ALGEBRA 1 FOR COMPUTER SCIENTISTS

MICHAEL KOMPATSCHER

kompatscher@karlin.mff.cuni.cz

These are the lecture notes to Algebra 1, given in Winter Term 2021/22. They will be updated regularly and follow closely David Stanovský's script *Základy Algebry pro informatiky*, which is available (in Czech) on his website `https://www2.karlin.mff.cuni.cz/~stanovsk/vyuka/2021/alginf.htm`.

The **goals** of this lecture are to

- introduce you to important algebraic structures (rings, fields, groups,...), their properties, and "abstract algebraic reasoning" in general
- show you that algebra (and number theory) are useful in CS:
  - for the efficient representation of data, e.g. using finite fields (error-correcting codes, secret sharing, cryptoanalysis), or modular arithmetic (Chinese remainder theorem),
  - as a source of difficult computational problems (discrete logarithms in cyclic groups, extracting roots modulo n, RSA),
- show how groups can be used to describe the symmetries of objects,
- discuss concrete applications: in cryptography (RSA, discrete logarithms and Diffie-Hellman, secret sharing), and error-correcting codes (Reed-Salomon).

Date: September 28, 2025.

Contents

Number theory

1. Prime factorization and the greatest common divisor

In this first chapter, we give an introduction to basic number theory. We are going to discuss some fundamental notions and results, including: divisibility, primes and prime factorisation, the Euclidean algorithm, congruences, Euler's theorem, and the Chinese remainder theorem. We will generalize some of these concepts in later sections (e.g. to polynomial rings), but it is still important to start with this special case.

Many of the results in this chapter have been known in one or another form since ancient times. However, they were first presented in a modern and rigorous way by Carl Friedrich Gauss in his famous book *Disquisitiones Arithmeticae* of 1801, which laid the foundation of modern number theory.

The mathematical object that we are going to study are the *natural numbers* $\mathbb{N} = \{1, 2, 3, \ldots\}$ and the *integers* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ together with the arithmetic operations $+, -, \cdot$ (addition, subtraction and multiplication). Note that we exclude 0 from the natural numbers, although some other authors might include it. For short, *"number"* in this chapter, always refers to an integer.

There are several different ways to formally define the integers: they can be constructed within set theory, or be introduced axiomatically (usually by *Peano axioms*, which are based on the principle of mathematical induction). None of these definitions are addressed here - for our purposes it is enough to have a basic/intuitive understanding of $\mathbb{N}$ and $\mathbb{Z}$ from secondary school.

1.1. Divisibility and the fundamental theorem of arithmetic.

Let a, b be integers. We say b *divides* a, and write $b \mid a$, if there exists an integer q, such that $a = b \cdot q$. In this case b is also called a *divisor* or *factor* of a. If b does not divide a, it makes sense to ask for its remainder after the division:

Proposition 1.1 (Division with remainder)**.** *Let $a, b \in \mathbb{Z}$, and $b \neq 0$. Then there exist* unique *numbers $q, r \in \mathbb{Z}$, such that*

$$a = q \cdot b + r \text{ and } 0 \leq r < |b|. \tag{1}$$

We call $q = a \operatorname{div} b$ the (integer) quotient *and $r = a \bmod b$ the* remainder*. Note that $b \mid a$ if and only if $a \bmod b = 0$.*

Proof. We are only going to discuss the case $a, b > 0$, other cases can be handled similarly. Let q be the largest number, such that $q \cdot b \leq a$, and let $r = a - q \cdot b$. Note that $0 \leq r < b$ (otherwise q would not be maximal). Therefore we found values q, r such (1) holds.

In order to prove that q and r are unique, let q_1, q_2 and r_1, r_2 be such that $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$, and $0 \leq r_1, r_2 < b$. Then $b(q_1 - q_2) = r_2 - r_1$, and thus $b \mid r_2 - r_1$; together with $0 \leq |r_2 - r_1| < |b|$ this implies $r_2 - r_1 = 0$. It follows that $r_1 = r_2$, and as a consequence $q_1 b = q_2 b \Rightarrow q_1 = q_2$. □

Note that the numbers 1 and -1 are special, in the sense that they divide all other integers. Also $\pm a \mid a$ holds for every $a \in \mathbb{Z}$. We therefore call $1, -1, a, -a$ the *trivial* divisors of a. Any natural number $p > 1$ that only has trivial divisors is called a *prime number*. All natural numbers that have non-trivial divisors are called *compound numbers*. A fundamental fact in number theory is that every number can be unambiguously be expressed as a product of prime numbers:

Theorem 1.2 (Fundamental theorem of arithmetic)**.** *For every natural number $a > 1$ there are pairwise different primes $p_1, p_2, \ldots, p_n$ and natural numbers $k_1, k_2, \ldots, k_n$ such that*

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}.$$

This product is called the prime factorization *or* prime decomposition *of a. It is unique, up to reordering the primes.*

The first recorded proof of this seemingly self-evident fact is by Euclid in the 4th century BC, and today every high school student knows it (or should know it). However, let's admit, who of you know how to prove it? The existence of factorization can be proved relatively easily by induction:

Proof of Theorem 1.2 (existence of prime factorization). For contradiction, assume that there are numbers that do not have a prime factorization; let a be the smallest such number. Note that a cannot be a prime itself, since then $a = a^1$ would be a prime factorization. Hence there exist two numbers b, c, such that $1 < b, c < a$ and $a = b \cdot c$. By the induction hypothesis, both b and c have prime factorizations. By taking the product of these prime factorizations, we obtain a prime factorization for a - contradiction! □

However we did not prove the *uniqueness* of the prime factorization, claimed by Theorem 1.2. We are going to prove it in the next section, using Bézout's identity.

A simple fact of the existence of prime decompositions is that there are infinitely many primes. If there are only finitely many, then let us number them by $p_1, p_2, \ldots, p_n$. By what we have seen, the number $p_1 \cdot p_2 \cdots p_n + 1$ must have a prime factorization (How can we use this to obtain a contradiction? Discuss!).

1.2. **Euclid's algorithm and Bézout's identity.** The *greatest common divisor* of two natural numbers a, b is the largest number c, such that $c \mid a$ and $c \mid b$. For short, we write $c = \gcd(a, b)$. Two numbers a, b are called *coprime*, if $\gcd(a, b) = 1$.

Similarly, the *least common multiple* of two numbers is the smallest number c, such that $a \mid c$ and $b \mid c$. We denote it by $c = \operatorname{lcm}(a, b)$. Using the fundamental theorem of arithmetic, it is easy to see that

$$a \cdot b = \gcd(a, b) \cdot \operatorname{lcm}(a, b),$$

(we leave the proof as an exercise). Furthermore $\gcd(\pm a, \pm b) = \gcd(a, b)$, therefore we will only deal with non-negative numbers in the following.

A possible way of calculating $\gcd(a, b)$ is by the means of prime factorizations. If we take for instance $168 = 2^3 \cdot 3 \cdot 7$ and $396 = 2^2 \cdot 3^2 \cdot 11$, then we see that $\gcd(168, 396) = 2^2 \cdot 3 = 12$, by taking the product of all prime factors that a and b have in common.

However this method has two main problems: Firstly, it requires that we already know the prime decompositions of both a and b. However, computing prime decompositions can be a hard task (for big numbers a, b) - in fact no reasonably efficient algorithm is known up to date.

Secondly, our method to compute $\gcd(a, b)$ is based on the assumption that every number has a *unique* prime factorization. If, in our example, the number 396 would have an alternative prime decomposition to $2^3 \cdot 3 \cdot 7$, we would get another

result. Therefore we are not able to prove the correctness of this method, without completing the proof of the basic theorem of arithmetic. [1]

A better method to calculate $\gcd(a, b)$ is *Euclid's algorithm*. It is based on the following observation, which is independent of the fundamental theorem of arithmetic:

Lemma 1.3. *For two any two integers $a, b \in \mathbb{Z}$ it holds that*

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Proof. Let $q = a \operatorname{div} b$. Then

$$a = q \cdot b + (a \bmod b).$$

This equation implies that any number c that divides b and $(a \bmod b)$ also divides a. On the other hand, $c \mid a$ and $c \mid b$ implies that $c \mid (a - q \cdot b)$, which is equal to $(a \bmod b)$. Thus c is a common divisor of a and b if and only if it is a common divisor of b and $(a \bmod b)$. It follows that $\gcd(a, b) = \gcd(b, a \bmod b)$. □

Now, for two numbers $a \geq b \geq 1$, Euclid's algorithm computes a sequence, of numbers, by exchanging the pair a, b, by $b, a \bmod b$, and iterating this step. More precisely, we define this sequence $a_0, a_1, a_2, \ldots$ by the induction $a_0 = a$, $a_1 = b$, and

$$a_{i+1} = a_{i-1} \bmod a_i.$$

When the sequence reaches $a_{n+1} = 0$, the algorithm outputs the previous value a_n as $\gcd(a, b)$.

In our example $\gcd(168, 396)$, Euclid's algortihm computes the sequence 396, 168, 60, 48, 12,0, and thus $\gcd(168, 396) = 12$.

Note that the algorithm always terminates, since $0 \leq a_{i+1} < a_i$, for every $i > 2$. It is further easy to see that the algorithm is correct, since, by Lemma 1.3:

$$\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_k, 0) = a_k.$$

The following theorem can be shown by studying Euclid's algorithm in more detail:

Proposition 1.4 (Bézout's identity)**.** *For each pair of integers $a, b \in \mathbb{Z}$, there exists integers $u, v \in \mathbb{Z}$ (so called* Bézout coefficients*), such that*

$$\gcd(a, b) = u \cdot a + v \cdot b$$

Proof. Let $a_0, a_1, a_2, \ldots, a_n$ be the sequence of numbers computed by the Euclidean algorithm. We claim that, for every index i, there are coefficients u_i, v_i such that $a_i = u_1 \cdot a + v_i \cdot b$. For the initial values this is clear, for $(u_0, v_0) = (1, 0)$ and $(u_1, v_1) = (0, 1)$. For an induction step $i \to i + 1$, note that $a_{i+1} = a_{i-1} \bmod a_i = a_{i-1} - q_i a_i$, for $q_i = a_{i-1} \operatorname{div} a_i$, and therefore

$$(u_{i+1}, v_{i+1}) = (u_{i-1}, v_{i-1}) - q_i \cdot (u_i, v_i).$$

We have shown above, that $\gcd(a, b) = a_{n-1}$, and thus $u = u_{n-1}, v = v_{n-1}$ are Bézout coefficients for a, b. □

---

[1] Note that in other "number systems", prime factorizations is indeed not unique. For instance, in the ring $\mathbb{Z}[\sqrt{5}]$, the element 4 has the two different prime factorizations $4 = 2 \cdot 2 = (1 + \sqrt{5})(-1 + \sqrt{5})$. Using our method, we would deduce $\gcd(4, 2) = 2$ from the first factorization, but $\gcd(4, 2) = 1$ from the second. We are going to discuss rings like $\mathbb{Z}[\sqrt{5}]$ later, in Section 5.

Example. For $\gcd(168, 396)$ we get

a_i	u_i	v_i
396	1	0
168	0	1
60	1	-2
48	-2	5
12	3	-7
0		

Hence $\gcd(168, 396) = 3 \cdot 396 - 7 \cdot 168$.

Using Bézout coefficients, we can prove the following auxiliary statement:

Lemma 1.5. *Let p be a prime, and $a, b \in \mathbb{Z}$ such that $p \mid ab$. Then $p \mid a$ or $p \mid b$ holds.*

Proof. Suppose that $p \nmid a$. Then $\gcd(p, a) = 1$, and by Proposition 1.4, there are integers u, v, such that $au + pv = 1$. Multiplying this identity with b, we obtain $abu + pbv = b$. Note that $p \mid abu$ (by assumption), and $p \mid pbv$. It follows that $p \mid abu + pbv = b$, which is what wanted to prove. Symmetrically, $p \mid ab$ and $p \nmid b$ implies $p \mid a$. Thus if $p \mid ab$, either $p \mid a$ or $p \mid b$ must hold. □

By induction, we can easily deduce the following consequence of Lemma 1.5:

Lemma 1.6. *Let p be a prime, and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid a_1 a_2 \cdots a_n$ then $p \mid a_i$ holds for at least one index $i \in \{1, 2, \ldots, n\}$.*

We can now finish the proof of the fundamental theorem of arithmetic:

Proof of Theorem 1.2 (uniqueness of prime factorization). For contradiction, let us assume that there is a natural number that does not have a unique prime factorization; let a be the smallest such number. Note that a cannot be a prime itself. Let

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_m^{k_m} = q_1^{l_1} \cdot q_2^{l_2} \cdots q_n^{l_n}$$

be two prime factorizations of a (which are not equal, up to reordering the primes). Since $p_1 \mid a$, by Lemma 1.6, there is a prime q_i in the right factorization, such that $p_1 \mid q_i$. Since q_i is a prime, it follows that $p_1 = q_i$. Therefore, if we define $b = a \operatorname{div} p_1$, we get:

$$b = p_1^{k_1 - 1} \cdot p_2^{k_2} \cdots p_m^{k_m} = q_1^{l_1} \cdot q_2^{l_2} \cdots q_i^{l_i - 1} \cdots q_n^{l_n},$$

which are two different prime factorizations of b. But $b < a$, contradicting the minimality of a. □

2. Modular arithmetic

2.1. **Congruences.** The symbol $\equiv$ for congruences, was introduced by Gauss in his *Disquisitiones Arithmeticae*, and makes it easier to write down computations modulo a given number m:

Definition. Let a, b, m be integers, and $m \neq 0$. We then say that a is congruent to b modulo m, and write

$$a \equiv b \pmod{m},$$

if $m \mid a - b$.

Note first, that $a \equiv b \pmod{m}$, if and only if a and b have the same remainder, after dividing with m: to see this, let $a = q_1 \cdot m + r_1$ and $b = q_2 \cdot m + r_2$ with $0 \leq r_1, r_2 < m$. Then $a - b = (q_1 - q_2)m + (r_2 - r_1)$. Because of this $m \mid a - b$ is equivalent to $m \mid r_2 - r_1$. But since $|r_2 - r_1| < m$, this is in turn equivalent to $r_2 - r_1 = 0$.

From this observation it directly follows "begin congruent modulo some fixed integer m" is an *equivalence relation*, i.e. it satisfies:

- $a \equiv a \pmod{m}$ (*reflexivity*),
- If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$ (*symmetry*),
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$ (*transitivity*).

The other important property of a congruence, is that it is invariant under the arithmetic operations:

Proposition 2.1 (Properties of congruences)**.** *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then*

$$a + c \equiv b + d \pmod{m}, \quad a - c \equiv b - d \pmod{m}, \quad a \cdot c \equiv b \cdot d \pmod{m},$$

and for every natural number $k \in \mathbb{N}$:

$$a^k \equiv b^k \pmod{m}.$$

Proof. Exercise. □

The above properties allow us to use $\equiv$ in a similar way to the equality sign $=$: Reflexivity means that $a = b$ implies $a \equiv b \pmod{m}$. By the symmetry of $\equiv$, it does not matter if we read congruences from left to right or right to left; the transitivity implies, that a chain of congruences $a_1 \equiv a_2 \pmod{m}, a_2 \equiv a_3 \pmod{m}, \ldots, a_{n-1} \equiv a_n \pmod{m}$ implies $a_1 \equiv a_n \pmod{m}$. Proposition 2.1 allows us to replace any number in a computation by a congruent number.

Let us demonstrate this with a simple example:

Exercise. Compute $(77^{123} + 66^{321}) \bmod 6$.

Solution. Note that $77 \equiv 5 \equiv -1 \pmod{6}$ and $66 \equiv 0 \pmod{6}$. Hence

$$77^{123} + 66^{321} \equiv (-1)^{123} + 0^{321} = -1 + 0 \equiv 5 \pmod{6}.$$

Thus $(77^{123} + 66^{321}) \bmod 6 = 5$. □

If we want to solve "equations" involving congruences, there are two very useful properties: We can reduce $cx \equiv cy$ by the factor c, if c is coprime with the modulus m. Furthermore, if all 3 numbers involved have a common factor, we can also divide them (including the modulus!) by it, to obtain an equivalent equation. We formally state these two properties in the following theorem:

Proposition 2.2 (Properties of congruences)**.** *Let a, b, c, m be integers, and $m \neq 0$. Then*

(1) *$a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{cm}$;*
(2) *If m and c are coprime, then $a \equiv b \pmod{m} \Leftrightarrow ca \equiv cb \pmod{m}$.*

Proof. Exercise. □

Exercise. Find all x, such that (a) $6x \equiv 9 \pmod{21}$; (b) $10x \equiv 5 \pmod{21}$.

Solution. We solve this exercise by using Proposition 2.2:

(a) Note that by (1), $6x \equiv 9 \pmod{21}$ is equivalent to $2x \equiv 3 \pmod{7}$. By (2) we can multiply both sides with 4, which gives us the equivalent equation $x \equiv 5 \pmod{7}$. Therefore, the solution are all x that are of the form $x = 5 + 7k$, $k \in \mathbb{Z}$.
(b) By (2), this identity is equivalent to $2x \equiv 1 \pmod{21}$. Since 11 is coprime to 21, we get (again by (2)) the equivalent equation $x \equiv 11 \pmod{21}$. Thus all $x = 11 + 21k$, $k \in \mathbb{Z}$ are solutions.

□

2.2. **Euler's theorem and the cryptosystem RSA.** We are next going to prove Euler's theorem. As motivation, let us look at another exercise, that looks similar to the previous ones:

Exercise. Compute the last digit of 77^{123} (in base 10).

Solution. The last digit of 77^{123} is equal to $77^{123} \bmod 10$. We can rewrite $77^{123} \equiv 7^{123} \equiv (-3)^{123} \pmod{10}$; but now (without a good strategy) we have to either compute the powers of either 7 or (-3) modulo 10. We do it for 7:

$$7^1 = 7, 7^2 = 49 \equiv 9, 7^3 \equiv 7 \cdot 9 \equiv 3, 7^4 \equiv 7 \cdot 3 \equiv 1, 7^5 \equiv 1 \cdot 7 \equiv 7, \dots$$

So the sequence $7, 9, 3, 1$ is just repeating itself (with period 4). Since $123 \bmod 4 = 3$, we obtain $7^{123} \equiv 7^3 \equiv 3 \pmod{10}$. □

The periodic behaviour of the sequence in the above example is not an accident, but a consequence of *Euler's theorem*. The length of the period is given by *Euler's function* φ, which is defined as follows:

Definition. *Euler's totient function* $\varphi(n)$, is the function that assigns to every natural number n the number of integers $k \in \{1, 2, \dots, n-1\}$, such that $\gcd(k, n) = 1$.

For example $\varphi(10) = 4$, since there are are 4 numbers that are coprime to 10, namely $1, 3, 7, 9$. For any prime p, it is not hard to see that $\varphi(p) = p - 1$.

However, calculating $\varphi(n)$ directly from its definition is not very efficient for big numbers n. Fortunately, there is a formula that makes it easier, if we already know the prime factorization:

Proposition 2.3. *Let $n = p_1^{k_1} \cdots p_m^{k_m}$ be a prime factorization for a natural number $n > 1$. Then*

$$\varphi(n) = p_1^{k_1 - 1}(p_1 - 1) \cdots p_m^{k_m - 1}(p_m - 1).$$

Exercise. Compute $\varphi(4056)$

Solution. $\varphi(4056) = \varphi(2^3 \cdot 3^1 \cdot 13^2) = 2 \cdot 1 \cdot 3^0 \cdot 2 \cdot 13^1 \cdot 12 = 1248$. □

The formula in Proposition 2.3 is quite easy to prove knowing the Chinese Remainder Theorem, which we will encounter in the next section.

We now are able to state Euler's theorem:

Theorem 2.4 (Euler's theorem)**.** *Let a, m be coprime, natural numbers. Then*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Leonhard Euler published this theorem in 1763. Already earlier, in 1736, he proved it for the special case, in which m is a prime number. This special case is sometimes also attribute to Pierre de Fermat, who already stated it 1640 in one of his letters (without giving a proof):

Corollary 2.5 (Fermat's little theorem)**.** *Let p be a prime number, and $p \nmid a$. Then*

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

For the rest of this section, we are going to prove Euler's theorem. For this, let $\Phi_m = \{k \in \{1, \dots, m-1\} \colon \gcd(k, m) = 1\}$. Euler's totient function then clearly is given by $\varphi(m) = |\Phi_m|$.

Lemma 2.6. *Let $f \colon X \to Y$ be a map between two* finite *sets X, Y of the same size. If f is injective, then f is also bijective.*

'Proof': Let $n = |X| = |Y|$. Then, since f is injective, it always assigns pairwise different elements of X to pairwise different elements. Thus, the image of X under f must contain n pairwise different elements, and is therefore equal to all of Y. So f is bijective. □

Although Lemma 2.6 might seem pretty obvious to you, you may try to think for a moment, why the same is not true for infinite sets (or look up *Hilbert's Hotel*). We use Lemma 2.6 in the proof of the following lemma:

Lemma 2.7. *Let $a, m \in \mathbb{N}$ be coprime natural numbers. and let f_a be the map*

$$\begin{aligned} f_a \colon \Phi_m &\to \Phi_m, \\ x &\mapsto ax \bmod m. \end{aligned}$$

Then f_a is well-defined and a bijective map.

Proof. We first show, that if $x \in \Phi_m$, then also $f_a(x) \in \Phi_m$. For this note that if x and a are coprime with m, then also ax is coprime with m: If this was not the case, there would be a prime p dividing both m and ax. By Lemma 1.5, then $p \mid ax$ implies that either $p \mid a$ or $p \mid x$. But then either x or a would have the common divisor p with m, which is a contradiction. Lemma 1.3 now implies that $1 = \gcd(m, ax) = \gcd(m, ax \bmod m)$, hence $f_a(x) = ax \bmod m \in \Phi_m$.

Next, we show that f_a is bijective. By Lemma 2.6, it is enough to prove that it is injective. So assume that $ax \bmod m = ay \bmod m$ for $x, y \in \Phi_m$. By Proposition 2.2 (2) this is equivalent to $x \bmod m = y \bmod m$. Since x and y are from the set $\{1, 2, \dots, m-1\}$, they must be equal. Thus f_a is injective, which finishes the proof. □

We are now ready to prove Euler's theorem:

Proof of Theorem 2.4. By Lemma 2.7, the map $f_a \colon \Phi_m \to \Phi_m$ is a bijection. This implies that

$$\prod_{b \in \Phi_m} b = \prod_{b \in \Phi_m} f_a(b) \equiv \prod_{b \in \Phi_m} ab = a^{\varphi(m)} \prod_{b \in \Phi_m} b \pmod{m}.$$

If we set

$$c = \prod_{b \in \Phi_m} b$$

this means that $c \equiv a^{\varphi(m)} \cdot c \pmod{m}$. Since c is the product of numbers that are coprime to m, also c must be coprime to m (this follows from Lemma 1.6; see also the proof of Lemma 2.7). By Proposition 2.2 (1) $c \equiv a^{\varphi(m)} \cdot c \pmod{m}$ is equivalent to $1 \equiv a^{\varphi(m)} \cdot 1 = a^{\varphi(m)} \pmod{m}$, which finished the proof of Euler's theorem. □

We remark that we will derive another proof of Euler's theorem later in Section 11.2, as the special case of *Lagrange's theorem* for $\mathbb{Z}_m^*$.

We are now ready to give a way more efficient solution to our previous exercise:

Exercise. Compute the last digit of 77^{123}.

Solution. By Proposition 2.3 we know that $\varphi(10) = 4$. Since further $\gcd(77, 10) = \gcd(7, 10) = 1$, we can apply Euler's theorem and get:

$$77^{123} \equiv 7^{123} = 7^{4 \cdot 30 + 3} = (7^4)^{30} \cdot 7^3 \equiv 1^{30} \cdot 3 = 3 \pmod{10}.$$

(We extended all the single solution steps in this example for clarity, in practice it can be however more convenient for you to abbreviate $7^{123} \equiv 7^3 \equiv 3 \pmod{10}$.) □

Exercise. Compute $10^{10^{10}} \bmod 21$

Solution. Using Proposition 2.3 we compute $\varphi(21) = 12$. Since $\gcd(21, 10) = 1$, so we can apply Euler's theorem to obtain:

$$10^{10^{10}} \equiv 10^{(10^{10} \bmod 12)} \pmod{21}.$$

To compute the exponent $10^{10} \bmod 12$ note first that $\gcd(10^{10}, 12) = \gcd(2^{10} \cdot 5^{10}, 12) = 4$, so we cannot apply Euler's theorem straight away. But, by Proposition 2.2 (2), $4k \equiv 2^{10} \cdot 5^{10} \bmod 12$ is equivalent to to $k \equiv 2^8 \cdot 5^{10} \equiv 1 \pmod{3}$. Therefore $(10^{10} \bmod 12) \equiv (4 \bmod 12)$. This implies that

$$10^{10^{10}} \equiv 10^{(10^{10} \bmod 12)} = 10^4 \equiv 4 \pmod{21}.$$

Thus $10^{10^{10}} \bmod 21 = 4$. □

Observation 2.8. *Lemma 2.7 implies, that for every pair of coprime numbers a, m, there is a unique $b \in \{1, 2, \ldots, m-1\}$ such that*

$$a \cdot b \equiv 1 \pmod{m}.$$

This b can be found in two different ways:

- *as $b \equiv a^{\varphi(m)-1} \bmod m$, by Euler's theorem;*
- *using the Euclidean algorithm: we calculate the Bézout coefficients (u, v) for $1 = \gcd(a, m)$, so $1 = ua + vm$. Then $b = u \bmod m$.*

We will see later, why knowing/computing such b for given a is useful. In the language of Section 5, we just described how to determine the *multiplicative inverse* of a in the ring $\mathbb{Z}_m$.

Number theory has numerous applications in computer science, especially in cryptography. An example of this is the *RSA cryptosystem* (named after the three mathematicians Rivest, Shamir, Adleman), that is used for so called *public-key encryption*.

In public-key encryption, the problem is as follows: Bob receives many messages from many different clients that he would like to encrypt. It is impractical to

exchange a secret password with every single one of them. Therefore Bob publishes a so-called *public key* with which everyone can generate encrypted messages. Bob secretly keeps a *private key*, with which only he can decrypt messages. We are going to describe how to generates the keys, and how to encrypt and decrypt a message in the RSA system:

At the beginning, Bob chooses two different primes p, q and computes their product $N = pq$. Then he randomly selects a number e, which is coprime with $\varphi(N) = (p-1)(q-1)$. Using Euclid's algorithm, he computes a number d, such that

$$de \equiv 1 \pmod{\varphi(N)}$$

(as in Observation 2.8). The numbers e and N are the public key, which Bob shares with everybody. The numbers d, p, q are the private key, which Bob keeps secret.

We next describe, how a client (Alice) can send a secret message to Bob. For simplicity, we assume that the message is a natural number x with $0 < x < N$. Using the public key Alice computes the value

$$y = x^e \bmod N,$$

and sends the result y to Bob. Bob, with the knowledge of the private key d can then encode the original message by computing

$$x = y^d \bmod N.$$

This works, since $de \equiv 1 \pmod{\varphi(N)}$, and therefore, by Euler's theorem:

$$y^d \equiv (x^e)^d = x^{ed} \equiv x^1 \pmod{N}.$$

If attackers intercept the message that Alice sent, they only know the encrypted message y and the public key N, e. In order to compute the original message x they would need to know some kind of procedure to compute x from $x^e \bmod N$ (so a method to compute the "e-th root modulo N"). The obvious solution would be to compute the prime factorization $N = pq$ of N, use it to compute d, and then proceed as Bob. However, up to date, there is no *efficient way* is know how to compute the prime factorization of a number (subject to certain assumptions, e.g. that the number has not too many small prime divisors, and the prime divisors are all about the same size). Thus, if p, q are picked big enough (at the state of the art, it is enough to choose primes with around 1000 digits), this attack will not succeed. Also (up to date) there is no other known algorithm to efficiently compute roots modulo N.

2.3. **The Chinese remainder theorem.** We finish the chapter on number theory with the Chinese remainder theorem. As the name suggests, this theorem was already known to the ancient Chinese - it is mentioned for instance in the book *The Art of War* by Sun Tzu from the 5th century BC.
It is said Sun Tzu used it to keep track of his soldiers: He knew he had 1,000 soldiers before a battle, and he wanted to count them after it. It is easy to make mistakes when counting big groups of people. So instead of counting them all at once, he let them first form groups of ten, then groups of eleven, and then groups of thirteen; each time he only counted how many soldiers were left after the "grouping up". In others words, he counted how many soldiers there were modulo 10, modulo 11 and modulo 13. By the Chinese remainder theorem, the total number of soldiers can then be determined from these remainders alone:

Theorem 2.9 (The Chinese remainder theorem)**.** *Let $m_1, m_2, \ldots, m_n$ be mutually coprime numbers, and let $M = m_1 \cdot m_2 \cdots m_n$. Let $u_1, u_2, \ldots, u_n$ be arbitrary integers. Then there exists a unique $x \in \{0, 1, \ldots, M-1\}$, such that*

$$x \equiv u_1 \pmod{m_1}, \quad x \equiv u_2 \pmod{m_2}, \ldots, \quad x \equiv u_n \pmod{m_n}.$$

Proof. We first prove the uniqueness of the solution x. For this, assume that there are two solutions $x, y \in \{0, 1, \ldots, M-1\}$, such that $x \equiv y \equiv u_i \pmod{m_i}$ for every i. Then, for every i:

$$m_i \mid x - y,$$

and since all m_i are coprime we obtain $M = m_1 \cdot m_2 \cdots m_n \mid x-y$. Since $|x-y| < M$, this implies that $x - y = 0$, so the two solutions are equal.

