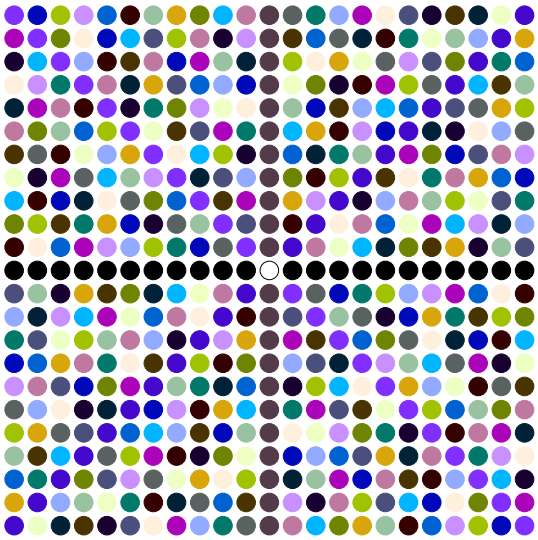
Algebra



Projective plane of the finite field $\mathbb{F}_{23}$ (see Exercice TODO*).*

Rémi Géraud, 2017–2018

Introduction

Note: this is work in progress
Last compilation: 28th October 2017

This course is intended as an algebraic survival kit. Algebra is a rich, modern, and fascinating discipline; it has a reputation of being abstract, difficult. In some respects this is true.

It also has a reputation of being devoid of applications, being a mere exercise for the mind, an aesthetic pleasure and certainly not a basic engineering skill. And this is certainly not the case.

Therefore the technologically able person will necessarily face, sooner or later, the need to understand at least some algebra — be it to understand a communication device's resilience to noise, to protect a file using encryption, to work out the properties of some complicated geometric object, or simply to explore the wonderful developments of 20th and 21st century mathematics.

While certainly not complete or perfect, the aim of this booklet is to introduce the main concepts, tools, and techniques of algebra, hinting at more advanced topics as well as applications.

We expect the reader to have basic knowledge of numbers, integer and rational, of polynomials, and of Euclid's algorithm for the greatest common divisor. A familiarity with common proof techniques, such as proof by contradiction or by enumeration is advisable. The results proven in this book should hopefully help the readers to convince themselves, as well as acquire a few tricks of the trade; accordingly we avoid some very efficient, but equally obscure, shortcuts.

The course will be thematic, pointing at mountains (Galois, categories, ...) but following a gentle path. Exercises and problem sets provide additional elements. We certainly hope that the reader, equipped with this modest survival guide, with interest, patience, and determination, will find the path through these advanced topics easier.

Calendar (approximative)

1. Mathematical background
   a) Prime numbers, Groups, Rings, Ideals, Spectrum of $\mathbb{Z}$
   b) Quotients, Polynomials, Spectrum of $\mathbb{Z}[X]$
   c) Finite fields, Quadratic residues, Legendre–Jacobi symbol, Quadratic reciprocity
   d) (Proof of the LQR)
2. Algorithmics in finite fields
   a) Euclidean algorithm, CRT, Exponentiation, Square roots
   b) Representation of finite fields, Irreducibility tests
   c) Primality tests, Smoothness
3. Applications
   a) Cryptography 1: DH key exchange, FS identification
   b) Cryptography 2: AJPS or NTRU encryption, RSA signatures
   c) Error-correcting codes: Hamming, BCH, Reed–Solomon

Note: When proofs are not given, it is usually because the reader is expected to be able to fill in the gaps. There will be very few exceptions to this rule, and they will always be explicitly indicated. Checking the provided examples is a good exercise.

Contents

Part I

Mathematical background

Chapter 1

Integers

In this chapter we set the bases of arithmetics with integers; we shall assume a familiarity with elementary operations and build upon this knowledge. The set of non-negative integers $0, 1, 2, \dots$ is denoted $\mathbb{N}$, and it is equipped with an "addition" operation, a "multiplication" operation, and a total order.

Fact 1 *Every non-empty subset of $\mathbb{N}$ has a smallest element.*

The set of integers $\dots, -1, 0, 1, \dots$ is denoted by $\mathbb{Z}$.

1.1 Integers and divisibility

Theorem 1 (Euclid) *Let $a, b \in \mathbb{Z}$, with $b \neq 0$. There exists a unique couple $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ such that*

$$a = bq + r \qquad \text{and} \qquad 0 \leq r < |b|$$

where $|b| = \max(-b, b)$.

Definition 1 (Divisibility) If $a, b \in \mathbb{Z}$, we say that "a divides b" (and we write $a|b$) if there exists $q \in \mathbb{Z}$ such that $aq = b$.

We may equivalently say:

- b is a multiple of a;
- a is a divisor of b;
- the remainder r of the Euclidean division of b by a is zero;
- $b \in a\mathbb{Z} = \{\dots, -2a, -a, 0, a, 2a, \dots\}$;
- etc.

Definition 2 (Prime number) A number p whose only divisors are ± 1 and $\pm p$ is called a prime number.

Theorem 2 (Euclid) *The set $\mathfrak{P} = \{2, 3, 5, \dots\}$ of prime numbers is infinitely large.*

Problem 1 *Given an integer $n \in \mathbb{Z}$, how to effectively decide whether $n \in \mathfrak{P}$?*

Definition 3 (Unit) The invertible elements of $\mathbb{Z}$, i.e., -1 and 1, are called units.

Definition 4 (Composite number) A number that is neither a unit nor a prime is called composite.

Theorem 3 (Euclid) *Every integer $n \in \mathbb{Z}$, $n \neq 0$, decomposes uniquely as*

$$n = up_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

where u is a unit, $p_1 < \cdots < p_r$ are prime numbers, and $n_1, \dots, n_r > 0$ are integers.

Problem 2 *Given $\mathbb{N}$, how to effectively find a divisor of n? A decomposition of n into its prime factors?*

Theorem 4 (Euclid) *Let $a, b \in \mathbb{Z}$ and $p \in \mathfrak{P}$. If $p|ab$ then $p|a$ or $p|b$.*

Proof: Assume $p \nmid a$, then define $A = \{n \geq 1 \text{ s.t. } p|an\}$. In particular $p \in A$ (and also $b \in A$) so that A is not empty, and $A \subset \mathbb{N}$, so by Fact 1 A has a smallest element; let this element be denoted by m. Since $p \nmid a$, $m > 1$.

Let $n \in A$, using Theorem 1 there exist integers q, r such that $n = mq + r$ with $0 \leq r < m$. Multiplying both sides by a, we have

$$(an) - (am)q = ar$$

whence $p|ar$ (indeed, $n \in A$ and $m \in A$). Since $r < m$, and m is by hypothesis the smallest element in A, $r \notin A$; therefore $r = 0$, which means that $m|n$.

