LECTURE NOTES FOR 3124 (MODERN ALGEBRA)

LEONARDO CONSTANTIN MIHALCEA

Contents

1. Notation and some basics

Throughout the notes: $\mathbb{N} = \{0, 1, 2, \ldots\}$ (the set of natural numbers); $\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$ (the set of integers); $\mathbb{Q} = \{a/b : a, b \in \mathbb{Z}, b \neq 0\}$ (the set of rational numbers); $\mathbb{R}$ is the set of real numbers (much harder to define rigorously), and $\mathbb{C} := \mathbb{R} + i\mathbb{R}$ is the set of complex numbers; here $i^2 = -1$.

It is interesting to observe that if one starts from $\mathbb{N}$ then one is naturally led to all the sets above, including the complex numbers. This can be done by considering roots of polynomial equations with coefficients in $\mathbb{Z}$. A subtle point is that *transcendental elements* such as e or π *cannot* be obtained in this way.

Exercise. Prove that $\mathbb{Z} \subsetneq \mathbb{Q}$ and $\mathbb{Q} \subsetneq \mathbb{R}$. That is, provide, with proof, examples of elements in $\mathbb{Q} \setminus \mathbb{Z}$ and $\mathbb{R} \setminus \mathbb{Q}$.

Let A, B be two sets and $f : A \to B$ be a function. Then f is **injective** if for all $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, we have $a_1 = a_2$. The function f is **surjective** if for any $b \in B$ there exists $a \in A$ such that $f(a) = b$. The **image** of f is $f(A) = \{b \in B : \exists a \in A, f(a) = b\}$.

2. Well ordering property and Mathematical Induction

Observe that $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ have a natural *order*, defined by $a < b$ iff $b - a > 0$.

Definition 2.1. *We say that a subset S of $\mathbb{Z}$ is* bounded below *if there exists $n_0 \in \mathbb{Z}$ such that if $x \in S$ then $x \geq n_0$.*

The following statement can be proved starting from the basic axioms in set theory (e.g. the Zermelo-Frenkel axioms + axiom of choice).

Proposition 2.1 (Well ordering property)**.** *Let $S \subset \mathbb{Z}$ be a nonempty subset of the integers which is bounded below. Then S contains a smallest element, denoted by* $\min S$.

Observe that this is not true if one does not require the hypothesis of bounded below (e.g. take $S = \mathbb{Z}$ or even S equal strictly positive rational numbers $\mathbb{Q}_{>0}$).

Theorem 2.1 (Principle of Mathematical Induction)**.** *Let $P(n)$ be a mathematical statement depending on an integer n, where $n \geq n_0$. (n_0 is fixed, e.g. $n_0 = 1$.) Assume that:*

1. *(base case) $P(n_0)$ is true;*
2. *(induction step) For all $n \geq n_0$, if $P(n)$ is true, then $P(n+1)$ is true.*

Then $P(n)$ is true for all $n \geq n_0$.

Proof. Consider the sets $A := \{n \geq n_0 : P(n) \text{ is true}\}$ and $B := \mathbb{Z}_{\geq n_0} \setminus A$. We need to show that $B = \emptyset$. We argue by contradiction. If $B \neq \emptyset$, then by the well ordering property it has a minimal element $b_0 \in B$. Observe that $n_0 \in A$ (by the base case), therefore $b_0 > n_0$. But then $b_0 - 1 \in A$, meaning that $P(b_0 - 1)$ is true. By the induction hypothesis this implies that $P(b_0)$ is also true, i.e. $b_0 \in A$, and this is a contradiction. □

Remark 2.1. *An equivalent and useful form of the principle of Mathematical induction replaces the induction step by the following:*

- *Assume $P(k)$ is true for all $n_0 \leq k \leq n$. Then $P(n+1)$ is true.*

Example 2.1. *Prove by induction that for all $n \geq 2$, $n! < n^n$.*

We need to check the base case and the induction step.

Base case: $n = 2$. *Clearly* $2! < 2^2$.

Induction step: *Assume that $n! < n^n$. We need to show that $(n+1)! < (n+1)^{n+1}$. We have:*

$$(n+1)! = n!(n+1) < n^n(n+1) < (n+1)^n(n+1) = (n+1)^{n+1}.$$

Here the first inequality follows from the induction hypothesis. □

Example 2.2. *Prove by induction that the number of edges in a complete graph with n vertices is $\binom{n}{2} = 1 + 2 + \ldots + (n-1) = \frac{n(n-1)}{2}$.*

Let K_n denote the complete graph with n vertices. By definition, any two vertices in it are connected by an edge.

Base case. *The complete graph K_1 has 0 edges and we are done.*

Induction step. *Assume that K_n has $1+2+\ldots+(n-1)$ edges. We need to show that K_{n+1} has $1+2+\ldots+n$ edges. But K_{n+1} is obtained from K_n by adding one vertex and n edges connecting that vertex to the vertices in K_n. This means that*

$$\#\{\textit{edges in } K_{n+1}\} = \#\{\textit{edges in } K_n\} + n = 1 + 2 + \ldots + (n-1) + n.$$

2.1. **Exercises.**

1. Use the Well Ordering Principle to show that every nonempty set of negative integers has a greatest element.

2. Conjecture a formula for A^n where $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Prove your conjecture using mathematical induction.

3. Show that any amount of postage that is an integer number of cents greater than 11 cents can be formed using just 4-cent stamps and 5-cent stamps.

4. Prove using mathematical induction that

$$1^3 + 2^3 + \ldots + n^3 = \Big(\frac{n(n+1)}{2}\Big)^2, \quad \forall n \geq 1.$$

3. The Division Algorithm and applications

Definition 3.1. *Let $a, b \in \mathbb{Z}$. We say a* divides *b, written $a|b$ if there exists $t \in \mathbb{Z}$ such that $b = at$.*

Question: For what numbers $a|b$ and $b|a$? Does $0|0$?

The main result of this section is the following:

Theorem 3.1 (The Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ such that $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r \leq b - 1$.*

Example 3.1. *What happens if $a = 36, b = 7$? What about $a = -36, b = 7$.*

Proof. Define

$$S := \{a - kb : k \in \mathbb{Z}\}; \quad T := S \cap \mathbb{N}.$$

Observe that T is non-empty (for instance take $k > a/b$) and it is bounded below by $n_0 = 0$. Then by the well ordering principle it has a smallest element $r := \min T$. Now take the (unique!) q such that $a - bq = r$. Observe that $r \geq 0$ (as $T \subset \mathbb{N}$) and that $r < b$. Indeed, if $r \geq b$, then $a - b(q+1) = r - b \in T$, and this contradicts the minimality of r. We now prove uniqueness. Assume there exist q_1, q_2, r_1, r_2 such that $a = bq_i + r_i$ and $0 \leq r_i \leq b - 1$ $(i = 1, 2)$. Then

$$bq_1 + r_1 = bq_2 + r_2 \Longleftrightarrow r_1 - r_2 = b(q_2 - q_1).$$

Thus the left hand side must be a multiple of b; but the hypothesis on r_i show that the only possible multiple of b is equals to 0. Then $r_1 = r_2$, from which $q_1 = q_2$. □

3.1. Greatest common divisor.

Definition 3.2. *Let $a, b \in \mathbb{Z}_{>0}$. A greatest common divisor $d := gcd(a, b)$ is a positive integer satisfying two properties:*

1. *d divides both a and b;*
2. *if d' is any other divisor of a and b then $d'|d$.*

Theorem 3.2. *(a) Any two positive integers a, b have a unique greatest common divisor.*

(b) Let a, b are positive integers and $d := gcd(a, b)$. Then there exists $r, s \in \mathbb{Z}$, not necessarily unique, such that $d = ar + bs$.

Example 3.2. *$gcd(24, 42) = 6$ and $6 = 2 \times 24 - 42 = 3 \times 42 - 5 \times 24$.*

Proof of Theorem 3.2. The idea again is to apply the well ordering property to a suitable set. Define

$$S := \{ar + bs : r, s \in \mathbb{Z}, ar + bs > 0\}.$$

This set is clearly nonempty (e.g. take $r = 1, s = 0$). Take $d_0 := \min S$ (this exists by the well ordering property). We claim that d_0 is the gcd. Let $d_0 = ar_0 + bs_0$.

First of all, any common divisor d of a, b must divide d_0, since $d|a$ and $d|b$ implies that $d|(ar + bs)$. This shows that $gcd(a, b)|d_0$. We need to prove the reverse divisibility; this

will follow once we show that $d_0|a$ and $d_0|b$. Consider the division algorithm: $a = d_0q+r$, where $0 \leq r < d_0$. We have that

$$r = a - d_0q = a - (ar_0 + bs_0)q = (1 - r_0)a - bs_0q.$$

Since $d_0 = \min S$ and $0 \leq r < d_0$ we must have that $r = 0$, meaning that $d_0|a$. Similarly $d_0|b$. This proves the existence part in (1) and part (2) simultaneously. The uniqueness is clear from the requirement that $gcd(a, b) > 0$. □

Corollary 3.1. *Let a, b be two positive integers, and assume that $as + br = k$. Then $gcd(a, b)|k$. In particular, if $k = 1$ then $gcd(a, b) = 1$.*

Two numbers a, b such that $gcd(a, b) = 1$ are called **coprime**.

A natural question is how to find (r, s) such that $ar + bs = gcd(a, b)$. One method is to use **Euclid's algorithm**, presented below.

3.2. **Euclid's algorithm.** We are given two numbers a, b, and we seek the $gcd(a, b)$. W.lo.g. $a > b$ and b does not divide a. (If $b|a$ then $gcd(a, b) = b$.) We perform the following operations.

- $a = bq + r_1$, where $0 \leq r_1 < b$;
- $b = r_1q_2 + r_2$; where $0 \leq r_2 < r_1$;
- $r_1 = r_2q_3 + r_3$, $0 \leq r_3 < r_2$;
- $\dots$;
- $r_{k-1} = r_kq_{k+1} + r_{k+1}$, where $0 \leq r_{k+1} < r_k$;
- $r_k = r_{k+1}q_{k+1}$ (i.e. $r_{k+2} = 0$.)

Then $gcd(a, b) = r_{k+1}$, i.e. it is the last nonzero remainder.

Example 3.3. *Calculate $gcd(30, 102)$.*

- $102 = 30 \times 3 + 12$;
- $30 = 12 \times 2 + 6$;
- $12 = 6 \times 2 + 0$.

Therefore $gcd(30, 102) = 6$.

Proof of Euclid's algorithm. We need to prove that $r_{k+1} = d := gcd(a, b)$. We will show that each divides the other; since they are positive numbers, this forces equality. Observe that $d|a$ and $d|b$ implies $d|r_1$ from the first equation. Continuing, at the sth step, the equation is $r_{s-2} = r_{s-1}q_s + r_s$ and by induction d divides r_{s-2} and r_{s-1}. Then d divides r_s. This shows that d divides r_{k+1}. To prove the converse divisibility, we go backwards in the sequence of equations, to show that r_{k+1} divides r_k, therefore it also divides r_{k-1}, then it also divides r_{k-2}, and so on. At the top we obtain that r_{k+1} divides both a and b, therefore it also divides the $gcd(a, b)$, by the definition of the gcd. □

As promised, Euclid's algorithm also gives a method to find r, s such that $ar + bs = gcd(a, b)$. This is obtained by going backwards in the series of divisions. We illustrate it in the case discussed above. We have

$$6 = 30 - 12 \times 2 = 30 - (102 - 30 \times 3) \times 2 = 102 \times (-2) + 30 \times 7.$$

Therefore $r = -2$ and $s = 7$. Of course, these numbers are not unique. For instance, for any $k \in \mathbb{Z}$,

$$ar + bs = a(r + kb) + b(s - ka),$$

meaning that once a solution (r, s) exists, then there are infinitely many.

Remark 3.1. *One important feature of the Euclid's algorithm is that it is quite efficient in actual calculations. In contrast, the* factorization problem *(i.e. factor a number into its prime factors), is* much *slower. This sits at the foundation of applications to cryptography.*

3.3. **Residue classes modulo n.**

Definition 3.3. *Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$. We say that they are* equivalent modulo n, *and write $a \equiv b \mod n$ if $n|(a - b)$. Equivalenty, a, b have the same remainder when divided by n.*

Proposition 3.1. *$a \equiv b \mod n$ is an equivalence relation.*

Proof. Easy check that it is *reflexive, symmetric* and *transitive.* □

Proposition 3.2. *Let $n \geq 2$ be an integer. Then there are exactly n equivalence classes for the equivalence modulo n. These classes have representatives $0, 1, 2, \ldots, n - 1$.*

Proof. If $a \in \mathbb{Z}$ is an integer, we use the division algorithm to write $a = nq + r$, where $0 \leq r \leq n - 1$. This implies that $a \equiv r \mod n$. If $0 \leq i, j \leq n - 1$ then $i \equiv j \mod n$ implies that $i = j$ (why ?). This finishes the proof. □

We denote by $\overline{i}$ the equivalence (or *congruence* class of i. By definition $\overline{i} = n\mathbb{Z} + i = \{nk + i : k \in \mathbb{Z}\}$.