Next we prove that there is a solution x. For this, let f be the function be defined by

$$f \colon \{0, \ldots, M-1\} \to \{0, 1, \ldots, m_1 - 1\} \times \{0, 1, \ldots, m_2 - 1\} \times \cdots \times \{0, 1, \ldots, m_n - 1\}$$
$$x \mapsto (x \bmod m_1, x \bmod m_2, \ldots, x \bmod m_n)$$

By the 'uniqueness' part of our proof, this map is injective. On the other hand, note that the domain $\{0, 1, \ldots, M-1\}$ and the codomain $\{0, 1, \ldots, m_1 - 1\} \times \{0, 1, \ldots, m_2 - 1\} \times \cdots \times \{0, 1, \ldots, m_n - 1\}$ of f have the same size, namely M. So by Lemma 2.6 f must be a bijection. In other words, every n-tuple $(u_1, u_2, \ldots, u_n)$ is in the image of exactly one x under f - this x is the unique solution to the system of equations. □

The proof of Theorem 2.9 is not constructive, in the sense that it only shows that there is a unique solution to every such system of equations, but it does not tell us, how to find it. We are going to describe a procedure by just giving the following example:

Exercise. Find a solution x to the following system of equations:

$$x \equiv 2 \pmod{3}, \quad x \equiv 1 \pmod{4}, \quad x \equiv 3 \pmod{5}.$$

Proof. From the first equation we can infer that $x = 2 + 3k$ for some $k \in \mathbb{Z}$. If we substitute this in the second equation, we get $(2 + 3k) \equiv 1 \pmod{4}$, and therefore $k \equiv 1 \pmod{4}$. So $k = 1 + 4l$ for some $l \in \mathbb{Z}$. Re-substituting, gives us $x = 5 + 12l$, $l \in \mathbb{Z}$. Plugging this into the third equation then implies $12l + 5 \equiv 3 \pmod{5}$, which simplifies to $l \equiv 4 \pmod{5}$; thus $l = 4 + 5m$ and as a consequence $x = 53 + 60m$ for $m \in \mathbb{Z}$. Note that $x = 53$ is the only solution that satisfies $x \in \{0, 1, \ldots, 59\}$. □

The Chinese remainder theorem applies in a more general sense also to polynomials - we will discuss this later in Section 8.1. Both for numbers and for polynomials, the Chinese remainder theorem has important applications in computer algebra: It allows to reduce a problem about a large object (a big number, or a polynomial of high degree) to several problems over with smaller objects (as for instance in the example of counting soldiers at the beginning of this section). This can be very advantageous, not only in parallel computing, but also when working with algorithms that exploit modular arithmetics. We refer the interested among you, e.g. to the Computer Algebra lecture.

Finally, using the Chinese theorem on residues, we can prove the formula to compute Euler's function in Proposition 2.3:

$$\varphi(p_1^{k_1} \cdots p_m^{k_m}) = p_1^{k_1-1}(p_1 - 1) \cdots p_m^{k_m-1}(p_m - 1).$$

Proof of Proposition 2.3. Note that it is enough to prove the following two rules for φ:

(1) $\varphi(p^k) = p^{k-1}(p-1)$, for every prime p and $k \in \mathbb{N}$
(2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, for coprime numbers a, b

It then follows directly from (1) and (2) that

$$\varphi(p_1^{k_1} \cdots p_m^{k_m}) \overset{(2)}{=} \varphi(p_1^{k_1}) \cdots \varphi(p_m^{k_m}) \overset{(1)}{=} p_1^{k_1-1}(p_1 - 1) \cdots p_m^{k_m-1}(p_m - 1).$$

To show (1), note that a number is coprime to p^k if and only if it is not a multiple of p. There are p^{k-1}-many multiples of p in the set $\{0, 1, \ldots, p^k - 1\}$. Thus $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

For (2) let us look at the map

$$f \colon \{0, 1, 2, \ldots, ab-1\} \to \{0, 1, 2, \ldots, a-1\} \times \{0, 1, 2, \ldots, b-1\}$$
$$x \mapsto (x \bmod a, x \bmod b)$$

By the Chinese remainder theorem, f is a bijective map. Now let us consider the restriction of f to the set Φ_{ab}. We are going to show that the image of this restriction is equal to $\Phi_a \times \Phi_b$. This would then prove (2), since then $\varphi(ab) = |\Phi_{ab}| = |\Phi_a \times \Phi_b| = |\Phi_a| \cdot |\Phi_b| = \varphi(a) \cdot \varphi(b)$.

To prove it, let $x \in \Phi_{ab}$, so $\gcd(x, ab) = 1$. This is equivalent to the statement that every prime divisor of ab does not divide x. By Lemma 1.5, this is equivalent to $\gcd(x, a) = 1$ and $\gcd(x, b) = 1$. Therefore f maps Φ_{ab} bijectively to $\Phi_a \times \Phi_b$, so $\varphi(ab) = \varphi(a) \cdot \varphi(b)$. □

Polynomials

3. Fields, rings and integral domains

3.1. **Definitions and examples.** In this chapter we are going to discuss, how some of the results on divisibility that we showed for integers $(\mathbb{Z}, +, -, \cdot, 0)$ can be generalized to other algebraic structures. But first we need to clarify: to which structures?

First and foremost, it makes sense to only consider *rings*, which are algebras that have an addition and multiplication operation (in a meaningful way). Besides the rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, you very likely already encountered the rings of real polynomials $\mathbb{R}[x]$ and integer polynomials $\mathbb{Z}[x]$. We are further going to look at other examples, such as the ring of *Gaussian integers* (which consists of the complex numbers with integer coefficients) and other extensions of $\mathbb{Z}$.

Integral domains are those rings, for which it makes sense to also discuss divisibility. All of the above examples are integral domains, however, they don't all share the properties of the integers. For example, elements can be uniquely decomposed into "primes" in $\mathbb{Z}[x]$ and the Gaussian integers. However this is not true for some other extensions of $\mathbb{Z}$ (such as $\mathbb{Z}[\sqrt{5}]$). For real valued polynomials in one variable it makes sense to define the greatest common divisor, and to compute it using Euclid's algorithm. However this fails for polynomials in more than one variable. Thus, there is a lot to explore.

We start by giving a formal definition of ring:

Definition. A *ring* $\mathbf{R} = (R, +, -, \cdot, 0)$ consists of a non-empty set R, together with binary operations $+\colon R \times R \to R$ and $\cdot\colon R \times R \to R$, a unary operation $-\colon R \to R$, and a constant $0 \in R$, such that for all $a, b, c \in R$:

$$\begin{aligned}
\text{(Associativity of } +) \qquad & a + (b + c) = (a + b) + c \\
\text{(Commutativity of } +) \qquad & a + b = b + a \\
\text{(additive identity)} \qquad & a + 0 = a \\
\text{(additive inverse)} \qquad & a + (-a) = 0 \\
\text{(Associativity of } \cdot) \qquad & a \cdot (b \cdot c) = (a \cdot b) \cdot c \\
\text{(Distributivity of } \cdot) \qquad & a \cdot (b + c) = (a \cdot b) + (a \cdot c), \\
& (a + b) \cdot c = (a \cdot b) + (b \cdot c)
\end{aligned}$$

A ring $\mathbf{R}$ is called a *commutative ring*, if additionally the identity $a \cdot b = b \cdot a$ holds for all $a, b \in R$. Further $\mathbf{R}$ is called a *ring with unity*, if it has an element $1 \in R$, such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

We formally distinguish between the set R, which is called the *carrier set* of the ring, and the ring $\mathbf{R} = (R, +, -, \cdot, 0)$ itself, which also contains the information about the algebraic operations $+, -, \cdot, 0$. When writing down terms over rings we can reduce parenthesis by using the standard convention that multiplications precede additions (so, for instance $a + b \cdot c = a + (b \cdot c)$). We further write $a - b$ instead of $a + (-b)$.

Definition. Let $\mathbf{R}$ be a commutative ring with unity $1 \neq 0$. Then $\mathbf{R}$ is called

- an *integral domain*, if it satisfies

$$a, b \neq 0 \Rightarrow a \cdot b \neq 0.$$

- a *field* if for every $a \neq 0$ there is an element b with $a \cdot b = 1$
  We then call b a (multiplicative) *inverse* of a and write $b = a^{-1}$.

Example. The sets of numbers $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ together with the standard operations $+, -, \cdot$ and constants $0, 1$ are commutative rings with unity. The integers $\mathbb{Z}$ are an integral domain, but not a field; $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all fields. We are later going to see that there also interesting examples of integral domains that lie between $\mathbb{Z}$ and $\mathbb{C}$, and fields that lie between $\mathbb{Q}$ and $\mathbb{C}$.

Example. Another important example are the finite commutative rings of the form

$$\mathbb{Z}_n = (\{0, 1, \ldots, n-1\}, +_{\bmod n}, -_{\bmod n}, \cdot_{\bmod n}, 0),$$

where n is a natural number. The operations here are all defined *modulo* n. Note that then following are equivalent:

(1) $\mathbb{Z}_n$ is a field,
(2) $\mathbb{Z}_n$ is an integral domain,
(3) n is a prime.

Proof. Every field is an integral domain (see Theorem 3.3), so (1)⇒(2). For (2)⇒(3) note that if n is a compound number $n = k \cdot l$, then $k, l \neq 0$, and $k \cdot_{\bmod n} l = 0$, so $\mathbb{Z}_n$ is not an integral domain. For (3)⇒(1), assume that n is a prime. Then by Observation 2.8, every element $a \neq 0$ has a multiplicative inverse (modulo n), so $\mathbb{Z}_n$ is a field. □

Example (Finite fields)**.** In addition to the fields $\mathbb{Z}_p$ from the last example, we are going to see that there is a finite field of size q if and only if q is a power of a prime. These fields are uniquely determined by their size. We are going to discuss finite fields in Section 9.

Example. For a given commutative ring $\mathbf{R}$, the ring of polynomials $\mathbf{R}[\mathbf{x}]$ consists of all formal expressions $a_0 + a_1 x + \cdots + a_n x^n$, such that the coefficients come from $\mathbf{R}$. We are going to give a more formal definition in Section 4.

Example. An example of a non-commutative ring is $\mathbf{M}_n(\mathbf{F})$, the ring of $n \times n$-matrices over a given field $\mathbf{F}$, with the standard matrix addition and matrix multiplication. In this lecture we are however only going to work with commutative rings.

By taking subsets of a ring (or a field) that are closed under the algebraic operations, we can obtain so called subrings (and subfields):

Definition. For a (commutative) ring $\mathbf{R} = (R, +, -, \cdot, 0)$, let $S \subseteq R$ be a subset of the carrier set, such that $0 \in S$, and for every $a, b \in S$ also $-a \in S, a + b \in S$ and $a \cdot b \in S$ (we say that S is *closed* under the operations of the ring). Then S, together with the restrictions of $+, -, \cdot, 0$ to S also forms a (commutative) ring $\mathbf{S}$. We call $\mathbf{S}$ a *subring* of $\mathbf{R}$, and write $\mathbf{S} \leq \mathbf{R}$.
A subring $\mathbf{S}$ of a field $\mathbf{R}$ is a field itself if $a \in S \setminus \{0\} \Rightarrow a^{-1} \in S$. In this case we call $\mathbf{S}$ a *subfield* of $\mathbf{R}$.

Example. The rational numbers $\mathbb{Q}$ are a subfield of the real numbers $\mathbb{R}$, and $\mathbb{R}$ is a subfield of the complex numbers $\mathbb{C}$. The integers $\mathbb{Z}$ are a subring of $\mathbb{Q}$ (but not a subfield!).

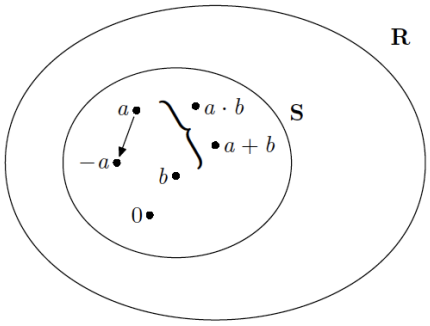


FIGURE 1. The subring **S** of **R**

In algebraic number theory, subrings (and subfields) of $\mathbb{C}$ that contain $\mathbb{Z}$ (respectively $\mathbb{Q}$) are important objects of study. We give some examples:

Example (Gaussian integers and Gaussian rationals)**.**

- The set $\mathbb{Z}[i] = \{a + ib \colon a, b \in \mathbb{Z}\}$ together with the standard arithmetical operations $+, -, \cdot$ forms the *Gaussian integers*. The Gaussian integers are a subring of $\mathbb{C}$. To see this, simply note that $\mathbb{Z}[i]$ contains 0 and is closed under subtraction $-(a+ib) = (-a) + i(-b)$, addition $(a+ib) + (c+id) = (a+c)+i(b+d)$ and multiplication $(a+ib)\cdot(c+id) = (ac-bd)+i(ad+bc)$.
- The set $\mathbb{Q}(i) = \{a + ib \colon a, b \in \mathbb{Q}\}$ together with the standard arithmetical operations $+, -, \cdot$ is a subfield of $\mathbb{C}$, the *Gaussian rational numbers*. Note that for $a+ib \in \mathbb{Q}(i) \setminus \{0\}$ also $(a+ib)^{-1} \in \mathbb{Q}(i)$, since $\frac{1}{a+ib} = \frac{1}{a+ib} \cdot \frac{a-ib}{a-ib} = \frac{a}{a^2+b^2} + i \cdot \frac{b}{a^2+b^2}$.

Example (Quadratic extensions)**.** More generally, for every $s \in \mathbb{Z}$ we can define

- the quadratic integers $\mathbb{Z}[\sqrt{s}] = \{a + \sqrt{s}b \colon a, b \in \mathbb{Z}\} \leq \mathbb{C}$
- the quadratic field $\mathbb{Q}[\sqrt{s}] = \mathbb{Q}(\sqrt{s}) = \{a + \sqrt{s}b \colon a, b \in \mathbb{Q}\} \leq \mathbb{C}$

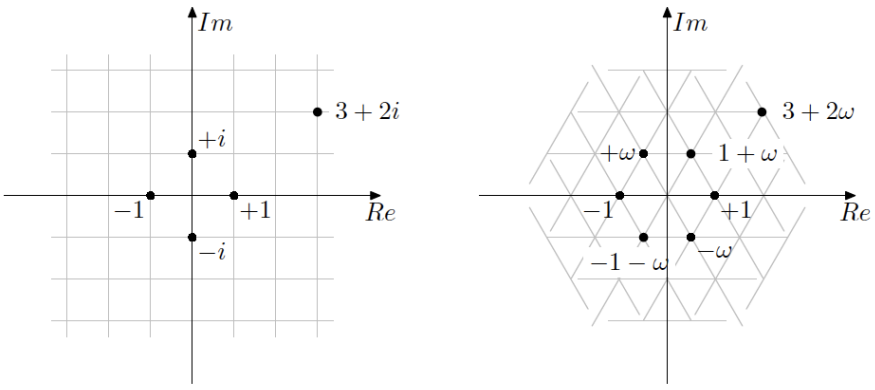


FIGURE 2. The Gaussian integers and Eisenstein integers

It is not hard to see that both $\mathbb{Z}[\sqrt{s}]$ and $\mathbb{Q}(\sqrt{s})$ are closed under $+, -, \cdot$, and therefore subrings of $\mathbb{C}$; with a little bit of extra work, you can also check that $\mathbb{Q}(\sqrt{s})$ is closed under multiplicative inverses, and therefore a subfield of $\mathbb{C}$. Depending on the integer s, the ring $\mathbb{Z}[\sqrt{s}]$ has different properties (we are for instance later going to prove that the Gaussian integers $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ have unique "prime" factorization, but $\mathbb{Z}[\sqrt{5}]$ does not).

Example (Eisenstein integers)**.** The set $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, where $\omega = e^{\frac{2\pi i}{3}} = \frac{-1+i\sqrt{3}}{2}$, is a complex third root of 1, is a subring of $\mathbb{C}$, called the *Eisenstein integers*. It is easy to see that $\mathbb{Z}[\omega]$ is closed under $+$ and $-$. Furthermore, since $\omega^2 = -1 - \omega$ we have that $\mathbb{Z}[\omega]$ is closed under multiplication $(a + b\omega)(c + d\omega) = ac + (ad + bc)\omega + bd\omega^2 = (ac - bd) + (ad + bc - bd)\omega$.

3.2. **Basic properties.** In modern mathematics it is standard to define abstract algebras using the smallest necessary set of axioms. In this section we are going to derive some simple properties from the axioms of commutative rings, which will be useful in the rest of the chapter.

Proposition 3.1. *Let $*$ be an associative operation on a set X, i.e. $x_1 * (x_2 * x_3) = (x_1 * x_2) * x_3$, for all $x_1, x_2, x_3 \in X$. Then the result of any product $x_1 * x_2 * \ldots * x_n$ does not depend on the position of brackets.*

Proof. left as exercise for motivated students. □

Because of Proposition 3.1, we can also write sums $a_1 + a_2 + \ldots + a_n$ and products $a_1 \cdot a_2 \cdot \ldots \cdot a_n$ in rings without specifying the bracketing.

Proposition 3.2 (Basic properties of commutative rings)**.** *Let $\mathbf{R}$ be a commutative ring and $a, b, c \in R$. Then*

(1) *If $a + c = b + c$, then $a = b$;*
(2) $a \cdot 0 = 0$
(3) $-(-a) = a$, $-(a + b) = -a - b$
(4) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$, $(-a) \cdot (-b) = a \cdot b$
(5) *if $\mathbf{R}$ is an integral domain, then $a \cdot c = b \cdot c$ and $c \neq 0$ imply $a = b$.*

Proof.
(1) If $a + c = b + c$, then also $(a + c) + (-c) = (b + c) + (-c)$. By the ring axioms we get $(a + c) + (-c) = a + (c + (-c)) = a + 0 = a$, and analogously $(b + c) + (-c)$. Hence $a = b$
(2) From $0 = 0 + 0$ it follows that $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Adding 0 to the left side gives us $0 + a \cdot 0 = a \cdot 0 + a \cdot 0$, which by (1) implies $0 = a \cdot 0$.
(3) Since $0 = a + (-a) = -(-a) + (-a)$, from (1) it follows that $a = -(-a)$. For the second equation, note that $0 = (a + b) + (-(a + b))$, but also $0 = a + (-a) + b + (-b) = (a + b) + (-a - b)$, so by (1) we obtain $-(a + b) = -a - b$.
(4) To show the first identity $-(a \cdot b) = (-a) \cdot b$, note that $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$. By subtracting $a \cdot b$ on both sides we get $-(a \cdot b) = (-a) \cdot b$. All other identities can be proved similarly.
(5) If $a \cdot c = b \cdot c$, then $0 = a \cdot c - b \cdot c = (a - b) \cdot c$. Since $\mathbf{R}$ is an integral domain, either $a - b$ or c must be equal to 0. But, by assumption $c \neq 0$, so $a - b = 0$, and thus $a = b$.

□

We remark that (5) helps to study divisibility in integral domains, and will allow us to construct their "quotient fields" in the next section. We finish this section by proving:

Proposition 3.3. *Every field* $\mathbf{R}$ *is an integral domain.*

Proof. For contraiction, let us assume that there are $a, b \in R$, $a, b \neq 0$ such that $a \cdot b = 0$. But then

$$b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0,$$

which contradicts to our assumptions. Note that we used Proposition 3.2 (2) in the last equation. □

3.3. **Quotient fields.** The ring of integers can naturally be extended to the field of rational numbers by forming fractions. Similarly, the ring of polynomials $\mathbb{R}[x]$ can be extended to the field of rational functions (formal expressions like $\frac{x^2+1}{4x^3-7}$). This idea can be generalized to any integral domain $\mathbf{R}$, the resulting field is called the *quotient field* of $\mathbf{R}$. In later sections we will see how quotient fields help us in finding greatest common divisors and performing Euclid's algorithm in polynomial rings.

Definition. Let $\mathbf{R}$ be an integral domain, and $M = R \setminus \{0\}$. Then we define a relation $\sim$ on the set $R \times M$ by

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

It is not hard to see, that this is an equivalence relation: both the reflexivity and symmetry of $\sim$ follow directly from the definition. For the transitivity let $(a, b) \sim (c, d) \sim (e, f)$, so $ad = bc$ and $cf = de$. This implies $adf = bcf = bde$. Since $d \neq 0$, we can cancel by d and get $af = be$ (here we used that $\mathbf{R}$ is an integral domain). We then define the *fraction* $\frac{a}{b}$ to be the equivalence class $[(a, b)]_\sim = \{(c, d) \colon (c, d) \sim (a, b)\}$. The *quotient field* $\mathbf{Q}$ then consists of the set Q of all fractions, together with the operations/constants

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{ad}, \quad -\frac{a}{b} = \frac{-a}{b}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}, \quad 0 = \frac{0}{1}, \quad 1 = \frac{1}{1}.$$

We are going to prove that $\mathbf{Q}$ is a field. But before of that we need to check if the operations are even well-defined.

Let us discuss this for the example of the addition: First, note that the denominator ad of the sum $\frac{ad+bc}{ad}$ must be non-zero (otherwise it would not be a fraction). But this follows from $a, d \neq 0$ and the fact that $\mathbf{R}$ is an integral domain.

Secondly, we need to prove that the result of the sum $\frac{a}{b} + \frac{c}{d}$ does not depend on how we represent both fractions. So let us pick representations $\frac{a}{b} = \frac{a'}{b'}$ (equivalent to $ab' = a'b$ in $\mathbf{R}$) and $\frac{c}{d} = \frac{c'}{d'}$ (equivalent to $cd' = c'd$). We then need to prove that also $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$. In other words, we want to show that $\frac{ad+bc}{ad} = \frac{a'd'+b'c'}{a'd'}$, which by definition, is equivalent to $(a'd')(ad + bc) = (ad)(a'd' + b'c')$. But this follows straightforwardly from $ab' = a'b$ and $cd' = c'd$. The proofs for $\cdot$ and $-$ are similar.

Theorem 3.4. *Let* $\boldsymbol{R}$ *be an integral domain, and* $\mathbf{Q}$ *be its quotient field. Then* $\mathbf{Q}$ *indeed is a field.*

Proof. We simply need to check the field axioms:

- Associativity of addition: $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} + \frac{cf+de}{df} = \frac{adf+b(cf+de)}{bdf} = \frac{adf+bcf+bde}{bdf} = = \frac{ad+bc}{bd} + \frac{e}{f} = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$.
- Commutativity of addition: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$.
- additive identity: $\frac{a}{b} + \frac{0}{1} = \frac{a\cdot 1+b\cdot 0}{b\cdot 1} = \frac{a}{b}$.
- additive inverse: $\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-ab)}{b^2} = \frac{0}{b^2} = 0$.
- Associativity and Commutativity of $\cdot$: follow directly from the Associativity and Commutativity of $\cdot$ in $\mathbf{R}$
- Unity element: $\frac{a}{a} \cdot \frac{1}{1} = \frac{a\cdot 1}{a\cdot 1} = \frac{a}{a}$.
- Distributivity: $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{acf+ade}{bdf} = \frac{abcf+abde}{b^2df} = \frac{ac}{bd} + \frac{ae}{bf}$.
- $0 = \frac{0}{1} \neq 1 = \frac{1}{1}$, because $0 \cdot 1 \neq 1 \cdot 1$.
- Note that $\frac{a}{b} = 0 = \frac{0}{1}$ is equivalent to $a \cdot 1 = b \cdot 0$, and therefore to $a = 0$
- Inverse: For any $\frac{a}{b} \neq 0$, we have that $a \neq 0$ and therefore $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$. Thus $\frac{b}{a}$ is the multiplicative inverse of $\frac{a}{b}$

□

Example. The rational field $\mathbb{Q}$ can be constructed as the quotient field of the integers $\mathbb{Z}$.

4. Polynomials

4.1. **Polynomial rings.** Polynomials are the main object of study in commutative algebra. In this section we will discuss basic properties of polynomials related to divisibility and roots. We start with the definition of polynomials and polynomial rings. Throughout this section, let $\mathbf{R}$ denote a commutative ring with unity.

Definition. A *polynomial* f over $\mathbf{R}$ in a single *variable* x, is an expression of the form

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$

such that $a_0, a_1, \ldots, a_n \in R$ and $a_n \neq 0$. We also write $f = \sum_{i=0}^{n} a_i x^i$ for short. The elements $a_0, a_1, \ldots, a_n$ are called *coefficients* of f, and the symbol x the *variable*. The number n is called the *degree* of the polynomial, or $\deg f$ for short. The coefficient a_n is also called the *leading coefficient*. A polynomial is called *monic*, if the leading coefficient is 1.

Except for the above, we also consider the *zero-polynomial* $f = 0$ as a polynomial, and set $\deg(f) = -1$.

We sometimes extend the coefficients of a polynomial $f = \sum_{i=0}^{n} a_i x^i$ to an infinite sequence by setting $a_i = 0$ for all $i > n$. Using this convention we define the following operations:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{\max(n,m)} (a_i + b_i) x^i, \quad -\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} (-a_i) x^i$$

$$\sum_{i=0}^{n} a_i x^i \cdot \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{m+n} \left(\sum_{j+k=i} a_j \cdot b_k \right) x^i$$

The set of all polynomials over $\mathbf{R}$ in variable x, together with the above operations, is usually denoted by $\mathbf{R}[x]$. We are going to prove that this algebraic structure is again a commutative ring, called a *polynomial ring*:

Theorem 4.1. *Let* $\mathbf{R}$ *be a commutative ring with unity. Then*

- $\mathbf{R}[x]$ *is a commutative ring with unity.*
- *If* $\mathbf{R}$ *is an integral domain, then also* $\mathbf{R}[x]$ *is an integral domain, and* $\deg(fg) = \deg(f) + \deg(g)$*, for all polynomials* $f, g \neq 0$*.*

Proof. To check that $\mathbf{R}[x]$ is a commutative ring, we simply need to check the axioms: So let $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{i=0}^{m} b_i x^i$, $h = \sum_{i=0}^{p} c_i x^i$ be arbitrary polynomials.

- The axioms for addition (associativity, commutativity, 0) follow directly from the axioms for addition on $\mathbf{R}$, and the coefficient-wise definition of $f + g$.
- Since the multiplication in $\mathbf{R}$ is commutative, we get that the i-th coefficient of the product polynomial $f \cdot g$ is equal to
$$\sum_{j+k=i} a_j \cdot b_k = \sum_{j+k=i} b_j \cdot a_k,$$
which is the i-th coefficient of $g \cdot f$. This implies that $f \cdot g = g \cdot f$.
- The polynomial 1 is the unity element of $\mathbf{R}[x]$, since
$$f \cdot 1 = \left(\sum_{i=0}^{n} a_i x^i\right) \cdot (1 + 0 \cdot x^1 + 0 \cdot x^2 + \ldots) = \sum_{i=0}^{n} \left(\sum_{j+k=i} a_j d_k\right) x^i,$$
such that $d_0 = 1$ and $d_i = 0$ else. Thus $\sum_{j+k=i} a_j d_k = a_i$ for every i, and the resulting polynomial $f \cdot 1$ is equal to f.
- Associativity of multiplication: The product $f \cdot (g \cdot h)$ is equal to
$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\left(\sum_{i=0}^{m} b_i x^i\right) \cdot \left(\sum_{i=0}^{p} c_i x^i\right)\right) = \left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{m+p} \left(\sum_{k+l=i} b_k c_l\right) x^i\right)$$
$$= \sum_{i=0}^{n+m+p} \left(\sum_{j+k+l=i} a_j b_k c_l\right) x^i,$$
which can be shown to be equal to $(f \cdot g) \cdot h$.
- Checking the distributivity axiom is left as an exercise.

If $\mathbf{R}$ is additionally a integral domain, and $f, g \neq 0$, this means that both their leading coefficients $a_n \neq 0$ and $b_m \neq 0$. Then, the coefficient of x^{n+m} in $f \cdot g = \sum_{i=0}^{m+n} (\sum_{j+k=i} a_j \cdot b_k) x^i$ is equal to $a_n \cdot b_m$, which is not 0, since $\mathbf{R}$ is an integral domain. Thus $\deg(fg) = \deg(f) + \deg(g)$ holds, and $\mathbf{R}[x]$ is an integral domain. □

Note further that for arbitrary $f, g \in \mathbf{R}[x]$ it further holds that $\deg(f + g) \leq \max(\deg f, \deg g)$ (but in general we don't get equality; for instance $-1 = \deg(0) = \deg(x + (-x)) < \max(\deg x, \deg -x) = 1$).