As $p, b \in A$, the above applies to them in particular, i.e., $m|p$ and $m|b$. Since p is prime, and $m > 1$, the first equation gives $m = p$; therefore $p|b$. □

Corollary 1 (Largest prime factor) *Let $n \in \mathbb{N}$, $n \geq 2$. If $n \notin \mathfrak{P}$, then there exists $p \in \mathfrak{P}$ such that $p|n$ and $p^2 \leq n$.*

Algorithm 1 (Trial division algorithm) *There exists an algorithm that takes an integer $n > 2$ as input, and finds whether n is prime or composite (in which case it outputs a divisor of n) by performing at most $\sqrt{n}$ trial divisions.*

1.2 Greatest common divisor and p-adic valuation

Let $\overline{\mathbb{N}} = \mathbb{N} \cup \{+\infty\}$, where the order and operations on $\mathbb{N}$ are extended to work with the symbol $+\infty$ as follows: for all $n \in \mathbb{N}$, $+\infty \geq n$, $(+\infty) + n = n + (+\infty) = +\infty$, and $(+\infty) + (+\infty) = +\infty$.[1]

Definition 5 (p-adic valuation) Let $p \in \mathfrak{P}$. The p-adic valuation $v_p : \mathbb{Z} \to \overline{\mathbb{N}}$ is the map defined as follows:

- $v_p(0) = +\infty$
- $v_p(1) = 0$
- For all $n \geq 1$, $v_p(-n) = v_p(n)$
- For all $n \geq 2$, $v_p(n)$ is the exponent of p in the decomposition of n in prime factors.

Example 1 Let $n = 539000 = 2^3 \cdot 5^3 \cdot 7^2 \cdot 11$. Then

$$v_2(n) = 3, v_3(n) = 0, v_5(n) = 3, v_7(n) = 2, v_{11}(n) = 1, v_{13}(n) = v_{17}(n) = \cdots = 0.$$

Theorem 5 (Prime decomposition in $\mathbb{Z}$) *Every $n \in \mathbb{Z}$, $n \neq 0$, can be uniquely written as*

$$n = \epsilon \prod_{p \in \mathfrak{P}} p^{v_p(n)},$$

where ϵ is a unit. In particular, $v_p(n) \geq 1 \Leftrightarrow p|n$, and $a|b \Leftrightarrow v_p(a) \leq v_p(b)$ for all $p \in \mathfrak{P}$.

Proposition 1 (Properties of p-adic valuation) *Let $a, b \in \mathbb{Z}$, and $p \in \mathfrak{P}$. The following are easy properties of the p-adic valuation:*

- $v_p(ab) = v_p(a) + v_p(b)$
- $v_p(a + b) \geq \min(v_p(a), v_p(b))$ *(equality if $v_p(a) \neq v_p(b)$)*
- $a|b \Leftrightarrow \forall p \in \mathfrak{P}, v_p(a) \leq v_p(b)$.

Remark 1 The p-adic valuation allows one to construct the p-adic absolute value on $\mathbb{Q}$ as $|p/q|_p = p^{v_p(q) - v_p(p)}$. These norms have surprising properties (they are, in particular, ultrametric), and the completion of $\mathbb{Q}$ with $|\cdot|_p$ instead of the usual absolute value $|\cdot|$ gives the field of p-adic numbers $\mathbb{Q}_p$ instead of the field of real numbers $\mathbb{R}$. (We shall not say more at this point, as we have not introduced formally the notion of fields yet).

Theorem 6 (Gauss) *Let $a, b, c \in \mathbb{Z}$ such that a and b are coprime, and $a|bc$. Then $a|c$.*

[1] Note that multiplication by $+\infty$ is not defined.

Proof: Let $p \in \mathfrak{P}$, it suffices to show that $v_p(a) \leq v_p(c)$. If $v_p(a) = 0$ this is immediate; let's therefore assume $v_p(a) > 0$, i.e., $p|a$. Since a and b are coprime, we have $v_p(b) = 0$. Finally, we know that $a|bc$ i.e. $v_p(a) \leq v_p(bc) = v_p(b) + v_p(c) = v_p(c)$. □

Definition 6 (Greatest common divisor) Let $a, b \in \mathbb{N}$, $a, b, > 0$. The set $C = \{q \in \mathbb{N} \text{ s.t. } q|a \text{ and } q|b\} \subset \mathbb{N}$ is finite (by Corollary 1), therefore it has a greatest element; this element is called the greatest common divisor of a and b and denoted $\gcd(a, b)$. Equivalently,

$$\gcd(a, b) = \prod_{p \in \mathfrak{P}} p^{\min(v_p(a), v_p(b))}.$$

Definition 7 (Coprime integers) Let $a, b \in \mathbb{Z}$. We say that a and b are coprime when the following equivalent properties hold:

$$\gcd(a, b) = 1 \quad \Leftrightarrow \quad \forall p \in \mathfrak{P}, p \nmid a \text{ or } p \nmid b \quad \Leftrightarrow \quad \forall p \in \mathfrak{P}, \min(v_p(a), v_p(b)) = 0.$$

Lemma 1 *Let $a, b \in \mathbb{Z}$, $a, b \neq 0$, and $d = \gcd(a, b)$. Then $\gcd(a/d, b/d) = 1$.*

Lemma 2 *Let $a, b, c \in \mathbb{Z}$. If $\gcd(a, b) = 1$, $a|c$, and $b|c$, then $ab|c$.*

Theorem 7 (Bézout) *Let $a, b \in \mathbb{Z}$. There exists $u, v \in \mathbb{Z}$ such that $\gcd(a, b) = au + bv$.*

Proof: Let $A = \{au + bv \text{ s.t. } u, v \in \mathbb{Z}\} \cap (\mathbb{N} - \{0\})$. This is a non-empty subset of $\mathbb{N}$, therefore by Fact 1 it has a smallest element that we denote c.

By definition, $c \in A$. For every integer $k \geq 1$, $ck \in A$ as well. Let's show that these are in fact *all* the elements of A: let $n \in A$, by Theorem 1 there exist $q, r \in \mathbb{Z}$ such that $n = cq + r$, with $0 \leq r < c$. Assuming $r \neq 0$, we have $r = n - cq \geq 1$; now since $c, n \in A$, $r = n - cq$ also belongs to A. But $r < c$ and c is by definition the smallest element of A, which leads to a contradiction: therefore, $r = 0$. As a consequence, $n = cq$, i.e., $A = \{ck \mid k \geq 1\}$.

If $ab \neq 0$, $|a| \in A$ and $|b| \in A$. By the above paragraph, this implies $c|a$ and $b|a$. Thus $c|\gcd(a, b)$ and since c is the smallest such number, $c = \gcd(a, b)$. At the same time, $c \in A$ means that there exists $u, v \in \mathbb{Z}$ such that $c = au + bv$. The remaining case $ab = 0$ is immediate. □

Corollary 2 (Bachet–Bézout theorem) *Let $a, b \in \mathbb{Z}$. Then a and b are coprime if and only if there exist integers u, v such that $1 = au + bv$.*

Algorithm 2 (Euclidean algorithm) *Let $a, b \in \mathbb{Z}$, $a \geq b$. The following algorithm computes $\gcd(a, b)$:*

1. *Let* $r_0 = a$, $r_1 = b$
2. *For* $i \geq 1$, *if* $r_i \neq 0$, *let* r_{i+1} *be the remainder of the Euclidean division of* r_{i-1} *by* r_i.
3. *For* $n \geq 1$, *if* $r_n = 0$, *the algorithm terminates and outputs* $(r_0, \ldots, r_n)$.

In particular, $r_n = \gcd(a, b)$.