Denote by $\mathbb{Z}/n\mathbb{Z}$ the equivalence classes modulo n. The previous proposition states that

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Define the following operations on $\mathbb{Z}/n\mathbb{Z}$:

$$\overline{i} + \overline{j} := \overline{i + j}; \quad \overline{i} \cdot \overline{j} := \overline{i \cdot j}.$$

Lemma 3.1. *The operations $+$ and $\cdot$ are well defined, i.e. they are independent of choices of representatives.*

Proof. We prove this for multiplication, and we leave the addition as an exercise. Let a_1, a_2, b_1, b_2 such that $\overline{a}_1 = \overline{a}_2$ and $\overline{b}_1 = \overline{b}_2$ as elements in $\mathbb{Z}/n\mathbb{Z}$. We need to show that $\overline{a_1 b_1} = \overline{a_2 b_2}$. The hypothesis means that $a_2 = a_1 + nk$ and $b_2 = b_1 + ns$ for some k, s. Then

$$a_2 b_2 = (a_1 + nk)(b_1 + ns) = a_1 b_1 + n(sa_1 + kb_1 + nks),$$

therefore $\overline{a_1 b_1} = \overline{a_2 b_2}$. □

Proposition 3.3. *The operations $+$ and $\cdot$ have the following properties:*

- *Both $+$ and $\cdot$ are commutative and associative;*
- *(distributivity)* $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$*;*
- $\overline{0} + \overline{i} = \overline{i}$*;* $\overline{1} \cdot \overline{i} = \overline{i}$*.*

Proof. Exercise. □

In the language defined later, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ will be a **ring**. This is very similar to the ring of integers $(\mathbb{Z}, +, \cdot)$, except that we may have two non-zero equivalence classes which multiply to $\overline{0}$. For example, in $\mathbb{Z}/6\mathbb{Z}$, $\overline{2} \cdot \overline{3} = \overline{0}$ (because $0 \equiv 6 \mod 6$).

This has to do with the fact that $6 = 2 \cdot 3$, thus it is not prime.

A residue class $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is called **invertible** if there exists $\bar{b}$ such that $\bar{a}\bar{b} = \bar{1}$ in $\mathbb{Z}/n\mathbb{Z}$.

Lemma 3.2. *Let $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. Then $\bar{a}$ is invertible if and only if $gcd(a, n) = 1$.*

Proof. As proved in Theorem 3.2, the condition $gcd(a, n) = 1$ is equivalent to the existence of some $k, r \in \mathbb{Z}$ such that $ak + nr = 1$. After taking residue classes, this is equivalent to $ak \equiv 1 \mod n$, i.e. $\bar{a}\bar{k} = \bar{1}$, meaning that $\bar{a}$ is invertible. □

Lemma 3.2 implies that there exist $\bar{0} \neq \bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ such that $\bar{a}\bar{b} = \bar{0}$ if and only if n is not prime.

Next we illustrate the usefulness of the operations in $\mathbb{Z}/n\mathbb{Z}$ in getting divisibility criteria.

Example 3.4. *Let $N = a_n a_{n-1} \dots a_1 a_0$ a number written in its decimal representation. (I.e. $a_0, a_1, \dots a_n$ are its digits, from $0, 1, \dots, 9$). Then $11|N$ if and only if $11|(a_0 - a_1 + a_2 - \dots + (-1)^N a_n)$. (Informally: 11 divides the alternate sum of its digits, starting from units.) This holds because*

$$N = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0 \equiv a_n (-1)^n + a_{n-1} (-1)^{n-1} + \dots + a_1 (-1) + a_0 \mod 11.$$

3.4. **Exercises.** 1. Prove Proposition 3.3.

4. Prime factorization and the fundamental theorem of arithmetic

A (positive) number p is *prime* if its only divisors are 1 and p. Two numbers $a, b > 0$ are *relatively prime* if $gcd(a, b) = 1$.

Lemma 4.1. *Let p be a prime number such that $p|ab$. Then $p|a$ or $p|b$.*

Proof. If p does not divide a, then $gcd(a, p) = 1$, and by Theorem 3.2 there exists r, s such that $ar + ps = 1$. Multiply by b to get $b = abr + pbs$. Since p divides both terms in the right hand side, it must divide b. □

Theorem 4.1 (Fundamental Theorem of Arithmetic)**.** *Let $n \in \mathbb{Z}$ be a positive number. Then n can be written as*

$$n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k},$$

where $p_1, \ldots, p_k$ are prime numbers, $a_i \in \mathbb{N} \setminus \{0\}$. Further, this decomposition is unique up to rearranging the factors.

Proof. We argue by induction on n. If n is prime, we are done. If not, there exists some positive number d such that $d|n$. Then $n = d \times (n/d)$ and induction applied to both d and n/d gives the decomposition. It remains to prove uniqueness. Let

$$n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k} = q_1^{b_1} \cdot \ldots \cdot q_s^{b_s},$$

where p_i's and q_j's are primes. Then p_1 divides $q_1^{b_1} \cdot \ldots \cdot q_s^{b_s}$, and the previous lemma implies that $p_1 = q_j$ for some j. W.l.o.g. can assume $j = 1$. Then necessarily $a_1 = b_1$, divide by $p_1^{a_1}$ and the result follows by induction. □

Example 4.1. $24 = 2^2 \times 3$; $3183624 = 2^3 \times 3^4 \times 17^3$.

Remark 4.1. *One can use prime factorization to determine $gcd(a, b)$ and $lcm(a, b)$ (the* lowest common multiple*). If*

$$a = p_1^{a_1} \cdots \quad ; b = p_1^{b_1} \cdots,$$

where $a_1, b_1 \geq 0$ then

$$gcd(a, b) = p_1^{\min(a_1, b_1)} \cdots ; \quad lcm(a, b) = p_1^{\max(a_1, b_1)} \cdots.$$

Finding the gcd using the prime factorization is very easy in theory, but may take a very long time in practice. This is because there are no efficient algorithms to find the prime factorization of a number. In fact, all the cryptographic applications are based on the fact that it is difficult to factor large numbers. Nevertheless, Euclid's algorithm presented above provides a very efficient algorithm to find the gcd; but this does *not* help with the factorization problem.

4.1. **Exercises.** TODO.

5. Polynomials and polynomial division

Definition 5.1. *A* **polynomial** *is a combination of the form*

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 + a_0,$$

where $n \in \mathbb{Z}_{\geq 0}$, $a_n \neq 0$, *and* x *is an indeterminate. The number* $\deg(P) := n$ *is called the* **degree** *of the polynomial and* a_i*'s are called the* **coefficients**. *The coefficient* a_n *is called the* **leading coefficient**. *If all* $a_i \in \mathbb{R}$ *then* $P(x)$ *is a polynomial with real coefficients. Unless otherwise is specified, we assume* $a_i \in \mathbb{C}$.

We denote by $\mathbb{C}[x]$ and $\mathbb{R}[x]$, the set of polynomials with complex, respectively real, coefficients.

Polynomials can be added and multiplied. W.l.o.g. we may assume $P(x) = \sum_{i=0}^n a_i x_i$, $Q(x) = \sum_{i=0}^n b_i x_i$, by allowing $a_n = 0$ or $b_n = 0$. Then

$$P(x) + Q(x) := \sum_{i=0}^{n} (a_i + b_i)x_i, P(x) \cdot Q(x) := \sum c_k x^k,$$

where $c_k = \sum_{i+j=k} a_i b_j$. The two operations are commutative, associative, and the multiplication is distributive with respect to the addition. Check this!

Lemma 5.1. *Let* $P(x), Q(x)$ *be two polynomials such that* $\deg P(x) = k$ *and* $\deg Q(x) = s$. *Then* $\deg(P(x) \cdot Q(x)) = k + s$.

Proof. This follows because the leading coefficient of $P(x) \cdot Q(x)$ is the product of the leading coefficients of the two polynomial. □

Definition 5.2. *Let* $P_1(x), P_2(x)$ *be two polynomials. We say that* $P_1(x)$ *divides* $P_2(x)$ *if* $P_1(x) = P_2(x)Q(x)$ *for some polynomial* $Q(x)$. *A polynomial is called* **reducible** *if it can be factored into polynomials of* positive *degree. A polynomial is called* **irreducible** *if it is not reducible.*

The irreducible polynomials play the same role as the prime numbers in integers. However, irreducibility *depends* on the coefficients we are allowed to work with (i.e. polynomials with real coefficients vs. polynomials with complex coefficients). For instance, the polynomial

$$x^2 + 1 = (x + i)(x - i)$$

is *reducible* over $\mathbb{C}$, but it is irreducible over $\mathbb{R}$. Clearly, any polynomial of degree 1 must be irreducible.

Let a be a number, considered to be real if we work with real coefficients. The **evaluation** map is

$$ev_a : \mathbb{C}[x] \to \mathbb{C}; \quad P(x) \mapsto P(a) \in \mathbb{C}.$$

Sometimes, we will refer to $ev_a(P(x) = P(a)$ as the **specialization** of $P(x)$ at $x \mapsto a$.

Lemma 5.2. *The evaluation map is compatible with polynomial operations, i.e.*

$$ev_a(P + Q) = ev_a(P) + ev_a(Q) : \quad ev_a(P \cdot Q) = ev_a(P) \cdot ev_a(Q).$$

Proof. The lemma translates into

$$(P+Q)(a) = P(a) + Q(a); \quad (P \cdot Q)(a) = P(a) \cdot Q(a).$$

This follows by definition of the operations in $\mathbb{C}[x]$. □

Theorem 5.1 (Polynomial division algorithm)**.** *Let $P(x), Q(x)$ be two polynomials with $Q(x) \neq 0$. Then there exist unique polynomials $T(x), R(x)$ such that $P(x) = Q(x)T(x) + R(x)$ and either $R(x) \equiv 0$ or $0 \leq \deg R(x) < \deg Q(x)$.*

Proof. The existence follows from the Long Division algorithm for polynomials. We now prove uniqueness. Assume that there are polynomials T_1, T_2, R_1, R_2 such that

$$P(x) = Q(x)T_i(x) + R_i(x), \quad \deg R_i(x) < \deg Q_i(x), \quad i = 1, 2.$$

If $T_1(x) = T_2(x)$ we are done, so we assume $\deg(T_1(x) - T_2(x)) \geq 0$. Then $R_1(x) - R_2(x) = Q(x)(T_2(x) - T_1(x))$. But

$$\deg(R_1(x) - R_2(x)) \leq \max\{\deg R_1(x), \deg R_2(x)\} < \deg Q(x) + \deg(T_2(x) - T_1(x)),$$

and this is a contradiction. □

Example 5.1. $x^6 + 4x^5 - x^2 + 5 = (x^2+1) \cdot (x^4 + 4x^3 - x^2 - 4x) + (4x + 5)$.

Corollary 5.1. *Let $P(x) \in \mathbb{C}[x]$. Then $x - a$ divides $P(x)$ if and only if $P(a) = 0$. Equivalently, $ev_a(P) = 0$.*

Proof. Apply the division algorithm and specialize $x \mapsto a$. □

There is an analogue of the $gcd(P, Q)$ where P, Q are polynomials, defined in the same way as for the integers. More precisely, the gcd is the polynomial $D(x)$ such that

- $D(x)|P(x)$ and $D(x)|Q(x)$;
- if $D'(x)$ divides both $P(x)$ and $Q(x)$ then $D'(x)$ divides $D(X)$.

One difference is that the gcd is no longer unique! The (mild) difference comes from the fact that two gcd's may differ by a non-zero constant. We can get uniqueness if we assume that $D(x)$ is a **monic** polynomial, i.e. the leading term equals to 1.

And as for integers there is now an **Euclid algorithm** to determine the gcd of two polynomials. It works in the same way, just replace each integer by a polynomial, and the usual division by polynomial division. As a corollary of Euclid's algorithm we obtain the following analogue of Euclid's algorithm:

Proposition 5.1. *Let $A(x), B(x) \in \mathbb{C}[x]$ be two polynomials, and let $D(x)$ be (any) gcd of A, B. Then*

$$D(x) = A(x)R(x) + B(x)T(x),$$

for some polynomials $R(x), T(x) \in \mathbb{C}[x]$.

Proof. As for integers, this follows from the Euclid's algorithm. □

Example 5.2. *Let $A(x) = x(x+1)$ and $B(x) = x(x-1)$. Then $gcd(A(x), B(x)) = x$ and*

$$x = \frac{1}{2}A(x) - \frac{1}{2}B(x).$$

Example 5.3. *Let $A(x) = x^3 - 1 = (x-1)(x^2+x+1)$ and $B(x) = (x+1)^2 = x^2 + 2x + 1$. Then $gcd(A(x), B(x)) = 1$ (after normalizing, i.e. multiplying by the appropriate constant). As an exercise, work out the Euclid's algorithm for $A(x), B(x)$ in this case.*

Corollary 5.2. *Let $P(x), S(x), T(x)$ be polynomials such that $P(x)$ is irreducible and $P(x)|S(x)T(x)$. Then $P(x)|S(x)$ or $P(x)|T(x)$.*

Proof. The proof is the same as the proof of the Lemma 4.1 above. Assume that $P(x)$ does not divide $S(x)$. Since $P(x)$ is irreducible, it follows that $gcd(P, S) = 1$. The previous proposition implies that there exist polynomials A, B such that

$$AP + BS = 1.$$

Multiply this expression by $T(x)$, to obtain that $APT + BST = T$. Since both APT and BST are divisible by P, the result follows. □

5.1. **Irreducible polynomials.** We start with the following statement (but the proof is beyond the scope of this course).

Theorem 5.2 (Fundamental theorem of algebra)**.** *Let $P(x) \in \mathbb{C}[x]$ be any non-constant polynomial. Then $P(x)$ has a complex root. Equivalently, there exists a complex number $a \in \mathbb{C}$ such that $x - a$ divides $P(x)$.*

Corollary 5.3. *Let $P(x) \in \mathbb{C}[x]$ be any non-constant polynomial. Then $P(x)$ is irreducible if and only if* $\deg P = 1$.