Also, if $\mathbf{R}$ is not an integral domain, the formula $\deg(fg) = \deg(f) + \deg(g)$ does not hold in general. For example in $\mathbb{Z}_4[x]$ we have $\deg(2x + 1) = 1$, but $(2x + 1) \cdot (2x + 1) = 1$, which has degree 0.

Inductively, we can define polynomials rings in multiple variables by setting $\mathbf{R}[x_1, x_2, \ldots, x_m] = (\mathbf{R}[x_1, x_2, \ldots, x_{m-1}])[x_m]$. If $\mathbf{R}$ is an integral domain, also $\mathbf{R}[x_1, x_2, \ldots, x_m]$ is an integral domain, by repeatedly applying Theorem 4.1. Thanks

to the distributivity in rings, every polynomial $f \in \mathbf{R}[x_1, x_2, \ldots, x_m]$ can be rewritten to an expression

$$f = \sum_{k_1,\ldots,k_m=0}^{n} a_{k_1,\ldots,k_m} x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}.$$

(Alternatively we could have introduced $\mathbf{R}[x_1, x_2, \ldots, x_m]$ directly by introducing polynomials in m variables like this, but then we would need to reprove a version of Theorem 4.1 for multiple variables).

4.2. **Polynomial maps.**

Definition. Let $\mathbf{R} \leq \mathbf{S}$ be integral domains, and let f be a polynomial

$$f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$$

and $u \in S$. We define the *value of the polynomial f at u* by

$$f(u) = a_0 + a_1 u + \ldots + a_n x^n \in S,$$

such that operations (multiplication, addition) are computed in the ring $\mathbf{S}$. The map that is defined by

$$S \to S, \quad u \mapsto f(u)$$

is called the *polynomial map* of the polynomial f.

For example, for $\mathbf{R} = \mathbb{Z}$ and $\mathbf{S} = \mathbb{C}$, the polynomial $f = x^2 + x + 1 \in \mathbb{Z}[x]$ and $u = i$ we get $f(i) = i$. The polynomial mapping defined by f maps $u \mapsto u^2 + u + 1$ for all $u \in \mathbb{C}$.

It is often necessary to distinguish between a polynomial f (as a 'formal expression'), and the polynomial map it defines: different polynomials can represent the same polynomial function! As an example, take the polynomial $f = x^p \in \mathbb{Z}_p[x]$. By Fermat's little theorem (Corollary 2.5), $f(u) = u$ for all values $u \in \mathbb{Z}_p$. Therefore $f = x^p$ and $g = x$ are two *different* polynomials, that define the *same* polynomial map.

(In fact, over every finite ring $\mathbf{R}$, there has to be a polynomial map that is represented by *infinitely many* different polynomials $\mathbf{R}[x]$. This holds since there are infinitely many different polynomials, but only finitely many maps from $\mathbf{R}$ to $\mathbf{R}$.)

4.3. **Division of polynomials with remainder.** Let $f, g \in \mathbf{R}[x]$ be two polynomials. Then we say that g *divides* f, and write $g \mid f$ if there exists a $h \in \mathbf{R}[x]$ such that $f = gh$. If $\mathbf{R}$ is an integral domain, and $g \mid f \neq 0$, then $\deg(g) \leq \deg(f)$ by Theorem 4.1 (2). If g does not divide f, it makes sense to ask for the remainder after the division:

Proposition 4.2 (Polynomial division with remainder)**.** *Let $\mathbf{R}$ be an integral domain, $\mathbf{Q}$ its quotient field, and $f, g \in \mathbf{R}[x]$, $g \neq 0$. Then there exists exactly one pair of polynomials $q, r \in \mathbf{Q}[x]$ such that*

$$f = g \cdot q + r \text{ and } \deg r \leq \deg g.$$

Further, if g is monic, then $q, r \in \mathbf{R}[x]$.

Thanks to the uniqueness of $q$and r, we can define the quotient $f \operatorname{div} g = q$ and the remainder $f \bmod g = r$. It is easy to see that $g \mid f$ holds if and only if $f \bmod g = 0$.

Proof. We first prove the existence of such q, r by describing an algorithm that computes them (the *polynomial long division* you discussed in the exercise class). For this algorithm we set $q_0 = 0$, $r_0 = f$ and then define recursively

$$q_{i+1} = q_i + \frac{l(r_i)}{l(g)} \cdot x^{\deg r_i - \deg g}, \quad r_{i+1} = r_i - \frac{l(r_i)}{l(g)} \cdot x^{\deg r_i - \deg g} \cdot g,$$

where $l(h)$ denotes the leading coefficient of a polynomial h. We end this recursion in the step n, if $\deg r_n$ is smaller than $\deg g$. This will certainly happen, since $\deg r_{i+1} < \deg r_i$, for every i. We can easily verify by induction that $f = gq_i + r_i$ holds for every i. Therefore the polynomials $q = q_n, r = r_n$ satisfy the conditions of the theorem. Note further that, if g is monic, the denominator of every fraction $\frac{l(r_i)}{l(g)}$ is 1, and therefore, all polynomials q_i, r_i are in $\mathbf{R}[x]$.

Next, we prove the uniqueness. For this, assume that there are polynomials $r, q, r', q' \in \mathbf{Q}[x]$, such that $f = gq + r = gq' + r'$ and $\deg r, \deg r' \leq \deg g$. Then $g(q-q') = r-r'$, and therefore $g \mid r-r'$. Since $\deg(r-r') < \deg g$, we get $r'-r = 0$. So $r' = r$. Since $\mathbf{Q}[x]$ is an integral domain, and $g \neq 0$, it follows that $q - q' = 0$, and therefore $q = q'$. □

4.4. **Roots and divisibilty.**

Definition. Let $\mathbf{R} \leq \mathbf{S}$ be commutative rings, $f \in R[x]$ and $a \in S$. We then say that a is a *root* of the polynomial f, if $f(a) = 0$.

For example $i \in \mathbb{C}$ is a root of $x^2 + 1 \in \mathbb{Z}[x]$ in $\mathbb{C} \geq \mathbb{Z}$. We show that the existence of roots is related to the divisors of a given polynomial.

Proposition 4.3. *Let $\mathbf{R}$ be an integral domain, $f \in R[x]$ and $a \in R$. Then a is a root of the polynomial f if and only if $x - a \mid f$.*

Proof. ($\Leftarrow$) Assume that $x - a \mid f$. Then $f = (x - a) \cdot g$ for a polynomial $g \in R[x]$, and so

$$f(a) = (a - a) \cdot g(a) = 0 \cdot g(a) = 0,$$

which shows that a is a root of f.
($\Rightarrow$) Let $q, r \in R[x]$ be the result of the polynomial division of f by $x - a$. So $f = (x - a) \cdot q + r$ with $\deg r < \deg(x - a) = 1$. Since $\deg r < 1$, r needs to be a constant polynomial. Note also that, since $x - a$ is monic, we get that $q, r \in R[x]$. By looking at the value of f at a we get

$$0 = f(a) = (a - a)q(a) + r(a) = 0 \cdot q(a) + r = r,$$

thus $r = 0$ and $x - a \mid f$. □

In the above proof we showed a fact that can be useful in general, namely that for every $f \in R[x]$ and $a \in R$:

$$f \bmod (x - a) = f(a).$$

We are going to use this fact in discussing interpolation in Section 8.1.

Next we prove that the degree of a polynomial gives us a bound on the number of roots:

Theorem 4.4 (Number of roots of a polynomial)**.** *Let $\mathbf{R}$ be an integral domain, and let $0 \neq f \in R[x]$ be a polynomial with $\deg f = n$. Then f has at most n roots in $\mathbf{R}$.*

Proof. We prove this by induction on the degree n. If $\deg f = 0$, then f is constant (and $f \neq 0$), so f has no roots. For an induction step $n \to n+1$, let $\deg(f) = n+1$. If f has no roots, then clearly the statement holds. So let us assume that there is a $a \in R$ with $f(a) = 0$. Then, by Proposition 4.3, there is a polynomial g with $f = (x-a)\cdot g$ and $\deg(g) = n$. If $b \neq a$ is another root of f, then $f(b) = (b-a)\cdot g(b) = 0$. Since $\mathbf{R}$ is an integral domain, it follows that $g(b) = 0$. Therefore every root of f is either a, or a root of g. By the induction hypothesis, g has at most n roots, so f has at most $n+1$ roots. □

Note that the number of roots of f can also be less than $\deg(f)$. For example $x^2 + 1$ has no roots, when seen as a polynomial over $\mathbb{Z}$. It has exactly one root, when seen as polynomial over $\mathbb{Z}_2$.

Theorem 4.4 only holds for integral domains $\mathbf{R}$, but not commutative rings in general (the proof fails, since then $f(b) = (b-a)\cdot g(b) = 0$ does not imply that $b - a = 0$ or $g(b) = 0$). For example, the polynomial $2x \in Z_4[x]$ has two roots $0, 2 \in \mathbb{Z}_4$, and the polynomial $x^2 + x \in \mathbb{Z}_6[x]$ has four roots $0, 2, 3, 5 \in \mathbb{Z}_6$.

5. Basic notions of divisibility

In this section, we introduce basic concepts such as divisibility, associated elements, the greatest common divisor and irreducible decompositions for polynomials. We define these concepts for the general integral domains $\mathbf{R}$ and we will illustrate them in the specific cases: for fields, for the integers $\mathbb{Z}$, for quadratic extensions $\mathbb{Z}[\sqrt{s}]$, and in particular for polynomial rings.

5.1. **Divisors and associates.**

Definition. We say that a *divides* b in the ring $\mathbf{R}$, and write $a \mid b$, if there exists an element $c \in R$, such that $b = ac$.

Caution: When talking about divisibility, the ring $\mathbf{R}$ always should be mentioned or be clear from the context. since the relations $\mid$ depends on the ring.For example

- $3x + 6 \mid x + 2$ in $\mathbb{Q}[x]$, because $x + 2 = \frac{1}{2} \cdot (3x + 6)$, but
- $3x + 6 \nmid x + 2$ in $\mathbb{Z}[x]$, because there exists no $f \in \mathbb{Z}[x]$, such that $x + 2 = f \cdot (3x + 6)$.

Definition. We say that a and b are *associates* or *associated elements*, and write $a \parallel b$, if $a \mid b$ and $b \mid a$. An element a is called *invertible* if and only if $a \parallel 1$. We then write a^{-1} for the *inverse of* a, that is, the element b such that $ab = 1$.

The divisibility relation $\mid$ is reflexive and transitive (so $a \mid b$ and $b \mid c$ implies $a \mid c$). Note that $\parallel$ is additionally symmetric, and therefore an equivalence relation.

Proposition 5.1. *Let* $\mathbf{R}$ *be an integral domain and* $a, b \in R$*. Then* $a \parallel b$ *if and only if there is an invertible element* $q \in R$ *such that* $a = bq$*.*

Proof. ($\Leftarrow$) Since $a = bq$ clearly $b \mid a$. On the other hand $b = aq^{-1}$, implies $a \mid b$. ($\Rightarrow$) If $a = 0$, then $a \parallel b$ implies $b = 0$ (and thus $a = b \cdot 1$). So let us assume that $a \neq 0$. Since $a \parallel b$ there are elements u, v such that $a = bu$ and $b = av$. Therefore $a = bu = avu$. By cancelling a we get $1 = vu$, and therefore u, v are invertible elements. □

Example.

- In a field, every nonzero element has an inverse. Therefore $a \parallel b$ for all $a, b \neq 0$.
- In the ring of integers $\mathbb{Z}$, the invertible elements are ± 1. Thus $a \parallel b$ is equivalent to $a = \pm b$.
- In every polynomial ring $\mathbf{R}[x]$, the invertible elements are exactly the polynomials $f = a_0$ of degree 0, whose coefficient a_0 is an invertible element of $\mathbf{R}$. So, if $\mathbf{R}$ is a field, all constant non-zero polynomials are invertible.
  For example in $\mathbb{Z}[x]$ we have $f \parallel g$ if $f = \pm g$. In $\mathbb{Q}[x]$ we have $f \parallel g$ if and only if $f = c \cdot g$, for some $0 \neq c \in \mathbb{Q}$.

In integral domains it is in general not possible to define a division with remainder, because we have no way of expressing that the remainder should be 'smaller' than a divisor. Still, it makes sense to define the congruence

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \mid a - b.$$

As for the integers (see Proposition 2.1), it is easy to show that for a fixed $m \in R$ this is an equivalence relation, which is invariant under $+, -, \cdot$. Later, in Section 7.2, we will see that a result similar to Proposition 2.2 holds if $\mathbf{R}$ is a so-called *Euclidean domain*.

5.2. **Greatest common divisor.**

Definition. Let $\mathbf{R}$ be a ring and $a, b, c \in \mathbf{R}$. We say that c is the *greatest common divisor of* a, b, and write $c = \gcd(a, b)$ if

- $c \mid a$, $c \mid b$ (so c is a common divisor of a and b)
- whenever $d \mid a$, $d \mid b$, then also $d \mid c$ (so c is the 'greatest' such).

We call a, b *coprime* if $\gcd(a, b) = 1$. The *least common multiple* $\operatorname{lcm}(a, b)$ is defined analogously.

Caution: The greatest common divisor, according to the above definition, must be handled with some care. For example in the ring of integers $\mathbb{Z}$ both $2 = \gcd(4, 6)$ and $-2 = \gcd(4, 6)$ satisfy the above condition, so there is not a unique greatest common divisor.

But, fortunately, the situation is not too bad: $\gcd(a, b)$ is unique up to associated elements. On one hand, if $c_1 = \gcd(a, b)$ and $c_2 = \gcd(a, b)$ then c_1 and c_2 are common divisors of a and b; by the second condition then $c_1 \mid c_2$ and $c_2 \mid c_1$, so they must be associated. On on the other hand, if $c_1 = \gcd(a, b)$ and $c_2 \parallel c_1$, then $c_2 = qc_1$ for an invertible element q, and therefore also satisfies Definition 5.2.

However there is another problem: In certain integral domains, it might happen that there is *no* element c that meets the criteria in Definition 5.2. For example, in the ring $\mathbb{Z}[\sqrt{5}]$, no greatest common divisor exists for

$$a = 4, \quad b = 2 + 2\sqrt{5}.$$

First note that $r = 2$ and $s = 1 + \sqrt{5}$ are common divisors of a and b, since $a = 2 \cdot 2 = (-1 - \sqrt{5})(1 - \sqrt{5})$, and $b = 2 \cdot (1 + \sqrt{5})$. But neither of them is 'bigger' ($r \nmid s$ and $s \nmid r$), and it can be shown that no z exists, such that $r, s \mid z$ and $z \mid a, b$.

5.3. **Irreducible polynomials and decompositions.** Let $\mathbf{R}$ be a ring. For every $a \in \mathbf{R}$ it then holds that $a \mid a$ and $1 \mid a$. A divisor of a is called a *trivial divisor* if it is an associated element of either 1 or a. All other divisors are called non-trivial.

Definition. An element $a \in \mathbf{R}$ is called *irreducible* if $a \neq 0$, $a \nparallel 1$ and it only has trivial divisors. In this case $a = bc$ implies that $b \parallel 1$ or $c \parallel 1$.

Example.

- There are no irreducible elements in a field (all non-0 elements are invertible!)
- In the ring $\mathbb{Z}$ the irreducible elements are exactly the numbers $\pm p$, where p is a prime.
- In a polynomial ring $\mathbf{R}[x]$ it is generally not easy to determine which polynomials are irreducible. But it always holds that:
  - a polynomial of degree 0 is irreducible if and only if it is an irreducible element of $\mathbf{R}$
  - a polynomial of degree 1 is irreducible if and only if it is not divisible by a non-invertible element of $\mathbf{R}$ (e.g. the polynomial $2x+2$ is irreducible in $\mathbb{Q}[x]$, but not in $\mathbb{Z}[x]$, since $2x + 2 = 2 \cdot (x + 1)$).

If $f \in \mathbf{R}[x]$ is a polynomial of degree ≥ 2, which has root a, then it cannot be irreducible because it has the non-trivial divisor $x - a$ (see Proposition 4.3). But caution: the opposite implication does not hold. For instance the polynomial $x^4 + 2x^2 + 1 \in \mathbb{Z}[x]$ has no root, but is not irreducible since $x^4 + 2x^2 + 1 = (x^2 + 1) \cdot (x^2 + 1)$. There is no general rule for polynomials of higher degrees, the situation depends on $\mathbf{R}$:

Example.

- In $\mathbb{C}[x]$ the irreducible polynomials are exactly the polynomials of degree 1 (by the *Fundamental Theorem of Algebra*)
- In $\mathbb{R}[x]$ the irreducible polynomials are the polynomials of degree 1 and the polynomials of degree 2, which don't have a root (left as exercise).
- In $\mathbb{Q}[x]$ there are polynomials of higher degree that are irreducible. For example $x^n - 2$ is irreducible for every $n \geq 2$ (see Eisenstein's criterion in Theorem 6.10). In general, it is not easy to determine if a polynomial over $\mathbb{Q}[x]$ is irreducible.

Example. Some primes (in $\mathbb{Z}$) are not irreducible in the Gaussian integers $\mathbb{Z}[i]$. For example $5 = (1 + 2i)(1 - 2i)$. It can be shown that the irreducible Gaussian integers are of the form:

- $\pm a$ and $\pm ia$, if a is a prime number and $a \equiv 3 \pmod 4$, or
- $a + ib$, such that $b \neq 0$ and $a^2 + b^2$ is a prime number.

Definition. Let $\mathbf{R}$ be a ring, and $a \in \mathbf{R}$. A *decomposition of a into irreducible elements* is a product $p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$ such that

$$a \parallel p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n},$$

$p_1, \ldots, p_n \in \mathbf{R}$ are irreducible, $p_i \nparallel p_j$ for all $i \neq j$, and $k_1, \ldots, k_n \in \mathbb{N}$. We say that a has a *unique* decomposition into irreducible elements, if

$$a \parallel p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n} \parallel q_1^{l_1} \cdot q_2^{l_2} \cdot \ldots \cdot q_m^{l_m}$$

implies that $m = n$, and there is a permutation π of the indices, such that $p_i \parallel q_{\pi(i)}$ and $k_i = l_{\pi(i)}$, for all i.

The seemingly complicated definition can be motivated by the following example in $\mathbb{Z}$: $12 = 2^2 \cdot 3 = 3^1 \cdot (-2)^2 \parallel (-2)^2 \cdot (-3)$. These are, formally speaking, 3 different decompositions of 12, but it still makes sense to consider them to be the same, since they only differ by the order and the sign $\pm$ of the individual irreducible factors.

When talking about decompositions into irreducible factors again the ring $\mathbf{R}$ matters (and thus must be explicitly mentioned, or be clear from the context). For example the polynomial $2x^2 + 2$ is irreducible in $\mathbb{Q}[x]$ but decomposes into the irreducibles $2 \cdot (x + 1)$ in $\mathbb{Z}[x]$.

Example. The following table shows the decompositions of some polynomials into irreducible factors (in 5 different polynomial rings):

	$x^2 + 1$	$2x^2 + 2$	$x^2 - 2$	$x^4 + 2x^2 + 1$
$\mathbb{Z}[x]$	irreducible	$2 \cdot (x^2 + 1)$	irreducible	$(x^2 + 1)^2$
$\mathbb{Q}[x]$	irreducible	irreducible	irreducible	$(x^2 + 1)^2$
$\mathbb{R}[x]$	irreducible	irreducible	$(x - \sqrt{2})(x + \sqrt{2})$	$(x^2 + 1)^2$
$\mathbb{C}[x]$	$(x - i)(x + i)$	$(2x - 2i)(x + i)$	$(x - \sqrt{2})(x + \sqrt{2})$	$(x - i)^2(x + i)^2$
$\mathbb{Z}_5[x]$	$(x + 2)(x + 3)$	$(x + 2)(2x + 1)$	irreducible	$(x + 2)^2(x + 3)^2$

In general integral domains, decompositions don't need to exist and don't need to be unique, as can be seen from the following two examples:

Example (Ring without decompositions)**.** Let $\mathbf{R}$ be the subring of $\mathbb{Q}[x]$ consisting of all the polynomial, whose coefficient a_0 is an integer. In this ring, the element $f = x$ does not have a decomposition into irreducible factors: To see this let us assume for contradiction, that g is an irreducible factor of f. Since $g \mid f$, either g is a constant or of the form $g = \frac{1}{a}x$ for some $a \in \mathbb{Z} \setminus \{0\}$ (since $f = a \cdot (\frac{1}{a}x)$). However, $g = \frac{1}{a}x$ is not irreducible, since it can always be further decomposed into $\frac{1}{a}x = 2 \cdot \frac{1}{2a}x$. Thus all irreducible factors of x must be constant, which is also not possible - contradiction!

Example (Ring with no unique decompositions)**.** In the ring $\mathbb{Z}[\sqrt{5}]$, the element 4 has two decompositions

$$4 = 2^2 = (1 + \sqrt{5})(-1 + \sqrt{5}).$$

It can be shown that $2, (1+\sqrt{5})$ and $(-1+\sqrt{5})$ are all irreducible and not associated to each other.

It therefore makes sense to define integral domains, in which every element has a unique decomposition into irreducible elements:

Definition. An integral domain is called a *unique factorization domain* (UFD) if every element that is not equal to 0, nor invertible has a unique decomposition into irreducible factors.

Example.

- Every field is a UFD (since element is either invertible or equal to 0)
- The integers $\mathbb{Z}$ are a UFD (by Theorem 1.2).

- If $\mathbf{R}$ is a field, then the polynomial ring $\mathbf{R}[x]$ is a UFD. The proof is similar to the proof for $\mathbb{Z}$, we are going to discuss it later (Theorem 6.4). By Gauss's theorem (Theorem 6.8) also the polynomial rings over a field in more than one variable are a UFDs, and $\mathbb{Z}[x]$ is a a UFD.
- Some rings $\mathbb{Z}[\sqrt{s}]$ are UFDs (e.g. for $s = -1, \pm 2, 3$), while some other are not (e.g. $s = -3, 5$). We will not discuss them further here.

5.4. **Divisibility in unique factorization domains.** The existence and uniqueness of a decomposition into irreducible element is a very powerful property. In this section we discuss some consequences for UFDs, that are mainly based on the following result:

Proposition 5.2. *Let $\mathbf{R}$ be a UFD, and $a, b \in R$, such that a has the following decomposition into irreducible elements:*

$$a \parallel p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}.$$

Then $b \mid a$ if and only if

$$b \parallel p_1^{l_1} \cdot \ldots \cdot p_n^{l_n},$$

for some $0 \leq l_i \leq k_i$.

Proof. ($\Leftarrow$) By assumption, there are invertible elements $q, r \in R$, such that $a = qp_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ and $b = rp_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$. If we define $c = qr^{-1}p_1^{k_1 - l_1} \cdot \ldots \cdot p_n^{k_n - l_n}$, then we can see that $a = bc$, and thus $b \mid a$.
($\Rightarrow$) Let $c \in R$ be an element such that $a = b \cdot c$, and let

$$b \parallel q_1^{s_1} \cdot \ldots \cdot q_u^{s_u}, \quad c \parallel r_1^{t_1} \cdot \ldots \cdot r_v^{t_v}$$

be the decompositions of b and c into irreducible elements. Then

$$a \parallel p_1^{k_1} \cdot \ldots \cdot p_n^{k_n} \parallel q_1^{s_1} \cdot \ldots \cdot q_u^{s_u} \cdot r_1^{t_1} \cdot \ldots \cdot r_v^{t_v}.$$

Note that the product on the right side is not necessarily a decomposition of a into irreducible elements, since some of the q_i and r_j might be equal (up to association). But, by combining these duplicates, we obtain another decomposition into irreducibles

$$a \parallel p_1^{k_1} \cdot \ldots \cdot p_n^{k_n} \parallel q_1^{s_1'} \cdot \ldots \cdot q_u^{s_u'} \cdot r_{i_1}^{t_{i_1}} \cdot \ldots \cdot r_{i_w}^{t_{i_w}}.$$

By the uniqueness of the factorization, for every $i \in \{1, 2, \ldots, u\}$ there exists a $j \in \{1, 2, \ldots, n\}$, such that $q_i \parallel p_j$, and $s_i \leq s_i' = k_j$. From this, it follows that $b \parallel p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$, for $l_i = s_i \leq k_i$. □

A direct consequence of Proposition 5.2 is that in UFDs the greatest common divisor of two elements always exists: It is enough to take a decomposition of both elements into irreducibles, and take the product of all irreducible factors that both decompositions have in common (up to associates). We have already seen this for the integers and their prime factorization:

$$\begin{aligned}\gcd(540, 336) &= \gcd((-2)^2 \cdot 3^3 \cdot 5, 2^4 \cdot (-3) \cdot 7) \\ &= \gcd(2^2 \cdot 3^3 \cdot 5^1 \cdot 7^0, 2^4 \cdot 3^1 \cdot 5^0 \cdot 7^1) = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 12\end{aligned}$$

In UFDs also an analogue to Lemma 1.5 holds: whenever an irreducible element p divides a product ab, then it already has to divide one of the factors. We prove these properties for general UFDs in the following Corollary of Proposition 5.2:

Corollary 5.3. *Let $\mathbf{R}$ be an UFD. Then*

(1) *For all $a, b \in R$, there exist the greatest common divisor* $\gcd(a, b)$.
(2) *If $p \in R$ is irreducible, and $p \mid ab$ then $p \mid a$ or $p \mid b$.*
(3) *There is no infinite sequence $a_1, a_2, a_3, \ldots \in R$ such that $a_{i+1} \mid a_i$ and $a_{i+1} \nmid a_i$.*

Proof. (1) Let us take irreducible elements $p_1, \ldots, p_n$ such that $p_i \nmid p_j$ for $i \neq j$ and $k_i, l_i \geq 0$ such that

$$a \parallel p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}, \quad b \parallel p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}.$$

(arbitrary decompositions of a, b into irreducible elements can be rewritten in such a way, by adding the 0-th powers of some p_i as a factor, if necessary). By Proposition 5.2, whenever $c \mid a, c \mid b$, then $c \parallel p_1^{m_1} \cdot \ldots \cdot p_n^{m_n}$ for exponents m_i that satisfy $0 \leq m_i \leq k_i$ and $0 \leq m_i \leq l_i$ for all $i = 1, \ldots, n$. In other words, $0 \leq m_i \leq \min(k_i, l_i)$, for every $i \in \{1, \ldots, n\}$. So the *greatest* common divisor c is given by the exponents $m_i = \min(k_i, l_i)$.
(2) As in (1), we can find irreducible elements p_i, and $k_i, l_i \geq 0$ such that $a \parallel p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, and $b \parallel p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$. Therefore $ab \parallel p_1^{k_1+l_1} \cdot \ldots \cdot p_n^{k_n+l_n}$. Since $p \mid ab$, by Proposition 5.2, also p must decompose into a product of powers of the irreducible elements $p_1, \ldots, p_n$. But since p is irreducible itself, there must be a i such that $p \parallel p_i$. As a consequence either $p \mid a$ holds (if $k_i > 0$), or $p \mid b$ (if $l_i > 0$).
(3) Each non-zero, non-invertible element a has a unique decomposition into irreducibles $a \parallel p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$. Therefore, we can assign to it the number $\nu(a) = k_1 + k_2 + \ldots + k_n$. We further set $\nu(a) = 0$ if a is invertible. It follows from the uniqueness of the decomposition, that $\nu(a)$ is well-defined. From Proposition 5.2 it follows that $a \mid b$ implies $\nu(a) \leq \nu(b)$, and $a \parallel b$ implies $\nu(a) = \nu(b)$.

For a contradiction assume now that there is a sequence $a_1, a_2, a_3, \ldots \in R$ such that $a_{i+1} \mid a_i$ and $a_{i+1} \nmid a_i$. This means that $\nu(a_1) > \nu(a_2) > \nu(a_3) > \cdots$, which is not possible (there is no infinite descending sequence of natural numbers) - contradiction! □

It is not hard to see that the results of this section do not hold in integral domains that are not UFDs:

Example. In $\mathbb{Z}[\sqrt{5}]$, the element 2 is irreducible, and $2 \mid (\sqrt{5}-1)(\sqrt{5}+1) = 4$. However $2 \nmid (\sqrt{5}-1), 2 \nmid (\sqrt{5}+1)$.

The fact that there are examples of rings, in which both gcd does not exists, and decomposition into irreducible are not unique is, in fact, not a coincidence. We are going to discuss this further in Section 7.1.

6. Divisibility in polynomial rings

6.1. **Polynomials in one variable over a field.** In this next section, we show (analogous to Section 1) that polynomials in *one* variable over a *field* $\mathbf{F}$ always have a unique decomposition into irreducible elements. In other words, $\mathbf{F}[x]$ is a UFD. The proofs are mostly analogous to the proofs for the integers $\mathbb{Z}$ in Section 1. Therefore we leave them an exercise.

Exercise 6.1. *Recall the description of the Euclidean algorithm in Section 1, and convince yourself that it also works for the polynomial ring $\mathbf{F}[x]$, when $\mathbf{F}$ is a field (using the polynomial division from Proposition 4.2).*

Why doesn't it work for the polynomials over a general integral domain? Why doesn't it work for polynomials in more than one variable?