Algorithm 3 (Extended Euclidean algorithm) *Let* $a, b \in \mathbb{Z}$, $a \geq b$. *Algorithm 2 can be extended to compute the integers* u, v *appearing in Theorem 7 (and therefore, also the gcd):*

1. *Let* $u_0 = v_0 = 0$ *and* $u_1 = v_1 = 1$
2. *For* $i \geq 1$, *let* q_i *be the quotient of the Euclidean division of* r_{i-1} *by* r_i. *Let*

$$u_{i+1} = u_{i-1} - u_i q_i \qquad \text{and} \qquad v_{i+1} = v_{i-1} - v_i q_i$$

Then $r_n = au_n + bv_n$.

Remark 2 The complexity of this algorithm can be estimated roughly using an easy result of Lamé: if Algorithm 3 terminates in n steps, then $a \geq \gcd(a, b)F_{n+2}$ and $b \geq \gcd(a, b)F_{n+1}$, where (F_k) is the Fibonacci sequence defined by

$$F_0 = 0, \qquad F_1 = 1, \qquad \forall n \geq 1, F_{n+1} = F_n + F_{n-1}.$$

The worst-case scenario consists of couples of the form $(a, b) = (F_{n+1}, F_n)$.

1.3 Base b numeration

Theorem 8 (Base change) *Let* $a \in \mathbb{Z}$ *and* $b \in \mathbb{N}$, $b \geq 2$, *then* a *can be written uniquely as*

$$a = \pm \sum_{k=0}^{A} b^k a_k,$$

where A *is the largest integer such that* $a_A \neq 0$. *The sequence* $(a_A, \ldots, a_0)$ *is called the base* b *representation of* a, *and* A *is called the* b*-ary length of* a.

Algorithm 4 (Integer exponentiation) *Let* $x \in \mathbb{Z}$ *and* $n \in \mathbb{N}$. *The naive computation of* x^n *performs* $n - 1$ *multiplications; the following natural algorithm improves this by leveraging the binary (2-ary) representation of* n.

Write $n = 2^{i_0} + 2^{i_1} + \cdots + 2^{i_k}$, *with* $i_0 < i_1 < \cdots < i_k$, *and note that*

$$x^n = x^{\sum_{\ell=0}^{k} 2^{i_\ell}} = \prod_{\ell=0}^{k} x^{2^{i_\ell}}.$$

Now computing $x^{2^{i_\ell}}$ can be done in i_ℓ squarings; and furthermore doing so provides $x^{2^{i_m}}$ for all $m < \ell$. As a result, to compute x^n we only perform $i_k + k$ multiplications.

Since $2^{i_k} \leq n$, i.e., $i_k \leq N$ where N is the binary length of n, and $k \leq i_k$, the total number of multiplications performed is bounded by $2N = 2\log_2(n)$.

1.4 Exercice set

Exercise 1. Prove Theorems 1 to 3.

Exercise 2. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $a, n \neq 0$. Prove that $(a-1)|(a^n-1)$.

Exercise 3. Find all $n \in \mathbb{N}$ such that $(n+1)|(n^2+1)$.

Exercise 4. Prove Corollary 1. Hint: use Theorem 4.

Exercise 5.

1. Show that if $2^n - 1 \in \mathfrak{P}$ then $n \in \mathfrak{P}$. (Such numbers are called Mersenne primes).

   Open question (2018): Are there infinitely many Mersenne primes?

   Show that $2^{11} - 1 \notin \mathfrak{P}$.

   Open question (2018): Are there infinitely many Mersenne non-primes?

2. Show that if $2^n + 1 \in \mathfrak{P}$, then n is a power of 2. (Such numbers are called Fermat primes).

   Open question (2018): Only 5 Fermat prime are known (3, 5, 7, 257, and 65537). Are there more? Are there infinitely many Fermat primes?

   Let $n = 2^{32} + 1$, we are going to show that $641|p$ (this result is originally due to Euler). Let $p = 641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$. Show that there exists $k \in \mathbb{Z}$ such that $(p-1)^4 = 1 + kp$ and conclude.

Exercise 6. Show that $1 + 2 + 2^2 + 2^3 + \cdots + 2^{26} \notin \mathfrak{P}$.

Exercise 7. Let $a, b \in \mathbb{Z}$. Show that $\prod_{p \in \mathfrak{P}} p^{\max(v_p(a), v_p(b))}$ is the least common multiple (lcm) of a and b.

Exercise 8. Let $p, q \in \mathfrak{P}$, $p \neq q$. Show that $pq \mid \left(p^{q-1} + q^{p-1} - 1\right)$.

Exercise 9. Let $a, b, c \in \mathbb{Z}$. Show that $\gcd\left(\gcd(a,b), c\right) = \gcd\left(a, \gcd(b,c)\right)$.

Exercise 10. Let $a, b \in \mathbb{Z}$, $a \geq 2$, $b \geq 1$, show that

$$\gcd\left(\frac{a^b - 1}{a-1}, a - 1\right) = \gcd(a-1, b).$$

Exercise 11. Write 42 in bases 2, 3, 4, 8, and 16.

Exercise 12. Let $(a_A, \ldots, a_0)$ be the base-10 representation of $a \in \mathbb{N}$. Show that $11|a$ if and only if

$$\sum_{k=0}^{A} (-1)^k a_k = 0.$$

Exercise 13. Write a computer program that implements Algorithms 2 to 4.

Exercise 14. Let $d : \mathbb{Z} \to \mathbb{Z}$ be the operation defined as follows:

1. $d(p) = 1$ for all $p \in \mathfrak{P}$;
2. $d(ab) = d(a)b + ad(b)$ for any $a, b \in \mathbb{Z}$;
3. $d(-a) = -d(a)$ for any $a \in \mathbb{Z}$.

This operation is called the arithmetic derivative.

1. Prove that $d(0) = d(1) = 0$.
2. Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, show that $d\left(a^n\right) = na^{n-1}d(a)$.
3. Show that $d(a) = 0$ if and only if $a \in \{0, 1\}$.
4. Let $a \in \mathbb{Z}$, show that
$$d(a) = \sum_{i=1}^{k} \frac{e_i}{p_i} a,$$
where $a = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorisation of a.
5. Write a program that computes the arithmetic derivative of an integer, and compute the derivatives of $a = 0, 1, 2, \ldots, 100$. This sequence begins with $0, 0, 1, 1, 4, 1, 5, \ldots$
6. Show that for any $a, b \in \mathbb{Z}$, $b \neq 0$,
$$d\left(\frac{a}{b}\right) = \frac{d(a)b - ad(b)}{b^2}.$$
7. Show that the logarithmetic derivative, defined by $L : a \mapsto d(a)/a$ is a totally additive function, i.e., for any $a, b \in \mathbb{Z}$, $a, b \notin \{0, 1\}$, $L(ab) = L(a) + L(b)$.

   Open question (2018): Let $D = d(\mathbb{Z})$ be the set of integers obtained by arithmetic derivation. Is there an even number $k \notin D$? This would disprove Goldbach's conjecture: *'Every even integer greated than 2 can be expressed as the sum of two primes'*.

   Open question (2018): Let $B = \{a \in \mathbb{Z} \mid d(d(a)) = 1\}$. Is B finite? This would disprove the twin prime conjecture: *'There are infinitely many twin primes, i.e., pairs of primes (p, q) s.t. $|p - q| = 2$'*.