Proof. This is immediate from the Fundamental Theorem of Algebra and the definition of the irreducibility. □

Remark 5.1. *Note that this is false if we do not work with complex coefficients. For example, the polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$.*

Proposition 5.2. *$P(x) \in \mathbb{R}[x]$ be any non-constant polynomial. Then $P(x)$ is irreducible if and only if either* $\deg P = 1$ *or* $\deg P = 2$ *and P has no real roots.*

Proof. If $\deg P = 1$ then it is clearly irreducible (by definition). Assume that $\deg P \geq 2$. Since P has no real roots by assumption, it cannot be divisible by any polynomial of degree 1 (with *real* coefficients). By the Fundamental Theorem of Algebra, P must have a complex, non-real, root, call it z_0. Since P has real coefficients, the conjugate $\overline{z_0}$ of z_0 is also a root. But then $P(x)$, regarded as a complex polynomial, is divisible by $(x - z_0)(x - \overline{z_0})$. We calculate

$$Q(x) := (x - z_0)(x - \overline{z_0}) = x^2 - (z_0 + \overline{z_0})x + z_0\overline{z_0},$$

and find that $Q(x) \in \mathbb{R}[x]$ is a polynomial with *real* coeffcients, dividing $P(x)$. By Long Division, the quotient $P(x)/Q(x)$ is again a polynomial with real coefficients. Since $P(x)$ is irreducible it follows that $P(x) = Q(x)$, and that, further, Q satisfies all the required properties. □

Corollary 5.4 (Prime decomposition for polynomials)**.** *(a) Let $P(x) \in \mathbb{C}[x]$ be any* monic *polynomial (i.e. the leading coefficient equals to 1), of degree $n \geq 1$, and with complex coefficients. Then $P(x)$ can be written as*

$$P(x) = (x - z_1)^{a_1} \cdot \ldots \cdot (x - z_k)^{a_k},$$

where $a_i \geq 1$ and $a_1 + \ldots + a_k = n$. This decomposition is unique up to reordering factors.

(b) $P(x) \in \mathbb{R}[x]$ be any monic *polynomial with real coefficients of degree $n \geq 1$. Then $P(x)$ can be written as*

$$P(x) = \prod_j (x^2 + c_j x + d_j) \prod_j (x - \lambda_j),$$

where all factors are irreducible over $\mathbb{R}$, c_j, d_j, λ_j are real numbers, and the total degree on the right equals to n. This decomposition is unique up to reordering factors.

Proof. The proof is the same as for the Fundamental Theorem of Arithmetic (Theorem 4.1 above), replacing the prime numbers by irreducible polynomials. These are determined by Corollaries 5.3 and 5.2 above. The uniqueness will now use Corollary 5.2, replacing Lemma 4.1 used before. □

Example 5.4. *The polynomial $x^3 + 1$ factors over $\mathbb{R}$ as*

$$x^3 + 1 = (x + 1)(x^2 - x + 1).$$

The quadratic polynomial has (complex, conjugate) roots

$$z_{1,2} = \frac{1 \pm i\sqrt{3}}{2}.$$

Then the factorization over $\mathbb{C}$ is

$$x^3 + 1 = (x + 1)(x - z_1)(x - z_2).$$

5.2. **Ideals and residue classes: an analogy to $\mathbb{Z}/n\mathbb{Z}$.** A consequence of the division algorithm in $\mathbb{Z}$ from §3.3 is that we can place numbers into equivalence classes, according to their remainders after division by a fixed $n \in \mathbb{Z}$. Same thing can be done with polynomials, but the resulting theory is getting much richer.

Let $P(x) \in k[x]$ where $k \in \{\mathbb{R}, \mathbb{C}\}$. Define

$$\langle P(x) \rangle = \{f(x)P(x) : f(x) \in k[x]\}.$$

This is a subset of $k[x]$, called the **ideal** generated by $P(x)$. It plays the role of the set $n\mathbb{Z}$ from §3.3.

Definition 5.3. *Let $P_1(x), P_2(x) \in k[x]$. We say that P_1, P_2 are* equivalent modulo the ideal $\langle P(x)\rangle$, *written $P_1 \equiv P_2 \mod \langle P(x)\rangle$, if*

$$P_1(x) - P_2(x) \in \langle P(x)\rangle.$$

Equivalently, we require that $P(x)|(P_1(x) - P_2(x))$.

Lemma 5.3. *The equivalence modulo an ideal is an equivalence relation.*

Proof. Exercise. □

We denote by $k[x]/\langle P(x)\rangle$ the set of equivalence classes, and we refer to this as a *quotient* by the ideal $\langle P(x)\rangle$. As in $\mathbb{Z}/n\mathbb{Z}$, the equivalence classes correspond to the possible reminders upon division by $P(x)$. For $r(x) \in k[x]$ we denote by $\overline{r(x)}$ its equivalence class in $k[x]/\langle P(x)\rangle$.

Example 5.5. *(a) Take $k = \mathbb{R}$ and $P(x) = x$. Then $2x + 1 \equiv x + 1 \mod \langle x\rangle$.*
(b) $x^2 - 1 \equiv 0 \mod \langle x - 1\rangle$.

As for $\mathbb{Z}/n\mathbb{Z}$, we may also add and multiply the equivalence classes by multiplying representatives. The key point here is that these operations are well defined, i.e. they do not depend on choices of representatives. (Exercise!)

An interesting fact is that one may detect irreducibility of a polynomial $P(x)$ by looking at the quotient by the ideal it generates.

Proposition 5.3. *Let $P(x) \in \mathbb{R}[x]$. Then $P(x)$ is reducible if and only if there are two representatives $\overline{a(x)}, \overline{b(x)} \neq \overline{0}$ such that $\overline{a(x)b(x)} = \overline{0}$ in $k[x]/\langle P(x)\rangle$.*

Proof. Exercise. □

Example 5.6. *Consider the quotient $\mathbb{R}[x]/\langle x\rangle$. Let $P(x) \in \mathbb{R}[x]$. The remainder of $P(x)$ under division by x must be a constant. Therefore*

$$\mathbb{R}[x]/\langle x\rangle \simeq \mathbb{R}$$

with $c \in \mathbb{R}$ corresponding to the set of polynomials of the form

$$xQ(x) + c.$$

Example 5.7. *Consider the quotient $\mathbb{R}[x]/\langle x^2 + 1\rangle$. This quotient has a class $\overline{x}$ which satisfies the identity:*

$$\overline{x}^2 = -1.$$

As before, let $P(x) \in \mathbb{R}[x]$. The remainder of $P(x)$ under division by x must be a polynomial of degree ≤ 1. Therefore

$$\mathbb{R}[x]/\langle x^1 + 1\rangle = \{ax + b : a, b \in \mathbb{R}, \overline{x}^2 = -1\} \simeq \mathbb{C}.$$

5.3. **Exercises.** 1. Describe the following equivalence classes:

(1) $\mathbb{R}[x]/\langle x+2\rangle$;
(2) $\mathbb{R}[x]/\langle x^2\rangle$.

2. Prove one has well defined operations of addition and multiplication in $k[x]/\langle P(x)\rangle$ using the usual addition and multiplication of representatives.

3. Prove Proposition 5.3.

6. Groups

6.1. Definition and basic examples.

Definition 6.1. *Let G be a set and $\star : G \times G \to G$ be a function. We write $a \star b$ for $\star(a, b)$, and we refer to this as a* **binary operation**.

- *The binary operation $\star$ is* **associative** *if $\forall\ a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$.*
- *The binary operation $\star$ is* **commutative** *if $\forall a, b \in G$, $a \star b = b \star a$.*

Examples:

- The addition/substraction $\pm$ in $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ etc;
- Matrix multiplication for G =matrices with coefficients in $\mathbb{Z}$: associative, but not commutative.
- vector product $\times$ in $\mathbb{R}^3$; (but not the scalar product, why ??)
- (The Rock-Paper-Scissor operation): consider the set $A := \{r, p, s\}$ with multiplication given by the rules of the game:
  (1) $r^2 = r, p^2 = p, s^2 = s$;
  (2) $r \cdot p = p$,$r \cdot s = r$, $p \cdot s = s$;
  (3) the operation is commutative, i.e. $r \cdot p = p \cdot r$.
  This multiplication is not-associative. For example $r \cdot (p \cdot s) = r \cdot s = r \neq s = p \cdot s = (r \cdot p) \cdot s$.
- Another example of non-associative operation is the mean value of two rational numbers: $x \oplus y = \frac{x+y}{2}$.

Definition 6.2. *Let $(G, \star)$ be a set with a binary operation. We say that G is a* **group** *(with respect to $\star$) if the following are satisfied:*

(1) *(associativity) $\star$ is associative;*
(2) *(identity element) There exist an element $e \in G$ (the identity element) such that for any $g \in G$, $g \star e = e \star g = g$;*
(3) *(inverse) For any $g \in G$ there exists an element denoted g^{-1} such that $g \star g^{-1} = g^{-1} \star g = e$.*

If in addition $\star$ is commutative then $(G, \star)$ is a **commutative group**.

Proposition 6.1. *Let $(G, \star)$ be a group.*

(1) *The identity element is unique;*
(2) *Fix $g \in G$. Then the inverse element g^{-1} is unique.*
(3) *for any $g \in G$, $(g^{-1})^{-1} = g$;*
(4) *for any $a, b \in G$, $(a \star b)^{-1} = b^{-1} \star a^{-1}$*

Proof. Largely homework. □

Examples: (1) $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus 0, \cdot)$, $(\mathbb{R}, +)$, $\mathrm{GL}_n(\mathbb{R}) = \{A \in M_{n,n}(\mathbb{R}) : \det A \neq 0\}$ (the general linear group); $\mathrm{SL}_n(\mathbb{R}) = \{A \in M_{n,n}(\mathbb{R}) : \det A = 1\}$ (the special linear group). Observe that the last two examples are *non-commutative*.

(2) Is $(\mathbb{R}, \cdot)$ a group ? How about $(\mathbb{Z}/n\mathbb{Z}, \cdot)$? What do we need to do to make them groups ? (remove 0 first; in the second example we also need that n is a prime number.)

Proposition 6.2. *Let $(G, \cdot)$ be a group and consider the equations $ax = b$ and $xa = b$ $(a, b \in G)$. These equations have unique solutions $x = a^{-1}b$ respectively $x = ba^{-1}$.*

Proof. Consider the equation $ax = b$. Then we multiply on the left by a^{-1} and use associativity to obtain $a^{-1}\cdot(a\cdot x) = a^{-1}\cdot b$, i.e. $x = a^{-1}\cdot b$. In a similar way, $x = b\cdot a^{-1}$. □

6.2. **Subgroups and group homomorphisms.**

Definition 6.3. *Let $(G, \star)$ be a group. A subset $H \subset G$ is called a* **subgroup** *if the following hold:*

- *$\forall a, b \in H$, the product $a \star b \in H$. (we say that the operation $\star$ is* **closed** *with respect to H.)*
- *$e \in H$.*
- *if $a \in H$ then $a^{-1} \in H$.*

Proposition 6.3. *A subset $H \subset G$ is a subgroup if and only if H is non-empty and for any $a, b \in H$, $a \star b^{-1} \in H$.*

Proof. The implication assuming that H is a subgroup is immediate from the definition. Conversely, assume that H is non-empty and for any $a, b \in H$, $a \star b^{-1} \in H$. Then if $a \in H$, then $a \star a^{-1} = e \in H$. Further, $a^{-1} = e \star a^{-1} \in H$ by hypothesis. So it remains to show that H is closed under $\star$. If $a, b \in H$, then $a \star b = a \star (b^{-1})^{-1}$, which is in H since $b^{-1} \in H$. □

Notation: If $(G, \star)$ is a group, $H \leq G$ means H is a subgroup.

Remark 6.1. *If H is a subgroup of $(G, \star)$, then $(H, \star)$ is a group on its own, with the same identity as G.*

Example 6.1. *(a) Denote by $\mathbb{Q}^* = \mathbb{Q} \setminus 0$ and similarly for $\mathbb{Z}^*, \mathbb{R}^*, \mathbb{C}^*$ etc. The groups $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot)$ are all subgroups of $(\mathbb{C}^*, \cdot)$. Observe that $(\mathbb{Z}^*, \cdot)$ is not a subgroup, since inverses of integers are in general not integers.*

(b) $2\mathbb{Z} \leq \mathbb{Z}$; $(0, \infty) \leq (\mathbb{R}^*, \cdot)$.

(c) The circle $S^1 = \{e^{i\theta} = \cos(\theta) + i\sin(\theta) \in \mathbb{C} : \theta \in \mathbb{R}\}$ is a subgroup of $(\mathbb{C}^*, \cdot)$.

(d) The **special linear group** $\mathrm{SL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det A = 1\}$ *is a subgroup of the* **general linear group**$(\mathrm{GL}_n(\mathbb{R}), \cdot)$*, where*

$$\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}.$$

Lemma 6.1. *Let $(G, \star)$ be a group and let $H_1, H_2 \leq G$ be subgroups. Then $H_1 \cap H_2$ is also a subgroup of G.*

Proof. Apply Proposition 6.3. □

Definition 6.4. *Let $f : (G_1, \star) \to (G_2, \circ)$ be a function. We say that f is a* **group homomorphism** *if for any $a, b \in G_1$, $f(a \star b) = f(a) \circ f(b)$. If there exists $g : (G_2, \circ) \to (G_1, \star)$ such that $fg = id_{G_2}$ and $gf = id_{G_1}$ then f, g are called* **isomorphisms** *and the groups G_1 and G_2 are* **isomorphic**.