Based on Euclid's algorithm, you can prove the following statement:

Proposition 6.2 (Bézout coefficients)**.** *Let* $\mathbf{F}$ *be a field. Then, for any two polynomials* $f, g \in F[x]$*, there exists a greatest common divisor* $\gcd(f, g)$*, and there exists polynomials* $r, s \in F[x]$ *(*Bézout coefficients*) such that*

$$\gcd(f, g) = r \cdot f + s \cdot g.$$

Example. The two polynomials $f = \frac{1}{3}x^2 + x = \frac{1}{3}x(x+3)$ and $g = x^2 + 2x - 3 = (x-1)(x+3)$ in $\mathbb{Q}[x]$ have the greatest common divisor $\gcd(f, g) = x + 3$, which is equal to $3f - g$.

Unfortunately we cannot relax the condition in Proposition 6.2 to general integral domains, or to polynomials of more than one variable:

Example. For polynomials $f, g \in \mathbb{Z}[x]$, in general, there are no Bézout coefficients. For example $\gcd(x+1, x-1) = 1$, however there are no polynomials $r, s \in \mathbb{Z}[x]$ such that $r \cdot (x+1) + s \cdot (x-1) = 1$, since $2r(1) = 1$, which can never happen for an integer polynomial r.

Example. For polynomials $f, g \in \mathbb{Q}[x, y]$, in general, there are no Bézout coefficients. For example $\gcd(x, y) = 1$, however there are no polynomials $r, s \in \mathbb{Q}[x, y]$ such that $r \cdot x + s \cdot y = 1$, since $r \cdot x + s \cdot y$ evaluated at $(0, 0)$ is always 0.

The good news is, that even in these polynomial rings, there always exists a greatest common divisor $\gcd(f, g)$ of two polynomials f, g, however this is not easy to prove. We will show it in the next subsections.

We continue with the prove for $\mathbf{F}[x]$:

Exercise 6.3. *Recall the proof of the fundamental theorem of arithmetic from Section 1, and think about how to modify it, so that it also works for* $\mathbf{F}[x]$*. We proved both the existence, and the uniqueness of the prime factorization by induction on the size of* $n \in \mathbb{N}$*. On what parameter should be base our induction for* $\mathbf{F}[x]$*? Why does the proof fail for* $\mathbb{Z}[x]$ *and* $\mathbb{Q}[x, y]$ *- and which are the properties we need for it to work?*

With the above exercise, you can prove the following analogy to the fundamental theorem of arithmetic:

Theorem 6.4. *Let* $\mathbf{F}$ *be a field. Then* $\mathbf{F}[x]$ *is a unique factorization domain.*

6.2. **Polynomials over a ring vs. polynomials over a quotient field.** We next are going to prove Gauss's theorem, which states that $\mathbf{R}[x]$ is even UFD if $\mathbf{R}$ is a UFD. The proof is based on the studying the divisibility in the extension $\mathbf{Q}[x]$, where $\mathbf{Q}$ is the quotient field of $\mathbf{R}$.

Definition. Let us call a polynomial $f = \sum_{i=0}^{n} a_i x^i \in \mathbf{R}[x]$ *primitive*, if $\gcd(a_1, \ldots, a_n) = 1$ (i.e. whenever an element c divides all coefficients, then $c \parallel 1$).

For example $2x^5 + 6x - 3$ is a primitive polynomial in $\mathbb{Z}[x]$.

The polynomial $x^2y + x$ is not primitive when seen as an element from $(\mathbb{Z}[x])[y]$ (since $\gcd(x^2, x) = x$), but it is primitive an element from $(\mathbb{Z}[y])[x]$ (since $\gcd(y, 1) = 1$). An important ingredient for our proof is then the following lemma about primitive polynomials:

Lemma 6.5 (Gauss' lemma)**.** *Let* $\mathbf{R}$ *be a UFD and* $f, g \in \mathbf{R}[x]$ *be primitive polynomials. Then* fg *is also a primitive polynomial.*

Proof. Let $f = \sum_{i=0}^{n} a_i x^i$ and $g = \sum_{i=0}^{m} b_i x^i$ be primitive. We then want to show that also fg is a primitive polynomial. For contradiction, assume that this is not true. Then (since $\mathbf{R}$ is a UFD) there is an irreducible element $p \in R$, which divides all the coefficients of fg. Let us choose the smallest j, such that $p \nmid a_j$ and the smallest k such that $p \nmid b_k$ (there must be such indices, since both f and g are primitive). The $(j+k)$-th coefficient of fg is then equal to

$$c_{j+k} = a_0 b_{j+k} + \cdots a_{j-1} b_{k+1} + a_j b_k + a_{j+1} b_{k-1} + \cdots + a_{j+k} b_0.$$

Because $p \mid a_i$ for all $i < j$ we get

$$p \mid a_0 b_{j+k} + \cdots + a_{j-1} b_{k+1}.$$

But since $p \mid b_i$ for all $i < k$ we get

$$p \mid a_{j+1} b_{k-1} + \cdots + a_{j+k} b_0.$$

So in the sum defining c_{j+k}, all summands to the left and to the right of $a_j b_k$ are multiples of p. However $a_j b_k$ is not divisible by p (by Corollary 5.3 (2)), and therefore also $p \nmid c_{j+k}$, which contradicts to our assumption that p divides all coefficients of fg. □

Gauss's lemma allows us to compare the divisibilty in $\mathbf{R}[x]$ and $\mathbf{Q}[x]$, which will be essential for the remaining proof.

Lemma 6.6. *Let* $\mathbf{R}$ *be a UFD,* $\mathbf{Q}$ *be its quotient field and* $f, g \in \mathbf{R}[x]$ *be primitive polynomials. Then*

$$f \mid g \text{ in } \mathbf{Q}[x] \quad \Leftrightarrow \quad f \mid g \text{ in } \mathbf{R}[x]$$

Proof. Clearly the implication ($\Leftarrow$) holds, as $\mathbf{R}[x]$ is a subring of $\mathbf{Q}[x]$.
For the other direction ($\Rightarrow$), since $f \mid g$ in $\mathbf{Q}[x]$, there is a polynomial $h \in \mathbf{Q}[x]$, such that $g = fh$. Let h be such a polynomial and choose $q \in Q$ such that qh is a primitive polynomial (it is enough to take $q = \frac{a}{b}$ where a is the gcd of the denominators and b is the gcd of the numerators of all coefficients of the polynomial h). Thus $g = fh$ implies $qg = f \cdot qh$, where on the right side we have the product of two primitive polynomials over $\mathbf{R}$. By Gauss's lemma also qg must be primitive, therefore $q \parallel 1$. It follows, that h is already a polynomial from $\mathbf{R}[x]$. □

The next theorem follows straight from the above lemma, we omit the proof:

Theorem 6.7 (gcd and irreducible elements in UFDs)**.** *Let* $\mathbf{R}$ *be a unique factorization domain,* $\mathbf{Q}$ *its quotient field, let* $f, g \in \mathbf{R}[x]$ *and let* c_f *(respectively* c_g*) be the greatest common divisor of the coefficients of* f *(respectively* g*). Then*

(1) $\gcd_{\mathbf{R}[x]}(f, g)$ *exists and is equal to the product* $c \cdot h$*, where* $c = \gcd_{\mathbf{R}}(c_f, c_g)$*, and* h *is the primitive polynomial in* $\mathbf{R}[x]$ *satisfying* $h = \gcd_{\mathbf{Q}[x]}(f/c_f, g/c_g)$.
(2) f *is irreducible in* $\mathbf{R}[x]$ *if and only if*
   - $\deg f = 0$ *and* f *is irreducible in* $\mathbf{R}$*, or*
   - $\deg f > 0$ *and* f *is primitive and irreducible in* $\mathbf{Q}[x]$.

Example. Consider the integer polynomials

$$f = 4x^2 + 8x + 4 = 4(x^2 + 2x + 1), \quad g = -6x^2 + 6 = -6(x^2 - 1).$$

Then $\gcd_{\mathbb{Z}}(4, -6) = 2$, $\gcd_{\mathbb{Q}[x]}(x^2+2x+1, x^2-1) = x+1$, and therefore $\gcd_{\mathbb{Z}[x]}(f, g) = 2 \cdot (x + 1)$.

We can use point (2) of Theorem 6.7 to show the existence of irreducible decompositions in $\mathbf{R}[x]$. It is though a bit complicated because we don't have Bézout's identity. In Section 7.1 we will show how to work around it and get (as an immediate consequence of Theorem 6.7 and Theorem 7.1) the following theorem:

Theorem 6.8 (Gauss's theorem)**.** *If* $\mathbf{R}$ *is a UFD, then also* $\mathbf{R}[x]$ *is a UFD.*

By multiple application of Gauss's theorem, it immediately follows that polynomials in arbitrarily many variables over a UFD (for example, the fields $\mathbb{Z}[x, y, \ldots]$, or $\mathbf{F}[x, y, \ldots]$ for any field $\mathbf{F}$) are also a UFD.

6.3. **Rational roots and Eisenstein's criterion for irreducibility.** You maybe know the following trick to find the rational roots of a polynomial from school, but you probably didn't realize that, to prove it, you need to work in unique factorization domains:

Proposition 6.9. *Let* $\mathbf{R}$ *be a UFD, and let* $\mathbf{Q}$ *be its quotient field. Let* $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ *and* $\frac{r}{s} \in Q$ *be a root (such that* $r, s \in R$ *are coprime). Then* $r \mid a_0$ *and* $s \mid a_n$*.*

Proof. If we look at the value of f at the root $\frac{r}{s}$, we get $\sum_{i=0}^{n} a_i (\frac{r}{s})^i = 0$. Multiplying with s^n then gives us the equation

$$a_0 s^n + a_1 r s^{n-1} + \ldots a_{n-1} r^{n-1} s + a_n r^n = 0.$$

Because r divides all elements $a_1 r s^{n-1}, a_2 r^2 s^{n-2}, \ldots, a_n r^n$, it also must divide $a_0 s^n = -(a_1 r s^{n-1} + \ldots a_{n-1} r^{n-1} s)$. But since r and s are coprime, it must divide a_0 (here we use that $\mathbf{R}$ is a UFD). Analogously s divides $a_0 s^n, a_1 r s^{n-1}, \ldots, a_{n-1} r^{n-1} s$, and therefore $s \mid a_n r^n$. Since r and s are coprime, $s \mid a_n$. □

Example. We find all the rational roots $\frac{r}{s}$ of the polynomial $f = 2x^5 - 3x^4 + 2x - 3$. By Proposition 6.9 $r \mid 3, s \mid 2$,so we get as candidates ± 1, ± 3, $\pm\frac{1}{2}$, $\pm\frac{3}{2}$. Computing the values of f at these numbers we see that $-\frac{3}{2}$ is the only rational root of f.

Example. By Proposition 6.9, any rational root of the polynomial $x^n - p$, for a prime p, must be of the form ± 1 or $\pm p$. But it is easy to check that none of these numbers are actually roots (if $n \geq 2$). Therefore, the root $\sqrt[n]{p}$ must be irrational (for every prime p, $n \geq 2$).

A similar trick gives us Eisenstein's criterion for irreducibility:

Theorem 6.10 (Eisenstein's criterion)**.** *Let* $\mathbf{R}$ *be a UFD, and let* $f = \sum_{i=0}^{n} a_i x^i$ *be a primitive polynomial in* $\mathbf{R}[x]$*.If there exists an irreducible element* $p \in R$*, such that* $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$*, and* $p^2 \nmid a_0$*, then* f *is irreducible in* $\mathbf{R}[x]$*.*

Proof. For contradiction, assume that $f = gh$ for two polynomials $g = \sum_{i=0}^{k} b_i x^i$, $h = \sum_{i=0}^{l} c_i x^i$ of degree at least 1. Since p divides $a_0 = b_0 c_0$, either $p \mid b_0$ or $p \mid c_0$ (by Corollary 5.3 (2)). However, by assumption $p^2 \nmid a_0$, therefore it is not possible that both b_0 and c_0 are divisible by p. Without loss of generality, let us assume that $p \mid b_0$, but $p \nmid c_0$. Then, since $p \mid a_1 = b_0 c_1 + b_1 c_0$, and $p \nmid c_0$, we get $p \mid b_1$. Since $p \mid a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$, and $p \mid b_0, b_1$, $p \nmid c_0$, we get $p \mid b_2$. By induction we get that all coefficients b_i of g are divisible by p. Therefore $p \mid g \mid f$, and thus f is not a primitive polynomial - contradiction! □

Example. By Eisenstein's criterion, the polynomial $x^n - p$, for a prime p, is irreducible in $\mathbb{Z}[x]$ (and thus also in $\mathbb{Q}[x]$).

7. Abstract divisibility theory

7.1. **Generalization of the fundamental theorem of arithmetic.** In this section we finish the discussion about divisibility, and show some results for integral domains in general. We are first going to characterize UFDs by two properties of their divisibility relation $|$, which will then allow us to finish the proof of Gauss's theorem.

Theorem 7.1. *Let* $\mathbf{R}$ *be an integral domain. Then* $\mathbf{R}$ *is a unique factorization domain if and only if*

(1) $\gcd(a, b)$ *exists for every pair of elements* $a, b \in R$*, and*
(2) *there is no infinite sequence* $a_1, a_2, a_3, \ldots \in R$*, such that* $a_{i+1} \mid a_i$ *and* $a_{i+1} \nmid a_i$ *for every* i*.*

Theorem 7.1 is interesting, since it gives a different characterization of UFDs that does not talk about decompositions. This can be very useful, since in practise (1) and (2) are often easier to check, than showing that every element has a unique factorization into irreducibles.

We already showed in Corollary 5.3 that every UFD has the properties (1) and (2). So in order to prove Theorem 7.1, we only need to prove that every integral domain that satisfies (1) and (2) is a UFD, i.e. every element has a unique factorization into irreducible elements. The proof will follow the same lines as Section 1. Showing the existence part is not hard. However, to prove the uniqueness will a bit more complicated, since we cannot use Bézout's identity (as we did for $\mathbb{Z}$ or $\mathbf{F}[x]$).

Proof of the existence of factorizations. Let $\mathbf{R}$ be an integral domain and let us assume that there is an element $a \in R$ with $a \neq 0$, $a \nmid 1$ that does not have a decomposition into irreducibles. We are then going to prove that (2) cannot hold. For this we recursively define a sequence $a_1, a_2, a_3, \ldots \in R$, such that for every $i \in \mathbb{N}$, a_i has no decomposition, and $a_{i+1} \mid a_i$ and $a_{i+1} \nmid a_i$.

- We set $a_1 = a$.
- For a general $i \in \mathbb{N}$, assume that we already constructed an element a_i that does not have a decomposition into irreducibles. In particular, a_i cannot be irreducible itself. Thus, there are two elements b, c, such that $b, c \nmid 1$ and $a_i = b \cdot c$. Either b or c has no decomposition into irreducibles (otherwise, $a_i = b \cdot c$ would also have a decomposition). We set a_{i+1} to be equal to the element that does not have a decomposition. Clearly $a_{i+1} \mid a_i$, and $a_{i+1} \nmid a_i$.

The existence of the sequence $a_1, a_2, a_3, \ldots \in R$ clearly contradicts to (2). Thus (2) implies that every element of $\mathbf{R}$ has a decomposition into irreducible elements. □

To prove the uniqueness of decompositions, we need to prove a statement similar to Lemma 1.5 In order to prove it, we use the following auxiliary lemma:

Lemma 7.2. *Let* $\mathbf{R}$ *be an integral domain, and let* $a, b, c \in R$ *be such that* $\gcd(a, b)$ *and* $\gcd(ac, bc)$ *exist. Then*

$$\gcd(ac, bc) = c \cdot \gcd(a, b).$$

The proof of Lemma 7.2 is a bit technical; so we don't discuss it in the lecture and only include it here for completeness' sake:

Proof of Lemma 7.2. Recall that the greatest common divisor is only determined up to the relation $\|$. So, it is enough to show that $\gcd(ac, bc) \mid c \cdot \gcd(a, b)$, and $c \cdot \gcd(a, b) \mid \gcd(ac, bc)$.

If $c = 0$, then $\gcd(ac, bc) = c \cdot \gcd(a, b) = 0$, so the equation clearly holds.

So let us assume that $c \neq 0$. For short, let us write $u = \gcd(ac, bc)$. We first show that $u \mid c \cdot \gcd(a, b)$. Since $u \mid ac$, there is an element x such that $ac = ux$. Since $u \mid bc$, there is an y such that $bc = uy$. Since c is a common divisor of ac and bc, also $c \mid u$, and thus there is a z such that $u = cz$. This implies $ac = czx$ and $bc = czy$. By cancelling c (here we use $c \neq 0$) on both sides of these equations we get $a = zx$ and $b = zy$. So z is a common divisor of both a and b, and therefore $z \mid \gcd(a, b)$. This gives us $u = cz \mid c \cdot \gcd(a, b)$, which is what we wanted to prove.

For the opposite direction, simply note that $c \cdot \gcd(a, b)$ divides both ca and cb, and therefore also $u = \gcd(ac, bc)$. □

We are now able to prove the following analogue of Lemma 1.5:

Lemma 7.3. *Let* $\mathbf{R}$ *be an integral domain such that* gcd *exists for every pair of elements. Let* p *be an irreducible element of* $\mathbf{R}$*. Then* $p \mid ab$ *implies that either* $p \mid a$ *or* $p \mid b$*.*

Proof. Let p be irreducible and $a, b \in R$ such that $p \mid ab$. Let us assume that $p \nmid a$. Since p is irreducible, this means $\gcd(a, p) = 1$. By Lemma 7.2 we obtain

$$\gcd(ab, pb) = b \cdot \gcd(a, p) = b.$$

Since p divides both ab and pb, it must also divide $\gcd(ab, pb) = b$, which is what we wanted to prove. □

This allows us to finish the proof of Theorem 7.1.

Proof of uniqueness of decompositions. Let $\mathbf{R}$ be an integral domain satisfying (1) and (2), and let us assume that there is an element $a \in R$ that does not have a unique decomposition into irreducible elements, so $a \parallel p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$ and $a \parallel q_1^{l_1} \cdot \ldots \cdot q_m^{l_m}$ are two distinct decompositions into irreducible elements. Also, without loss of generality, we can pick an a is such that the first decomposition is of minimal 'length' $k_1 + k_2 + \ldots + k_n$. By Lemma 7.3 there must be a factor q_i in the second product, such that $p_1 \mid q_i$. In fact, since, both p_1 and q_i are irreducible, it holds that $p_1 \parallel q_i$. Cancelling with this element gives us two distinct decompositions $p_1^{k_1 - 1} \cdot \ldots \cdot p_n^{k_n} \parallel q_1^{l_1} \cdot \ldots \cdot q_i^{l_i - 1} \cdot \ldots \cdot q_m^{l_m}$, such that the first one has length $k_1 + k_2 + \ldots + k_n - 1$. This is a contradiction to the minimality of a! Therefore $\mathbf{R}$ is a UFD. □

With Theorem 7.1 we are now ready to finish the prove of Gauss's theorem:

Proof of Theorem 6.8. Let $\mathbf{R}$ be a UFD. In order to show that $\mathbf{R}[x]$ is also a UFD, it is enough to check conditions (1) and (2) of Theorem 7.1. By Theorem 6.7, every pair of polynomials $f, g \in \mathbf{R}[x]$ has a greatest common divisor, so (1) holds. To show (2) let us assume for contradiction that there is a sequence $f_1, f_2, f_3, \ldots \in \mathbf{R}[x]$ such that $f_{i+1} \mid f_i$ and $f_{i+1} \nparallel f_i$ for every i. This implies $\deg(f_1) \geq \deg(f_2) \geq \cdots \geq 0$. Since this is an infinite sequence, there is an n, such that $\deg f_n = \deg f_{n+1} = \deg f_{n+2} = \cdots$. For every $j \geq n$, let u_j be the leading coefficient of f_j. Then, the sequence $u_n, u_{n+1}, u_{n+2}, \ldots$ in $\mathbf{R}$ satisfies that $u_{j+1} \mid u_j$ and $u_{j+1} \nparallel u_j$ for every $j \geq n$. But this is impossible, since $\mathbf{R}$ is a UFD!

So $\mathbf{R}[x]$ satisfies conditions (1) and (2) of Theorem 7.1 and is therefore a UFD. □

7.2. **Euclid's algorithm and Bézout coefficients.** In this section, we are going to discuss, in which integral domains Euclid's algorithm works (as a way to determine $\gcd(a, b)$ and its Bézout coefficients). We already saw that versions of Euclid's algorithm work in $\mathbb{Z}$ and $\mathbf{F}[x]$ for fields $\mathbf{F}$. However, we also saw that in some rings, even UFDs (like $\mathbb{Z}[x]$, or $\mathbb{Q}[x, y]$), Bézout coefficients do not always exists.

The basic ingredient for Euclid's algorithm in $\mathbb{Z}$ and $\mathbf{F}[x]$ was to have a division with remainder, together with a 'measure' on how 'big' the remainder is. We give a formal definition of the integral domains that have this property:

Definition. An integral domain $\mathbf{R}$ is called *Euclidean* if there is a *Euclidean norm* ν, that is, a function

$$\nu\colon R \to \mathbb{N} \cup \{0\},$$

which satisfies

(1) $\nu(0) = 0$
(2) If $a \mid b$, $b \neq 0$, then $\nu(a) \leq \nu(b)$;
(3) for all $a, b \in R$, $b \neq 0$, there exists $q, r \in R$ such that

$$a = bq + r \text{ and } \nu(r) < \nu(b).$$

Condition (3) says that for each pair a, b there exists a quotient q and a remainder r (with no claim of uniqueness!), such that the remainder is 'smaller' than the element b we divide through. Note that $\nu(b) = 0$ if and only if $b = 0$: this holds since the remainder r after dividing any other element a by $b \neq 0$ must have a lower Euclidean norm that $\nu(b)$, so $\nu(b) > \nu(r) \geq 0$.

Example. The following UFD's are Euclidean domains:

- Every field is a Euclidean domain, with the Euclidean norm $\nu(0) = 0$ and $\nu(a) = 1$ if $a \neq 0$.
- The integers $\mathbb{Z}$ are Euclidean, with $\nu(a) = |a|$.
- If $\mathbf{F}$ is a field, then the polynomial ring $\mathbf{F}[x]$ is a Euclidean field, with the norm

  $$\nu(f) = 1 + \deg(f).$$

  We already discussed this in Proposition 4.2. Note that we need to add 1 so the degree of f, such that $\nu(0) = 0$.
- Some quadratic extensions $\mathbb{Z}[\sqrt{s}]$ are Euclidean (e.g. for $s = -1, \pm 2, 3$), while other are not (e.g. $s = -3, 5$). In the previous case, a norm is given by

  $$\nu(a + b\sqrt{s}) = |a^2 - sb^2|.$$

  It can be showed that ν satisfies both property (1) and (2) for all values of $s \in \mathbb{Z}$ (exercises). However to show property (3) is non-trivial and depends on s.
  For Gaussian integers $a, b \in \mathbb{Z}[i], b \neq 0$, we can find a quotient q by first computing $a \cdot b^{-1}$ in $\mathbb{C}$, and setting q to be the Gaussian integer closest to it. The remainder is then defined as $r = a - qb$ (see Figure 3 for an example). We leave it as an exercise that this 'division with remainder' indeed satisfies (3).

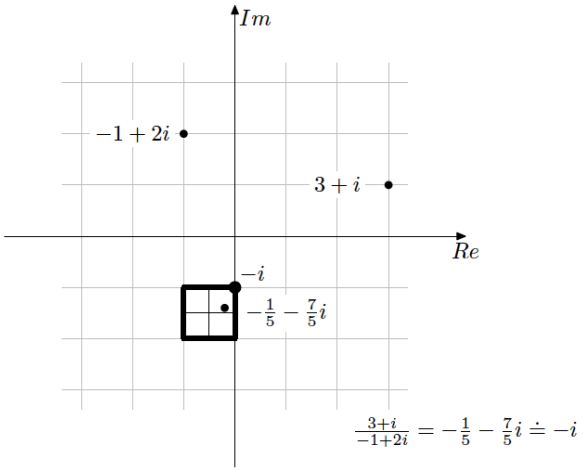


FIGURE 3. Division with remainder in $\mathbb{Z}[i]$.

There are UFDs that are not Euclidean (such as $\mathbb{Z}[x]$, or $\mathbb{Q}[x, y]$). For the example of integer polynomials $\mathbb{Z}[x]$, the map $\nu(f) = 1 + \deg f$ is not a Euclidean norm, since (3) does not hold: For example for the polynomials $3x$ and $2x$ there are no $q, r \in \mathbb{Z}[x]$ such that $3x = q \cdot 2x + r$ and $\deg(r) = 0$. But also $\deg(r) = -1$ is not possible, since then $r = 0$ and $3x = 2qx$, but such a polynomial q does not exist in $\mathbb{Z}[x]$. Note that this example just shows that this particular function ν is not a Euclidean norm, but we did not disprove that $\mathbb{Z}[x]$ is Euclidean. For this, we would need to exclude the possibility of any Euclidean norm $\mathbb{Z}[x] \to \mathbb{N} \cup \{0\}$, which is more complicated. However, we are next going to show that in Euclidean domains Euclid's algorithm works, and Bézout coefficients always exists. Since we also saw that this is not true for $1 = \gcd(3x, 2x)$ in $\mathbb{Z}[x]$, we know that $\mathbb{Z}[x]$ is not Euclidean.

We start by describing (the generalized version of) Euclid's algorithm

Euclid's algorithm (over a Euclidean domain $\mathbf{R}$).

- Input: $a, b \in R$, with $\nu(a) \geq \nu(b)$
- Output: $\gcd(a, b)$ and coefficients $u, v \in R$ such that $\gcd(a, b) = u \cdot a + v \cdot b$
  - $a_0 = a, \quad u_0 = 1, \quad v_0 = 0$
    $a_1 = b, \quad u_0 = 0, \quad v_0 = 1$
  - for every $i = 2, 3, \ldots$ do the following:
    let q, r be such that $a_i = qa_{i-1} + r$ and $\nu(r) < \nu(a_{i-1})$. Then set

$$a_{i+1} = r, \quad u_{i+1} = u_{i-1} - qu_i, v_{i+1} = v_{i-1} - qv_i.$$

    If $a_{i+1} = 0$, output a_i, u_i, v_i.

Theorem 7.4 (Correctness of Euclid's algorithm)**.** *Let* $\mathbf{R}$ *be an Euclidean domain. Then, on input* $a, b \in R$*, Euclid's algorithm indeed outputs* $\gcd(a, b)$ *and* Bézout coefficients $u, v \in R$ *such that*

$$\gcd(a, b) = u \cdot a + v \cdot b.$$

Proof. Since $\nu(a_0) > \nu(a_1) > \nu(a_2) > \cdots \geq 0$, the algorithm must stop after finitely many steps. Let $i = n$ be the step in which this happens. To prove the correctness of the algorithm, we are going to show that

(1) $\gcd(a_{i-1}, a_i) = \gcd(a_i, a_{i+1})$ for all $i = 1, \ldots, n$ (if one of them exists).
(2) for all $i = 0, \ldots, n$ it holds that $a_i = u_i \cdot a + v_i \cdot b$.

If both hold, then the algorithm is correct, since then

$$\gcd(a, b) = \gcd(a_0, a - 1) = \gcd(a_1, a_2) = \cdots = \gcd(a_{n-1}, a_n) = \gcd(a_n, 0) = a_n.$$

To show (1) and (2),note that the equation $a_{i-1} = a_i q + a_{i+1}$ holds for all $i = 1, \ldots, n$. By this equation, every common divisor of a_{i-1}, a_i is also a common divisor of a_i, a_{i+1}, and vice versa (compare with Lemma 1.3). Therefore $\gcd(a_{i-1}, a_i) = \gcd(a_i, a_{i+1})$ for all $i = 1, \ldots, n$. Point (2) can be showed by induction on i. Clearly (2) is true for $i = 0, 1$. For an induction step from $i - 1, i$ to $i + 1$,let us assume that $a_{i-1} = u_{i-1}a + v_{i-1}b$ and $a_i = u_i a + v_i b$. Then

$$\begin{aligned} a_{i+1} &= a_{i-1} - a_i q = u_{i-1}a + v_{i-1}b - (u_i a + v_i b)q \\ &= (u_{i-1} - u_i q) \cdot a + (v_{i-1} - v_i q) \cdot b = u_{i+1}a + v_{i+1}b, \end{aligned}$$

thus (2) holds. □

With Theorem 7.4 it is relatively straightforward to prove that every Euclidean domain is a UFD, we just need to prove the following lemma first:

Lemma 7.5. *Let* $\mathbf{R}$ *be a Euclidean domain and* $a, b \in R$ *with* $a, b \neq 0$*. If* $a \mid b$ *and* $a \nmid b$*, then* $\nu(a) < \nu(b)$*.*

Proof. By our assumptions

- $b = au$ for some $u \in R$,
- $a = bq + r$ for some $q, r \in R$ and $\nu(r) < \nu(b)$.