Exercise 15. The product of prime numbers $p_1 = 2, \ldots, p_k$ is known as the k-th primorial, and is denoted $\#P_n$.

1. Write a program to compute $\#P_n$ for small values of n. The first values are $2, 6, 30, 210, 2310, \ldots$
2. Show that for all $n \leq p_n$, $\gcd(n, \#P_n + 1) = 1$. Deduce from this a constructive proof of the infinitude of prime numbers.
3. Show that $2^n \leq \#P_n \leq p_n^n$. We will later see that a consequence of the prime number theorem gives $p_n \approx n \ln n$. Compute a lower and an upper bound for $\#P_{75}$. In fact, $\#P_{75} \approx 2^{512}$.
4. The n-th fortunate number is the smallest positive integer f_n such that $\#P_n + f_n$ is prime. For instance, $\#P_7 = 2 \cdot 3 \cdot \cdots \cdot 17 = 510510$, and $f_7 = 19$ since 510529 is the first prime immediately after $\#P_7$.
5. Show that $f_n > p_n$, and in fact that if $d | f_n$, then $d > p_n$.
6. Write a program that computes f_n for small values of n. The first values are $3, 5, 7, 13, 23, 17, 19, 23, 37, \ldots$

   Open question (2018): Is there any f_n that is not prime?

Exercice 16. The goal of this exercise is to show that $\sqrt{3} \notin \mathbb{Q}$ in two different ways.

1. Assume that $\sqrt{3} \in \mathbb{Q}$, and show that this implies a solution to the equation $3a^2 = b^2$ with non-zero integers a, b. Show such an equation has no solution by computing $v_3 \bmod 2$ on each side. (This is essentially Euclid's method).
2. Let E be the set
$$E = \left\{ b \in \mathbb{N} - \{0\} \mid \exists a \in \mathbb{N}, \sqrt{3} = \frac{a}{b} \right\}.$$
   a) Show that if $\sqrt{3} = a/b$, then $\sqrt{3} = a'/b'$ with
$$a' = 3b - a$$
$$b' = a - b$$
   b) Show that $a' > 0$ and $b' < b$
   c) Show that $b' > 0$ and $a' < a$
   d) Assuming that E is not empty, it has a smallest element b_0. Using the above three points, derive a contradiction.

   (This is essentially Fermat's method)

Chapter 2

Groups

The notion of group is ubiquitous, as it captures a very common structure in mathematics. We will immediately restrict our attention to some specific groups in the remainder of this course.

2.1 Basic definitions

Definition 8 (Group) A non-empty set G together with an operation $G \times G \to G$, $(x, y) \mapsto x \cdot y$, and such that

- $\forall x, y, z \in G, (x \cdot y) \cdot z = x \cdot (y \cdot z)$ (Associativity)
- $\exists e \in G, \forall x \in G, e \cdot x = x \cdot e = x$ (Existence of a neutral element)
- $\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e$ (Existence of all inverses)

is called a group. If furthermore, for all $x, y \in G$, $x \cdot y = y \cdot x$, then G is said to be a commutative or Abelian group.

Remark 3 In the above definition, we use the "multiplicative" notation for group composition. The inverse of an element $x \in G$ is usually denoted x^{-1}. Exponentiation by a positive integer n is denoted $x^n = x \cdot x \cdot \cdots \cdot x$, and extended with $x^0 = e$ and $x^{-n} = (x^{-1})^n$.

An alternative is the "additive" notation, where composition of x and y is written $x + y$, and the inverse of x is denoted $-x$. Exponentiation by a positive integer n is denoted nx or $[n]x = x + x + \cdots + x$ ($n > 0$ terms), and extended with $0x = e$ and $[-n]x = -[n]x$.

Definition 9 (Group morphism) Let G and H be groups. An application $f : G \to H$ is a group morphism if f preserves the group structure, i.e.,

- $f(e_G) = e_H$;

- $\forall x \in G, f(x)^{-1} = f\left(x^{-1}\right)$;
- $\forall x, y \in G, f(xy) = f(x)f(y)$.

Remark 4 The collection of groups, together with group morphisms, constitutes the category of groups, Grp. Similarly one can define the category of Abelian groups.

Definition 10 (Order) If G is finite, its order is the number of its elements (its cardinal).

Example 2

- The trivial group $0 = \{e\}$, with composition law $e \cdot e = e$. This is the smallest of all groups.[1] Its order is 1.
- The set $\mathbb{Z}$ (resp. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) with composition law the usual addition, with neutral element 0, is an Abelian group called the additive group of integers (resp. rational, real, complex numbers). It has infinite order.
- The set $\mathbb{N}$, endowed with the usual addition law, is not a group: indeed, not all element have inverses.
- The set $\mathbb{Z}$, endowed with the special composition law $(x, y) \mapsto x - y$ is not a group: indeed, $x - (y - z) \neq (x - y) - z$.
- The set $\mathbb{Q}^*$ (resp. $\mathbb{R}^*$, $\mathbb{C}^*$) obtained by removing 0 from $\mathbb{Q}$ (resp. etc.), with composition law the usual multiplication and neutral element 1, is an Abelian group called the multiplicative group of rationals (resp. etc.). It has infinite order.
- The set $\mathbb{Z}^*$ does not form a multiplicative group, since some non-zero integers do not have an integer inverse.
- Let X be a set, and $S = \mathrm{Aut}(X)$ the set of all permutations (i.e., reorderings) of X. Then S, along with the composition law of functions, and the identity application for neutral element, is a group called the symmetric group of X and usually denoted $\mathfrak{S}_X$. If $|X| = n$, then $\mathfrak{S}_X$ is of order $n!$; for $n \geq 3$, $\mathfrak{S}_X$ is non-Abelian.
- The set of invertible $n \times n$ matrices, together with the operation of matrix multiplication and matrix inverse, for a group called the general linear group of degree n, denoted GL_n.

Definition 11 (Direct product) Let $G_1, \ldots, G_n$ be groups. The direct product $G = G_1 \times \cdots \times G_n$ is a group, whose elements are of the form $x = (x_1, \ldots, x_n)$ with $x_i \in G_i$, the composition law is the element-wise application of each G_i's law, i.e.,

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$$

[1] There is no "set of all groups"; but 0 is the initial and terminal object in the category of groups, which gives a precise and rigorous sense to the notion that it is "smallest".

and the neutral element is $e = (e_1, \ldots, e_n)$ where e_i is G_i's neutral element. The inverse of $x = (x_1, \ldots, x_n)$ is $x^{-1} = (x_1^{-1}, \ldots, x_n^{-1})$.

Remark 5 For Abelian groups, this notion is also called the direct sum $G_1 \oplus \cdots \oplus G_n$.

2.2 Subgroups

Definition 12 (Subgroup) Let $(G, \cdot, e)$ be a group and $H \subset G$, such that

- $e \in H$; (Existence of the neutral element)
- $\forall x, y \in H, xy \in H$; (Stability under multiplication)
- $\forall x \in H, x^{-1} \in H$; (Stability under inversion)

then H is said to be a subgroup of G, and we write $H \leq G$. Equivalently, H is a subgroup of G if and only if H is non-empty and for all $x, y \in H$, $xy^{-1} \in H$.