Remark 6.2. *In the definition of an isomorphism $\varphi : G \to H$, it is enough to require that φ is a bijective group homomorphism. (Why ?)*

Proposition 6.4. *Assume that $f : (G_1, \star) \to (G_2, \circ)$ is a group homomorphism. Then:*

- *$f(e_1) = e_2$ where e_i is the identity in G_i;*
- *$\forall a, b \in G_1$, $f(a \star b^{-1}) = f(a) \circ f(b)^{-1}$.*

Proof. To prove (a), note that $f(e_1) = f(e_1 \star e_1) = f(e_1) \circ f(e_1)$, thus $f(e_1) = e_2$ after simplifying. To prove the second part it suffices to show that $f(a^{-1}) = f(a)^{-1}$. To this end, observe that $f(a) \circ f(a^{-1}) = f(a \star a^{-1}) = f(e_1) = e_2$. Then the claim follows because of the uniqueness of inverses. □

Example 6.2. *(a) The map $exp : (\mathbb{R}, +) \to (0, \infty)$, $x \mapsto e^x$ is an isomorphism. (What is the inverse ?)*

(b) The determinant map $\det : (\mathrm{GL}_n(\mathbb{R}), \cdot) \to (\mathbb{R} \setminus 0, \cdot)$ *is a group homomorphism.*

(c) The determinant from the additive groups, $\det : (M_n(\mathbb{R}), +) \to (\mathbb{R}, +)$ *is* **not** *a group homomorphism.*

Proposition 6.5. *Let $f : G \to H$ be a group homomorphism. The* **kernel** *of f, denoted* $\ker(f)$ *is defined by*

$$\ker(f) = \{g \in G : f(g) = e_H\}.$$

The **image** *of f, denoted* $\mathrm{Im}(f)$*, is the subset of H given the image of the map f, i.e.*

$$\mathrm{Im}(f) := \{h \in H : \exists g \in G, f(g) = h\}.$$

By definition, $\ker(f) \leq G$ *and* $Im(f) \leq H$.

Proof. We prove the statement about the kernel; the proof about the image is similar. We apply Proposition 6.3. Observe that $e_G \in \ker(f)$. If $a, b \in \ker(f)$, then $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_G e_G = e_G$. This shows that $ab^{-1} \in \ker(f)$ and we are done. □

Proposition 6.6. *Let $f : (G, \star) \to (H, \circ)$ be a group homomorphism. Then the following hold:*

(a) f is injective $\iff \ker(f) = \{e_G\}$;

(b) f is surjective $\iff \mathrm{Im}(f) = H$.

Proof. If f is injective, then $\ker(f) = \{e_G\}$ by definition. Conversely, assume that $g_1, g_2 \in G$ satisfy $f(g_1) = f(g_2)$. Then by properties of group homomorphisms $e_H = f(g_1)f(g_2)^{-1} = f(g_1 g_2^{-1})$. Then $g_1 g_2^{-1} \in \ker(f)$, thus $g_1 g_2^{-1} = e_G$, giving $g_1 = g_2$.

The surjectivity follows from definitions. □

From now on we will use "$\cdot$" for the group multiplication, or we we will simply omit the multiplication symbol.

Definition 6.5. *Let $(G, \cdot)$ be a group and let $g \in G$. The* order *of g, denoted $|g|$, is the smallest integer $n \geq 1$ such that $g^n = e_G$. If no such n exists, then the order of g is ∞.*

We denote by $|G|$ the order of G and by $|g|$ (for $g \in G$) the order of the element g.

Example 6.3. *(a) In $G = \mathbb{Z}/10\mathbb{Z}$, the elements $\overline{1}, \overline{3}, \overline{7}, \overline{9}$ have order 10; the elements $\overline{2}, \overline{4}, \overline{6}, \overline{8}$ have order 5, the element $\overline{5}$ has order 2 and $\overline{0}$ has order 1.*

(b) Let $G = (\mathbb{C}^*, \cdot)$. If $x \neq 1$ and $x \in \mathbb{R}$, then the order of x is infinity. If $x = e^{2\pi i/n}$ then the order of x is n.

(c) Take $G = (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$. Then the identity has order 1 (as always), and the order of the other elements are:

$$|(\overline{1}, \overline{0})| = |(\overline{0}, \overline{1})| = |(\overline{1}, \overline{1})| = 2.$$

Definition 6.6. *(a) A subset $A \subset G$ is a* generating set *if any $g \in G$ can be written as a product of elements in A, and their inverses, i.e.*

$$g = a_1^{n_1} \cdot \ldots \cdot a_s^{n_s},$$

where $n_i \in \mathbb{Z}$ and $a_i \in A$.

(b) A group is cyclic *if it has a generating set with 1 element. If this is the case, we write $G = \langle a \rangle$, where a is the generator.*

We denote by $\langle A \rangle$ the subgroup generated by A. The next proposition justifies this terminology. shows that this is indeed a subgroup.

Proposition 6.7. *For $\emptyset \neq A \subset G$, the set $\langle A \rangle$ is a subgroup of G.*

Proof. The identity e_G is in $\langle A \rangle$ (just take all powers $n_i = 0$). Take $g_1 = a_1^{n_1} \cdot \ldots \cdot a_s^{n_s}$ and $g_2 = b_1^{m_1} \cdot \ldots \cdot b_p^{n_p}$ where all $a_i, b_j \in A$. By possibly adding some powers of e_G we may assume that $s = p$. Then

$$a \cdot b^{-1} = (a_1^{n_1} \cdot \ldots \cdot a_s^{n_s}) \cdot (b_{n_s}^{-n_p} \cdot \ldots \cdot b_1^{-n_1}) \in \langle A \rangle$$

by definition of $\langle A \rangle$. Then the result follows from Proposition 6.3. □

Example 6.4. *Take $G = \mathbb{Z}/4\mathbb{Z}$. These are the subgroups generated by a single element in G:*

$$\langle \overline{0} \rangle = \{\overline{0}\}; \quad \langle \overline{1} \rangle = \langle \overline{3} \rangle = \mathbb{Z}/4\mathbb{Z}; \quad \langle \overline{2} \rangle = \{\overline{0}, \overline{2}\}.$$

7. More in-depth examples of groups

7.1. **The dihedral group D_{2n}.** Fix a regular polygon P with vertices labelled $1, 2, \ldots, n$ and imagine it as a **solid plate**. Then D_{2n} is the group of **rigid symmetries** of P_n.

There are two such basic symmetries:

- The (clockwise) **rotation** r which sends the label $i \mapsto i+1$ (for ease of notation we take labels $\mod n$, i.e., $r(n) = 1$.
- The **reflection** s across the axis of symmetry which fixes 1 and bisects P_n into two congruent sides (if n is odd).

Example 7.1. *D_6 (the rigid symmetries of an equilateral triangle) is the same as the full symmetric group S_3.*

A rigid symmetry is completely determined by how any neighboring labels are mapped. For example, take labels $1, 2$ and φ any rigid symmetry. Then φ is determined by the following:

- $\varphi(1)$ and $\varphi(2)$ are connected by an edge;
- To determine where $\varphi(3)$ goes, travel $\varphi(1) \to \varphi(2)$, then take the next edge.

Example 7.2. *Visualize the symmetries of a square.*

In the next lemma we write explicitly how r, s act on labels.

Lemma 7.1. *(a) For any integer k, $r^k(i) = i + k$, where labels are interpreted $\mod n$.*
(b) $s(i) = n + 2 - i$ (again interpreting results $\mod n$).

Proof. **Homework** □

Lemma 7.2. *(a) The orders of r and s in D_{2n} are $|r| = n$ and $|s| = 2$;*
(b) $s \neq r^i$ for any $0 \leq i \leq n-1$;
(c) $r^i s = sr^{-i}$ for any $0 \leq i \leq n$.
(d) The elements $1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}$ are distinct. In particular, D_{2n} is not abelian if $n \geq 3$.
(e) $D_{2n} = \{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$.

Proof. Part (a) follows from the definition of the order. For (b), just evaluate both sides at $i = 1$. Part (c) is induction on $i \geq 1$. To check that $rs = sr^{-1}$, evaluate both sides at the labels 1 and 2. Part (d) follows by evaluating all these elements at two consecutive labels (say 1 and 2), and then checking that the outputs are distinct. We leave details as **homework**.

For (e), the previous parts prove that the elements listed are distinct. Now take any rigid symmetry φ. There are n possibIlities for $\varphi(1)$, 2 possibilities for $\varphi(2)$. Once $\varphi(1)$ and $\varphi(2)$ are fixed, then $\varphi(j)$ is completely determined for $j \geq 3$. This argument shows that there are *at most* $2n$ rigid symmetries φ. But since we already produced $2n$ distinct ones in part (d), it follows that D_{2n} must consist exactly of these elements. □

Proposition 7.1. *The set $(D_{2n}, \circ)$ equipped with composition of symmetries $\circ$ is a group, called the* **dihedral group**.

Proof. Composition of rigid symmetries is again a rigid symmetry, therefore $\circ$ is a binary operation on D_{2n}. Each such symmetry corresponds to a function, and composition of functions is associative; therefore $\circ$ is associative. The identity element is the identity symmetry (no labels are moved). Finally, each symmetry is reversible, showing that each element has an inverse. □

7.2. **The groups $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^*$.** Recall the notation $\mathbb{Z}/n\mathbb{Z} := \{\ \bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ for the set of equivalence classes of residues modulo n.

Definition 7.1. *Denote by $(\mathbb{Z}/n\mathbb{Z})^\times$ to be the set of* **invertible elements** *in $\mathbb{Z}/n\mathbb{Z}$ with respect to the multiplication, i.e. those elements $\overline{a}$ such that $ab \equiv 1 \mod n$ for some b. Sometimes the invertible elements are also called* **units** *in $\mathbb{Z}/n\mathbb{Z}$.*

The following follows from Lemma 3.2.

Lemma 7.3. *The set $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} : gcd(a, n) = 1\}$, i.e. an element $\overline{a}$ is invertible if and only if $gcd(a, n) = 1$.*

Recall that on $\mathbb{Z}/n\mathbb{Z}$ we defined two operations:

$$\bar{i} + \bar{j} = \overline{i+j}; \quad \bar{i} \cdot \bar{j} = \overline{ij}.$$

Proposition 7.2. *(a) $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group;*
(b) $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ is a group.

Proof. Part (a) follows from Lemma 3.1 and the definition of the addition. For part (b), the only thing one needs to show is that if $\overline{a}, \overline{b}$ are invertible, then so is their product. The hypothesis means that there exists a', b' such that $\overline{a}\overline{a'} = \overline{bb'} = \overline{1}$. Then

$$\overline{abb'a} = \overline{aa'} = \overline{1},$$

and the claim is proved. □

We will see later on that the two operations give $\mathbb{Z}/n\mathbb{Z}$ a structure of a *ring*. Also note that by definition and Lemma 7.3, observe that if n is prime, then $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z}\backslash\{\overline{0}\}$.

Example 7.3. $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. *The elements $\overline{1}$ and $\overline{3}$ have order 4; the element $\overline{2}$ has order 2.*

Example 7.4. *The group $(\mathbb{Z}/4\mathbb{Z})^\times$ consists of the elements $\overline{1}$ and $\overline{3}$. This group (with multiplication) is isomorphic to $(\mathbb{Z}/2\mathbb{Z}, +)$.*

Proof of Theorem 7.2. Parts (a) and (b) follow from Lemma 3.1 and the definition of the addition.

For part (c), assume n is prime, and take $1 \leq a \leq n-1$. Then $gcd(a, n) = 1$ therefore one can write $ka + ns = 1$. This means that $ka \equiv 1 \mod n$, i.e. a is invertible modulo n. Obviously $\overline{0}$ is not invertible. This finishes the proof of (c).

The only thing one needs to show is that if $\overline{a}, \overline{b}$ are invertible, then so is their product. The hypothesis means that there exists a', b' such that $\overline{a}\overline{a'} = \overline{bb'} = \overline{1}$. Then

$$\overline{abb'a} = \overline{aa'} = \overline{1},$$

and the claim is proved. □

We now study some properties of the group $\mathbb{Z}/n\mathbb{Z}$ and its group of units.

Proposition 7.3. *(a) The group $\mathbb{Z}/n\mathbb{Z}$ is cyclic, i.e. it is generated by one element.*
(b) An element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.

Proof. Clearly $\overline{1}$ generates $\mathbb{Z}/n\mathbb{Z}$. We now prove (b). If $\overline{a}$ generates $\mathbb{Z}/n\mathbb{Z}$, then $\overline{1} = k\overline{a} = \overline{ka}$ for some k. This means that $\overline{a}$ is invertible. Conversely, assume that $\overline{a}$ is a unit, thus $ab \equiv 1 \mod n$. Then for any k we have $\overline{k} = kb\overline{a}$, showing that $\overline{a}$ generates $\mathbb{Z}/n\mathbb{Z}$. □

Definition 7.2. *The* **Euler function** $\Phi : \{1, 2, \ldots\} \to \{1, 2, l \ldots, \}$ *is defined by*

$$\Phi(n) := \#(\mathbb{Z}/n\mathbb{Z})^{\times} = \#\{a : gcd(a, n) = 1\}.$$

Example 7.5. *(a) $\Phi(4) = 2$, $\Phi(15) = 8$;*
(b) If p is a prime, $\Phi(p^n) = p^n - p^{n-1}$. (Idea: substract all multiples of p in the set $1, 2, \ldots, p^n$.)
(c) One can show that if $gcd(a, b) = 1$, then

$$\Phi(a \cdot b) = \Phi(a) \cdot \Phi(b).$$

Combined with (b), this implies a formula for any *$\Phi(n)$, given its prime decomposition $n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$.*

7.3. **Exercises.**

8. Cyclic groups

8.1. **On generators.** Recall the definition:

Definition 8.1. *A group G is cyclic if it is generated by a single element $x \in G$, i.e. $G = \{1, x^{\pm 1}, \cdots, x^{\pm k}, ...\}$ (but elements are not necessarily distinct).*

When x is a generator for a cyclic group, then with the previous notation $G = \langle x \rangle$.