Since $b \nmid a$ the remainder r cannot be 0. We get $0 \neq r = a - bq = a - auq = a(1 - uq)$, and therefore a divides r. It follows that $\nu(a) \leq \nu(r) < \nu(b)$. □

Theorem 7.6. *Every Euclidean domain* $\mathbf{R}$ *is a unique factorization domain.*

Proof. It is enough to check if the criterion from Theorem 7.1 holds for $\mathbf{R}$. The existence of greatest common divisors $\gcd(a, b)$ for every pair $a, b \in R$ follows directly from Theorem 7.4. Further, by Lemma 7.5, any infinite chain $a_1, a_2, a_3, \ldots \in \mathbf{R}$ of proper divisors $a_{i+1} \mid a_i$, $a_{i+1} \nmid a_i$ would need to satisfy $\nu(a_1) > \nu(a_2) > \nu(a_3) > \cdots \geq 0$ - therefore no such chain exists. □

8. Computations modulo polynomials

8.1. **The Chinese remainder theorem and interpolation.** The Chinese remainder theorem (Theorem 2.9) told us that certain systems of integer equations modulo congruences have a solution. As it turns out, analogue statements hold for more general classes of rings. In this section we are going to discuss it for the polynomial ring $\mathbf{F}[x]$, where $\mathbf{F}$ is a field. An important application is then polynomial interpolation.

Theorem 8.1 (Chinese remainder theorem for polynomials)**.** *Let $\mathbf{F}$ be field, let $m_1, \ldots, m_n \in \mathbf{F}[x]$ be pairwise coprime polynomials, let $d = \sum_{i=1}^{n} \deg m_i$, and let $u_1, \ldots, u_n \in \mathbf{F}[x]$ be arbitrary polynomials. Then there exists exactly one polynomial $f \in \mathbf{F}[x]$ of degree $\deg f < d$ that satisfies the system of equations:*

$$\begin{aligned} f &\equiv u_1 \pmod{m_1} \\ f &\equiv u_2 \pmod{m_2} \\ &\vdots \\ f &\equiv u_n \pmod{m_n}. \end{aligned}$$

Proof. We first prove that, if there is a solution, it must be unique. So let us assume that there are two polynomials $f, g \in \mathbf{F}[x]$ of degree $\deg f, \deg g < d$ such that $f \equiv g \equiv u_i \pmod{m_i}$ for all $i = 1, \ldots, m$. Note that this implies $m_i \mid f - g$, for every i. Since the polynomials m_i are coprime, and $\mathbf{F}[x]$ is a UFD, this implies that

$$m_1 \cdot m_2 \cdot \ldots \cdot m_n \mid f - g.$$

The product on the left side has degree d, while $\deg(f - g) < d$ by assumption. But this is only possible, if $f - g = 0$, hence $f = g$.

Next we prove that there is indeed a solution. For this, let

$$P_d = \{f \in \mathbf{F}[x] \colon \deg f < d\}.$$

Note that P_d can be regarded as a d-dimensional vector spaces over $\mathbf{F}$ (with basis $1, x, x^2, \ldots, x^{d-1}$, the usual polynomial addition $+$, and scalar multiplication $c \cdot f$ for $c \in \mathbf{F}$). Let $d_i = \deg m_i$ for every $i = 1, \ldots, m$. Then we define the map

$$\begin{aligned} \phi \colon P_d &\to P_{d_1} \times P_{d_2} \times \cdots \times P_{d_n} \\ f &\mapsto (f \bmod m_1, f \bmod m_2, \ldots, f \bmod m_n). \end{aligned}$$

It is not hard to check that $(af + g) \bmod m = a \cdot (f \bmod m) + (g \bmod m)$ for all $f, g, m \in \mathbf{F}[x]$ and $a \in \mathbf{F}$. As a consequence also $\phi(af + g) = a\phi(f) + \phi(g)$, so also ϕ is a vector space homomorphism. At the same time P_d and $P_{d_1} \times P_{d_2} \times \cdots \times P_{d_n}$ have the same dimension d. By the previous paragraph ϕ is an injective map. By a result from linear algebra, $\phi(P_d)$ must also have dimension d. Therefore ϕ is a vector space isomorphism and hence a bijection (in some sense this is analogous to Lemma 2.6). So for every element $(u_1, u_2, \ldots, u_n) \in P_{d_1} \times P_{d_2} \times \cdots \times P_{d_n}$, there

exists a unique $f \in P_d$ such that $\phi(f) = (u_1, u_2, \ldots, u_n)$. This f is the solution we were looking for. □

As for the integers, this proof was not constructive, i.e. it does not give us an algorithm to compute the actual solution to the system of equations $f \equiv u_1 \pmod{m_1}, f \equiv u_2 \pmod{m_2}, \ldots, f \equiv u_n \pmod{m_n}$. However, it is not hard to generalize the algorithm we already know from the integers:

Exercise. Find a polynomial $f \in \mathbb{Q}[x]$ of degree < 5 such that

$$f \equiv 1 \pmod{x^3+1} \quad \text{and} \quad f \equiv x+1 \pmod{x^2+1}.$$

Solution. Let f be a solution to the above equations. By the second congruence, there is a polynomial $g \in \mathbb{Q}[x]$, such that $f = g \cdot (x^2+1) + x + 1$. Substituting this expression for f in the first congruence and simplifying gives us

$$g \cdot (x^2+1) \equiv -x \pmod{x^3+1}. \tag{2}$$

(3)

In order to proceed now (and calculate g) we need to multiply (2) with an element that is inverse to (x^2+1) modulo x^3+1. We can compute such an inverse, by finding the Bézout coefficients u, v of $1 = \gcd(x^3+1, x^2+1) = u(x^3+1) + v(x^2+1)$. Euclid's algorithm (see Section 7.2) gives us $u = \frac{1}{2}(x+1)$ and $v = \frac{1}{2}(-x^2-x+1)$. So $v \cdot (x^2+1) \equiv 1 \pmod{x^3+1}$, and so multiplying (2) with v gives us

$$g \equiv \frac{1}{2}(x^3+x^2-x) \equiv \frac{1}{2}(x^2-x-1) \pmod{x^3+1}.$$

As a consequence, $g = \frac{1}{2}(x^2-x-1) + h \cdot (x^3+1)$ for some $h \in \mathbb{Q}[x]$. Re-substituting in f and simplifying gives us

$$f = \frac{1}{2}(x^4 - x^3 + x + 1) + h(x^3+1) \cdot (x^2+1) \text{ for } h \in \mathbb{Q}[x].$$

By setting $h = 0$ we get the only solution of degree < 5, which is $f = \frac{1}{2}(x^4 - x^3 + x + 1)$. □

An important application of the Chinese remainder theorem is *interpolation*. For this let us recall that for every polynomial $f \in F[x]$ and $a, u \in F$ we have

$$f(a) = u \Leftrightarrow f \equiv u \pmod{x-a}.$$

This follows from Proposition 4.3: $x - a$ divides the polynomial $f - u$ if and only if a is a root of the polynomial $f - u$ i.e. $f(a) - u = 0$.

If we apply the Chinese remainder theorem to equations of the form $f \equiv u \pmod{x-a}$ we get the *interpolation theorem*, which says that if fix n function values, then there is exactly one polynomial of degree $< n$, which interpolates these values:

Corollary 8.2 (interpolation theorem)**.** *Let* $\mathbf{F}$ *be a field, let* $a_1, \ldots, a_n \in F$ *be pairwise different elements, and let* $u_1, \ldots, u_n \in F$ *be arbitrary. Then there exists a unique polynomial* $f \in \mathbf{F}[x]$ *of degree* $< n$ *such that* $f(a_i) = u_i$ *for all* $i = 1, \ldots, n$.

Proof. The polynomial $f \in \mathbf{F}[x]$ is the unique solution to the equations $f \equiv u_i \pmod{x-a_i}$ for all $i = 1, \ldots, n$. □

Unlike for the general case of the Chinese remainder theorem, in the special case of Corollary 8.2, we can compute the solution f directly via a formula:

$$f = \sum_{i=1}^{n} \left(u_i \cdot \prod_{j \neq i} \frac{x - a_j}{a_i - a_j} \right).$$

This polynomial is also called the *Lagrange polynomial* (for the pairs (a_i, u_i)). It is easy to see that the polynomial function given by f indeed runs through all pairs (a_i, u_i), since

$$f(a_k) = 0 + \ldots + 0 + u_k \cdot \prod_{j \neq k} \frac{a_k - a_j}{a_k - a_j} + 0 + \ldots + 0 = u_k \cdot 1 = u_k.$$

It follows immediately from the Interpolation theorem that the Lagra.nge polynomial is the unique such polynomial of degree $< n$.

A nice consequence of the interpolation theorem is the following fact about *finite* fields:

Corollary 8.3 (Representation of functions over finite fields)**.** *Let* $\mathbf{F}$ *be a finite field, and* $\phi\colon F \to F$ *an arbitrary function. Then there exists exactly one polynomial* $f \in F[x]$ *with* $\deg f < |F|$*, such that* $\phi(a) = f(a)$ *for all* $a \in F$*.*

Proof. We obtain the polynomial f by applying the Interpolation theorem to all pairs $(a, \phi(a))$ with $a \in F$. □

So Corollary 8.3 allows us represent all functions on F by polynomials. This can be very useful in computational settings, since it allows for more efficient representation and computations with functions (see also Section 9).

Side note: Corollary 8.3 does not hold for *infinite* fields like $\mathbb{R}$. Nevertheless, polynomials play an important role in real valued analysis: as you might already know, there are different ways to approximate continuous real valued functions by polynomials: Taylor polynomials allow us to approximate a function locally, around a given point. The Weierstrass theorem tells us further, that every function $\phi\colon [u, v] \to \mathbb{R}$ can be uniformly approximated by polynomials $f \in \mathbb{R}[x]$ (this means that for every $\epsilon > 0$ there is a polynomial $f \in \mathbb{R}[x]$ such that $|\phi(a) - f(a)| < \epsilon$ for all $a \in [u, v]$).

Exercise 8.4. *Try to come up with an analogue of the Lagrange interpolation polynomials for higher dimensions, and think about how to modify the statement of Corollary 8.3, such that it hold for n-ary functions* $\phi\colon F^n \to F$*, for arbitrary* $n \in \mathbb{N}$*.*

8.2. **Quotient rings modulo polynomials.** In this section we describe how we can construct new rings from $\mathbf{F}[x]$, by forming the *quotient rings* modulo a given polynomial m (also called *factor rings*). This construction can be compared with the construction of $\mathbb{Z}_m$ from $\mathbb{Z}$, and (as we will see) can be used to construct all finite fields.

Definition. Let $\mathbf{F}$ be a field, and $m \in F[\alpha]$ a polynomial of degree $n \geq 1$. The *quotient ring* $\mathbf{F}[\alpha]/(m)$ then consists of the polynomials of degree $< n$, together with operations that all computed modulo m. So

$$\mathbf{F}[\alpha]/(m) = (\{f \in \mathbf{F}[\alpha]\colon \deg f < n\} +, -, \odot, 0, 1),$$

where $+, -, 0, 1$ are defined as in $\mathbf{F}[\alpha]$, and $f \odot g = f \cdot g \bmod m$.

First of all, let us check that $\mathbf{F}[\alpha]/(m)$ is also a commutative ring. All the axioms that only involve $+$, $-$ and 0 clearly hold, since these operations have the same definition on $\mathbf{F}[\alpha]/(m)$ as on $\mathbf{F}[\alpha]$. For the associativity of $\odot$, recall first that $f \equiv g \pmod m$ if and only if $f \bmod m = g \bmod m$, and $f \bmod m \equiv f \pmod m$. We want to show $f, g, h \in \mathbf{F}[\alpha]/(m)$:

$$f \odot (g \odot h) = (f \odot g) \odot h.$$

By definition, this is equivalent to

$$f \cdot (g \cdot h \bmod m) \bmod m = (f \cdot g \bmod m) \cdot h \bmod m,$$

which in turn, by the above rules, is equivalent to the congruence

$$f \cdot (g \cdot h) \equiv (f \cdot g) \cdot h \pmod m.$$

This congruence identity holds however for all polynomials f, g, h, since $\cdot$ is associative in $\mathbf{F}[\alpha]$. In a similar way we can prove the commutativity and distributivity of $\odot$, we leave it to the reader.

Example. Let us consider the quotient ring $\mathbb{R}[\alpha]/(\alpha^2+1)$. Its elements are of the form $a + b\alpha$, for $a, b \in \mathbb{R}$. The addition on $\mathbb{R}[\alpha]/(\alpha^2+1)$ is $(a+b\alpha)+(c+d\alpha) = (a+c)+(b+d)\alpha$, while the product of two elements is equal to

$$\begin{aligned}(a+b\alpha) \odot (c+d\alpha) &= ac + (ad+bc)\alpha + bd\alpha^2 \mod (\alpha^2+1) \\ &= (ac-bd) + (ad+bc)\alpha.\end{aligned}$$

Note that this corresponds to the addition and multiplication over the complex numbers. This is not a coincidence: If we identify the symbol i with α, then $\mathbb{R}[\alpha]/(\alpha^2+1) = \mathbb{C}$ (formally speaking, the map $a+b\cdot\alpha \mapsto a+b\cdot i$ is an *isomorphism* from $\mathbb{R}[\alpha]/(\alpha^2+1)$ to $\mathbb{C}$). The explanation for this phenomenon is rather easy: modulo (α^2+1), the value of α^2 is -1, i.e. $\alpha^2 \equiv -1 \pmod{\alpha^2+1}$. In other words, α has exactly the property that defines the imaginary unit i.

Similarly, it can be seen that the quotient ring $\mathbb{Q}[\alpha]/(\alpha^2+1)$ is equal to the rational Gaussian numbers $\mathbb{Q}(i)$ (again, formally speaking they are just *isomorphic*, i.e. equal up to renaming the elements).

Example. For a finite field $\mathbb{Z}_p$, the properties of $\mathbb{Z}_p[\alpha]/(\alpha^2+1)$ depend on the prime p:

- The quotient ring $\mathbb{Z}_2[\alpha]/(\alpha^2+1)$ has 4 elements, but is not a field, and not even an integral domain, since
$$(\alpha+1) \odot (\alpha+1) = \alpha^2 + 1 \bmod (\alpha^2+1) = 0.$$
- The quotient ring $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ has 9 elements. It is a field, although this is not immediately clear.

The following proposition gives a characterization of the cases, in which a quotient ring is a field:

Proposition 8.5 (Quotient of irreducible polynomials)**.** *Let* $\mathbf{F}$ *be a field, and* $m \in F[\alpha]$ *a polynomial of degree* ≥ 1*. Then the following are equivalent:*

(1) $\mathbf{F}[\alpha]/(m)$ *is a field,*
(2) $\mathbf{F}[\alpha]/(m)$ *is an integral domain,*
(3) m *is an irreducible polynomial in* $\mathbf{F}[\alpha]$.

Proof. (1) $\Rightarrow$ (2) follows from Proposition 3.3.

(2) $\Rightarrow$ (3): If m is not an irreducible polynomial in $\mathbf{F}[\alpha]$, then we can write it as $m = f \cdot g$, for two polynomials with $\deg f, \deg g < \deg m$. It then holds that $f \odot g = m \bmod m = 0$ in $\mathbf{F}[\alpha]/(m)$, thus $\mathbf{F}[\alpha]/(m)$ is not an integral domain.

(3) $\Rightarrow$ (1): Let us assume that m is irreducible and $f \in \mathbf{F}[\alpha]/(m)$ with $f \neq 0$. Our goal is to construct the inverse of f. Since m is irreducible, it holds that $1 = \gcd(f, m)$ in $\mathbf{F}[\alpha]$. By Bézouts identity, there are $u, v \in \mathbf{F}[\alpha]$ such that $1 = uf + vm$. Let us define $\tilde{u} = u \bmod m$. Then $\tilde{u} \odot f = \tilde{u}f \bmod m \equiv uf \equiv 1 \pmod m$. Thus $\tilde{u}$ is the inverse of f. □

In the following, we are often going to use the standard multiplication symbol $\cdot$ instead of $\odot$; the meaning however should always be clear from the context (similarly to how we used the same symbols of addition/multiplication over $\mathbb{Z}$ and $\mathbb{Z}_m$). The construction just described in Proposition 8.5 will be important in the next section, where we discuss finite fields.

We continue now by giving another important application of Proposition 8.5: Every field can be extended to a field, in which a given polynomial has a root. (For $\mathbb{Q}$ this might seem trivial, since you probably already know that every rational polynomial has a root in $\mathbb{C}$, by the Fundamental Theorem of Algebra. However, the proof of the Fundamental Theorem of Algebra is not easy, and the following propositions are actually an important step in it).

Proposition 8.6. *Let $\mathbf{F}$ be a field and $f \in F[x]$ be a polynomial of degree ≥ 1. Then there exists a field $\mathbf{S} \geq \mathbf{F}$, such that f has a root in S.*

Proof. Let m be an irreducible factor of f, and let $m = \sum_{i=0}^{n} a_i x^i$. It is enough to find a field $\mathbf{S} \geq \mathbf{F}$, in which m has root, since then also f, as a multiple of m, has a root. We define $\mathbf{S} = \mathbf{F}[\alpha]/(m)$. By Proposition 8.5, $\mathbf{S}$ is a field. Furthermore in $\mathbf{S}$ the polynomial m has the root $\alpha \in \mathbf{S}$, since

$$m(\alpha) = \left(\sum_{i=0}^{n} a_i (\alpha^i) \right) \bmod m(\alpha) = m(\alpha) \bmod m(\alpha) = 0.$$

□

Example.
- The rational polynomial $f = x^3 - 2 \in \mathbb{Q}[x]$ induces the field $\mathbb{Q}[\alpha]/(\alpha^3 - 2)$, in which α is a root of f. If we identify α with $\sqrt[3]{2}$, it can be seen that this field is isomorphic to $\mathbb{Q}(\sqrt[3]{2})$.
- The polynomial $f = x^3 - 2 \in \mathbb{Z}_7[x]$ induces the field $\mathbb{Z}_7[\alpha]/(\alpha^3 - 2)$, which has 7^3 many elements and which you probably have not encountered yet.

By induction we can refine Proposition 8.6, and find an extension $\mathbf{S} \geq \mathbf{F}$, in which f even decomposed into linear factors:

Corollary 8.7 (Splitting field)**.** *Let $\mathbf{F}$ be a field and $f \in F[x]$ be a polynomial of degree ≥ 1. Then there exists a field $\mathbf{S} \geq \mathbf{F}$, such that f can be written as the product of polynomials of degree 1.*

Proof. We prove this by induction on the degree of f. If the degree of f is 1, then $f = ax + b$, and we are already done. Otherwise, $\deg f > 1$. By Proposition 8.6, there is an extension $\mathbf{U} \geq \mathbf{F}$, such that f has a root u in U. Then f decomposes into $f = (x - u) \cdot g$, for some $g \in \mathbf{U}[x]$. Since $\deg g < \deg f$, we can apply the induction hypothesis to g, to obtain a field $\mathbf{S} \geq \mathbf{U}$, in which g decomposes into factors of degree 1. Since $\mathbf{S}$ is also a field containing $\mathbf{F}$, this finishes the proof. □

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

FIGURE 4. The operation tables of the 4-element field $\mathbb{Z}_2[\alpha]/(\alpha^2+\alpha+1)$ with $\beta = \alpha + 1$

9. Finite fields and some applications

9.1. **Finite fields and data representation.** An important application of quotient rings is the construction of finite fields. Let p be a prime number, and $m \in \mathbb{Z}_p[\alpha]$ be an irreducible polynomial of degree k. Then, by Proposition 8.5, the quotient ring $\mathbb{Z}_p[\alpha]/(m)$ is a field. Its carrier set consists of all the polynomials over $\mathbb{Z}_p$ of degree $< k$, so it has size p^k. In this way we can for example construct the 4-element field $\mathbb{Z}_2[\alpha]/(\alpha^2+\alpha+1)$, whose operation table you can see in Figure 4. Note that this field is different from the ring $\mathbb{Z}_4$. (And in general, for any $k > 1$, every p^k-element field is different form the ring $\mathbb{Z}_{p^k}$!)

In the same way we can construct the fields

- $\mathbb{Z}_2[\alpha]/(\alpha^3+\alpha+1)$ or $\mathbb{Z}_2[\alpha]/(\alpha^3+\alpha^2+1)$, with 8 elements
- $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ or $\mathbb{Z}_2[\alpha]/(\alpha^2 \pm \alpha + 2)$, with 9 elements

A priori, it is not clear if there are fields of all prime power sizes p^k (and how many). But, by the following theorem there is exactly one field of size p^k (up to isomorphism). So in the example above $\mathbb{Z}_2[\alpha]/(\alpha^3+\alpha+1)$ or $\mathbb{Z}_2[\alpha]/(\alpha^3+\alpha^2+1)$ are both equal (up to renaming their elements), and describe the unique 8-element field.

Theorem 9.1. *Let p be a prime number, and $k \in \mathbb{N}$. Then*

1. *There is an irreducible polynomial of degree k over $\mathbb{Z}_p$, and therefore there exists a field of size p^k,*
2. *every field of size p^k can be constructed as quotient ring $\mathbb{Z}_p[\alpha]/(m)$, for some irreducible polynomial of degree k,*
3. *when $m_1, m_2 \in \mathbb{Z}_p[\alpha]$ are two irreducible polynomials of degree k, then $\mathbb{Z}_p[\alpha]/(m_1)$ and $\mathbb{Z}_p[\alpha]/(m_2)$ are isomorphic (in other words, the choice of m does not matter).*

The proof of this theorem is harder than it might appear. Even to show the existence of a field of size p^k is not trivial; we can obtain it as a splitting field of $\mathbb{Z}_p$ with respect to the polynomial $f = x^{p^k} - x$ (the construction in Corollary 8.7). The proof of the rest of Theorem 9.1 requires however some more advance techniques, which we are not going to discuss here.

We are going to denote the field of size p^k by $\mathbb{F}_{p^k}$ (you might also encounter the notation $\mathbf{GF}(p^k)$, since finite fields are also known as *Galois fields*).

Finite fields, in particular those of size 2^k, have many applications in computer science. They can be used to optimise both the representation of data and the performance of computations. We start in this section by discussing the representation of data.

FIGURE 5. A k-bitvector as an element of $\mathbb{F}_{2^k} = \mathbb{Z}_2[\alpha]/(m)$

The basic data objects used by computers are *bit vectors*, i.e. k-tuples, such that every entry is either 0 or 1 (a *bit*). Let $m \in \mathbb{Z}_2[\alpha]$ be an irreducible polynomial of degree k. Then we can identify a bit vectors of $(a_0, a_1, \ldots, a_{k-1})$ with the element $a_0 + a_1\alpha + a_2\alpha^2 + \cdots a_{k-1}\alpha^{k-1} \in \mathbb{Z}_2[\alpha]/(m) = \mathbb{F}_{2^k}$. In other words, the bit vectors of a fixed length k can be represented by the elements of the finite field $\mathbb{F}_{2^k}$.

Some standard operations on bit vectors can be also nicely described in the field $\mathbb{F}_{2^k}$. For example, moving to bit to the left (or right) of a given entry of a bitvector corresponds to multiplying (or dividing) with α. Flipping the i-th bit of $(a_0, a_1, \ldots, a_{k-1})$ corresponds to adding $(0, \ldots, 0, 1, 0, \ldots, 0)$ (where 1 is on the i-th coordinate). The bitwise XOR-operation is the field addition. The bitwise AND corresponds to the *coefficient-wise* multiplication of the corresponding polynomials (attention, this is *not* the field multiplication of $\mathbb{F}_{2^k}$).

Besides this, fields give us two very useful operations: the field multiplication $\cdot$ and inversion $^{-1}$. One application of them is in creating cyphers. The idea behind this is, roughly speaking, that small local changes in the input, quickly propagate to global changes in the input under operations that involve the (non-linear) field operations. We give an example:

Example. A symmetric cypher is a cypher for which the same key is used for the encryption and decryption. One of the most common symmetric cyphers is the *Advanced Encryption Standard* (*AES*, also known as *Rijndael* after one of its inventors). AES works with bit vectors of length 8, which corresponds to elements of the field

$$\mathbb{F}_{256} = \mathbb{Z}_2[\alpha]/(\alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1).$$

The data that is to be encoded is split up into blocks of 128 bits each; every such block can be represented by a 4×4-matrix over the field $\mathbb{F}_{256}$ (since $256^{16} = 2^{128}$). To create a cypher, AES repeats the following 4 steps for every block several times (plus an extra steps at the beginning and end, which we will ignore here). In the first step we substitute every entry u of the matrix as follows

$$u \mapsto u^{-1} \cdot (1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4) + (1 + \alpha + \alpha^5 + \alpha^8) \bmod \alpha^8 + 1,$$

where the inverse u^{-1} is computed in $\mathbb{F}_{256}$, but the rest of the operations is done in the polynomial ring $\mathbb{Z}_2[\alpha]$. In the second phase, the i-th row of the matrix is cyclically shifted $(i-1)$-many times. The third step mixes up every column on the matrix in the following way: we regard the column $(a_0, a_1, a_2, a_3) \in \mathbb{F}_{256}^4$ as the coefficients of the polynomial $f = a_0 + a_1x + a_2x^2 + a_3x^3 \in \mathbb{F}_{256}[x]$, and substitute the column according to the operation

$$f \mapsto f \cdot (\alpha + x + x^2 + (\alpha + 1)x^3) \bmod (x^4 + 1).$$

In the forth step a selected part of the key is (bitwise) added to the matrix.

The first 3 transformations are bijective, but also have the property that local changes in the input very quickly propagate to global changes in the output. Therefore adding (part of) the codeword in step 4 and iterating the procedure will result in a cypher that has very good cryptographic properties. However, knowing the codeword, it is not too hard to decode this cypher, since all 4 steps can be reversed in an efficient way: Step 4 can be reversed by just subtracting the correct part of the codeword again, and Step 2 by cyclically shifting the rows back. Step 1 and 3 can be reversed using the algebraic structure of the appearing rings (hint: Bézout identities).

Corollary 8.3 and its generalization to functions of higher arities (Exercise 8.4) are also of big importance for computing in finite fields: they show that inf fact every operation over a finite field can be represented by polynomials (of bounded degree). This fact is also used (among others) in cryptanalysis. We are going to see more applications with Secret Sharing (Section 9.2) and with error-correcting codes (Section 9.3).

9.2. **Secret sharing.** Imaging the following scenario: the army has a secret code that allows it to fire nuclear missiles. Apparently it's not good for one person to have the code and to launch missiles at his own will. Not even two lunatics should be able to fire missiles. The president therefore orders that the launch of the missiles requires the consent of at least three members of the five-member staff. How can this be arranged?

In general, we are talking about a (k, n)-*secret sharing scheme* if n participants share a secret, the disclosure of which requires the presence of at least k of them. Throughout this section we will assume that the secret t is an element of some field $\mathbb{F}$ (in practice usually a bitvector of length m is shared, interprete either as m secrets from the field $\mathbb{Z}_2$, or as one secret from the field $\mathbb{F}_{2^m}$).

For the case $k = n$ a very simple scheme can be used. In this case, the owner of the secret issues random values $a_i \in \mathbb{F}$ to all of the participants and publishes the value $c = t + \sum_{i=1}^{n} a_i$. In order to disclose the secret, each of the participants has to disclose their share a_i of the secret; then t can be retrieved as $t = c - \sum_{i=1}^{n} a_i$.

If not all participants are present, for instance if there are only $n - 1$, nothing definitive can be said about the value of t: the missing element can change the value of the sum to any another value. Guessing a codeword at random will only lead to success with probability $\frac{1}{|T|}$. In practice, when bitvectors are used, this means that the probability of guessing one bit correctly is $\frac{1}{2}$, and for m-bits it is $\left(\frac{1}{2}\right)^m$. Thus, picking m large enough gives high security.

But what to do when $k < n$, as in our nuclear missile scenario? A classic solution for the general (k, n)-secret sharing scheme is the so-called *Shamir protocol*. Here, the owner of the secret randomly chooses a polynomial $f \in \mathbb{F}[x]$ of degree $< k$ such that $f(0) = t$ (i.e. the secret is the 0-th coefficient of f) and keeps it secret. She then selects n different elements $0 \neq a_1, a_2, \ldots, a_n \in \mathbb{F}$ (these can be public) and gives the values of the polynomial $f(a_1), f(a_2), \ldots, f(a_n)$ to the participants.

If k participants decide to disclose their share of the secret, they can take their values and compute a polynomial of degree $< k$ that interpolates all the given points. By the Interpolation Theorem (Corollary 8.2), this polynomial must be equal to f. So evaluating it at 0 then results in the codeword $f(0) = t$.

On the other hand, if there are only $k-1$ participants present, they do not find anything about the absolute term f, since there are $|\mathbb{F}|$ polynomials of degree $< k$ that run through their $k-1$ points, each of which has a different value at 0 (again by the Interpolation Theorem). In practise this means that, if the field with 2^m elements (with $2^m > n$), is used for the m-bit key, then the probability that a random guess leads to the codeword is $\frac{1}{2^m}$.