Example 3

- Let G be a group. Then G and $0 = \{e\}$ are subgroups of G. 0 is called the trivial subgroup of G. If $H \leq G$ and $H \neq \{e\}, G$ then H is called a proper subgroup of G.
- Let G be a group and $x \in G$. Then $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$ (the group generated by x) is an Abelian subgroup of G. The order of $x \in G$ is by definition the order of the subgroup it generates.
- A particularly important class of groups are the groups $\langle x \rangle$ (generated by a single element x) that are finite. These are called cyclic groups.
- $\{q \in \mathbb{Q}^* \text{ s.t. } q > 0\}$ is a subgroup of $\mathbb{Q}^*$.
- $\mu_2(\mathbb{Q}^*) = \{\pm 1\}$ is a subgroup of $\mathbb{Q}^*$.
- Let $f : G \to H$ be a group morphism, and define $\ker f = \{g \in G \text{ s.t. } f(g) = e_H\}$ the kernel of f. Then $\ker f$ is a subgroup of G, and $\ker f = 0 = \{e\}$ if and only if f is injective.
- Let $n \in \mathbb{Z}$, then $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.
- The derived group (or commutator group) G' (or $[G, G]$) is the subgroup of G generated by all commutators (elements of the form $[g, h] = g^{-1}h^{-1}gh$ where $g, h \in G$). A perfect group is a group G such that $G = G'$.

Proposition 2 (Unions and intersections of subgroups) *Let G be a group, and $(H_i)_{i \in I}$ be a family of subgroups of G.*

- *$\bigcap_{i \in I} H_i$ is a subgroup of G;*

- *$H_i \cup H_j$ is a subgroup of G if and only if ($H_i \subset H_j$ or $H_j \subset H_i$).*

Corollary 3 *Let $a, b \in \mathbb{Z}$, $a, b \neq 0$, then $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{lcm}(a, b)\mathbb{Z}$.*

Amongst subgroups, some are particularly interesting:

Definition 13 (Normal subgroup) A subgroup N of a group G is called a normal subgroup[2] if it is invariant under conjugation, i.e., for all $n \in N$ and all $g \in G$, $gng^{-1} \in N$. When that is the case, we write $N \triangleleft G$.

Example 4

- Let G be a group, then $G \triangleleft G$ and $0 = \{e\} \triangleleft G$. A group that has no other normal subgroups is called a simple group.[3]
- The center of G is defined as $Z(G) = \{z \in G \mid \forall g \in G, zg = gz\}$; it is a normal subgroup of G: $Z(G) \triangleleft G$. A group G is Abelian if and only if $Z(G) = G$.
- The derived group is a normal subgroup.
- If G is an abelian group and $H \leq G$, then $H \triangleleft G$.

2.3 Group quotients

Lemma 3 *Let G be a group and $H \leq G$. The relation*

$$x \sim_H y \qquad \Leftrightarrow \qquad x - y \in H$$

is an equivalence relation.

Definition 14 (Quotient group) Let G be a group, and $H \triangleleft G$. The set of equivalence classes under $\sim_H$ is denoted G/H and called the quotient group of G by H. (Informally, we may say "G mod H".)

Remark 6 One way to think about G/H is to consider elements of H as "neutral", i.e., we remain in the same equivalence class by multiplying or dividing by elements of H (resp., in additive notation, adding or subtracting).

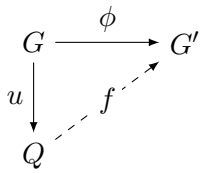
Remark 7 The requirement that $H \triangleleft G$ (and not just $H \leq G$) makes G/H a group, and not merely a set. Indeed, the group law is compatible with this quotient. The reader will easily check that H being normal is equivalent to the group law being compatible with the quotient.

[2] In the literature, they are sometimes also referred to as "invariant" or "distinguished" subgroups. Galois, who first stressed the importance of such subgroups, called them "propres".

[3] All finite simple groups have been classified; the proof was computer-assisted, and counts tens of thousands of pages, published in several hundred journal articles, written by about 100 authors, and written mostly between 1955 and 2004.

Theorem 9 (Universality) *Let G be a group and $H \triangleleft G$. The (categorical) quotient of G by H is a group Q, together with a morphism $u : G \to Q$ such that $\ker u = H$ which is universal in the following sense.*

If $\phi : G \to G'$ is any morphism such that $H \subset \ker \phi$, then there is a unique induced morphism f which makes the following diagram commute:



Definition 15 (Short exact sequence) A diagram of groups and morphisms

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is a short exact sequence if the following properties hold:

- f is injective;
- $\ker g = \operatorname{Im} f$;
- h is surjective.

This is equivalent to stating that $A \triangleleft B$, and $C \simeq B/A$.

Theorem 10 (First isomorphism theorem) *Let $f : G \to H$ be a group morphism. Then $\ker f \triangleleft G$, and $\operatorname{Im} f \simeq G/\ker f$. Conversely, if $N \triangleleft G$, the kernel of the quotient map $q : G \to G/N$ is N itself; therefore the normal subgroups are precisely the kernels of morphisms with domain G.*

Example 5

- $G/G \simeq 0$ and $G/\{e\} \simeq G$.
- $\mathbb{R}/\mathbb{Z}$ is isomorphic to the circle group $\mathbb{S}^1$.
- $\mathbb{R}^2/\mathbb{Z}^2$ is isomorphic to a torus. More generally, if $\vec{u}, \vec{v} \in \mathbb{R}^2$ are non-colinear, then $\Lambda = \{a\vec{u} + b\vec{v} \mid a, b \in \mathbb{Z}\}$ is an additive subgroup of $\mathbb{R}^2$, i.e., an Euclidean lattice, and $\mathbb{R}^2/\Lambda$ is a torus.
- The Abelianisation of G is the group $G^{\text{ab}} = G/G'$; it is an Abelian group. In particular, a group G is Abelian if and only if $G' \simeq 0$.[4]

[4] An important interpretation of G^{ab}, which is beyond the scope of this course, is as $H_1(G, \mathbb{Z})$: the first homology group of G with integral coefficients.

- Let X be a topological space, and $x \in X$. The set of loops $\gamma : [0,1] \to X$, $\gamma(0) = \gamma(1) = x$ can be endowed with a natural group structure; quotiented by the homotopy equivalence relationship ($\gamma \sim \eta \Leftrightarrow \gamma$ can be continuously deformed into η), this gives the first homotopy group $\pi_1(X)$. The Abelianised of $\pi_1(X)$, denoted $H_1(X)$, is called the first homology group. Both $\pi_1(X)$ and $H_1(X)$ are central objects of interest in algebraic topology.