As first examples, note that the groups $(\mathbb{Z}, +), (\mathbb{Z}/n\mathbb{Z}, +)$ are cyclic groups, with generators 1, respectively $\overline{1}$. The choice of the single generator is not unique:

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle; \quad \mathbb{Z}/n\mathbb{Z} = \langle \overline{a} \rangle \text{ where } (a, n) = 1,$$

meaning that $\overline{a}$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $gcd(a, n) = 1$ (cf. Proposition 7.3).

Proposition 8.1. *Let $(G, \cdot)$ and $x \in G$ an element. Then the following hold:*

- *If $|x| = \infty$ then $x^i \neq x^j$ for any $i, j \in \mathbb{Z}$, $i \neq j$;*
- *If $|x| = n$ then $\langle x \rangle$ consists of the distinct elements $G = \{1, x, \ldots, x^{n-1}\}$.*

Proof. Since $x \in G$, the set $\{x^k : k \geq 0\} \subset G$, thus $|x| \leq |G|$. We prove the reverse inequality. We distinguish the two cases in the proposition.

Case 1. $|x| = \infty$. If $x^i = x^j$ then $x^{i-j} = 1$, which is impossible. It follows that there are infinitely many elements in G, thus $|G| = |x| = \infty$.

Case 2. $|x| = n$. Let $g = x^k \in G$. By the division algorithm, $k = nq + r$ where $0 \leq r < n$. Then $x^k = (x^n)^q x^r = x^r$, from which we deduce that $|G| \leq n$. On the other side, since $|x| = k$, there are at least k distinct powers of x. This finishes the proof. □

One way to restate Proposition 8.1 is as follows:

Corollary 8.1. *In the hypotheses above, $|x| = |\langle x \rangle|$, i.e. the order of x equals the order of the subgroup it generates.*

Example 8.1. *(A family of cyclic groups in $\mathrm{SL}_2(\mathbb{R})$.) Let $G := \mathrm{SL}_2(\mathbb{R})$ and fix $a \in \mathbb{R}$. Define the matrix*

$$x_a := \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in G.$$

Observe that $(x_a)^k = x_{ka}$; in other words,

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & ka \\ 0 & 1 \end{pmatrix}.$$

The subgroup generated by x_a is isomorphic to $\mathbb{Z}$.

This gives a family of cyclic groups in SL_2 indexed by $a \in \mathbb{R}$. Two such groups are the same, i.e. $\langle x_a \rangle = \langle x_b \rangle$, if and only if $a = \pm b$.

8.2. **Classification and first properties of cyclic groups.** The next proposition states that up to isomorphism there exist only two cyclic groups: the additive groups $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.

Theorem 8.1. *Let $G = \langle x \rangle$ be a cyclic group.*

- *If $|G| = \infty$ then G is isomorphic to $(\mathbb{Z}, +)$;*
- *If $|G| = n$ then G is isomorphic to $(\mathbb{Z}/n\mathbb{Z}, +)$.*

Proof. Let $|G| = \infty$. Then $|x| = \infty$. Define the function $\varphi : G \to \mathbb{Z}$ given by $\varphi(x^k) = k$. $(k \in \mathbb{Z})$. It is easy to see this is an isomorphism.

Let now $|G| = |x| = n$. Then by the previous proposition $G = \{1, x, \ldots, x^{n-1}\}$ (distinct elements). Define the function $\varphi : G \to \mathbb{Z}/n\mathbb{Z}$ given by $\varphi(x^k) = \overline{k}$. $(0 \leq k \leq n-1)$. It is easy to see this is a surjective group homomorphism. To prove it is an isomorphism we need to check injectivity. Let $\varphi(x^a) = \varphi(x^b)$. Then $\overline{a} = \overline{b}$, thus $\overline{a-b} = 0$, from which we deduce that n divides both $a - b$ and $b - a$. W.l.o.g. we can assume that $a \leq b$. Then $0 \leq b - a \leq n - 1$, and the divisibility condition forces $a = b$, hence $x^a = x^b$. □

Example 8.2. *(Groups of order 2.) The only group of order 2 is (isomorphic to) $\mathbb{Z}/2\mathbb{Z}$.*

Example 8.3. *(Groups of order 3.) Let $G = \{1, x, y\}$. By analyzing the multiplication table of G, we find that the only group of order 3 is (isomorphic to) $\mathbb{Z}/3\mathbb{Z}$. There are two identifications:*

$$1 \leftrightarrow \overline{0}; \quad x \leftrightarrow \overline{1}; \quad y \leftrightarrow \overline{2} \quad \text{and} \quad 1 \leftrightarrow \overline{0}; \quad x \leftrightarrow \overline{2}; \quad y \leftrightarrow \overline{1}.$$

This proves that there are two isomorhisms $\varphi : (\mathbb{Z}/3\mathbb{Z}, +) \to (\mathbb{Z}/3\mathbb{Z}, +)$. (One is the identity $\overline{k} \mapsto \overline{k}$, the other is $\overline{k} \mapsto -\overline{k}$.)

Example 8.4 (Groups of order 4)**.** *Up to isomorphism, there are only two groups of order 4: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Idea: write down the possible multiplication tables.*

Example 8.5 (Groups of order 5 and 6)**.** *This example will become much easier to prove once we know Lagrange's Theorem, which implies that the order of an element in a group must divide the order of the group.*

There is a single group of order 5: $\mathbb{Z}/5\mathbb{Z}$.

There are three groups of order 6: $\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the (non-abelian!) group S_3, the symmetric group in 3 letters.

Theorem 8.2. *Any subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle x \rangle$. W.l.o.g we can assume that H is not the trivial subgroup. Consider the number

$$a := \min\{k > 0 : x^k \in H\}.$$

The assumption implies that this minimum exists. We claim that $H = \langle x^a \rangle$. Clearly $\langle x^a \rangle \subset H$, thus it suffices to show the reverse inclusion. Let $h \in H$. Then $h = x^k$ for some integer k. By the division algorithm, $k = na + r$ where $0 \leq r < a$. Then

$x^k = (x^a)^q x^r \in H$, from which we deduce that $x^r \in H$. Since $0 \leq r < a$, and from the definition of a, we obtain that $r = 0$. Then $x^k = (x^a)^q \in H$. This proves that $H \subset \langle x^a \rangle$, and it finishes the proof. □

We now relate the order of an element in a cyclic group by the order the the group.

Proposition 8.2. *Let $G \simeq \mathbb{Z}/n\mathbb{Z}$ be a finite cyclic group, and let $\overline{a} \in G$. Then the following hold:*

(a) If $k\overline{a} = \overline{0}$, then k is a multiple of the order of $\overline{a}$.

(b) The order of $\overline{a}$ equals $\frac{n}{gcd(a,n)}$.

Proof. Assume $k\overline{a} = \overline{0}$, and let n_0 be the order of $\overline{a}$. By the division algorithm, $k = n_0 q + r$, where $0 \leq r \leq n_0$, and $r\overline{a} = \overline{0}$. Then by the definition of the order, $r = 0$; this proves (a).

For (b), denote by n_0 be the order of $\overline{a}$. Then $n_0 a \equiv 0 \mod n$, i.e. $n | a n_0$. Part (a) implies that n is a multiple of n_0, thus n/n_0 divides a. Then n/n_0 divides $gcd(a, n)$, i.e $\frac{n}{n_0} s = gcd(a, n)$. This implies that $\frac{n}{gcd(a,n)}$ divides n_0. On the other side $\frac{n}{gcd(a,n)} a \equiv 0 \mod n$, showing that n_0 divides $\frac{n}{gcd(a,n)}$, and we are done. □

Observe that part (b) of the above proposition generalizes Proposition 7.3. In particular, we deduce the following corollary:

Corollary 8.2. *Let a, b, n be positive integers.*

- *The order of the subgroup generated by $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ is $\frac{n}{gcd(a,n)}$.*
- *If b is a multiple of a then*

$$\langle \overline{a} \rangle = \langle \overline{b} \rangle \iff gcd(a, n) = gcd(b, n).$$

Proof. Exercise! □

8.3. **Group homomorphisms from cyclic groups.** An important property of cyclic groups is about the group homomorphisms from a cyclic group. This will be useful to rule out that many familiar groups are cyclic, e.g. $\mathbb{Q}$ or $\mathbb{R}$.

Lemma 8.1. *Let $\varphi : G \to H$ be a group homomorphism. If G is cyclic then so is $\varphi(G)$.*

Proof. Exercise! □

Proposition 8.3. *Let $\varphi : G \to H$ be a group homomorphism, and assume that $G = \langle x \rangle$ is cyclic. Then φ is completely determined by the image of x.*

Proof. If $\varphi_h(x) = h$ then $\varphi_h(x^k) = h^k$ for any $k \in \mathbb{Z}$. But G consists of all such elements x^k, so φ_h is uniquely determined by the choice of $\varphi_h(x)$. Conversely, it is immediate to see that if φ_h and φ'_h would be two such homomorphisms, then $\varphi_h(x^k) = h^k = \varphi'_h(x^k)$, thus $\varphi = \varphi'$. □

Proposition 8.4. *Let $G = \langle x \rangle$ be a cyclic group, and let H be an arbitrary group.*

(1) *Assume that* $|G| = \infty$. *Then for each* $h \in H$, *there exists a unique group homomorphism* φ_h *such that* $\varphi_h(x) = h$.
(2) *Assume that* G *is generated by* x *and that* $|G| = n$. *Then for each* $h \in H$, *there exists* at most *one group homomorphism* $\varphi : G \to H$ *such that* $\varphi(x) = h$. *This homomorphism exists if and only if the order of* h *divides the order of* x.

Proof. We prove part (1) first. Since $|G| = \infty$, it follows that the elements x^k, $k \in \mathbb{Z}$ are distinct. Then by the group homomorphism property, if $\varphi(x) = h$, then $\varphi(x^k) = h^k$. One checks that

$$\varphi(x^a \cdot x^b) = \varphi(x^{a+b}) = h^{a+b} = \varphi(x^a) \cdot \varphi(x^b),$$

therefore this is the (unique!) homomorphism we seek.

For part (2), observe first that as in (1), since $\varphi(x) = h$, and because of the group homomorphism property, we obtain that $\varphi(x^k) = h^k$. So there is at most one such homomorphism. We need to prove existence, i.e. that φ is well defined; this issue arises because powers of x are no longer distinct.

First, observe that $|x| = n$, therefore $e_H = \varphi(x^n) = h^n$. Therefore, if one applies Proposition 8.2 to the (cyclic!) subgroup generated by x, we must have that the order of h divides n. Then for powers of the form $0 \leq kq + r \leq n - 1$, we have

$$\varphi(x^{kq+r}) = h^{kq+r} = h^r,$$

and one may check directly that this is well defined. □

Remark 8.1. *In fact, one can show that there is a one-to-one correspondence between group homomorphisms* $\varphi : G \to H$ *and elements of* H *of order dividing the order of* x.

Example 8.6. *As an application, we can determine all isomorphisms* $\varphi : \mathbb{Z} \to \mathbb{Z}$. *Any such isomorphism sends a generator of* $\mathbb{Z}$ *to another generator. But* $\mathbb{Z}$ *has only generators* ± 1, *thus there are only two possible such assignments:*

$$\varphi(1) = 1; \quad \psi(1) = -1.$$

By the previous proposition both φ *and* ψ *extend uniquely to group homomorphisms:* $\varphi(x) = x$ *and* $\psi(x) = -x$.

Example 8.7.
- *There are* 12 *homomorphisms* $\varphi : \mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$, *because* $\mathbb{Z} = \langle 1 \rangle$, *and* 1 *may be sent to any of the* 12 *elements in* $\mathbb{Z}/12\mathbb{Z}$.
- *There are 2 homomorphisms* $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$; *again* $\mathbb{Z}/4\mathbb{Z} = \langle \overline{1} \rangle$ *and by Proposition 8.4 part (2),* $\overline{1}$ *may be sent to both* $\overline{0}, \overline{1}$.
- *There are* 3 *homomorphisms* $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$, *since* $\mathbb{Z}/3\mathbb{Z} = \langle \overline{1} \rangle$ *but in this case by Proposition 8.4 part (2),* $\overline{1}$ *may be sent only to* $\overline{0}, \overline{3}$ *and* $\overline{6}$.
- *There is just one homomorphism* $\mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}$ *and one homomorphism* $\mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/9\mathbb{Z}$ *(the trivial homomorphism).*

8.4. **Exercises.**

9. Symmetric groups

9.1. **Definitions and basic properties.** Let Ω be a set, and define

$$S_\Omega := \{f : \Omega \to \Omega : f \text{ is a bijection } \}.$$

Proposition 9.1. *$(S_\Omega, \circ)$ is a group, where $\circ$ is the composition of functions.*

Proof. The associativity follows from associativity of composition of functions. The identoty is the identity function $x \mapsto x$. If $f : \Omega \to \Omega$ is a bijection, there is a well defined inverse $f^{-1} : \Omega \to \Omega$; this is the inverse of f, also when regarded as en element in S_Ω. □

If Ω is a finite set, let $\Omega = \{a_1, ..., a_n\}$. Then S_Ω is the symmetric group in n letters, denoted S_n. (Note that the structure of S_Ω depends only on the cardinality of Ω, and not on Ω itself.)