The scheme can be easily modified for more specific tasks. For example, what if the president has decided that three of the five mad generals can fire missiles, or she herself? Then she can use a $(3, 8)$ scheme, in which each of the generals get one part, and she keeps three.

Besides storing information that is highly sensitive and highly important (missile launch codes, numbered bank accounts, and other stuff from Bond movies), secret sharing schemes have also day-to-day applications. They are important in cloud computing environments: a key can then be distributed over many servers by a threshold secret sharing mechanism. The key is then reconstructed when needed. Another real world application is in creating digital signatures for official documents.

Exercise 9.2. *A two-storey office in Kocourkov houses 10 officials on each floor, plus a director. The office may issue a decision with a round stamp, if at least 5 officials from the 1st floor are present and 3 from the 2nd floor, or at least 2 from the 1st floor, 8 from the 2nd floor, and the director. Design a key-sharing scheme for creating a safe stamp. (Similarities to the city of Prague are purely coincidental.)*

9.3. **Error-correcting codes.** The problem we study in this section is: How to detect and eliminate random errors in a data stream? A typical situation is the transmission of information over an unreliable channel (noise, data loss, etc.), but the same question also applies to the distortion that happens under long-term storage of data.

The mathematical model of the situation is as follows: the transmitter sends a word of length k in an alphabet A (in the setting with bit vectors $A = \mathbb{Z}_2$). The channel randomly changes some letters, and the receiver has to detect if there was an error, and to reconstruct the original message. In our simple setting (which is not realistic, but a good starting point) we assume that that at most e errors occur in each word of length k, and that errors consist in flipping the value of a bit (no bits are added or deleted).

One of the easiest ways of detecting an error is to do a parity test: for this, we attach to the original message (of length k) an extra bit, such that the sum of all bits is equal to 0 (modulo 2). If exactly one error occurs during the transmission, the checksum for the received message will return 1 and we know that there was a mistake. This system is time and space efficient, but does not allow to fix an error, since we don't know it happened. Furthermore, if 2 (or an even number) of errors happened, no mistake will be detected.

A second naive approach is to repeat the letters: we simply repeat each letter n-many times and assume that in each consecutive n-tuple there will be less than $n/2$ errors. We can then reconstruct the original message by "voting": the character which appears more often in an n-consecutive tuple was a character in the original message. This scheme works with a fairly weak channel reliability, but is very space

consuming: the length of the message is multiplied by a factor n. Is there a better procedure?

First, let's summarize what we're looking for. We want to replace every word of length k with a code word of some length $n \geq k$. These code words should further have the property that, after replacing a bounded number of characters, it is still possible to unambiguously reconstruct the original word.

Let us first define the so-called *Hamming distance*: for the words $u, v \in A^n$ the distance $\delta(u, v)$ is equal to the number of positions at which these words differ. A *self-correcting code* of type $(k, n; d)$ is then any function $\phi\colon A^k \to A^n$ such that for all $u, v \in \phi(A^k)$ in the image $u \neq v$ it holds that $\delta(u, v) \geq d$. For example, adding a parity bit is a $(k, k+1; 2)$-code, while character repetition is a $(1, n; n)$-code.

Let us call $C = \phi(A^k)$ the set of *code words*. For practical use it is also important that

- both $\phi\colon A^k \to C$ and $\phi^{-1}\colon C \to A^k$ can be computed efficiently.
- for each $u \in A^n$ it is possible to efficiently compute a codeword $v \in C$ such that $\delta(u, v)$ is minimal.

Because of this, often so called *linear codes* are used: then the alphabet A is equal to a field, and the representation function ϕ is linear. Thus the set of codewords C is a linear subspace of the vectorspace A^n.

Observe, that a code of type $(k, n; d)$ is able to correct $e = \lfloor \frac{d-1}{2} \rfloor$ many errors: when $\leq e$ letters of a code word u are changed, the result is a word v with $\delta(u, v) \leq e$. Because all codewords have a distance of at least $2e + 1$ from each other, u is the only codeword at distance $\leq e$ from v (if there was an other codeword u' with $\delta(u', v) \leq e$ we would get $2e+1 \leq \delta(u, u') \leq \delta(u, v) + \delta(v, u') \leq 2e$ - contradiction).

The first interesting error-correcting code were developed by Richard Hamming in the 1950ies, when designing some of the first computers at Bell laboratories. The so-called *Hamming (4, 7)-code* is able to correct one error in each seven, transmitted bits, at the cost of extending the length of the original message by a factor $\frac{7}{4}$. The basic idea is to use the linear map $\phi\colon \mathbb{Z}_2^4 \to \mathbb{Z}_2^7$, which is given as $\phi(u) = uM$, where M is the following matrix:

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

In other words, the codewords are computed by adding to the original codeword of length 4 a control sequence of length 3, each of which letter is a linear combination of the characters of the original message. Note that the images of the base vectors (i.e. the rows of the matrix) have each a Hamming distance of at least 3 from each other; it is not difficult to prove that this also holds for all codeword pairs. The Hamming-code is therefore a code of type $(4, 7; 3)$ that is able to correct 1 error. Verifying that a 7-letter word u is a codeword is also easy: for this we take the first four letters of u, compute their image under ϕ and check the result is equal to u.

If we detect an error, and if we assume that exactly one error occurred, we have exactly 7 positions where it could have occured. So we can correct it rather quickly by simply checking all 7 possibilities. Using linear algebra, even more efficient procedure can be found to correct a singe mistake, but this is beyond the scope of our

text.

In the 1960ies, the so-called *Reed-Salomon codes*, based on polynomial interpolation were developed. They have, in a certain sense, an optimal ratio of errors to length, and are the most widely used codes today. The alphabet then is again a finite field $\mathbb{F}$. The original word $(a_0, \dots, a_{k-1})$ is identified with the polynomial $\sum_{i=0}^{k-1} a_i x^i \mathbb{F}[x]$, and the codeword is computed by evaluating this polynomial at n-many pairwise different values $u_1, \dots, u_n \in \mathbb{F}$. So formally the Reed-Salomon (k, n)-code is defined as

$$\phi\colon F^k \to F^n, \quad f = \sum_{i=0}^{k-1} a_i x^i \mapsto (f(u_1), f(u_2), \dots, f(u_n)).$$

The inverse of ϕ can be efficiently computed by just taking the interpolation polynomials for the given function values.

If two polynomials of degree $< k$ coincide in at least k values, they must be identical (uniqueness part in Corollary 8.2). In other words, two different polynomials $f \neq g$ of degree $< k$ must have strictly less than k values in common. Thus $\phi(f)$ and $\phi(g)$ differ in $> n - k$ coordinates, so Reed-Salomon codes are of type $(k, n; d)$ for some $d \geq n - k + 1$. As a consequence they are able to correct $\lfloor \frac{n-k}{2} \rfloor$ many mistakes.

In practice, often $\mathbb{F} = \mathbb{F}_{256}$ and $n = 255$ are chosen together with a value of k that is suitable for the application (the smaller k, the more errors the code corrects, but the worse the ratio between the length of the original word and code words). For example, for $k = 253$, the code corrects one error for the price of word extension by about 1% , for $k = 127$ the code corrects 64 errors for the price of doubling the word length.

Furthermore, a special selection of points is often used in practice ($u_i = \alpha^{i-1}$, where α is a generator of the cyclic group $\mathbb{F}^*$, see Section 13), which simplifies the encoding and decoding using a fast Fourier transform. This significantly can increase the speed of the algorithm (standard substitution and interpolation algorithms run in quadratic time, which can be too slow for big amounts of data).

To successfully put it into practice, it remains to describe the algorithm for finding the nearest one codeword. For short codes correcting one error, this can be achieved by simply going though all options (as with Hamming codes), but in general this is not an easy task and we refer readers to specialized literature.

9.4. **Mutually orthogonal latin squares and experimental design.** A *latin square* on a set X is a square matrix $(a_{i,j})_{i,j \in I}$ indexed set I with entries $a_{i,j} \in X$ satisfying the following condition: Each element of X appears in each row and each column exactly once. Note that it immediately follows that $|I| = |X|$. So if $I = X$, we can regard a latin square $(a_{i,j})_{i,j \in I}$ as the operation table of a binary operation $*$ with $u * v = a_{u,v}$.

Example.

(1) Every (completed) sudoku is a latin square over the set $X = \{1, \dots, 9\}$
(2) The following 3 examples are latin squares on the set $X = \{0, 1, 2\}$:

0	1	2
1	2	0
2	0	1

0	2	1
2	1	0
1	0	2

0	2	1
1	0	2
2	1	0

The corresponding operations from left to right are $u * v = u + v \bmod 3$, respectively $-u - v \bmod 3$ and $u - v \bmod 3$.

(3) If $\mathbf{R}$ is a ring, then the operation $+$ defines a latin square over the set R with entries $(a+b)_{a,b\in R}$. If $\mathbf{F}$ is a field, then also the multiplication $\cdot$ is a latin square over $F^* = F \setminus \{0\}$ with entries $(a \cdot b)_{a,b\in F^*}$. We will see in Section 10, that every operation table of a group multiplication is a latin square.

Two latin squares $(a_{i,j})_{i,j\in I}$ and $(b_{i,j})_{i,j\in I}$ over sets X and Y are called *mutually orthogonal*, if each pair from $X \times Y$ appears just once in the list $((a_{i,j}, b_{i,j}) : i, j \in I)$.

Example. There are only two latin squares over the set $X = \{0, 1\}$, namely

$$\begin{array}{|cc|}\hline 0 & 1 \\ 1 & 0 \\ \hline\end{array} \qquad \begin{array}{|cc|}\hline 1 & 0 \\ 0 & 1 \\ \hline\end{array}$$

Because of this it is not hard to see that there are no mutually orthogonal latin squares of order 2 (either the pairs $(0,1)$ and $(1,0)$ would appear twice, or the pairs $(0,0)$ and $(1,1)$). There exist mutually orthogonal latin squares of order 3: The first and third square in the above example (2) can be seen to be mutually orthogonal. However, the first and second squares in (2) are not mutually orthogonal, since, when pairing them up, e.g. $(0,0)$ appears twice.

Exercise. From a standard deck of cards draw all the cards with the four figures (J, Q, K, A) from all four suits $(\diamondsuit, \heartsuit, \clubsuit, \spadesuit)$. Arrange the cards in a 4×4 square, such that in each row and in each column every figure and every suit appears exactly once.

Solution. The problem here actually consists to find two mutually orthogonal latin squares on four elements. The first set is the set of figures $X = \{J, Q, K, A\}$ in the second in the case of the set of suits $Y = \{\diamondsuit, \heartsuit, \clubsuit, \spadesuit\}$.

The squares must be Latin, because every row and column should contain all 4 elements of X respectively Y. Further the squares must be orthogonal to each other, since every card (that is, every element from $X \times Y$) can only be used one time. At first it is not clear if there is a solution and how to find it, but it is not difficult to verify that the following configuration works:

$$\begin{array}{|cccc|}\hline \text{A}\diamondsuit & \text{K}\heartsuit & \text{Q}\clubsuit & \text{J}\spadesuit \\ \text{K}\clubsuit & \text{A}\spadesuit & \text{J}\diamondsuit & \text{Q}\heartsuit \\ \text{Q}\spadesuit & \text{J}\clubsuit & \text{A}\heartsuit & \text{K}\diamondsuit \\ \text{J}\heartsuit & \text{Q}\diamondsuit & \text{K}\spadesuit & \text{A}\clubsuit \\ \hline\end{array}$$

We are going to show how to construct such a solution in Proposition 9.3. □

Exercise. A military parade is to be attended by 36 soldiers from 6 regiments, each consisting of 6 soldiers of 6 different ranks. Arrange the soldiers into a 6×6 square so that in each row and column there is one representative of each regiment and each rank.

It is not hard to see that the task in this exercise is again to find two orthogonal squares, this time on 6 elements. However, Gaston Tarry showed in 1901 that such squares do not exist. So a natural question is: for which numbers $n \in \mathbb{N}$ do mutually orthogonal squares of order n exist? This question was answered in 1959, showing that mutually orthogonal squares exists for all $n \neq 2, 6$.

In 1782, Euler discovered a partial solution for prime powers n, which we can easily construct using finite fields (Euler described them differently, the concept of finite fields was unknown at the time).

Proposition 9.3. *Let n be a power of a prime number and $n \neq 2$. Then there exist $n-1$ latin squares of order n that are all mutually orthogonal to each other.*

Proof. Let $\mathbb{F}_n$ be the field with n elements. Then, for each $0 \neq a \in \mathbb{F}_n$, let us define the square matrix $(au+v)_{u,v\in\mathbb{F}_n}$. First note that for a fixed a this is a latin square: If there are two entries in row u in position v_1, v_2 with the same value, then $au+v_1 = au+v_2 \Rightarrow v_1 = v_2$. Similarly if there are two entries in the same column v with such that $au_1 + v = au_2 + v$, then this implies $au_1 = au_2$, and therefore $u_1 = u_2$. Because $\mathbb{F}_n$ is finite, each element of $\mathbb{F}_n$ appears exactly once in every row/column.

In order to prove that two squares $(au+v)_{u,v\in\mathbb{F}_n}$ and $(bu+v)_{u,v\in\mathbb{F}_n}$ are mutually orthogonal, let us assume that there are pairs (u_1, v_1) and (u_2, v_2) such that both squares have the same values at these positions, in other words:

$$au_1 + v_1 = au_2 + v_2 \text{ and } bu_1 + v_1 = bu_2 + v_2.$$

This implies $a(u_1 - u_2) = v_2 - v_1 = b(u_1 - u_2)$. Since $a \neq b$, this equation only holds if $u_1 = u_2$ and thus $v_1 = v_2$. □

Proposition 9.4. *If there are mutually orthogonal latin squares of order m and n, then there are also such squares of order $m \cdot n$.*

Proof. Let $(a_{i,j})_{i,j\in I}$ and $(b_{i,j})_{i,j\in I}$be two mutually orthogonal latin squares over X_1, X_2 of size m, and let $(u_{k,l})_{k,l\in J}$ and $(v_{k,l})_{k,l\in J}$be two mutually orthogonal latin squares over sets Y_1, Y_2 of size n. Then we define the matrices $((a_{i,j}, u_{k,l}))_{(i,k)\times(j,l)\in I\times J}$ with entries from $X_1 \times Y_1$ and $((b_{i,j}, v_{k,l}))_{(i,k)\times(j,l)\in I\times J}$ with entries from $X_2 \times Y_2$. It is not too hard to show that these are mutually orthogonal latin squares, we leave it as an exercise. □

Corollary 9.5. *For every $n \not\equiv 2 \pmod 4$ there exist mutually orthogonal matrices of order n.*

Proof. Let $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ be a prime decomposition of n. Since $n \not\equiv 2 \pmod 4$, none of the prime powers $p_i^{k_i}$ is equal to 2^1. By Proposition 9.3 there exist mutually orthogonal latin squares of order $p_i^{k_i}$ for all $i = 1, \ldots, m$. By repeatedly applying Proposition 9.4 we can also construct mutually orthogonal latin squares of order n. □

For $n = 2$ we have already shown that mutually orthogonal latin squares do not exist, for $n = 6$ by the already mentioned result no example exists. You might be tempted to conjecture (like Euler) that for no number $n \not\equiv 2 \pmod 4$ mutually orthogonal latin squares exists. However, in 1958, it was shown that for all $n \geq 10$, there is also a solution. Thus $n = 2, 6$ are the only exceptions.

However, it remains unclear up to this day how many orthogonal squares of a fixed size n can exist. It is not difficult to prove that there are at most $n-1$, so Proposition 9.3 gives the optimal answer for prime powers n. But for other numbers it is unknown. For $n = 10$ for instance, there are provably less than 9 such squares, but how many is unknown. (The existence of $n-1$ mutually orthogonal

Latin squares of order n is equivalent to the existence of a projective plane of order n, connecting the problem with finite geometries).

And what about the *design of experiments* mentioned in the section title? Consider the following problem: We have n varieties of a given crop, n types of fertilizer and n types of pesticide and want to find out which combination is best. If we wanted to try all the combinations, we need n^3 experiments; which is a lot (especially if you're a researcher with scarce funding).

Wouldn't n^2 be enough? To still get a balanced experiment set-up there are then two reasonable conditions: every object (crop, fertilizer, pesticide) is used the same number of times (n times) and further we would like each pair of objects to be used just once (so that we can better trace back interesting outcomes to a specific combination of variables). A solution to this problem is a Latin square $(a_{i,j})_{i,j}$ over the set $\{1, 2 \ldots, n\}$. We divide the experimental field into $n \times n$ fields, such that we sow the i-th crop variety in the i-th row, pour the j-th fertilizer into the j-th column and use the $a_{i,j}$-th pesticide on index (i, j).

Now consider adding another factor, such as n degrees of irrigation. We can construct a second latin square $(b_{i,j})_{i,j}$ for it and we will irrigate the field with index $b_{i,j}$; But it's not good to take this square arbitrarily: if, for example, we choose $b_{i,j} = a_{i,j}$ then plants who receive the same pesticide use also the same level of water. If we pick $(b_{i,j})$ to be an orthogonal square to $(a_{i,j})$ however, this problem will not appear.

This was a simple example of a problem that is studied in *design theory*, an area of mathematics which deals with the construction of objects with various requirements for "balance", and has application in design of statistical experiments.

Groups

10. Groups

10.1. **Definition and examples.** One of the main motivations for group theory is to study the symmetries and transformations of mathematical objects. The name *group* originally came from Galois theory and referred to a 'group' (in the sense of 'set') of permutations G that are closed under composition. So for all permutation $\pi, \sigma \in G$ also their composition $\pi \circ \sigma$ is an element of G.

The abstraction of this concept created a big branch of algebra, called *group theory*. Applications of group theory can be found in many different areas of mathematics, such as in combinatorics (finite groups) and geometry (linear groups).

Definition. A *group* $\mathbf{G} = (G, *, ', e)$, consists of a set G, a binary operation $*\colon G \times G \to G$, a unary operation $'\colon G \to G$ and a constant $e \in G$, such that for all $a, b, c \in G$ the following identities hold:

$$a * (b * c) = (a * b) * c, \qquad a * e = e * a = a, \qquad a * a' = a' * a = e.$$

The group is additionally called *Abelian* if for all $a, b \in G$:

$$a * b = b * a.$$

The element e is called the *neutral* element. For every $a \in G$, the element a' is called the *inverse element* of a.

Similar to rings, we formally distinguish the *carrier set* G and the group $\mathbf{G} = (G, *, ', e)$, which additionally contains the information about the algebraic structure.

For specific examples of groups often the notation $\cdot, ^{-1}, 1$ (multiplicative notation) or $+, -, 0$ (additive notation) is used to describe the group operations. The additive notation is usually reserved for Abelian groups.

Definition. Let $\mathbf{G} = (G, *, ', e)$ be a group and $H \subseteq G$ be a subset of the carrier set, such that $e \in H$, and for all $a, b \in H$ also

$$a' \in H \text{ and } a * b \in H.$$

We then say that H is closed under the group operations of $\mathbf{G}$. In this case, also $\mathbf{H} = (H, *|_H, '|_H, e)$, where $|_H$ denotes the restriction to H is a group. We call $\mathbf{H}$ a *subgroup* of $\mathbf{G}$, and write for short $\mathbf{H} \leq \mathbf{G}$. Every group $\mathbf{G}$ has $\{e\}$ and $\mathbf{G}$ as subgroups; these two are called the *trivial* subgroups.

There are countless examples of groups in mathematics; but we will only give examples of four important families of groups, which find very widespread use: permutation groups, matrix groups, groups describing geometric transformations and groups stemming from rings.

Example. The *symmetric group* $\mathbf{S}_X$ consists of the set of all the permutations on a given non-empty set X, together with the binary operation $\circ$ (which composes two permutations), $^{-1}$ (which outputs the inverse function), and the neutral element $id\colon x \mapsto x$, so

$$\mathbf{S}_X = (\{\pi\colon \pi \text{ is a permutation of } X, \}, \circ, ^{-1}, id).$$

For finite sets $X = \{1, \ldots, n\}$, we also write $\mathbf{S}_n$ instead of $\mathbf{S}_X$. The subgroups of $\mathbf{S}_X$ are called *permutation groups*. Some important examples are

- the alternating group $\mathbf{A}_n \leq \mathbf{S}_n$, which contains all even permutations.

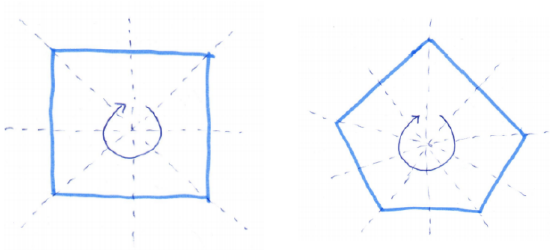


FIGURE 6. The dihedral groups $\mathbf{D}_8$ and $\mathbf{D}_{10}$

- Let us label the vertices of a regular n-gon by the numbers $1, 2, \ldots, n$ (clockwise). The dihedral group $\mathbf{D}_{2n} \leq \mathbf{S}_n$ consists then of all the permutations of $\{1, 2, \ldots, n\}$ that preserve the edges of the n-gon. This corresponds to all symmetries (reflections and rotations) of the n-gon (see Figure 6).
- various other symmetry groups of geometric objects, automorphism groups of graphs and other mathematical structures.

Example. A special type of permutation group are groups describing geometric transformations of geometrical spaces (Euclidean, affine, projective, ...) that preserve certain properties. An example of this is the *Euclidean group* $\mathbf{E}_n$, which consists of all *isometries* of the Euclidean space $\mathbb{R}^n$ (so all the permutations of $\mathbb{R}^n$ that preserve all distances). This gives us another possible way to describe the dihedral group $\mathbf{D}_{2n}$; namely as the subgroup of all elements of $\mathbf{E}_2$ that map the entire regular n-gon to itself.

Example (Matrix groups)**.** If $\mathbb{F}$ is a field, and $n \in \mathbb{N}$, then the *general linear group* $\mathbf{GL_n}(\mathbf{F})$ consists of the regular $n \times n$ matrices with entries from $\mathbb{F}$. The operations are the matrix multiplication $\cdot$, the matrix inversion $^{-1}$, and the identity matrix I as the neutral element, so

$$\mathbf{GL_n}(\mathbf{F}) = (\{A\colon A \text{ is a regular } n \times n \text{ matrix over the field } \mathbf{F}\}, \cdot, ^{-1}, I).$$

The subgroups of the general linear group are called *matrix groups*. Examples include:

- the *special linear group* $\mathbf{SL_n}(\mathbf{F})$, consisting of all matrices with determinant 1;
- the *orthogonal group* $\mathbf{O_n}(\mathbf{F})$, which consists of all orthogonal matrices, i.e. all matrices A such that $AA^T = I$ (Over the field $\mathbb{R}$, these are all the matrices, whose rows form an orthonormal basis with respect to the standard inner product).

Permutation and matrix groups are, in a sense, universal examples: Every group G can be represented as a permutation group and every finite group can be represent as a matrix group (you can learn more about this in Algebra 2).

Example. The quaternion group $\mathbf{Q}_8$ is defined on the set $\{\pm 1, \pm i, \pm j, \pm k\}$. Its multiplication $\cdot$ is defined by

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ jk = i,\ ki = j,$$

and $xy = -(yx)$ and $(-x)y = x(-y) = -(xy)$ for all $x, y \in \{i, j, k\}$.

A big source of Abelian groups are groups derived from commutative rings:

Example. Let $\mathbf{R} = (R, +, -, 0, \cdot)$ be a ring. Then $(R, +, -, 0)$ is an Abelian group. Examples here include many 'arithmetical' groups, such as $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and the group $\mathbb{Z}_n$ of elements $\{0, 1, 2, \ldots, n-1\}$ together with the addition modulo n.

Example. Let $\mathbf{R} = (R, +, -, 0, \cdot)$ be a commutative ring with unity 1, and let R^* be the set of invertible elements in $\mathbf{R}$. Then $\mathbf{R}^* = (R, \cdot, ^{-1}, 1)$ is an Abelian group, the *multiplicative group* of $\mathbf{R}$. It is easy to verify that $\mathbf{R}^*$ indeed satisfies the group axioms, most of them follow directly from the ring axioms for $\mathbf{R}$. Furthermore $a^{-1} \cdot a = 1$ for all $a \in R^*$, by the definition of invertible element.

- If $\mathbf{R}^*$ is a field, then $\mathbf{R}^* = (R \setminus \{0\}, \cdot, ^{-1}, 1)$.
- For every polynomial ring $(\mathbf{R}[x])^* = \mathbf{R}^*$, since the only invertible elements are the constant polynomials, which are invertible in $\mathbf{R}^*$
- $\mathbb{Z}^* = (\{1, -1\}, \cdot, ^{-1}, 1)$.
- For every $n \in \mathbb{N}$ the group $\mathbb{Z}_n^*$ consists of the elements $a \in \{1, \ldots, n-1\}$, which are coprime to n.

An important tool in the construction of groups is the direct product:

Definition. The *direct product* of a family of groups $\mathbf{G}_i = (G_i, *_i, '^i, e_i)$ for $i \in 1, \ldots, n$ is defined as the group

$$\prod_{i=1}^{n} \mathbf{G}_i = \mathbf{G}_1 \times \mathbf{G}_2 \times \cdots \times \mathbf{G}_n = (G_1 \times \cdots \times G_n, *, ', e),$$

such that its operations are defined coordinate-wise,i.e. for elements $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in G_1 \times \cdots \times G_n$:

$$\begin{aligned}(a_1, \ldots, a_n) * (b_1, \ldots, b_n) &= (a_1 *_1 b_1, \ldots, a_n *_n b_n),\\ (a_1, \ldots, a_n)' &= ((a_1)'^1, \ldots, (a_n)'^n),\\ e &= (e_1, \ldots, e_n).\end{aligned}$$

It is not hard to see that these operations satisfy the group axioms, implying that the direct product of groups is also a group.

In the case in which the groups $\mathbf{G}_1 = \cdots = \mathbf{G}_n = \mathbf{G}$ are equal, we call their direct product a *direct power* of $\mathbf{G}$, and denote it by $\mathbf{G}^n$.

W remark that we can analogously also define the direct products of rings (or of other families of algebraic structures of the same type).

As in the case of commutative rings, the definition of groups contains only the minimum number of necessary axioms. In the following proposition we derive some direct consequences:

Proposition 10.1 (Basic properties of groups)**.** *Let $\mathbf{G} = (G, *, ', e)$ be a group and $a, b, c \in G$. Then*

(1) *If $a * c = b * c$ or $c * a = c * b$, then $a = b$;*
(2) *if $a * b = a$ or $b * a = a$, then $b = e$;*
(3) *if $a * b = e$ or $b * a = e$, then $b = a'$;*
(4) *$(a')' = a$;*
(5) *$(a * b)' = (b') * (a')$.*

Proof.

(1) If $a * c = b * c$, then $(a * c) * c' = (b * c) * c'$. By the group axioms we can rewrite the left side to $(a * c) * c' = a * (c * c') = a * e = a$, and similarly the right side to $(b * c) * c' = b$. Thus $a = b$. The proof for $c * a = c * b$ is symmetric.
(2) If $a * b = a = a * e$, then (1) implies $b = e$. The proof is symmetric for $b * a = a$.
(3) If $a * b = e = a * a'$, then (1) implies $b = a'$. The proof is symmetric for $b * a = e$.
(4) This follows directly from $a' * a = e$ and the uniqueness of the inverse element of a' shown in (3).
(5) For this, note that $(a * b) * (b' * a') = a * (b * b') * a' = a * e * a' = a * a' = e$. By (3) we get $(a * b)' = b' * a'$.

□

Note also that, by the associativity of $*$, we don't need to care about brackets when writing down products $a_1 * a_2 * \ldots * a_n$ of more than two group elements (Proposition 3.1).

10.2. **Powers and the order of a group element.** In the last section we already mentioned that group operations are sometimes denoted by different symbols. Starting from this section, we are going to stick to the multiplicative notation, if not stated otherwise. So we are going to write $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ for a general group.

In the multiplicative notation, for an element $a \in G$ and $n \in \mathbb{Z}$, then we define the *n-th power of a* by

$$a^n = \begin{cases} 1 & \text{if } n = 0 \\ \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ times}} & \text{if } n > 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{-n \text{ times}} & \text{if } n < 0 \end{cases}$$

The following rules hold for powers:

Proposition 10.2 (powers)**.** *Let $\mathbf{G}$ be a group, $a, b \in G$ and $k, l \in \mathbb{Z}$. Then*

$$a^{k+l} = a^k \cdot a^l, \qquad a^{kl} = (a^k)^l = (a^l)^k.$$

If $\mathbf{G}$ is and Abelian group, then additionally $(ab)^k = a^k b^k$ holds.

Proof. We prove $a^{k+l} = a^k \cdot a^l$. If $k, l \geq 0$, we immediately see that the number of a's appearing on both the products on the left and right side are equal; thus the identity holds. Analogously we can deal with $k, l \leq 0$ (then we get a product of the same number of inverses a^{-1} on both sides).