Theorem 11 (Lagrange) *Let G be a finite group, and H a subgroup of G. We have $|G| = |H| \cdot |G/H|$, and in particular, the order of H divides the order of G.*

Proof: Let $x \in G$, let $xH = \{xh \mid h \in H\}$. The map $H \to xH$ defined by $h \mapsto xh$ is a bijection, therefore $H \simeq xH$. In other terms, all the equivalence classes have the same cardinal. Since G is the disjoint union of its equivalence classes, the result immediately follows. □

Corollary 4 *Let G be a finite group of prime order. Then the only subgroups of G are 0 and G.*

2.4 $\mathbb{Z}$ as a group

Lemma 4 *Let $n \in \mathbb{N}$, $n > 0$ then $(n) = n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.*

Theorem 12 (Subgroups of $\mathbb{Z}$) *Let $H \leq \mathbb{Z}$, then there exists $n \in \mathbb{Z}$ such that $H \simeq (n)$.*

Proof: The result is immediate if $H = \{0\} = 0$, by taking $n = 0$; therefore let's assume $H \neq 0$. Let $A = H \cap \{\mathbb{N} - \{0\}\}$, which is a non-empty subset of $\mathbb{N}$. By Fact 1 there is a smallest element in A that we denote by n.

Since H is a subgroup of $\mathbb{Z}$, and since $n \in H$, we have $(n) \subset H$.

Conversely, let $h \in H$, then there exists by Theorem 1 two integers $q, r \in \mathbb{Z}$ such that $h = nq + r$ with $0 \leq r < n$. As $n \in H$, so does $nq \in H$. Therefore $r = h - nq \in H$.

Assume $r > 0$, then $r \in H$ and $r < n$ lead to a contradiction, since by definition n is the smallest element of H. Therefore $r = 0$. As a consequence, $h = nq \in (n)$. □

Definition 16 (Integers modulo n) Let $n \in \mathbb{N}, n > 0$. The group $\mathbb{Z}/(n)$ (also occasionally denoted $\mathbb{Z}/n\mathbb{Z}$) is called the group of integers modulo n. The corresponding short exact sequence is

$$0 \to (n) \hookrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}/(n) \to 0$$

Remark 8 We may equivalently say the following:

- $x - y \in (n)$

- $x - y = 0$ in $\mathbb{Z}/(n)$
- $x \equiv y \bmod n$)
- $n|(x - y)$
- x and y are congruent modulo n
- etc.

Proposition 3 *Let $n \in \mathbb{N}$, $n > 0$. Then $\mathbb{Z}/(n)$ has order n, and*

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

where $\overline{x} = \{x + nk \mid k \in \mathbb{Z}\}$ is the equivalence class of x.

Proof: Let $a \in \mathbb{Z}$. There are by Theorem 1 integers $q, r \in \mathbb{Z}$ such that $a = nq + r$ with $0 \leq r < n$. Since $a - r \in (n)$, we have $\overline{a} = \overline{r}$.
Furthermore, for any distinct a, b in $\{0, 1, \ldots, n-1\}$, $n \nmid (a - b)$, i.e., $\overline{a} \neq \overline{b}$. □

Remark 9 A direct product of rings can be constructed, analogously to the direct product of groups.

Theorem 13 (Subgroups of $\mathbb{Z}/(n)$) *Let $n > 1$ and $H \leq \mathbb{Z}/(n)$. Then H has order $d|n$. Conversely, for every $d|n$, there is a unique subgroup of $\mathbb{Z}/(n)$ which has order d, and is isomorphic to $\mathbb{Z}/(d)$.*

Proof: The first statement is just Theorem 11. Let $G = \mathbb{Z}/(n)$ and assume $H \leq G$. Let $\psi : Z \to G$ be the canonical surjection (i.e., reduction mod n) and $\phi : \mathbb{Z} \to G \to G/H$. Then $\ker \phi \leq \mathbb{Z}$, therefore by Theorem 12 there exists $d \in \mathbb{Z}$ such that $\ker \phi \simeq (d)$. Then by Theorem 10 $H \simeq \mathbb{Z}/(d)$. Finally, $\ker \psi \leq \ker \phi$ so that $d|n$. □

Corollary 5 *Let $n \in \mathbb{Z}$, $n > 1$, and $k \in \mathbb{Z}/(n)$. The cyclic group generated by k can be generated by $\gcd(k, n)$, and it has order $n/\gcd(k, n)$.*

Proof: Since $\gcd(k, n)|k$ we have $(k) \subset \gcd(k, n)$. Conversely, write $uk + vn = \gcd(k, n)$: by Theorem 7 this has a solution $u, v \in \mathbb{Z}$, therefore $\gcd(k, n)$ belongs to the group generated by k modulo n. Hence, $\gcd(k, n) \subset (n)$. Finally, Theorem 13 gives the order as $n/\gcd(k, n)$. □

Corollary 6 *Let $n \in \mathbb{Z}$, $n > 1$, and $k \in \mathbb{Z}/(n)$. Then k generates all of $\mathbb{Z}/(n)$ if and only if $\gcd(k, n) = 1$.*

Theorem 14 (Chinese remainder theorem) *Let $m, n \in \mathbb{Z}$, $n, m > 1$ and $\gcd(n, m) = 1$. Then the map $\mathbb{Z} \to \mathbb{Z}/(n) \times \mathbb{Z}/(m)$, which maps an integer to its equivalence classes modulo n an m, induces an isomorphism*

$$\mathbb{Z}/(nm) \simeq \mathbb{Z}/(n) \times \mathbb{Z}/(m).$$

Proof: Notice that the orders are equal, so we only need to show that the map, let's call it ϕ, is injective. Let $k \in \ker \phi$, then $n|k$ and $m|k$; as $\gcd(n, m) = 1$, we thus have $nm|k$. Hence $\ker \phi \subset (nm)$; and it is immediate that $(nm) \subset \ker \phi$. □

Remark 10 An important use of this theorem is as follows. Let $a \in \mathbb{Z}/(n)$ and $b \in \mathbb{Z}/(m)$, we want to find $c \in \mathbb{Z}/(nm)$ such that $\phi(c) = (a, b)$. To that end, start from the Bézout equation $un+vm = 1$, which has solutions $u, v \in \mathbb{Z}$ by Theorem 7. Then let $c = unb+vma$.

Remark 11 The Chinese theorem (CRT for short) often appears as a practical way to speed up computations. Instead of working in a full-sized ring, we may break the computation into several independent and smaller tasks, only to reassemble the results in a final and simple stage.

For instance, to multiply 1234 by 5678 modulo $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$, we compute the products modulo each subfactor. Calling X the result of multiplication:

$$\begin{aligned} X &\equiv 1234 \cdot 5678 \equiv 0 \times 0 \equiv 0 \bmod 2 \\ X &\equiv 1234 \cdot 5678 \equiv 1 \times 2 \equiv 2 \bmod 3 \\ &\vdots \quad \equiv \quad \vdots \\ X &\equiv 1234 \cdot 5678 \equiv 9 \times 9 \equiv 4 \bmod 11 \\ X &\equiv 1234 \cdot 5678 \equiv 1 \times 3 \equiv 3 \bmod 13 \end{aligned}$$

then use the CRT to construct X modulo 30030 from the above information.

2.5 Cyclic groups

Lemma 5 *A finite group G of order n is cyclic if and only if there exists $x \in G$ of order n.*

Proof: Assume G is cyclic, i.e., there exists $x \in G$ such that $G = \langle x \rangle$. In particular, x has order n. Conversely, assume there exists $y \in G$ of order n; then $\langle y \rangle$ is a subgroup of G of order n, therefore $G = \langle y \rangle$, i.e., G is cyclic. □

Example 6

- The group $\mathbb{Z}$ is cyclic, with generator 1.
- Let $n \in \mathbb{Z}$, $n > 1$, the group $(\mathbb{Z}/(m), +)$ is cyclic, of order n.