To simplify notation we will assume from now on that $\Omega = \{1, ..., n\}$. The elements of S_n are called **permutations**. There are two ways of writing a pemutation $\sigma \in S_n$: **matrix notation**, and **cycle notation**. We will explain this on an example. Consider the bijection $\sigma : S_{10} \to S_{10}$ given by

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

The *matrix notation* displays the inputs and outputs as the two rows of a matrix:

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

The *cycle notation* displays any way of tracing the cycles in σ:

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

So (1 5 8 10) is the cyclic permutation sending $1 \to 5 \to 8 \to 10 \to 1$ and keeping all the other numbers fixed, and the product is the composition is such cycles.

Proposition 9.2. (1) *Every two disjoint cycles commute.*

(2) *Every permutation $\sigma \in S_n$ can be written as a product of disjoint cycles. (i.e. cycles which do not have any digit in common). The decomposition is unique up to cyclically reordering the elements in a given cycle, and up to reordering the cycles themselves.*

(3) *The order of a permutation is the l.c.m. of the lengths of cycles in its cycle decomposition.*

Proof. Part (1) is immediate. Part (2) is left as an exercise (just trace the cycles in σ). We prove part (3). We start by considering a single cycle $w = (i_1, i_2, \ldots, i_k)$. Then $w^2 = (i_1, i_3, i_5, \ldots)$, i.e. it is the cycle (or product of cycles) obtained from the initial cycle with the step 2. Similarly, w^3 uses step 3 and so on. In particular, the first time

when one obtains the identity is when the step equal to k, i.e the order of a k-cycle equals to k. (In particular, this also means that the cyclic group generated by the k-cycle w is isomorphic to $\mathbb{Z}/k\mathbb{Z}$, via the morphism given by $w \mapsto \overline{1}$.)

In general, write w as a product of disjoint cycles, and let $n_1, \ldots, n_k$ denote the lengths of the cycles. Since disjoint cycles commute, it follows that $w^{lcm(n_1,\ldots,n_k)} = id$. This means that the order of w must divide $lcm(n_1, \ldots, n_k)$. On the other side, since the cycles are disjoint, if $w^N = id$, it follows that N must be a multiple of each n_i. But then the order of w must equal to the lcm in question, and this finishes the proof. □

Example 9.1. *As before, let*

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

Then the cycle decomposition is

$$\sigma = (1, 5, 8, 10)(2, 3, 4)(6, 7);$$

(we ignore the cycles of length 1*). The order of this permutation is* 12*.*

It is easy to find inverses of a permutation σ in the matrix and cycle notation:

- in the matrix notation, exchange the two rows. With σ above we obtain:

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

- In the cycle notation, one simply reverses the order of indices in each cycle:

$$\sigma^{-1} = (10\ 8\ 5\ 1)(4\ 3\ 2)(7\ 6)(9) = (1\ 10\ 8\ 5)(2\ 4\ 3)(6\ 7)(9)$$

  where the last equality follows from cyclically permuting indices so that each cycle begins with the smallest index.

Two permutations u, v are **conjugate** if there exists $w \in S_n$ such that $v = w^{-1}uw$.

Proposition 9.3. *(a) The relation of conjugation is an equivalence relation.*
(b) Two permutations are conjugated if and only if they have the same cycle type.

Proof. Part (a) is left as an exercise. For part (b), consider $v = wuw^{-1}$. One can write u as a product of disjoint cycles, let's say $u^{(1)}, u^{(2)}, \ldots, u^{(k)}$. Then

$$wuw^{-1} = (wu^{(1)}w^{-1})(wu^{(2)}w^{-1}) \ldots (wu^{(k)}w^{-1}).$$

Using this, we see that it suffices to assume that u is a single cycle $u = (i_1, \ldots, i_s)$. We now calculate $wuw^{-1}(i)$. Assume first that $w^{-1}(i) = i_p$ (one of the labels in the cycle u); then

$$wuw^{-1}(i) = wuw^{-1}(w(i_p)) = w(i_{p+1}).$$

If $w^{-1}(i)$ is not in $\{i_1, \ldots, i_s\}$ then $wuw^{-1}(i) = i$. This implies that $w(i_1, \ldots, i_s)w^{-1}$ is the cycle $(w(i_1), w(i_2), \ldots w(i_s))$. □

We record the following identity obtained within the proof:

Corollary 9.1. *Let $u = (i_1, \ldots, i_p) \in S_n$ be a cycle and $w \in S_n$ a permutation. Then*

$$w(i_1, \ldots, i_p)w^{-1} = (w(i_1), \ldots, w(i_p)).$$

Remark 9.1. *The previous proposition also implies two facts:*

1. *There is a partition of S_n into equivalence classes;*
2. *each equivalence class is determined by a partition of n, i.e. a sequence $\lambda = (\lambda_1, \ldots, \lambda_k)$ such that $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k \geq 0$ and $\lambda_1 + \lambda_2 + \ldots + \lambda_k = n$.*

Example 9.2. *Consider the symmetric group S_3. The partitions of 3 are $(1,1,1)$, $(2,1)$ and (3).*

The corresponding number of elements in each conjugacy class is $1, 3, 2$ and each equivalence class contains the following:

- *There is 1 permutation with cycle type $(1,1,1)$: the identity $(1)(2)(3)$;*
- *There are 3 permutations with cycle type $(2,1)$: $(12)(3), (13)(2)$ and $(1)(23)$;*
- *There are 2 permutations with cycle type (3): (123) and (132).*

Note $6 = 1 + 3 + 2$, expressing the fact that S_3 is the disjoint union of its equivalence classes.

Example 9.3. *Consider the symmetric group S_4. The partitions of 4 are $(1,1,1,1)$, $(2,1,1)$,$(2,2)$, $(3,1)$ and (4). The number of elements in each conjugacy class is $1, \binom{4}{2}, 1/2\times \binom{4}{2}, \binom{4}{3} \times 2!, 3!$. Note that*

$$1 + \binom{4}{2} + \frac{1}{2} \times \binom{4}{2} + 4 \times 2! + 3! = 1 + 6 + 3 + 8 + 6 = 24 = |S_4|.$$

9.2. **Any group is a subgroup of a symmetric group.**

Proposition 9.4. *Let G be a group of order n. Then G is isomorphic to a subgroup of S_n.*

Proof. We construct an isomorphism from G to a subgroup of $S_G = S_n$. Pick $g \in G$, and define $\varphi_g : G \to G$ by $\varphi_g(x) = gx$. Since G is a group, φ_g is a bijection, i.e. $\varphi_g \in S_G = S_n$. Now define

$$\Psi : G \to S_G; \quad g \mapsto \varphi_g.$$

We show this is an injective group homomorphism. To check it is a homomorphism, $\Psi(g_1g_2) = \varphi_{g_1} \circ \varphi_{g_2}$. Since this is an equality of functions, we need to show

$$\varphi_{g_1g_2}(x) = \varphi_{g_1} \circ \varphi_{g_2}(x); \quad \forall x \in G.$$

Indeed $\varphi_{g_1g_2}(x) = (g_1g_2)x$ and $\varphi_{g_1} \circ \varphi_{g_2}(x) = g_1(g_2x)$ and the two are obviously equal, by associativity.

To show Ψ is injective, we calculate its kernel. We have

$$\ker(\Psi) = \{g \in G : \Psi(g) = (id : G \to G)\} = \{g \in G : gx = x \ \forall x \in G\} = \{e_G\}.$$

Finally, since Ψ is injective, it follows that G is isomorphic to its image $\Psi(G) \leq S_G$. $\square$

The group homomorphism Ψ defined in the proof of the proposition above is called the **left regular representation of** G. A direct way to define this group homomorphism is as follows. Enumerate elements of G in some order, for instance $e_G = x_1, \dots, x_n$ where $n = |G|$. Then

$$\Psi(g) = \begin{pmatrix} x_1 & x_2 & x_3 & \dots & x_n \\ gx_1 & gx_2 & gx_3 & \dots & gx_n \end{pmatrix}$$

The key is that the bottom row is just a permutation of the top.

Example 9.4. *We illustrate the construction of* Ψ *in the case* $G = \mathbb{Z}/3\mathbb{Z}$. *Then* $G = \{\overline{0}, \overline{1}, \overline{2}\}$. *The map* $\varphi_{\overline{a}}(\overline{k}) = \overline{a+k}$. *This gives the following homomorphism* Ψ*:*

$$\Psi(\overline{0}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} \\ \overline{0} & \overline{1} & \overline{2} \end{pmatrix}; \Psi(\overline{1}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} \\ \overline{1} & \overline{2} & \overline{0} \end{pmatrix} : \Psi(\overline{2}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} \\ \overline{2} & \overline{0} & \overline{1} \end{pmatrix}.$$

9.3. **The alternating group.** A cycle $(i\ j)$ of length 2 is called a **transposition**, and if the cycle is $s_i := (i\ i+1)$ it is a **simple transposition**. One can show that S_n has a presentation with generators given by the simple transpositions, and relations

$$s_i^2 = id; \quad s_i s_j = s_j s_i, \quad |i-j| \geq 2; \quad s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}.$$

The last is called a **braid relation**.

Given a permutation $w \in S_n$, an **inversion** is a pair $(i < j)$ such that $w(i) > w(j)$. The **length** of a permutation w is the number of its inversions.

Example 9.5. *(a) The length of a simple transposition is* 1*;*
(b) The length of a transposition (i, j) *is* $2(j-i)-1$.

Proposition 9.5. *The following hold:*
(a) $\ell(uv) \equiv \ell(u) + \ell(v) \mod 2$*;*
(b) If $w := (i_1, \dots, i_k)$ *is a* k*-cycle, then* $\ell(w) = k - 1 \mod 2$.

Proof. To prove (a), consider the product

$$\Delta := \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

This is a polynomial in variables $x_1, \dots, x_n$. For each $w \in S_n$, one may permute the variables in Δ according to w, i.e.

$$w.\Delta(x_1, \dots, x_n) = \Delta(x_{w(1)}, \dots, x_{w(n)}).$$

Observe that $id.\Delta = \Delta$ and that in general

$$w.\Delta = (-1)^{\ell(w)} \Delta.$$

On the other side, it is clear that $u.(v.\Delta) = (uv).\Delta$, and combined with the previous equation this gives $(-1)^{\ell(uv)} = (-1)^{\ell(u)} \cdot (-1)^{\ell(v)}$. This proves the result.

We now prove (b). Consider the product $u := (i_1, i_2, \ldots, i_k)(i_1, i_k)$. Then $u(i_1) = i_1$, and $u(j) = j$ for j not a label in the cycle. One checks that in fact $u = (i_2, \ldots, i_k)$. Then by part (a),

$$\ell((i_1, i_2, \ldots, i_k)) \equiv \ell(u) + \ell((i_1, i_k)) \mod 2.$$

By induction $\ell(u) \equiv k - 2 \mod 2$, and of course $\ell((i_1, i_k)) \equiv 1 \mod 2$. This finishes the proof. □

Definition 9.1. *The* alternating group A_n *is the subset of* S_n *consisting of permutations of even length.*

Proposition 9.6. *A_n is a subgroup of S_n.*

Proof. This follows from proposition 9.5. □

Example 9.6. *By Proposition 9.5, the alternating group A_4 consists of all permutations which are either 3-cycles, or a product of two 2-cycles, or identity. There are $\binom{4}{3} \times 2 = 8$ permutations which are 3-cycles, and 3 products of two 2-cycles. Thus A_4 has $8+3+1 = 12$ elements. Observe that $12 = 4!/2$.*

Proposition 9.7. *The alternating group has order $n!/2$. (Later, this will be expressed as: A_n has index 2 in S_n.)*

Proof. Let $w \in S_n$. If $\ell(w)$ is even then $wA_n = A_n$. If $\ell(w)$ is odd, then $\ell((1,2)w)$ is even by Proposition 9.5, whihc implies that $wA_n = (1,2)A_n$. Then $S_n = A_n \cup (1,2)A_n$ and we are done. □

9.4. **Exercises.**

10. Cosets and Lagrange theorem

Let G be a group and $H \leq G$ be a subgroup.

Definition 10.1. *A (left)* coset *of H is a set xH for some $x \in G$. Any element in this coset is called a* coset representative. *The set of all (left) cosets of H is denoted by G/H.*

Example 10.1. *Let $G = S_3$ and $H = \langle (12) \rangle$ (the group generated by the permutation that exchanges $1 \leftrightarrow 2$; this is called a* **simple transposition***). Since (12) has order 2, it follows that $|H| = 2$. In fact, $H = \{id, (12)\}$. Then any coset xH will be a set of size 2, and it consists with multiplying on the left by elements of H. Here are some examples:*

$$idH = H; \quad (12)H = H;$$

$$(23)H = \{(23), (23)(12) = (132)\}; \quad (123)H = \{(123), (123)(12) = (13)\}.$$

We may also consider the right cosets:

$$Hid = H; \quad H(12) = H;$$

$$H(23) = \{(23), (12)(23) = (123)\}; \quad H(123) = \{(123), (12)(123) = (23)\}.$$

One can make a similar definition for right cosets Hh, and in that case we obtain $H\ G$. Note the following:

Proposition 10.1. *(a) $x_1H = x_2H \iff (x_2)^{-1}x_1H = H \iff (x_1)^{-1}x_2 \in H$.*
(b) $x_1H \cap x_2H$ is either empty or $x_1H = x_2H$.
(c) $|xH| = |Hx| = |H|$ for any $x \in G$.

