ and $\langle G_2, \circ \rangle$ are **isomorphic** if there exists a bijection $\phi : G_1 \longrightarrow G_2$ that preserves the relationships between the elements, that is, such that

$$\phi(x * y) = \phi(x) \circ \phi(y) \qquad \text{for all } x \text{ and } y$$

The bijection in question is called an **isomorphism.** ■

In the example above, $\phi(0) = 1$, $\phi(1) = 3$, $\phi(2) = 2$, $\phi(3) = 6$, $\phi(4) = 4$, $\phi(5) = 5$ is an isomorphism between $\langle \mathbb{Z}_6, + \rangle$ and $\langle \mathbb{Z}_7 \setminus \{0\}, \cdot \rangle$.

Exercise 2.16 Calculations in $\langle \mathbb{Z}_2 \times \mathbb{Z}_2, + \rangle$ is a group. (You calculate with ordered pairs from $\mathbb{Z}_2$, and add component by component.) Calculations with the invertible elements in $\mathbb{Z}_8$ under multiplication is a group as well. Write down the group tables, and find an isomorphism between the groups.

Exercise 2.17 We have two groups: $\langle G, + \rangle$ and $\langle H, \cdot \rangle$, and an isomorphism ϕ between them.

(a) Denote the identities in G and H by 0 and 1, respectively. Show that $\phi(0) = 1$.

(b) Detnote the inverse of an element $g \in G$ by $-g$ and denote the inverse of an element $h \in H$ by h^{-1}. Show that $\phi(-g) = \big(\phi(g)\big)^{-1}$.

Exercise 2.18: ***Important!*** According to **Cayley's theorem** every finite group G is isomorphic to a subgroup of the symmetric group S_G. Prove this!

Example 2.6: ***The Group Isomorphism of the Slide Rule*** One example of isomorphic groups are the real numbers under addition, and the positive real numbers under multiplication. Thus there exists a bijection $\phi : \mathbb{R}_+ \longrightarrow \mathbb{R}$ such that

$$\phi(x \cdot y) = \phi(x) + \phi(y).$$

This isomorphism was of very large practical importance until the arrival of the electronic calculator. As anyone who has calculated by hand surely has noted, it's significantly easier to add than to multiply. If you want to know what $a \cdot b$ equals, you can using the isomophism find $\phi(a)$ and $\phi(b)$, add them, and using the inverse find $\phi^{-1}\big(\phi(a) + \phi(b)\big) = a \cdot b$. The addition is so much easier that this roundabout way pays!

2.3 More Exercises

Groups

Exercise 2.33 (If you have studied vectors:) For vectors in three-dimen space there are several operations. Combined with which of these opera do we have a group, and in this case, is it Abelian?

(a) scalar product (also called dot product).

(b) vector product (also called cross product).

(c) vector addition.

Exercise 2.34 Show that in every group $\langle g, * \rangle$ it holds that

$$a * b = a * c \quad \Rightarrow \quad b = c.$$

Write down *all* the details in the argument!

Exercise 2.35 Prove that the relationship

$$(\pi * \sigma)^{-1} = \sigma^{-1} * \pi^{-1}$$

holds for arbitrary group elements π and σ.

Exercise 2.36 $2\mathbb{Z}$ denotes the even numbers (numbers that can be writte as 2 times a number from $\mathbb{Z}$). $\langle 2\mathbb{Z}, + \rangle$ is a subgroup of $\langle \mathbb{Z}, + \rangle$.

(a) What does the quotient group $\mathbb{Z}/2\mathbb{Z}$ consist of, and what does the tabl look like?

(b) Find some well-known group that is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

(c) Does the quotient group G/H have to be isomorphic to some subgroup of G?

Exercise 2.37 Show that group isomorphism is an equivalence relation.

Exercise 2.38 We let U_n denote the set of invertible elements in $\mathbb{Z}_n$.

(a) Is $\langle U_8, \cdot \rangle$ cyclic, and in that case, which elements generate the group?

(b) Same question about $\langle U_9, \cdot \rangle$.

Exercise 2.39 Let S_6 denote the group of bijections on $\{1, 2, 3, 4, 5, 6\}$.

(a) Does S_6 have some subgroup of the order 7? Explain!

(b) Find a subgroup of S_6 of the order 2.

Exercise 2.40 Let G be a group, and let K and H be subgroups of G.

(a) Is it true that $K \cap H$ has to be a subgroup of G? Give a proof or a counterexample!

(b) Is it true that $K \cup H$ has to be a subgroup of G? Give a proof or a counterexample!