- Let $n \in \mathbb{Z}$, $n > 1$, and let $\mu_n = \{\exp(2ki\pi/n) \mid 0 \leq k < n\}$. Then $\{\mu_n, \times\}$ is a cyclic subgroup of $\mathbb{C}^*$, of order n, called the group of complex n-th roots of unity.
- The group $(\mathbb{Z}/(2) \times \mathbb{Z}/(3), +)$ is cyclic, of order 6, and has generator $(1, 1)$.
- More generally, $G_1 \times G_2$ is cyclic if and only if $\gcd(n_1, n_2) = 1$, where n_1 and n_2 are the orders of G_1 and G_2 respectively. If furthermore $G_1 = \langle x_1 \rangle$ and $G_1 = \langle x_2 \rangle$, then $G_1 \times G_2 = \langle (x_1, x_2) \rangle$.

Corollary 7 (Groups of prime order are cyclic) *Let G be a finite group of prime order p. Then G is cyclic.*

Proof: Let $x \neq e$, then the order of x divides p by Theorem 11. Since p is prime, this means that x has order p. In particular, every element other than e generates G. □

Theorem 15 (Subgroups of a cyclic group) *Let G be a cyclic group of order n. Then,*

1. *Every subgroup of G is cyclic.*
2. *For every $d|n$, $d \geq 1$, $H_d = \{x \in G \mid x^d = e\}$ is a subgroup of G, of order d.*
3. *The map $d \mapsto H_d$ is a bijection between the (positive) divisors of n and the subgroups of G.*

In particular, for every $d|n$, H_d is the unique subgroup of G of order d.

Proof: Let G be a cyclic group of order n, and x a generator of G.

1. Let $H \leq G$, and δ be the smallest integer such that $x^\delta \in H$. Then $\langle x^\delta \rangle \leq H$. Let $y \in H$, there exists an integer m such that $y = x^m$ (because G is cyclic). Furthermore, there exist integers $q, r \in \mathbb{Z}$, $0 \leq r < \delta$, such that $m = \delta q + r$ (Theorem 1). Therefore, $x^r \in H$, which implies $r = 0$. Thus, $m = \delta q$, i.e., $y = (x^\delta)^q \in \langle x^\delta \rangle$, i.e., H is cyclic.
2. Let $d|n$, $d \geq 1$. One easily checks that $H_d \leq G$ as it satisfies all the axioms of being a subgroup. Observe that $\left(x^{n/d}\right)^d = x^n = e$, so that $x^{n/d} \in H_d$. The order of $x^{n/d}$ is $n/\gcd(n/d, n) = d$, so that d divides the order of H_d (Theorem 11). Since $H_d \leq G$, it is cyclic by the previous bullet point. If y is a generator of H_d, then $y^d = e$, so that the order of y divides d. But since the order of y and the order of H_d are the same, we conclude that H_d has order d.
3. Let $H \leq G$. For every $h \in H$, we have $h^d = e$, so that $H \subset H_d$. Since H_d has order d, in fact $H = H_d$. Now let d, d' be two positive divisors of n such that $H_d = H'_d$; these groups have same order, therefore $d = d'$.

□

Definition 17 (Euler totient) Let $n \in \mathbb{Z}$, $n \geq 1$, the number of integers smaller than n and coprime with n is called Euler's totient and denoted $\varphi(n)$.

Remark 12 There are $\varphi(n)$ generators of a cyclic group of order n.

Example 7

- $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$
- For $p \in \mathfrak{P}$, $\varphi(p) = p - 1$. For $p, q \in \mathfrak{P}$, $p \neq q$, $\varphi(pq) = (p-1)(q-1)$
- For $p \in \mathfrak{P}$, $r \in \mathbb{N}$, $r \geq 1$, we have $\varphi(p^r) = p^r - p^{r-1}$.

Lemma 6 *Let $n \in \mathbb{Z}$, $n \geq 1$, then*

$$n = \sum_{d|n} \varphi(d).$$

Proof: Define the following sets:

$$F = \left\{ \frac{i}{n} \mid 1 \leq i \leq n \right\}$$
$$F_d = \left\{ \frac{i}{d} \mid 1 \leq i \leq d \text{ and } \gcd(i,d) = 1 \right\}.$$

In particular, $F = \bigcup_{d|n} F_d$: indeed, every element $i/d \in F_d$ can be written as ki/n with $kd = n$, which belongs to F (as $i \leq d$); conversely every element of F has an irreductible counterpart in one of the F_d. Furthermore, if $i/d = i'/d'$ belongs to $F_d \cap F_{d'}$, then $d'i = di'$ which gives $i = i'$ and $d = d'$ since i and d (resp. i' and d' are coprime). Therefore the union is disjoint and this gives the result, since $|F| = n$ and $|F_d| = \varphi(d)$. □

Theorem 16 (Euler) *Let $a, b \in \mathbb{N}$, $a \geq 1$, $b \geq 2$, then $a^{\varphi(b)} \equiv 1 \bmod b$.*

Proof: Let $t = \varphi(b)$, and $b_1, \ldots, b_t$ be the integers between 1 and b that are coprime with b. For each $i = 1, \ldots, t$ there exist integers q_i, r_i, $0 \leq r_i < b$, such that $ab_i = bq_i + r_i$. We have

$$\prod_{i=1}^{t} ab_i \equiv \prod_{i=1}^{t} r_i \bmod b.$$

Furthermore, $\gcd(ab_i, b) = 1$, therefore $\gcd(r_i, b) = 1$, and $r_i \neq 0$.

Assume there are $i \neq j$ such that $r_i = r_j$, then $ab_i \equiv ab_j \bmod b$, i.e., $b|a(b_j - b_i)$. Since $\gcd(a, b) = 1$ by hypothesis, then $b|(b_j - b_i)$, which entails $b_i = b_j$. This is a contradiction, and therefore $r_i \neq r_j$.

As a result,

$$\prod_{i=1}^{t} ab_i \equiv \prod_{i=1}^{t} b_i \bmod b, \qquad \text{i.e.,} \qquad (a^t - 1) \prod_{i=1}^{t} b_i \equiv 0 \bmod b.$$

Since each b_i is coprime with b, so is their product, and we have $a^t \equiv 0 \bmod b$. □

Corollary 8 (Fermat's little theorem) *Let $a \in \mathbb{N}$, $a \geq 1$, and $p \in \mathfrak{P}$. Then $p|(a^p - a)$, i.e., $a^{p-1} \equiv 0 \bmod p$.*

Theorem 17 (Representation of cyclic groups) *Let G be a cyclic group of order n. Then $G \simeq (\mathbb{Z}/(n), +)$.*

Proof: Let G be a cyclic group of order n, and let $g \in G$ be a generator. Let $f : G \to \mathbb{Z}/(n)$ be the map defined by $f(g^k) = k \bmod n$, for every $k \in \mathbb{Z}$. This map is well-defined, as whenever $g^k = g^{k'}$ we have $n|(k - k')$, i.e., $k \equiv k' \bmod n$. Furthermore,

$$f(g^{k+k'}) = (k + k') \bmod n = (k \bmod n) + (k' \bmod n) = f(g^k) + f(g^{k'})$$

so that f is a group morphism. It is surjective (by design), and injective (as G and $\mathbb{Z}/(n)$ have the same order). □