In the remaining cases, a certain number of a and a^{-1} in the product on the right hand side cancel out. Let us assume for instance that $k > 0 > l$ and $|l| < |k|$; then

$$a^k \cdot a^l = \underbrace{a \cdot \ldots \cdot a}_{k} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{-l} = \underbrace{a \cdot \ldots \cdot a}_{k+l} \cdot \underbrace{a \cdot \ldots \cdot a}_{-l} \cdot \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{-l} = a^{k+l}.$$

the right side consists of the product of k-many copies of a and $(-l)$-many copies of a^{-1}. All other cases can be dealt with in the same way.

We leave the proof of the remaining identities as an exercises. □

If we look at a group $\mathbf{G} = (G, +, -, 0)$ in the *additive notation*, the expression $\underbrace{a + a + \ldots + a}_{n \text{ times}}$ is usually shortened to $n \cdot a$. Then Proposition 10.2 implies

$$(k + l) \cdot a = k \cdot a + l \cdot a, \quad (kl) \cdot a = k \cdot (la), \quad k \cdot (a + b) = k \cdot a + k \cdot b,$$

where the last equality only applies to Abelian groups.(If you think these identities resemble the definition of vector space, you are on the right track. The theory of Abelian groups is to a large extent equal to the theory of *modules* over $\mathbb{Z}$, where modules are a generalization of vector spaces. However, we are not going to discuss modules in this course).

Definition. The *order of a group* $\mathbf{G}$ is defined as the size of its carrier set; we write $|\mathbf{G}|$ for it.
Let a be an element of a group $\mathbf{G}$. Then we define $\mathrm{ord}(a)$, the *order of* a, to be the smallest $n \in \mathbb{N}$ such that $a^n = 1$. If no such n exists then we set $\mathrm{ord}(a) = \infty$.

It might seem confusing that we use "order" to describe two different concepts for groups; but we will see in the next section that the order of an element is equal to the order of the subgroup it generates. We give a few examples:

Example.

- $\mathrm{ord}(2) = 7$ in $\mathbb{Z}_7$, since $7 \cdot 2 \equiv 0 \pmod 7$, but $n \cdot 2 \not\equiv 0 \pmod 7$ for all $n = 1, \ldots 6$:
- $\mathrm{ord}(2) = 3$ in the multiplication group $\mathbb{Z}_7^*$, since $2^3 \equiv 1 \pmod 7$, but $2^n \not\equiv 1 \pmod 7$ for $n = 1, 2$.

Thus it is important to always specify, with respect to which group we study the order of an element.

Example. Infinite groups can have elements of arbitrary order:

- In $\mathbb{Q}$, we have $\mathrm{ord}(0) = 1$ and $\mathrm{ord}(a) = \infty$ for all $a \neq 0$
- In $\mathbb{Q}^*$, we have $\mathrm{ord}(1) = 1$, $\mathrm{ord}(-1) = 2$ and $\mathrm{ord}(a) = \infty$ for all $a \neq \pm 1$
- In the group $\mathbb{C}^*$ we have $\mathrm{ord}(e^{2\pi i/k}) = k$ for every $k \in \mathbb{N}$.

Example. Finite groups of the same order do not have to have elements of the same orders

- In $\mathbb{Z}_6$, we have $\mathrm{ord}(0) = 1$, $\mathrm{ord}(1) = 6$, $\mathrm{ord}(2) = 3$, $\mathrm{ord}(3) = 2$, $\mathrm{ord}(4) = 3$, $\mathrm{ord}(5) = 6$; so we get elements of orders $1, 2, 3, 6$
- In $\mathrm{Sym}(3)$ we have $\mathrm{ord}(id) = 1$, $\mathrm{ord}((i, j)) = 2$, $\mathrm{ord}((i, j, k)) = 3$, so there are elements of order $1, 2$ and 3.

Note that (in the finite case) the order of each element divides the order of the whole group. This is not a coincidence, but follows from Lagrange's theorem, which we are going to prove in the next section.

Proposition 10.3 (The order of a permutation)**.** *Let $\pi \in \mathbf{S}_n$ be a permutation. Then its order is equal to the least common multiple of the length of its cycles.*

Proof. It is easy to see that a cycle of length l has order l. Next, assume that $C_1, \ldots, C_m$ are the disjoint cycles, such that $\pi = C_1 \circ \cdots \circ C_m$. As they are disjoint, $\pi^k = (C_1 \circ \cdots \circ C_m)^k = C_1^k \circ \cdots \circ C_m^k$ holds for every k. It is now not hard to see that $(C_1 \circ \cdots \circ C_m)^k = id$ if k is a multiple of all cycle lengths; thus the least common multiple of all cycle lengths is equal to the order of π. □

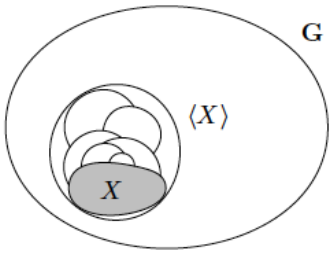


FIGURE 7. The subgroup generated by X

11. Subgroups

11.1. Generators.

Lemma 11.1. *The intersection of a family of subgroups is again a subgroup.*

Proof. Let $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ be a group and $(\mathbf{H}_i)_{i\in I}$ a family of subgroups of $\mathbf{G}$. Let $H = \bigcap_{i\in I} H_i$ be the intersection of the carrier sets of the $\mathbf{H}_i$. We then are going to show that H is closed under the group operations.

Since $1 \in H_i$ for all $i \in I$, clearly also $1 \in H$. Next, assume that $a, b \in H$. This implies that $a, b \in H_i$ for all $i \in I$. Since every H_i is closed under $\cdot$, we get that $a \cdot b \in H_i$ for all $i \in I$. In other words $a \cdot b$ must be in the intersection $H = \bigcap_{i\in I} H_i$.

Finally note that $a \in H$ means that $a \in H_i$ for all $i \in I$. Since every $\mathbf{H}_i$ is a subgroup, also $a^{-1} \in H_i$ for every $i \in I$. In other words $a^{-1} \in H = \bigcap_{i\in I} H_i$. Thus H is closed under the group operations, and thus $\mathbf{H} = (H, \cdot, ^{-1}, 1)$ forms a subgroup of $\mathbf{G}$. □

Definition. Let $\mathbf{G}$ be a group and $X \subseteq G$ be a subset of its carrier set. Then we define the *subgroup generated by* X as the smallest subgroup of $\mathbf{G}$ (with respect to inclusion) that contains X. For short, we write $\langle X\rangle_{\mathbf{G}}$ for the subgroup generated by X. Such a group always exists, we can simply take the intersection

$$\langle X\rangle_{\mathbf{G}} = \bigcap\{\mathbf{H} \leq \mathbf{G} \colon X \subseteq H\}.$$

By definition $\langle X\rangle_{\mathbf{G}}$ contains X, and is a subset of every subgroup containing X; and by the previous Lemma 11.1, it is a subgroup of $\mathbf{G}$ itself.

Given a subset $X \subseteq G$, how can we compute the subgroup generated by it? For finite groups it is possible to use a 'greedy' algorithm: we start with the elements of the set X and add to it all products and inverses of elements of X. We iterate this step and stop, when we are unable to add any new elements. Then our set is closed under the group operations and thus equal to the subgroup generated by X (see Figure 7).

However, it is sometimes more effective to use the following statement, which is also true for infinite groups.

Proposition 11.2. *Let* $\mathbf{G}$ *be a group and* $X \subseteq G$*. Then*

$$\langle X\rangle_{\mathbf{G}} = \{a_1^{k_1} \cdot a_2^{k_2} \cdot \ldots \cdot a_n^{k_n} \colon\ n \in \mathbb{N}, a_1, \ldots, a_n \in X, k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Proof. Let us for short write M for the set on the right hand side of the above equation. To show that M is equal to $\langle X\rangle_{\mathbf{G}}$, we need to show that

(1) M is a subgroup of $\mathbf{G}$,
(2) M contains X,
(3) M is the smallest subgroup containing X.

It is not hard to see that M is closed under the group multiplication $\cdot$. Further $1 = a^0 \in M$, and for every element $a = a_1^{k_1} \cdot a_2^{k_2} \cdot \ldots \cdot a_n^{k_n} \in M$, also it inverse $a^{-1} = (a_1^{k_1} \cdot a_2^{k_2} \cdot \ldots \cdot a_n^{k_n})^{-1} = a_n^{-k_n} \cdot \ldots \cdot a_2^{-k_2} \cdot a_1^{-k_1} \in M$. Therefore (1) holds.

For (2), simply note that for every $a \in X$ also $a = a^1 \in X$.

To see (3), let $\mathbf{H}$ be an arbitrary subgroup of $\mathbf{G}$ containing X. Then, for every $a \in X$ and $k \in \mathbb{Z}$ it also must contain a^k. Since $\mathbf{H}$ is closed under the group multiplication, it also must contain all expressions $a_1^{k_1} \cdot a_2^{k_2} \cdot \ldots \cdot a_n^{k_n}$, such that all a_i are in X, thus H contains M. □

As direct consequences we obtain the following:

Corollary 11.3. *Let* $\mathbf{G}$ *be a group and* $a \in G$. *Then* $\langle a\rangle_{\mathbf{G}} = \{a^k \colon k \in \mathbb{Z}\}$.

Corollary 11.4. *Let* $\mathbf{G}$ *be an* Abelian *group and* $u_1, u_2, \ldots, u_n \in G$. *Then*

$$\langle u_1, u_2, \ldots, u_n\rangle_{\mathbf{G}} = \{u_1^{k_1} \cdot u_2^{k_2} \cdot \ldots \cdot u_n^{k_n} \colon k_1, \ldots, k_n \in \mathbb{Z}\}.$$

If we use the additive notation $\mathbf{G} = (G, +, -, 0)$ for an Abelian group, then $\langle u_1, u_2, \ldots, u_n\rangle_{\mathbf{G}} = \{k_1u_1 + k_2u_2 + \ldots + k_nu_n \colon k_1, \ldots, k_n \in \mathbb{Z}\}$. (So the generated subgroup can be obtained similarly to the span of some vectors in a vector space. However, be careful: Notions such as linear independence, basis, and dimension, cannot be directly generalized!).

Example. It is a recurring problem to figure out which subgroups are generated by a given set:

- $\langle \frac{3}{4}, \frac{1}{3}\rangle_{\mathbb{Q}} = \{k\frac{3}{4} + l\frac{1}{3} \colon k, l \in \mathbb{Z}\} = \{\frac{k}{12} \colon k \in \mathbb{Z}\} = \langle \frac{1}{12}\rangle_{\mathbb{Q}}$. Here, the first and last equation follow from Corollary 11.4. The second equality holds, since $\frac{3}{4}, \frac{1}{3} \in \langle \frac{1}{12}\rangle$ on one hand and $\frac{1}{12} \in \langle \frac{3}{4}, \frac{1}{3}\rangle_{\mathbb{Q}}$ on the other hand (since $\frac{1}{12} = \frac{3}{4} - 2 \cdot \frac{1}{3}$).
- $\langle \frac{3}{4}, \frac{1}{3}\rangle_{\mathbb{Q}^*} = \{(\frac{3}{4})^k \cdot (\frac{1}{3})^l \colon k, l \in \mathbb{Z}\} = \{3^l 4^k \colon k, l \in \mathbb{Z}\}$.

Example. Another important problem is to find a minimal (or particularly nice) set of generators for a given group. So, given a group $\mathbf{G}$, find a 'small' set X such that $\langle X\rangle_{\mathbf{G}} = G$.

- $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$, $\mathbb{Z}^* = \langle -1\rangle$, $\mathbb{Q}^* = \langle -1, \text{primes }\rangle$.
- $\mathbb{Z}_n = \langle 1\rangle$, however the multiplication group $\mathbb{Z}_n^*$ does not need to be generated by one element. For example $\mathbb{Z}_7^* = \langle 3\rangle$, but $\mathbb{Z}_8^* = \langle 3, 5\rangle$, and every generating set of $\mathbb{Z}_8^*$ is least of size 2.
- There are (infinite) groups that don't have a minimal set of generators. For instance $\{\frac{1}{n} \colon n \in \mathbb{N}\}$ generates $\mathbb{Q}$, and omitting finitely many elements gives us still a set of generators, but a minimal subset does not exists.

Proposition 11.5 (Generators of permutation groups)**.**

- *The symmetric group* $\mathbf{S}_n$ *is generated by all transpositions.*
- *The alternating group* $\mathbf{A}_n$ *is generated by all cycles of length 3.*

Proof. Every permutation can be written as the product of cycles. A cycle of arbitrary length can be decomposed into transpositions as follows

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

Therefore $\mathbf{S}_n$ is generated by all transpositions.

The alternating group $\mathbf{A}_n$, by definition, consists of all permutations that can be written as a product of an even number of transpositions. Therefore it is enough to show that every product of 2 transpositions can be written as a product of 3-cycles. But this holds since $(ij) \circ (ij) = id$, $(ij) \circ (jk) = (ijk)$ and $(ij) \circ (kl) = (kil) \circ (ijk)$ for all pairwise different elements i, j, l, k. □

The above set of generators of $\mathbf{S}_n$ is not of minimal size, as can be seen from the following example:

Example.

$$\mathbf{S}_n = \langle (12), (123 \dots n) \rangle$$

Proof. Thanks to Proposition 11.5, we know that every permutation can be written as the product of transpositions. Thus it is enough to show that (12) and $(123 \dots n)$ generate all transpositions. First we show that we can generate the transposition $(k\, k+1)$ for every $k = 1, 2, \dots, n-1$. But this can be easily shown by the induction $(k+1\, k+2) = (123 \dots n) \cdot (k\, k+1) \cdot (123 \dots n)^{-1}$.

Next, we show that for a fixed k all the permutations $(k\, k+i)$ are generated. This can be shown by induction on $i = 1, 2, \dots$; an induction step can be shown by $(k\, k+i+1) = (k+i\, k+i+1) \circ (k\, k+i) \circ (k+i\, k+i+1)^{-1}$. □

Proposition 11.6 (Order of an element vs. order of subgroup)**.** *Let* $\mathbf{G}$ *be a group and* $a \in G$*. Then*

$$\operatorname{ord}(a) = |\langle a \rangle_{\mathbf{G}}|$$

Proof. By Corollary 11.3, the subgroup generated by a is equal to $\langle a \rangle_{\mathbf{G}} = \{a^k \colon k \in \mathbb{Z}\}$. Now there are two cases: Either all elements a^k are pairwise different from each other. Then $|\{a^k \colon k \in \mathbb{Z}\}| = \infty$, and clearly also $\operatorname{ord}(a) = \infty$. In the other case, there are numbers $k \geq 0$, $l > 0$, such that $a^k = a^{k+l}$. In fact, this equation is equivalent to the same equation *any* $k \in \mathbb{Z}$ (you can see this by multiplying with suitable powers of a on both sides). In particular it is equivalent to $1 = a^0 = a^l$. Let l be the minimal number such that it holds. Then, by definition $\operatorname{ord}(a) = l$. But on the other hand, since $a^k = a^{k+l}$, for all k: $\langle a \rangle_{\mathbf{G}} = \{e, a, a^2, \dots a^{l-1}\}$, thus $|\operatorname{ord}(a)| = |\langle a \rangle_{\mathbf{G}}|$. □

11.2. **Langrange's theorem.** A fundamental property of finite groups is the fact that the order of a subgroup divides the order of the whole group, i.e.

$$\mathbf{H} \leq \mathbf{G} \Rightarrow |\mathbf{H}| \mid |\mathbf{G}|.$$

In particular, thanks to it, the order of an element always divides the order of the entire group. The proof of this theorem by Lagrange is not complicated: we divide the whole group $\mathbf{G}$ into several subsets, all of which are pairwise disjoint and of the same size as $\mathbf{H}$. The number of elements of group $\mathbf{G}$ will be equal to the number of elements $\mathbf{H}$. times the number of these subset.

Definition. Let $\mathbf{G}$ be a group and $\mathbf{H}$ be a subgroup of $\mathbf{G}$.

- The set $aH = \{ah \colon h \in H\}$, where $a \in G$, is called a *left coset* of H.

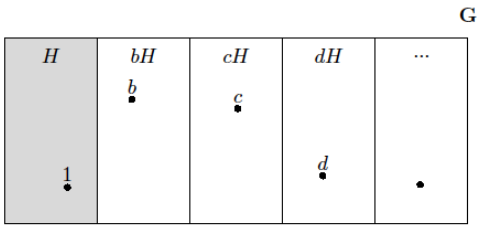


FIGURE 8. A group **G**, subgroup **H**, and a transversal of the cosets of **H**.

- A set T is called a *transversal* of the cosets of H if $|T \cap aH| = 1$ for every $a \in G$.
- The *index* of a subgroup **H** is defined as the number of its cosets:

$$[\mathbf{G} : \mathbf{H}] = |\{aH \colon a \in G\}|$$

Note that, in this definition we defined the cosets of **H** by multiplying with elements from the left. We can also look at cosets that we obtain by multiplication from the right, i.e. *right cosets* $Ha = \{ah \colon h \in H\}$. In general the right and left cosets of a subgroup are different.

Example. Let $n \in \mathbb{N}$, and $\mathbf{H} = \{x \in \mathbb{Z} \colon n \mid x\}$. Then it is not hard to see, that for $a \in Z$ the coset is given by

$$a + H = \{a + h \colon h \in H\} = \{a + kn \colon k \in \mathbb{Z}\} = \{u \in \mathbb{Z} \colon u \equiv a \pmod{n}\}.$$

In this example two cosets $a + H$ and $b + H$ are either equal (if $a \equiv b \pmod{n}$), or disjoint. We are going to prove that this fact also holds in general.

Example. Let $\mathbf{H} = \mathbf{A}_n \leq \mathbf{S}_n = \mathbf{G}$. Then $\pi A_n = A_n \pi = A_n$ holds for every even permutation π, and $\pi A_n = A_n \pi$ for every odd π. The group $\mathbf{S}_n$ therefore composes into two composition classes with transversal set $T = \{id, (12)\}$.

The left and right cosets do not always have to be equal, as can be seen from the following example:

Example. Let $\mathbf{G} = \mathbf{S}_3$, and $\mathbf{H} = \{id, (12)\}$. We can easily compute the left and right coset of H with respect to (13), which are:

$$H \circ (13) = \{(13), (123)\}, \text{ but } (13) \circ H = \{13), (132)\}.$$

We can prove Lagrange's theorem by showing two properties of cosets: if two cosets of a given subgroup are not equal, they are disjoint; and all cosets have the same size.

Lemma 11.7. *Let* $\mathbf{H} \leq \mathbf{G}$*. Then, for all* $a, b \in G$*, either* $aH = bH$*, or* $aH \cap bH = \emptyset$*.*

Proof. Let us assume that $aH \cap bH \neq \emptyset$. Then we are going to prove that $aH = bH$. Let $c \in aH \cap bH$, so there are elements $h_1, h_2 \in H$ such that $c = ah_1 = bh_2$. Then, for every $ah \in aH$ we have

$$ah = ah_1 h_1^{-1} h = b \underbrace{h_2 h_1^{-1} h}_{\in H},$$

thus $ah \in bH$. □

Lemma 11.8. *Let* $\mathbf{H} \leq \mathbf{G}$. *Then, for all* $a \in G$: $|aH| = |H|$.

Proof. In order to prove this statement, let us define the map $f\colon G \to G$, by $f(x) = ax$. This map is injective, since $ax = f(x) = f(y) = ay$ implies that $x = y$ (by multiplying with a^{-1} on both sides). It is even a bijection, since every element $b \in G$ is the image $b = f(a^{-1}b)$. Since $f(H) = aH$, $f|_H$ must be a bijection between H and aH, and thus $|aH| = |H|$. □

Using these lemmas we are next going to prove Langrange's theorem. We remark that its statement is even correct for infinite groups (using cardinal arithmetic, i.e. $|A| \cdot |B| = |A \times B|$), however we will just apply it to finite groups.

Theorem 11.9 (Lagrange's theorem)**.** *Let* $\mathbf{G}$ *be a group and* $\mathbf{H}$ *a subgroup. Then*

$$|\mathbf{G}| = |\mathbf{H}| \cdot [\mathbf{G} : \mathbf{H}]$$

Proof. Let T be a transversal set (with respect to the cosets of $\mathbf{H}$). Then

$$G = \bigcup_{a \in T} aH.$$

By Lemma 11.7 these cosets are all disjoint, and by Lemma 11.8 they are of the same size as $|H|$. Thus

$$|\mathbf{G}| = \sum_{a \in T} |aH| = \sum_{a \in T} |H| = |T| \cdot |H| = [\mathbf{G} : \mathbf{H}] \cdot |\mathbf{H}|.$$

In the last equation we use $|T| = [\mathbf{G} : \mathbf{H}]$, which just follows from the definition of the transversal set. □

Example. A special case of Lagrange's theorem is Euler's theorem (Theorem 2.4), which we already proved directly. For an alternative proof we can set $\mathbf{G} = \mathbb{Z}_n^*$ and $\mathbf{H} = \langle a \rangle$. By Lagrange's theorem then $\operatorname{ord}(a) = |\mathbf{H}|$ must divide $|\mathbb{Z}_n^*| = \varphi(n)$, and therefore

$$a^{\varphi(n)} = a^{\operatorname{ord}(a) \cdot k} = (a^{\operatorname{ord}(a)})^k = 1^k = 1,$$

or, in the language of number theory, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

To conclude this section, we will a criterion that characterizes the situation in which two elements lie in the same coset with respect to H

Proposition 11.10. *Let* $\mathbf{G}$ *be a group and* $\mathbf{H}$ *a subgroup. For all* $a, b \in G$ *it then holds that:*

(1) $aH = bH$ *if and only if* $a^{-1}b \in H$;
(2) $Ha = Hb$ *if and only if* $ab^{-1} \in H$.

Proof. We only show (1), since (2) can be shown symmetrically. For the implication ($\Rightarrow$), let us assume that $aH = bH$. This implies that $b \in aH$, so there is an element $h \in H$ such that $b = ah$. Thus $a^{-1}b = h \in H$.

To show the implication ($\Leftarrow$) let us assume that $a^{-1}b \in H$. This implies in particular that

$$b = a \cdot \underbrace{a^{-1}b}_{\in H} \in aH.$$

So b is both an element of aH and bH. Thus, by Lemma 11.7, $aH = bH$. □

Exercise 11.11. *Show, using Proposition 11.10, that there is a bijection between the left and right cosets of* $\mathbf{H}$*, given by* $aH \mapsto Ha^{-1}$*.*

12. Group actions

In many situations, it is helpful to interpret a given group as a group of permutations on a certain set. For example, the abstract group $\mathbb{Z}_n$ can be interpreted as a permutation group of the plane, where the number k corresponds to the (anticlockwise) rotation by an angle $k \cdot (2\pi/n)$ (=$k \cdot \frac{360}{n}$ degrees). The sum of the two numbers k_1, k_2 in $\mathbb{Z}_n$ then corresponds to the composition of the respective rotations by $k_1 \cdot (2\pi/n)$ and $k_2 \cdot (2\pi/n)$ degrees. The neutral element 0 corresponds to to the identity map (=rotation by 0 degrees), and the inverse $-k$ in $\mathbb{Z}_n$ corresponds to the inverse rotation (by the angle $-k \cdot (2\pi/n) = (n-k) \cdot (2\pi/n)$). This observation motivates the following definition.

Definition. An *action of a group* $\mathbf{G}$ *on a set* X is a map $\pi \colon G \to S_X$ such that

$$\pi(g \cdot h) = \pi(g) \circ \pi(h), \pi(g^{-1}) = \pi(g)^{-1} \text{ and } \pi(1) = id,$$

for all $g, h \in G$. For short, we are going to write $g(x)$ for the image of x under the the permutation $\pi(g)$.

It follows from this definition that the neutral element 1 of G acts as a the identity map, g^{-1} acts as the inverse permutation of $\pi(g)$, and the relation $(gh)(x) = g(h(x))$ holds. We can imagine that the elements of the group $\mathbf{G}$ 'move' the elements of the set X, such that when two group elements are multiplied, the corresponding 'move' are composed.

Example. A trivial example is the group action of a permutation group $\mathbf{G} \leq \mathbf{S}_X$ on the set X, which is simply given by $\pi(g) = g$.

Example. The action of $\mathbb{Z}_n$ on the plane $X = \mathbb{R}^2$ that we described in the first paragraph is given by the map $\pi \colon \mathbb{Z}_n \to \mathbf{S}_{\mathbb{R}^2}$ such that $\pi(k)$ is the permutation

$$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} \cos(k \cdot 2\pi/n) & -\sin(k \cdot 2\pi/n) \\ \sin(k \cdot 2\pi/n) & \cos(k \cdot 2\pi/n) \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix}$$

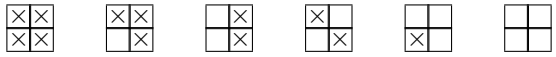
Example. Similarly, every matrix groups $\mathbf{G} \leq GL_n(F)$ can be interpreted as permutations of the corresponding vector space $X = F^n$. The action π then maps a matrix $A \in \mathbf{G}$ simply to the linear map $\pi(A) \colon x \mapsto A \cdot x$ for all vectors $x \in X$.

This seemingly abstract concept of group action on a set has some very nice application in combinatorics. It allows us to answer questions of the following type: How many objects are there, up to a given symmetry?

For example: How many ways are there to color the squares on a Rubik's cube, using only 6 colors, up to rotational symmetry (or up to moves using the cube's mechanics)? As such numbers can get very big quite quickly, we are, for the beginning, just look at an easy model problem:

Example. Let us color the 4 fields of a 2×2 square with 2 colors (white $\square$ and black $\boxtimes$). How many such 2-colorings are there up to rotations (of the whole 2×2 square)?

In the example with the Rubic's cube, it seems to be impossible to list all possible colorings by hand. However, for our model problem, we can show directly that the answers is 6 since there are the following 6 distinct colorings:



Let us first clarify what is meant by counting "objects up to symmetry" in this example. The objects X are the colorings of the 4 squares with 2 colors, so $|X| = 2^4 = 16$. The "symmetries" are the rotations of the square around its central point that map the square to itself, i.e. the rotation by 0, 90, 180 and 270 degrees. As discussed before, these rotations can be modelled by the action of $\mathbf{G} = \mathbb{Z}_4$ on X (such that $g(x)$ is the rotation of the coloring x by $g \cdot 360/n$ degrees). Two colorings $x, y \in X$ are then considered the same (or equivalent), if there is a rotation g such that $g(x) = y$.

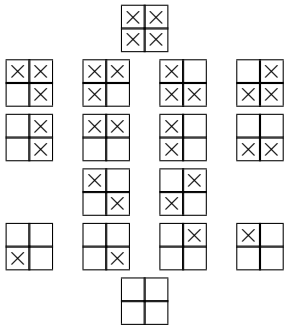
This motivates the following definition for general group actions:

Definition. The *transitivity relation* $\sim$ on X is defined by $x \sim y$ if and only if there is a $g \in G$, such that $g(x) = y$.

Lemma 12.1. *The transitivity relation $\sim$ is an equivalence relation on X.*

Proof. Reflexivity: For every x: $1(x) = id(x) = x$, and therefore $x \sim x$. Symmetry: Assume $x \sim y$, so there is a $g \in G$ such that $g(x) = y$. Then $g^{-1}(y) = x$, and therefore also $y \sim x$. Transitivity: Let $x \sim y \sim z$, so there are group elements $g, h \in G$ such that $g(x) = y$ and $h(y) = z$. Then $(h \cdot g)(x) = h(g(x)) = h(y) = z$, and therefore $x \sim z$. □

Example. In our example, the transitivity relation on the set of 2-colorings on a 2x2 square is given by the following diagram:



such that every row is an equivalence class of $\sim$. These equivalence classes are called the *orbits* of the group action.

Definition. A point $x \in X$ is called a *fixpoint* of an element $g \in G$ if $g(x) = x$. For the set of all fixpoints of some g, let us write

$$X_g = \{x \in X \colon g(x) = x\}.$$

Vice-versa, the *stabilizer* G_x of an element $x \in X$ is the set of all group elements, which fix x, i.e.

$$G_x = \{g \in G \colon g(x) = x\}.$$

Example. In our example, the stabilizers of both monochromatic colorings are the full group $\mathbb{Z}_4$. The stabilizer of  is just the identity, ($\{0\} \leq \mathbb{Z}_4$) while the stabilizer of  consists of the identity and the rotation by 180 degrees ($\{0, 2\} \leq \mathbb{Z}_4$)

Lemma 12.2. *For every $x \in X$, the stabilizer $\mathbf{G}_x$ is a subgroup of $\mathbf{G}$.*

Proof. Clearly $\mathbf{G}_x$ contains the neutral element 1 of $\mathbf{G}$, since $1(x) = id(x) = x$. For every $g, h \in \mathbf{G}_x$ note that $(g \cdot h)(x) = g(h(x)) = g(x) = x$, so also $gh \in \mathbf{G}_x$. Furthermore $g(x) = x$ implies $g^{-1}(x) = x$, so $g^{-1} \in \mathbf{G}_x$. □

Proposition 12.3 (orbit size vs. index of stabilizer)**.** *Let $\mathbf{G}$ be a group acting on a set X. Then, for every $x \in X$, we have*

$$|[x]_\sim| = [\mathbf{G} : \mathbf{G}_x].$$

Proof. The index $[\mathbf{G} : \mathbf{G}_x]$ is equal to the number of cosets of $\mathbf{G}_x$ in $\mathbf{G}$. We define the map:

$$\phi\colon \{gG_x\colon g \in G\} \to [x]_\sim, \qquad gG_x \mapsto g(x).$$

In order to prove the theorem, we are going to show that ϕ is a bijection.