Proof. (a) is clear. For (b), assume $x_1H \cap x_2H \neq \emptyset$, and let $g \in x_1H \cap x_2H$. Then $g = x_1h_1 = x_2h_2$. Then

$$gH = x_1h_1H = x_1H; \quad gH = x_2h_2H = x_2H.$$

To prove (c) we need to construct a bijection $\varphi : xH \to Hx$. Define $\varphi(xh) = hx$. This is clearly injective and surjective. □

Remark 10.1. *A similar characterization works for right cosets. In fact, there is a bijection between G/H (the set of left cosets), and $H\backslash G$ (the set of right cosets), given by*

$$xH \mapsto (xH)^{-1} = Hx^{-1}.$$

We can define an equivalence relation by $x \simeq y$ iff $xH = yH$. It is easily checked that this is reflexive, symmetric and transitive. Note also that each equivalence class has the same number of elements: the order of H. Recall that G/H denotes the set of equivalence classes.

Corollary 10.1 (Lagrange Theorem)**.** *Let G be a finite group and $H \leq G$ a subgroup. Then*

$$|G/H| = \frac{|G|}{|H|}.$$

In particular, the order of H divides the order of G.

Proof. The cosets of H partition G into equivalence classes, and each equivalence class has the same size equal to $|H|$. By definition, the number of equivalence classes equals to $|G/H|$. Then the claim follows. □

Definition 10.2. *The cardinality of G/H is called the index of H in G, and it is denoted by $|G : H|$. Lagrange theorem says that*

$$|G : H| = \frac{|G|}{|H|}.$$

Corollary 10.2. *Let G be a finite group and $x \in G$. Then $|x|$ divides $|G|$.*

Proof. Apply Lagrange's theorem to the cyclic group generated by x. □

Corollary 10.3. *Let p be a prime number, and let G be a finite group of order p. Then G is cyclic, in particular G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Let $x \in G$ such that $x \neq 1$. By Corollary 10.2, the order of x divides p. Since p is prime, the order of x equals p, which means that G is the cyclic group generated by x. □

Remark 10.2. *The converse of either Lagrange Theorem or of Corollary 10.2 is not true. For example:*

- *Take $n = |G|$. Then G has an element of order n iff G is cyclic. We know that not all groups are cyclic (e.g. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).*
- *Consider the alternating group A_5, which has order $5!/2 = 60$. It is known that it does not have a subgroup of order 30. (It is a simple group, and any subgroup or order 30 has index 2, thus a normal subgroup.)*

However, two partial converses hold:

- *(Cauchy theorem.) If p is prime then G has an element of order p.*
- *G has a subgroup of order p^k where p^k is the maximal power of p dividing $|G|$. (This is called a Sylow subgroup.)*

10.1. **Exercises.**

11. Normal subgroups

Let G be any group and $H \leq G$ a subgroup. Define $N_G(H) := \{x \in G : xHx^{-1} = H\} = \{x \in G : xH = Hx\}$. This is called the *normalizer* of H in G.

Lemma 11.1. *The normalizer $N_G(H)$ is a subgroup of G.*

Proof. Clearly $id \in N_G(H)$. If $g_1, g_2 \in N_G(H)$ then

$$(g_1g_2)H = g_1Hg_2 = H(g_1g_2),$$

thus $g_1g_2 \in N_G(H)$. Similarly,

$$(g_1H)^{-1} = H^{-1}g_1^{-1} = Hg_1^{-1} \text{ and } (Hg_1)^{-1} = g_1^{-1}H;$$

since $Hg_1 = g_1H$ this shows that $g_1^{-1} \in N_G(H)$. This finishes the proof. □

Remark 11.1. *If $x \in N_G(H)$, the condition $xHx^{-1} = H$ is equivalent $xHx^{-1} \subset H$. To see that, it suffices to show the reverse inclusion $H \subset xHx^{-1}$. Since $x^{-1} \in N_G(H)$, we have:*

$$x^{-1}Hx \subset H \Longrightarrow H \subset xHx^{-1}.$$

Definition 11.1. *Let $H \leq G$ be a subgroup. We say that H is* **normal** *if $N_G(H) = G$. Equivalently, for any $x \in G$, $xHx^{-1} \subset H$.*

The main property of normal subgroup is that we can 'divide' by them, and define a group operation on the quotient G/H:

$$xH \circ yH = (xy)H.$$

In general this operation *does* depend on the choice or representatives x, y. The next proposition shows this is not the case if H is normal.

Proposition 11.1. *The multiplication $\circ$ is well defined if and only if for any $x \in G$, $xHx^{-1} = H$. This is equivalent to any of the following statements:*

- *$N_G(H) = G$;*
- *$xH = Hx$ for all $x \in G$.*

Proof. Assume that $xHx^{-1} = H$. This is equivalent to $xH = Hx$. We prove the multiplication is well defined. Let x_1, x_2 such that $x_1H = x_2H$ and let y_1, y_2 such that $y_1H = y_2H$. Then

$$x_1y_1H = x_1Hy_1 = x_2Hy_1 = x_2Hy_2 = x_2y_2H,$$

finishing the proof of this implication.

We now prove the converse. Let $x \in G$. Then $xH = xH \circ H = H \circ xH$, which means that $hxH = xH$ for any $h \in H$ i.e. $HxH = xH$. This implies that $Hx \subset xH$, for all $x \in G$. Taking inverses, and using that $H^{-1} = H$, we obtain

$$x^{-1}H \subset Hx^{-1}, \quad \forall x \in G.$$

As x^{-1} varies over all elements in G as x varies in G, this proves the reverse inclusion. □

We denote the fact that H is normal in G by $H \trianglelefteq G$. In this case, the quotient $(G/H, \circ)$ is a group called the *quotient group*. It has identity $1.H$ and inverses given by $(xH)^{-1} = x^{-1}H$. Note that

$$(xH)^{-1} = Hx^{-1} = x^{-1}H,$$

where the last equality holds because of normality.

Remark 11.2. *A normal group $H \trianglelefteq G$ comes as a 'package':*

- *a quotient subgroup $(G/H, \circ)$;*
- *a group homomorphism $\pi : G \to G/H$ sending $g \mapsto gH$ such that $\ker \pi = H$.*

The homomorphism π is called the **projection**.

Lemma 11.2. *Let $f : G \to H$ be any group homomorphism. Then $\ker(f)$ is a normal subgroup of G.*

Proof. For any $g \in G, x \in \ker(f)$, we have that

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g) \cdot 1_H \cdot f(g)^{-1} = 1_H.$$

Thus $gxg^{-1} \in \ker(f)$ and we are done. □

Some examples of normal subgroups:

(1) Let G be an abelian group. Then any subgroup is normal. (Definition!)
(2) The alternating group A_n is normal in S_n. (Either use Proposition 9.5 directly, or use it to show that $e : S_n \to \{\pm 1\}$ given by $w \mapsto (-1)^{\ell(w)}$ is a group homomorphism.)
(3) Let G be any group (possibly infinite) and $H \leq G$ a subgroup of index 2, i.e. $|G : H| = 2$. Then H is normal in G.

    Proof. Let $x \notin G$. Since $G = H \cup xH = Hx \cup H$ (disjoint union) we have $xH = G \setminus H = Hx$. □

(4) $\mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$; (use the homomorphism det).

Theorem 11.1 (Cauchy's theorem for abelian groups)**.** *Let G be a finite abelian group and p a prime such that $p||G|$. Then G has an element of order p.*

Proof. We argue by induction on $|G| > 1$. The base case is clear. If $G =< x >$ is cyclic of order a such that $p|a$ then take $y := x^{a/p}$. Assume that G is not cyclic, and take $x \in G$ such that $x \neq 1$. Notice that $|x| < |G|$. If p divides the order of x we are done by induction. If p does not divide the order of x, then $< x >$ is normal in G and p divides the order of $G/ < x >$. By induction hypothesis there exists $y < x > \in G/ < x >$ of order p. This means that there exists $y \in G$ such that $y \notin < x >$ but $y^p \in < x >$. In particular, $< y^p > \subset < x >$ which implies that $< y^p > \neq < y >$. (Otherwise y would be in $< x >$.) Let k be the order of y. Then the order of y^p is

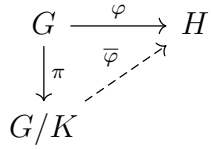
$$|y^p| = \frac{k}{gcd(p, k)}.$$

Since $< y^p > \neq < y >$ we must have that $gcd(p,k) \neq 1$, which forces $p|k$. Then by the induction hypothesis $< y >$ contains an element of order p. $\square$

11.1. **Exercises.**

12. Isomorphism Theorems

Lemma 12.1. *Let $\varphi : G \to H$ be a group homomorphism and let $K \trianglelefteq G$ be a normal subgroup such that $K \subset \ker(\varphi)$. Then there is a well defined group homomorphism $\overline{\varphi} : G/K \to H$ defined by $\overline{\varphi}(gK) = \varphi(g)$.*



Proof. We need to prove several things:

• **$\overline{\varphi}$ is well defined.** Take $g_1, g_2 \in G$ such that $g_1K = g_2K$. We need to show that $\varphi(g_1) = \varphi(g_2)$. By hypothesis $g_2 = g_1k$ where $k \in \ker(\varphi)$. Then

$$\varphi(g_2) = \varphi(g_1k) = \varphi(g_1)\varphi(k) = \varphi(g_1);$$

here the second equality follows since $k \in \ker(\varphi)$.

• **$\overline{\varphi}$ is a group homomorphism.** This follows because φ is a group homomorphism:

$$\overline{\varphi}(g_1K \circ g_2K) = \overline{\varphi}(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1K)\overline{\varphi}(g_2K).$$

The fact that $\overline{\varphi}(gK) = \varphi(g)$ follows from definition. □

Recall the following lemma (cf. Proposition 6.6 above):

Lemma 12.2. *Let $\varphi : G \to H$ be a group homomorphism. Then φ is injective if and only if* $\mathrm{Ker}(\varphi) = \{1\}$.

Theorem 12.1 (First Isomorphism Theorem)**.** *Let $\varphi : G \to H$ be a group homomorphism. Then*

$$G/\ker\varphi \simeq Im(\varphi).$$

Proof. By Lemma 12.1 we have an induced homomorphism $\overline{\varphi} : G/\ker(\varphi) \to H$, which in turn induces a homomorphism $\widetilde{\varphi} : G/\ker(\varphi) \to Im(\varphi)$ defined by

$$\widetilde{\varphi}(g\ker(\varphi)) = \varphi(g).$$

We check that this is an isomorphism.

To start, the definition of $\widetilde{\varphi}$ implies that it is surjective. To prove injectivity we calculate the kernel:

$$\ker\widetilde{\varphi} = \{g\ker(\varphi) : \varphi(g) = 1\} = \ker(\varphi) = 1_{G/\ker(\varphi)}.$$

Then the claim follows from Lemma 12.2. □

Theorem 12.2 (Third Isomorphism Theorem)**.** *Let G be a group and let $K, H \trianglelefteq G$ such that $H \subset K$. Then $K/H \trianglelefteq G/H$ and*

$$(G/H)/(K/H) \simeq G/K.$$

Proof. Consider the diagram

$$\begin{array}{ccc} G & \xrightarrow{\pi_K} & G/K \\ \downarrow{\scriptstyle \pi_H} & \nearrow{\scriptstyle \pi} & \\ G/H & & \end{array}$$

Since $H \subset \ker(\pi_K) = K$, Lemma 12.1 implies that there exists a group homomorphism

$$\pi : G/H \to G/K; \quad \pi(gH) = gK.$$

We apply the first isomorphism theorem 12.1 to π. By definition $Im(\pi) = G/K$. We calculate

$$\ker(\pi) = \{gH : \pi(gH) = 1.K\} = \{gH : gK = K\} = K/H.$$

This finishes the proof. □

12.1. **Examples.** We show several examples for the first isomorphism theorem.

(1) $(\mathbb{Z}/15\mathbb{Z})/(3\mathbb{Z}/15\mathbb{Z}) \simeq \mathbb{Z}/3\mathbb{Z}$. (Apply the third isomorphism theorem.)
(2) For any groups G, H, the quotient $(G\times H)/(1\times H) \simeq G$. (Consider the projection morphism $G \times H \to G$, defined by $(g, h) \mapsto g$.)
(3) $\mathbb{R}^7/\mathbb{R}^3 \simeq \mathbb{R}^4$ where $\mathbb{R}^4$ is a subgroup of $\mathbb{R}^7$ by $(x_1, x_2, x_3, x_4) \mapsto ((x_1, x_2, x_3, x_4, 0, 0, 0)$. (Use the projection from $\mathbb{R}^7$.)
(4) $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$. (Consider the determinant map $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$.)
(5) $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$. (consider the 'signature' map $\varepsilon : S_n \to \{\pm 1\}$, defined by $w \mapsto (-1)^{\ell(w)}$.
(6) $\mathbb{R}/\mathbb{Z} \simeq S^1 = \{z \in \mathbb{C} : |z| = 1\}$. Use the exponential map $f : \mathbb{R} \to S^1$, $x \mapsto e^{2\pi ix} = \cos(2\pi x) + i \sin(2\pi x)$. This map is surjective, and its kernel is $\mathbb{Z}$.
(7) If a, b are two relatively prime numbers, then $\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. (Use the projection $x \mapsto (x \mod a, x \mod b)$.)

Theorem 12.3 (The Correspondence Theorem)**.** *Let $H \trianglelefteq G$. Then there is a one-to-one correspondence between subgroups of G/H and subgroups of G containing H. The correspondence is given by*

$$K \mapsto K/H; \quad \overline{K} \mapsto \pi^{-1}(\overline{K}),$$

where $\pi : G \to G/H$ is the natural projection.

Further, the correspondence theorem preserves the index:

$$|G : K| = |G/H : K/H|.$$

Proof. Let $\mathcal{S}_1$ denote the set of all subgroups K such that $H \subset K \subset G$, and let $\mathcal{S}_2$ denote the set of subgroups of G/H. Define the map $\Phi : \mathcal{S}_1 \to \mathcal{S}_2$ by $K \mapsto K/H$. We need to show that Φ is a bijection.