First we show that $\phi(gG_x)$ does not depend on the representation of the coset. So let $g, h \in G$ such that $gG_x = hG_x$. By Proposition 11.10, this is equivalent to

$$gG_x = hG_x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow h^{-1}g(x) = x \Leftrightarrow g(x) = h(x),$$

and thus ϕ is indeed a well-defined map.

By the same equivalence, ϕ is an injective map (different cosets are mapped to different elements under ϕ). Moreover ϕ is surjective, since by the definition of $\sim$ for every $y \in [x]_\sim$, there is an element $g \in G$, such that $g(x) = y$. Thus ϕ is a bijection. □

If a group is finite, then Proposition 12.3, together with Lagrange's theorem implies that

$$|\mathbf{G}| = |\mathbf{G}_x| \cdot |[x]_\sim|.$$

In particular, the size of every orbit must divide the order of the group (note that this holds in our example).

12.1. **Counting orbits with Burnside's lemma.** Let $X/_\sim$ denote the set of all the classes of an equivalence relation $\sim$ on X. In our setting (when $\sim$ is the transitivity relation), $X/_\sim$ is thus the set of orbits. *Burnside's lemma* (also called *Burnside's counting theorem*) then allows us to compute this number:

Theorem 12.4 (Burnside's lemma)**.** *Let $\mathbf{G}$ be a finite group acting on a set X. Then*

$$|X/_\sim| = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g|.$$

Proof. Let

$$M = \{(g, x) \in G \times X\colon g(x) = x\}.$$

We can compute the size of this M in two ways: on one hand, we can first compute the number of pairs $(g, x) \in M$ for fixed x (so the size of the stabilizer sets G_x), and then sum over all x. On the other hand, we can first determine the number of pairs $(g, x) \in M$ for fixed g (so the size of the fixpoint sets X_g), and then sum over all g. So

$$|M| = \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|.$$

If we divide this number by $|G|$, we get

$$\frac{1}{|G|}\cdot\sum_{g\in G}|X_g| = \frac{1}{|G|}\cdot\sum_{x\in X}|G_x| = \frac{1}{|G|}\cdot\sum_{x\in X}\frac{|G|}{|[x]_\sim|} = \sum_{x\in X}\frac{1}{|[x]_\sim|}$$
$$= \sum_{O\in X/_\sim}\sum_{x\in O}\frac{1}{|[x]_\sim|} = \sum_{O\in X/_\sim}\sum_{x\in O}\frac{1}{|O|} = \sum_{O\in X/_\sim}|O|\frac{1}{|O|} = \sum_{O\in X/_\sim}1,$$

which is equal to the size of $X/_\sim$. □

Example. Let us return to the motivational example, with $\mathbf{G} = \mathbb{Z}_4$ acting on colorings X. The identity fixes all elements of X, so $|X_0| = |X| = 16$. The rotation by 90 degrees maps the left upper corner to the left lower corner, the left lower corner to right lower corner and so on. So we get that the elements of X_1 must have the same color on all 4 boxes. Thus $|X_1| = 2$. A 180 degree rotation interchanges the right upper with the left lower box, and the left upper with the right lower box. So $|X_2|$ has 4 elements. For a rotation by 270 degrees, we get, similarly to 90 only monochromatic colorings as fixpoints, so $|X_3| = 2$. Burnside's lemma then gives us

$$|X/_\sim| = \frac{1}{|4|}(16+2+4+2) = 6,$$

which is the correct answer, as we already know.

Exercise. A children's game contains three red, three green and three blue squares tiles. In how many ways can they be arranged into a 3×3 square? Here, two configurations are considered equal if (a) we can get one by the other by rotation, or (b) by rotations and reflections.

Solution. For the first problem (a), we need to consider the action of $\mathbb{Z}_4$ (the 4 rotations) on the set of colorings X of 3×3 squares with 3 red, 3 green, and 3 blue tiles (so $|X| = \binom{9}{3}\cdot\binom{6}{3} = 1680$). In the case (b), where also reflections are allowed, we get an action of the dihedral group $\mathbf{D}_8$.

Note that a configuration is a fixpoint of a group element $g\in\mathbb{Z}_4$ (or $g\in\mathbf{D}_8$), if and only if g maps every red tile to a red tile, every green tile to a green tile, and every blue tile to a blue tile. This allows us quite easily to determine the number X_g, depending on the 'type' of g:

We present a table, in the which the first column lists different types of group elements G, in the second column we write the number of elements of the given type and the third column shows the number of fixed points in X of these elements:

g	#	$\lvert X_g\rvert$
id	1	1680
rotation by $\pm 90°$	2	0
rotation by 180°	1	0
reflection at diagonal axis	2	36
reflection at perpendicular axis	2	36

By Burnside's lemma we obtain

(a) $\frac{1}{4}(1680+2\cdot 0+1\cdot 0) = 420$,
(b) $\frac{1}{8}(1680+2\cdot 0+1\cdot 0+2\cdot 36+2\cdot 36) = 228$.

□

Exercise. Let's assume that you are a crafty football fan. How many different necklaces can you make for (a: Sparta Praha) from three reds, three yellows and three blue balls, (b: Bohemians Praha) from six green and three white balls? (Which group describes the symmetry here? (Note that rotating a neckless by 180 degree and reflecting it at the midpoint will give you the same result).

Exercise. How may ways are there to color the faces of a cube with 2 colors? How many dice are there (=labelings of the faces of a cube with the numbers from 1 to 6). And how many dice are there such that the numbers of opposite sides add up to 7? all these questions are up to *rotational symmetry*

Solution. Let X be the set of 2-colorings of the cube. Let Y be the set of dice, and let Z be the set of dice such that opposite sides add up to 7. The rotational symmetries of a cube are described by a group $\mathbf{G}$. We actually do give a full description of $\mathbf{G}$, to apply Burnside's lemma, it is enough to know all elements of G and their actions on X (and Y, Z respectively). We can make a table, listing all rotations depending on their axis and angle:

g	#	$\lvert X_g\rvert$	$\lvert Y_g\rvert$	$\lvert Z_g\rvert$
Identity	1	2^6	6!	48
axis though centers of opposite faces, $\pm 90°$	6	2^3	0	0
axis though centers of opposite faces, $+180°$	3	2^4	0	0
axis though centers of opposite edges, $+180°$	6	2^3	0	0
diagonal axis, $\pm 120°$	8	2^2	0	0

We then get

- $|X/_\sim| = \frac{1}{24} \cdot (2^6 + 2^3 + 2^4 + 2^3 + 2^2) = 10$
- $|Y/_\sim| = \frac{1}{24} \cdot (6!) = 30$
- $|Z/_\sim| = \frac{1}{24} \cdot (48) = 2$

In fact, you might already know that the two possibilities in the case $|Z/_\sim| = 2$, can be described by the clockwise and counterclockwise ordering of the numbers $1, 2, 3$, when looking at the corner of the cube that shares these numbers. □

Burnside's lemma can be used in a number of other applications, e.g. if we want to find out the number of some structures of a given size up to isomorphism.

Example. Let X be the set of all (loopless) graphs with vertices $1, 2, 3, 4$, So $|X| = 2^6$. Two graphs are isomorphic, if there is a permutation $\pi \in \mathbf{S}_4$ that maps an edge to edge and a non-edge to a non-edge.The so the orbits of $\mathbf{S}_4$ on X contain the mutually isomorphic graphs, and the number of non-isomorphic graphs is equal to the number orbit. In order to count this number (using Burnside's lemma) we create a table of the number of fixpoints.

In this case it is easiest to look at the permutations depending on their 'cycle type':

g	#	$\lvert X_g\rvert$
id	1	2^6
(..)	6	2^4
(..)(..)	3	2^4
(...)	8	2^2
(....)	6	2^2

It follows that the number of graphs with 4 vertices up to isomorphisms is

$$\frac{1}{24}(2^6 + 6 \cdot 2^4 + 3 \cdot 2^4 + 8 \cdot 2^2 + 6 \cdot 2^2) = 11$$

We finish by showing an interesting result about permutation groups with an elegant proof. A permutation group is called *transitive* if it has only one orbit (with respect to its natural action). For example, the groups $\mathbf{S}_n$, $\mathbf{A}_n$, $\mathbf{D}_n$ are transitive, but $\langle (12)(34) \rangle$ is not.

Theorem 12.5 (Jordan's theorem)**.** *Every finite transitive permutation group* $\mathbf{G}$ *on an at least two-element set* X *contains a permutation without a fixed point.*

Proof. According to Burnside's lemma, the number of orbits $|X/_\sim|$ is equal to the average number of fixed points $\frac{1}{|G|} \cdot \sum_{g \in G} |X_g|$. But transitivity on the other hand implies $|X/_\sim| = 1$. At the same time, the identity id has $|X| \geq 2$ fixpoints, (i.e. an above-average amount). If every other permutation had at least one fixpoint, this would imply that

$$1 = |X/_\sim| = \frac{1}{|G|} \cdot \sum_{g \in G} |X_g| \geq \frac{|G| + 1}{|G|} > 1,$$

which is a contradiction. Thus, there is a permutation without fixpoints. □

13. Cyclic groups

13.1. **Subgroups, generators, elementary properties.** A group $\mathbf{G}$ is called *cyclic*, if it is generated by one element, i.e.

$$\mathbf{G} = \langle a \rangle_{\mathbf{G}},$$

for some $a \in G$. Thanks to Corollary 11.3 the elements of a cyclic subgroup are then powers of the generator:

$$G = \{a^k \colon k \in \mathbb{Z}\},$$

and as a consequence G is an Abelian group. If $\mathrm{ord}(a) = n < \infty$, then we know by Proposition 11.6, that $|G| = n$ and $G = \{e, a, a^2, \ldots, a^{n-1}\}$. We give some examples of cyclic groups:

Example.

- The groups $\mathbb{Z}$ and $\mathbb{Z}_n$ (for every $n \in \mathbb{N}$) are cyclic, with generator 1.
- The group $\mathbb{C}_n \leq \mathbb{C}^*$ consisting of the roots of the polynomial $x^n - 1$ is cyclic, with $\mathbb{C}_n = \langle e^{\frac{2\pi}{n}} \rangle$
- The multiplication group of every finite field is cyclic (see Section 13.2)
- Some groups $\mathbb{Z}_n^*$ are cyclic ($\mathbb{Z}_6^* = \{1, 5\} = \langle 5 \rangle$), while other are not ($\mathbb{Z}_8^* = \{1, 3, 5, 7\}$ is not cyclic).
- Every group $\mathbf{G}$ of prime order is cyclic: For this, consider one of its subgroups $\langle a \rangle$ generated by any element $a \neq 1$. Then, by Lagrange's theorem, this subgroup must divide the order of $\mathbf{G}$. Since $|\langle a \rangle| \neq 1$, it must have the same order as $\mathbf{G}$, thus $\langle a \rangle = \mathbf{G}$.

We next study some elementary properties of cyclic groups.

Proposition 13.1. *Every subgroup of a cyclic group is also a cyclic group.*

Proof. Let $\mathbf{G} = \{a^k \colon k \in \mathbb{Z}\}$, be a cyclic group, generated by some $a \in G$, and let $\mathbf{H}$ be a subgroup. If $H = \{1\}$, then H is also a cyclic group (with generator 1). Otherwise H contains some power of a. Let n be the smallest positive number such that $a^n \in H$ (note that such a *positive* number must always exist since $a^{-k} \in H \Leftrightarrow a^k \in H$). Then clearly $\langle a^n \rangle \subseteq H$. We claim that even equality holds. For contradiction, assume that there is a $l \in \mathbb{N}$, such that $a^l \in H \setminus \langle a^n \rangle$. By the minimality of n, $l > n$; furthermore l cannot be a multiple of n, since $a^l \notin \setminus \langle a^n \rangle$. Therefore we can write $l = q \cdot n + r$ for a remainder $0 < r < n$. Note that then

$$a^r = a^{l-qn} = a^l \cdot (a^n)^{-q} \in H,$$

but since $r < n$, this is a contradiction to the minimality of n! □

Example. Every subgroup of $\mathbb{Z}$ is of the form

$$\langle k \rangle = k\mathbb{Z} = \{x \in \mathbb{Z} \colon k \mid x\},$$

for some $k \in \mathbb{Z}$. With the exception of $\{0\}$, these subgroups all are of infinite order. Note that $k\mathbb{Z} = l\mathbb{Z}$, if and only if $k = \pm l$. Furthermore $k\mathbb{Z} \leq l\mathbb{Z}$ if and only if k is a multiple of l. So, in other words, the inclusion order on the subgroups of $\mathbb{Z}$ corresponds to the (inverse) order of the numbers $\mathbb{N} \cup \{0\}$ by divisibility.

The situation is more complicated for finite cyclic groups, since many different elements can generate the same subgroups.

Lemma 13.2. *Let $\mathbf{G} = \langle a \rangle$ be a cyclic group. Then*

(1) $\langle a^l, a^k \rangle = \langle a^{\gcd(l,k)} \rangle$,
(2) *If $|G| = n$, then* $\langle a^l \rangle = \langle a^{\gcd(l,n)} \rangle$

Proof. (1) Since both l and k are multiples of $\gcd(l,k)$, clearly $a^l, a^k \in \langle a^{\gcd(l,k)} \rangle$, and thus $\langle a^l, a^k \rangle \subseteq \langle a^{\gcd(l,k)} \rangle$. On the other hand, we can write $\gcd(l,k) = ul + vk$ for some $u, v \in \mathbb{Z}$, by Bézout's identity., and therefore

$$a^{\gcd(l,k)} = a^{ul+vk} = (a^l)^u \cdot (a^k)^v \in \langle a^l, a^k \rangle,$$

which implies $\langle a^l, a^k \rangle \supseteq \langle a^{\gcd(l,k)} \rangle$.

(2) If $|G| = n$, then $a^n = 1$, and by (1): $\langle a^l \rangle = \langle a^l, a^n \rangle = \langle a^{\gcd(l,n)} \rangle$.

□

Proposition 13.3 (Generator of cyclic groups)**.** *Let $\mathbf{G} = \langle a \rangle$ be a cyclic group.*

- *If $|G|$ is infinite, then a and a^{-1} are the only generators.*
- *If $|G| = n$ is finite, then the generators are all elements a^k, such that k and n are coprime.*

Proof.

- Clearly a and a^{-1} are always generators of $\mathbf{G}$. For any $k \in \mathbb{N}$: $\langle a^k \rangle = \{(a^k)^n \colon n \in \mathbb{Z}\} = \{a^{kn} \colon n \in \mathbb{Z}\}$. Since, in the infinite case, all powers of a must be distinct (see also the proof of Proposition 11.6), we get that $a \notin \langle a^k \rangle$, for $k \neq 1, -1$, and therefore $\langle a^k \rangle \neq \mathbf{G}$.
- By Lemma 13.2, $\langle a^k \rangle = \langle a^{\gcd(k,n)} \rangle$, for every k. So, if k and n are coprime, we get $\langle a^k \rangle = \langle a \rangle = \mathbf{G}$. On the other hand, if $\gcd(k,n) = d \neq 1$, then $\langle a^k \rangle = \{a^d, a^{2d}, \ldots, a^{d \cdot \frac{n}{d}}\}$, which is a proper subgroup (not containing a).

□

Example (The subgroups of $\mathbb{Z}_n$)**.** The group $\mathbb{Z}_n$ is cyclic and generated by 1. So its subgroups are also cyclic and thus of the form

$$\langle k \rangle = k\mathbb{Z}_n = \{ku \bmod n \colon u = 0, \dots, n-1\},$$

for $k \in \{0, 1, \dots, n-1\}$. By Lemma 13.2 (2) two subgroups $k\mathbb{Z}_n = l\mathbb{Z}_n$ are equal if $\gcd(k, n) = \gcd(l, n)$. Thus, the subgroups of $\mathbb{Z}_n$ correspond to the divisors of n. For two divisors $k, l \mid n$ we further have $k\mathbb{Z}_n \leq l\mathbb{Z}_n$ if k is a multiple of l. So, in other words, the inclusion order on the subgroups of $\mathbb{Z}_n$ corresponds to the (inverse) order of the divisors of n according to divisibility.

Example. The group $\mathbb{Z}_{11}^* = \langle 2 \rangle$ is cyclic of order 10. So its subgroups are also cyclic and of the form $\langle 2^k \rangle = \{2^{ku} \mod 11 \colon u = 0, \dots, 10\}$, for $k \in \{0, 1, \dots, 9\}$. By Lemma 13.2 (2) two subgroups $\langle 2^k \rangle = \langle 2^l \rangle$ if $\gcd(k, 10) = \gcd(l, 10)$. Thus, the subgroups of $\mathbb{Z}_{11}^*$ are

$$\langle 2^1 \rangle = \mathbb{Z}_{11}^*,\ \langle 2^2 \rangle = \{1, 4, 5, 9, 3\},\ \langle 2^5 \rangle = \{1, 10\},\ \langle 2^{10} \rangle = \{1\}.$$

Every generator $\mathbb{Z}_{11}^*$ is of the form 2^k, such that k is coprime to 10. Thus $2^1 = 2$, $2^3 = 8$, $2^7 = 7$, $2^9 = 6$ are all the generators. Note that these are just the numbers that don't belong to any of the proper subgroups listed above This fact generalized to all multiplication groups $\mathbb{Z}_p^*$, where p is a prime (we'll see later that they are always cyclic).

It follows from Proposition 13.3 that a cyclic group of order n has exactly $\varphi(n)$ generators, where φ denotes Euler's totient function. In fact, we can use Euler's function, more generally, to count in a cyclic group the number of elements of a given order:

Proposition 13.4. *A cyclic group of order n has exactly $\varphi(d)$ elements of order d, for every d that divides n.*

Proof. Let $\mathbf{G} = \langle a \rangle$ be a subgroup of order n. By Lemma 13.2 its subgroups are of the form $\langle a^k \rangle$, for divisors of $k \mid n$. The only subgroup of order d is then $\langle a^{\frac{n}{d}} \rangle = \{a^{\frac{n}{d}}, a^{2\frac{n}{d}}, \dots, a^{d\frac{n}{d}}\}$. By Proposition 13.3, an element $a^{i\frac{n}{d}}$ generates $\langle a^{\frac{n}{d}} \rangle$ if and only if i and d are coprime. Therefore $\langle a^{\frac{n}{d}} \rangle$ has $\varphi(d)$ generators, and, as a consequence, there are $\varphi(d)$ elements of order d in $\mathbf{G}$. □

As a direct consequence, we obtain the following nice fact about Euler's function:

Proposition 13.5. *For every $n \in \mathbb{N}$:*

$$\sum_{d \mid n} \varphi(d) = n.$$

Proof. Let us consider the group $\mathbb{Z}_n$ (or any other cyclic group of order n). By Lagrange's theorem, the order of every element of $\mathbb{Z}_n$ must divide n. By Proposition 13.4, $\mathbb{Z}_n$ has exactly $\varphi(d)$ elements of order d, for every divisor $d \mid n$. Since $\mathbb{Z}_n$ has n elements in total, we get $\sum_{d \mid n} \varphi(d) = n$. □

13.2. **The multiplication group of finite fields are cyclic.** The statement given in the title of the subsection has far-reaching implications in the theory of finite fields. We are going to use the following criterion for cyclic groups:

Lemma 13.6. *Let $\mathbf{G}$ be a finite group, such that for every natural number k, there are at most k many solution of the equation $x^k = 1$ in G. Then $\mathbf{G}$ is cyclic.*

Proof. Let $n = |G|$ be the order of the group G. For every k, let u_k denote the number of elements of G of order k. By Lagrange's theorem, u_k can only be different from 0 if $k \mid n$. Thus $n = \sum_{k|n} u_k$ (we count the elements of G depending on their order, as in the proof of Proposition 13.5).

Next assume that $u_k \neq 0$, for some k. Then there must be an element $b = a^d$ of order k. It generates a cyclic subgroup $\langle b\rangle = \{1, a^d, a^{2d}, \dots, a^{(k-1)d}\}$. Note that all elements of this subgroup satisfy the identity $x^k = 1$. However, since there are at most k many such elements, $\langle b\rangle$ must already contain all elements satisfying x^k. In particular it contains all elements of order k. By Proposition 13.3 (2), we know that $\langle b\rangle$ has $\varphi(k)$ many generators. Thus $u_k = \varphi(k)$.

If there was a $k \mid n$ with $u_k = 0$, then $n = \sum_{k|n} u_k$ would be smaller to $\sum_{k|n} \varphi(k)$, which is a contradiction to Proposition 13.5. So, in particular $u_n \neq 0$. In other words, $\mathbf{G}$ has an element a of order n, which implies $\mathbf{G} = \langle a\rangle$ □

Theorem 13.7. *Let* $\mathbf{F}$ *be a field and* $\mathbf{G} \leq \mathbf{F}^*$ *be a finite subgroup of its multiplication group. Then* $\mathbf{G}$ *is cyclic.*

Proof. By Theorem 4.4, there are at most k many roots of the polynomial $x^k - 1$ in $\mathbf{F}$. In other words, the equation $x^k = 1$ has at most k many solutions. This is also true in the group $\mathbf{G}$, so by Lemma 13.6, $\mathbf{G}$ is cyclic. □

Theorem 13.7 in particular implies to the multiplication groups of finite fields, which are cyclic. The generators of $\mathbf{F}^*$ are also called *primitive elements*. Primitive elements a are used for example in the fast Fourier transformation algorithm, which can evaluate and interpolate polynomials in points $1, a, \dots, a^n$ in time $\mathcal{O}(n \log n)$ (while for n randomly selected points we need quadratic time).

For the field $\mathbb{Z}_p$, Theorem 13.7 can be phrased purely in elementary number theory: Then it says that for every prime p there exists a number $a \in \{2, \dots, p-1\}$ (a generator of $\mathbb{Z}_p^*$) such that each $b \in \{1, 2, \dots, p-1\}$ can be expressed in exactly one way as $b = a^k \bmod p$ for some $k = 1, 2, \dots, p-1$.

13.3. **Discrete logarithms and cryptography.** Let $\mathbf{G} = \langle a\rangle$ be a cyclic group of order n. Then, let us define the map

$$exp\colon \mathbb{Z}_n \to G, \quad i \mapsto a^i.$$

This map is called a discrete *exponential function*, and it follows from the earlier subsections that it is bijective. The inverse map is called a discrete *logarithm*. In other words,the discrete logarithm of the element $b \in G$ assigns to it the number $k \in \{0, 1, \dots, n-1\}$, such that $b = a^k$; we will denote it by $k = \log_a b$.

Computing a discrete exponential is easy. Naively, it might seem like we need to perform k multiplications to compute a^k. However actually only $2\lfloor \log_2 k\rfloor$ steps are needed.

For this, note that k can be represented in binary as $k = \sum_{i=0}^{\lfloor \log_2 k\rfloor} u_i 2^i$, with $u_i \in \{0, 1\}$.

Therefore

$$a^k = a^{\sum_{i=0}^{\lfloor \log_2 k\rfloor} u_i 2^i} = \prod_{i\colon u_i = 1} a^{2^i}.$$

So to compute a^k, we only need to compute the values of the powers $a, a^2, a^4 = (a^2)^2, a^8 = (a^4)^2, \dots$, and then multiply those powers appearing in the binary representation of k. This can be done in $\leq 2\lfloor \log_2 k\rfloor$ steps.

Experiments indicate however, that computing the discrete logarithm is difficult for many cyclic groups. Finding the logarithm by brute force (by going through all n possible exponents) is exponentially slower than computing the exponential function (as described above). For some groups the calculation is easy (see the example $\mathbb{Z}_n$ below), but for example for the multiplication groups $\mathbb{Z}_p^*$, where p is prime, or for groups derived from elliptic curves over finite fields, there exist no better known algorithms than those using the brute force method.

Example. Consider a cyclic group $\mathbb{Z}_n = \langle a \rangle$. The logarithm $\log_a(b)$ is then the unique value of $k \in \{0, 1, \ldots, n-1\}$ such that $k \cdot a \equiv b \pmod{n}$. Such a value can be easily found with Euclid's algorithm: By Proposition 13.3, a and n must be coprime, and thus we can compute the Bézout coefficients u, v such that $1 = ua + vn$. Because of this $b = bua + bvn$. Modulo n, we get $b \equiv bua \pmod{n}$, thus $k = bu \bmod m$ is the logarithm of b.

We will however continue with examples of cyclic group $\mathbf{G}$ for which the discrete exponential is computationally manageable, but not the logarithm (in practice, $\mathbb{Z}_p^*$ for primes $p > 2^{1000}$ is an example). We will show two cryptographic algorithms based on discrete logarithms: the Diffie-Hellman key exchange protocol (this is the most common algorithm of its kind) and ElGamal encryption for public key cryptography (this algorithm is sometimes used in practice, although versions of the RSA algorithm from Section 2.2 are more popular).

Diffie-Hellman key exchange: Alice and Bob need to come up with a common secret password (a common *key*), while they can only communicate via a corrupted channel (e.g. a wire-tapped phone). How to do it?

First, Alice and Bob agree on some cyclic group and a generator, $\mathbf{G} = \langle a \rangle$. Next, Alice chooses a number m and Bob a number n from interval $2, \ldots, |G| - 1$, each will keep his number secret. Then they do the following: Alice computes $u = a^m$ and sends the value to Bob, while Bob computes $v = a^n$ and sends it to Alice.

Then Alice computes $v^m = (a^n)^m = a^{mn}$ and Bob computes $u^n = (a^m)^n = a^{mn}$. Both obtained the same element a^{nm}, and take it as the common key.

If an enemy listened to their communication, what would they find out? They would know the group $\mathbf{G}$, the generator a and the values of $u = a^m$ and $v = a^n$. In order to obtain the common key, they would need to calculate the element a^{mn}. This task is also called the *Diffie-Hellman's problem*. The obvious solution is to compute the discrete logarithm of u and v to get the numbers m, n, multiply them and calculate a^{mn}. However, this solution is not computational feasible and no effective procedure to do it is currently know.

ElGamal encyption: In ElGamal encryption, the recipient chooses a cyclic group $G = \langle a \rangle$, a random number k from the interval $2, \ldots, |G| - 1$, and computes $b = a^k$. He publishes the public key, G, a, b, while keeping the private key k secret.

A sender of the message selects a random number l from the interval $2, \ldots, |G|-1$, which he destroys after sending his message. Instead of his original message $x \in G$, he sends the encrypted message

$$y = (a^l, x \cdot b^l).$$

The recipient receives this pair $y = (u, v)$ and decrypts it using k as follows:

$$v \cdot u^{-k} = x \cdot b^l \cdot (a^l)^{-k} = x \cdot b^l \cdot b^{-l} = x.$$

If we, as attackers, could compute the discrete logarithm quickly, we would immediately get the private key k (from the public key a, b), and thus could also encrypt the message. However, also other ways of attacking El Gamal's algorithm are known for specific groups $\mathbf{G}$. Because of this, for instance ElGamal encyption with the groups $\mathbf{G} = \mathbb{Z}_p^*$ is not considered safe. However, in general, no attack is known, and ElGamal is considered safe, on sufficiently large groups derived from elliptic curves.

One of the basic concepts in cryptography is the concept of a *one-way function*. To put it very simply, it is a bijective map f such that the values $f(x)$ can be computed quickly/efficiently, but there is no known way to get statistically significant information about the values under the inverse map $f^{-1}(y)$.

Examples are

- any discrete exponential function $\exp\colon \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*, k \mapsto a^k \bmod p$ for big enough primes p
- The map $\mathbb{Z}_N \to \mathbb{Z}_N, a \mapsto a^k \bmod N$, for big enough product of 2 primes $N = pq$ and coprime k (see the discussion about RSA encryption in Section 2.2)

Why is this a good feature in cryptography? Here an example:

Alice and Bob want to remotely play a game. Alice will toss coins, and Bob has to guess if it is heads or tails. But how can Bob know that Alice didn't cheat when Bob couldn't look at the coin? Let's choose a one-way function f on a big-enough set $\{1, \dots, n\}$. If Alice throws a head, she chooses a random odd number x, for tails she selects an even number x. She then sends Bob the value $f(x)$. Because f is one-way, Bob can't compute the value of x (not even in a probabilistic way). He chooses his guess and tells it to Alice. Now Alice publishes the number x and Bob immediately sees if he has won. To check that Alice did not cheat, he only needs to compute $f(x)$ and compares it with the value he got at the beginning. If the values disagree, Alice cheated. Can Alice cheat on Bob so that he does not find out? For this, let's assume that she threw head, and Bob guessed correctly. In order for Alice to cheat, she would need to shows Bob an even value x_0 such that $f(x_0) = f(x)$. But such x_0 does not exist since f is a bijection!