We first show Φ is surjective. For that, let $\overline{K} \leq G/H$ be any subgroup. Define

$$K := \Phi^{-1}(\overline{K}) = \{g \in G : gH \in \overline{K}\}.$$

Then K is a subgroup of G containing H (homework !), and by definition $\Phi(K) = \overline{K}$.

We now show Φ is injective. Let $K_1, K_2 \in \mathcal{S}_1$ such that $K_1/H = K_2/H$. Let $x \in K_1$. Then $xH \in K_1/H = K_2/H$, meaning that $x = k_2 h$ for some $k_2 \in K_2$ and $h \in H$. But $H \subset K_2$, therefore

$$x = k_2 h \in K_2.$$

We conclude that $K_1 \subset K_2$. Similarly $K_2 \subset K_1$ and we are done.

It now remains to show the assertion about the index. We will construct a bijection $G/K \to (G/H)/(K/H)$. (Warning: K may not be normal, so G/K is *not* a group!) Define

$$f : G/K \to (G/H)/(K/H); \quad f(gK) = (gH)K/H.$$

This is a well defined map: if $g_1 K = g_2 K$, then $g_2 = g_1 k$ for some $k \in K$, thus

$$f(g_2 H) = (g_2 H)K/H = (g_1 H)(kH)K/H = (g_1 H)K/H = f(g_1 H).$$

The map f is surjective by definition. We now prove it is injective. Assume $f(g_1 H) = f(g_2 H)$. Then $(g_1 H)K/H = (g_2 H)K/H$, which means that $g_2 H = (g_1 H)(kH)$ for some $k \in K$. Using the multiplication in G/H, this means that $g_2 H = g_1 kH$, i.e. $g_2 = g_1 kh$ for some $h \in H$. But then $g_2 K = g_1 khK = g_1 K$, since $kh \in K$. □

Remark 12.1. *One can prove more directly the correspondence theorem by defining $\Psi : \mathcal{S}_2 \to \mathcal{S}_1$ by $\overline{K} \mapsto \pi^{-1}(K)$ and then showing that Φ and Ψ are inverse to each other.*

Remark 12.2. *One may also show that the correspondence theorem preserves normal groups, i.e.*

$$K \trianglelefteq G \iff K/H \trianglelefteq G/H.$$

Remark 12.3. *If all groups in the correspondence theorem are finite then*

$$|G/H : K/H| = \frac{|G/H|}{|K/H|} = \frac{|G|/|H|}{|K|/|H|} = \frac{|G|}{|K|} = |G : K|.$$

Example 12.1. *Describe subgroups of $\mathbb{Z}/15\mathbb{Z}$. In this case $G = \mathbb{Z}$ and $H = 15\mathbb{Z}$. We look for subgroups K such that $15\mathbb{Z} \subset K \subset \mathbb{Z}$. Since $\mathbb{Z}$ is cyclic, each such K is generated by an element $\overline{a}$ such that $a|15$. There are 4 such elements: $1, 3, 5, 15$. Then the correspondence is given by:*

$$\mathbb{Z} \leftrightarrow \mathbb{Z}/15\mathbb{Z}; \quad 3\mathbb{Z} \leftrightarrow 3\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/5\mathbb{Z};$$
$$5\mathbb{Z} \leftrightarrow 5\mathbb{Z}/15\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z}; \quad 15\mathbb{Z} \leftrightarrow 15\mathbb{Z}/15\mathbb{Z} \simeq \{id\}.$$

Example 12.2. *One can use the correspondence theorem to prove that in some cases there exist groups of a fixed index. For instance, if H is normal in G of index 4, then G/H is a group of order 4. Then G/H is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In particular, it has a subgroup of index 2, implying that G also has a subgroup K of index 2. Such a group is automatically normal.*

Where is the *second* isomorphism theorem ?

Theorem 12.4 (Second Isomorphism Theorem)**.** *Let G be a group and $A, B \leq G$. Assume that $A \leq N_G(B)$. Then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$ and*

$$AB/B \simeq A/A \cap B.$$

Sketch of the proof. The hypothesis on A implies that AB is a subgroup of G. To prove that $B \trianglelefteq AB$ take $a \in A$, and $b, x \in B$. Then

$$(ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} \in B$$

because $A \leq N_G(B)$. Same idea shows that $A \cap B \trianglelefteq A$.

To prove the claimed isomorphism we will apply the 1st isomorphism theorem to the map $\varphi : A \to AB/B$ by $\varphi(a) = aB$. Notice that this is given by the sequence of homomorphisms

$$A \hookrightarrow AB \mapsto AB/B,$$

therefore the composition must be again a homomorphism. We have

$$\ker \varphi = \{a \in A : aB = B\} = \{a \in A : a \in B\} = A \cap B.$$

The map is clearly surjective. □

12.2. **Exercises.**

13. Rings

13.1. Definition and examples.

Definition 13.1. *A* **ring** $(R, +, \cdot)$ *is a set with two operations* $+$ *and* $\cdot$ *such that the following are satisfied:*

- $(R, +)$ *is an abelian group; the identity element is called* 0.
- *the operation* $\cdot$ *is associative and with multiplicative identity denoted by* 1.
- *the operation* $\cdot$ *is distributive with respect to* $+$*, meaning that* $a\cdot(b+c) = a\cdot b+a\cdot c$ *and* $(b + c) \cdot a = b \cdot a + c \cdot a$ *for any* a, b, c.

If in addition the operation $\cdot$ is commutative then R is called a *commutative ring*. A commutative ring where $(R \setminus 0, \cdot)$ is a group is called a *field*. A *subring* $(S, +, \cdot)$ of $(R, +, \cdot)$ is a subgroup $(S, +) \leq (R, +)$ such that the operation $\cdot$ is closed in S, i.e. for any $x, y \in S$, $x \cdot y \in S$. Unless we otherwise specify, if R has 1, then $1 \in S$.

If R, S are rings, a *ring homomorphism* is a map $\varphi : R \to S$ which is a homomorphism of abelian groups, and it is compatible with multiplication:

$$\varphi(a + b) = \varphi(a) + \varphi(b); \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

The *kernel* of a ring homomorphism is its kernel regarded as a group homomorphism:

$$\ker(\varphi) = \{x : \varphi(x) = 0\}.$$

Example 13.1. *Here are several important examples:*

- $R = (\mathbb{Z}, +, \cdot)$. *More generally,* $R = (\mathbb{Z}/n\mathbb{Z}, +\cdot)$.
- Polynomial rings in one variable. *If* R *is a commutative ring, then one can consider* $R[x]$*- polynomials with coefficients in* R *and in the variable* x. *The addition and multiplications are defined as for the usual polynomials.*
- Polynomial rings in several variables. *More generally, if* R *is a ring, one can consider* $R[x_1, \ldots, x_n]$ *- polynomials in* n*-variables with coefficients in* R. *Its elements are:*

$$R[x_1, \ldots, x_n] := \{\sum a_{i_1 \ldots i_n} x_1^{i_1} \cdot \ldots x_n^{i_n} : a_{i_1 \ldots i_n} \in R\}.$$

- Matrix rings. *Let* R *be a commutative ring, and* $M_n(R)$ *the set of* $n \times n$ *matrices with coefficients in* R. *Then one can add and multiply matrices in the usual way. The resulting structure is a ring, called a matrix ring. Note: Matrix rings are* not *commutative.*
- Fields*:* $\mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}$ *(p-prime), rational functions*

$$\mathbb{C}(x) := \{\frac{P(x)}{Q(x)} : P, Q \in \mathbb{C}[x], Q \neq 0\}.$$

Remark 13.1. *In these notes we assume that rings have multiplicative identity. However, there are examples where which we would like call rings, but have no identity. One such instance is vectors in* R^3*, with componentwise addition, and multiplication given by cross product.*

Lemma 13.1. *Let R be a ring and $a, b \in R$. Then the following hold:*

- $0 \cdot a = 0$;
- $(-1) \cdot a = -a$;
- $(-a) \cdot b = -(a \cdot b)$.

Proof. We have that $0 \cdot x = (0+0) \cdot x = 0 \cdot x + 0 \cdot x$; then apply the cancellation property in the additive group $(R, +)$. The result in (b) follows because

$$0 = (1-1) \cdot a = a + (-1 \cdot a).$$

The part (c) is holds because $(-a) \cdot b = (-1) \cdot (a \cdot b)$. □

13.2. **Ideals.**

Definition 13.2. *An* ideal *of a ring R is a subset $I \subset R$ such that $(I, +)$ is a subgroup of $(R, +)$ and for any $r \in R, x \in I$, both $rx, xr \in I$.*

It follows from definition that an ideal $I = R$ if and only if $1 \in I$.

Proposition 13.1. *Let R be a ring, and I an ideal of R. Then R/I is a ring with the induced operations:*

$$(a + I) + (b + I) = (a + b) + I; \quad (a + I) \cdot (b + I) = ab + I.$$

Proof. Since I is an ideal, it is in particular a normal subgroup of R. Therefore $(R/I, +)$ is a group. It remains to show that the multiplication $\cdot$ is independent of the choice of representatives; then the remaining part follows immediately. The details are left as homework. □

Definition 13.3. *Let S be a subset of R. The ideal generated by S, denoted by $\langle S \rangle$, consists of the finite combinations $\sum a_i s_i$ where $a_i \in R$ and $s_i \in S$. An ideal which can be generated by a single element is called* principal.

Example 13.2. *(a) $R = \mathbb{Z}$. The ideal $\langle 2 \rangle = 2\mathbb{Z}$; $\langle 2, 3 \rangle = \mathbb{Z}$.*

(b) Consider the polynomial ring $R[x]$. The ideal generated by $P(x)$ consists of all multiples of $P(x)$. For instance, $\langle x - 2 \rangle$ consists of all polynomials $P(x)$ such that $P(2) = 0$ (i.e. P has a root $x = 2$).

(c) The kernel of any ring homomorphism is an ideal.

13.3. **Ideals in univariate polynomial rings.** TODO. Goal: Show that for k a field, every ideal in $k[x]$ is principal. Discuss prime ideals in this context.

13.4. **Prime and maximal ideals.**

Definition 13.4. *Let I be an ideal of a ring R. We say that I is a* maximal ideal *if for any non-trivial ideal J such that $I \subset J$, we have that $J = I$.*

We say that I is a prime ideal *if for any $x, y \in R$ such that $xy \in I$, then either $x \in I$ or $y \in I$.*

Definition 13.5. *Let $(R, +\cdot)$ be a commutative ring. (a) We say that $x \in R$ is a* zero divisor *if $x \neq 0$ and there exists $y \neq 0$ such that $xy = 0$.*

(b) We say that R is an integral domain *if R has no zero divisors.*

Example 13.3. *In $\mathbb{Z}/4\mathbb{Z}$, the element $\overline{2}$ satisfies $\overline{2}^2 = \overline{0}$, therefore it is a zero divisor. More generally, if n is not a prime, then $\mathbb{Z}/n\mathbb{Z}$ has zero divisors. However, $\mathbb{Z}$ is an integral domain; any field is also an integral domain.*

Proposition 13.2. *Let R be a commutative ring. Then the following hold:*

(a) An ideal I is prime if and only if R/I is an integral domain.

(b) An ideal I is maximal if and only if R/I is field.

Proof. Since R is commutative, it follows that R/I is commutative. Assume that I is prime, and take $a, b \in R$ such that $(a + I) \cdot (b + I) = 0$ in R/I. Then $ab \in I$, and since I is prime, either $a \in I$ or $b \in I$; equivalently, either $a + I$ or $b + I$ equal to 0 in R/I. Conversely, assume that R/I is an integral domain, and take $a, b \in R$ such that $ab \in I$. Then $(a + I) \cdot (b + I) = 0$ in R/I, and as before it follows that either $a \in I$ or $b \in I$.

We now prove (b). Assume that I is maximal, and take any $x + I \in R/I$. We need to show that if $x + I \neq 0$, then $x + I$ is invertible. The hypothesis on x and I implies that the ideal generated by I and x must be the whole R. This means that there exists $r \in R$ such that $rx + a = 1$ for some $a \in I$. But then $(r + I) \cdot (x + I) = 1 + I$ in R/I, showing that $x + I$ is invertible. Conversely, assume that R/I is a field. If J is an ideal containing I, then J/I is an ideal of R/I. But since R/I is a field, it follows that either J/I is either the zero ideal, or the full ring R/I. In the first situation $J = I$, and in the second $J = R$, showing that I is maximal. □

Corollary 13.1. *Any maximal ideal is prime.*

Proof. Let I be the ideal in question. Then R/I is a field, which is a particular case of an integral domain. Thus I is also prime. □

Example 13.4. *(a) The ideal $\langle x - 2\rangle \subset \mathbb{R}[x]$ is maximal; the same ideal is only prime in $\mathbb{Z}[x]$; for instance $\langle 2, x - 2\rangle$ is a maximal ideal. This follows because one can define a homomorphism $\varphi : \mathbb{R}[x] \to \mathbb{R}$ sending $P(x) \mapsto P(2)$. The kernel of this ring homomorphism is $\langle x - 2\rangle$. Using this, we obtain ring isomorphisms:*

$$\mathbb{R}[x]/\langle x - 2\rangle \simeq \mathbb{R}; \quad \mathbb{Z}[x]/\langle x - 2\rangle \simeq \mathbb{Z}.$$

The ideal $\langle x\rangle \subset \mathbb{C}[x, y]$ is prime, but not maximal.

13.5. **Exercises.**