Corollary 9 *Two cyclic groups are isomorphic if and only if they have the same order.*

Corollary 10 (Representation of prime order groups) *Let G be a finite group of prime order p. Then $G \simeq (\mathbb{Z}/(p), +)$.*

Proof: Corollary 7 and Theorem 17. □

Theorem 18 (Cauchy) *Let G be an Abelian finite group of order n. Let p be a prime divisor of n, then there exists $x \in G$ of order p.*

Proof: Denote $a_1, \ldots, a_n$ the elements of G, and $\alpha_1, \ldots, \alpha_n$ their respective orders. Let the map $f : \Gamma = \prod_{i=1}^{n} \mathbb{Z}/(\alpha_i) \to G$ be defined by $f((k_1, \ldots, k_n)) = a_1^{k_1} \cdots a_n^{k_n}$. One easily checks that f is well-defined and is in fact a group morphism. Furthermore, f is surjective since

$$f((0, \ldots, 1, \ldots, 0)) = a_i$$

where the "1" is placed in i-th position. By Theorem 10, $G \simeq \Gamma / \ker f$ and in particular

$$|\Gamma| = |\ker f| \cdot |G|.$$

Since p divides $|G|$, this implies that p divides $|\Gamma| = \alpha_1 \cdots \alpha_n$. Therefore, there exists $i \in \{1, \ldots, n\}$ such that $p | \alpha_i$, so that

$$a_i^{\alpha_i/p} \neq e \qquad \text{and} \qquad \left(a_i^{\alpha_i/p}\right)^p = e.$$

Hence $a_i^{\alpha_i/p}$ has order p. □

Corollary 11 (Abelian groups of square-free order are cyclic) *Let G be a finite group of order n such that n is square-free, i.e., $v_p(n) \leq 1$ for all $p \in \mathfrak{P}$. Then G is cyclic, of order n.*

Proof: Let $n = p_1 \cdots p_r$ where each $p_i \in \mathfrak{P}$. By Theorem 18 there exists $a_i \in G$ of order p_i for each $i = 1, \ldots, r$. Furthermore, for every $1 \leq s \leq r$, the element $a_1 \cdots a_s$ has order $p_1 \cdots p_s$. In particular, $a_1 \cdots a_r$ has order n, which concludes the argument using Lemma 5. □

Theorem 19 *Let G be a finite group of order n. Then G is cyclic if an only if $\gcd(n, \varphi(n)) = 1$.*

Definition 18 (Group of units) Let $n \in \mathbb{Z}$, $n > 1$. The integers modulo n that are coprime to n form a multiplicative group called the group of units and denoted $(\mathbb{Z}/(n))^\times$.

Remark 13 The order of $(\mathbb{Z}/(n))^\times$ is $\varphi(n)$.

Corollary 12 (Exponentiation in a cyclic group) *Let G be a cyclic group of order n, and $g \in G$. Let $k \in \mathbb{Z}$. Then $g^k = g^{k \bmod \varphi(n)}$.*

We will not prove the following theorem, but it highlights why the study of cyclic groups is fundamental to understanding the structure of general Abelian groups:

Theorem 20 (Kronecker) *Let G be a finite abelian group. Then*

$$G \simeq \bigoplus_{i=1}^{n} C_{q_i}$$

where C_q is the cyclic group of order q, and q_i are powers of prime.

Example 8

- Let $G = \mathbb{Z}/(15)$, then by the CRT $G \simeq \mathbb{Z}/(3) \times \mathbb{Z}/(5)$. One concrete realisation of this division is $\mathbb{Z}/(15) \simeq \{0, 5, 10\} \oplus \{0, 3, 6, 9, 12\}$.
- Let G be an Abelian group of order 8. Then G is isomorphic either to $\mathbb{Z}/(8)$, $\mathbb{Z}/(4) \oplus \mathbb{Z}/(2)$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus Z_2$.

2.6 Exercise set

Exercise 1. Let G be a group with neutral element e. Show that if for all $x \in G$, $x^2 = e$, then G is Abelian.

Exercise 2. Let G be a finite group of even order, with neutral element e. Show that there exists $x \in G$, $x \neq e$, such that $x^2 = e$.

Exercise 3. Let G be a group, and A and B be subgroups of G. Let

$$AB = \{ab \mid a \in A, b \in B\}. \qquad \text{and} \qquad BA = \{ba \mid a \in A, b \in B\}.$$

Show that $AB = BA$ if and only if AB is a subgroup of H.

Exercise 4. Let $n > 1$ and $k|n$ be integers. Prove that if $k|n$ then $(n) \subset (k)$. Does the converse hold?

Exercise 5. Let $n \in \mathbb{Z}$ such that $n \equiv 3 \bmod 7$ and $n \equiv 4 \bmod 11$. What is equivalence class of n modulo 77?

Exercise 6. Prove the short five lemma: In the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

where every row is a short exact sequence, if g and h are isomorphisms, then so is f.

Exercise 7. Show that for every $n \in \mathbb{Z}$, n odd, $\varphi(n) = \phi(2n)$.

> **Open question (2018)**: Is there, for every even integer n, an integer $m \neq n$ such that $\varphi(n) = \phi(m)$?
>
> **Open question (2018)**: Is there an integer $n \notin \mathfrak{P}$, such that $\varphi(n)|(n-1)$?

Exercise 8. Let $n \in \mathbb{Z}$, $n \geq 1$. Show that $\varphi(n)|n!$.

Exercise 9. Find all the $p \in \mathfrak{P}$ such that $p|(2^p + 1)$.

Exercise 10. Show that $a \mid b$ implies $\varphi(a) \mid \varphi(b)$. Does the converse hold?

Exercise 11. Every commercial book is given an International Standard Book Number, or ISBN. Since 2007, this number consists in 13 digits (describing the publisher, country group, etc.) $x_1, \ldots, x_{13}$. An ISBN is valid if

$$x_1 + x_3 + \cdots + x_{13} \equiv -3\,(x_2 + x_4 + \cdots + x_{12}) \bmod 10.$$

Write a program that checks whether a given ISBN is valid. What is the 13-th digit in the ISBN `978041547370X`?

Exercise 12. Implement fast modular addition and multiplication using the Chinese remainder theorem.

Exercise 13. Compute $2^{2017} \bmod 64$. Implement fast modular exponentiation using Euler's theorem.

Exercise 14. Can one combine the two previous exercises to perform exponentiation even faster? Implement this.

Exercise 15. Let $A_1, A_2, \ldots$ be a sequence of Abelian groups, and assume that we have an exact sequence

$$A : \cdots \xrightarrow{d_4} A_3 \xrightarrow{d_3} A_2 \xrightarrow{d_2} A_1 \xrightarrow{d_1} A_0 \xrightarrow{d_0} A_{-1} \xrightarrow{d_{-1}} \cdots$$

i.e., $\ker d_k = \operatorname{im} d_{k+1}$, i.e., $d_k d_{k+1} = 0$. Such a sequence is called a chain complex. Show that for every $n \in \mathbb{Z}$, $\operatorname{im} d_{n+1}$ is a normal subgroup of $\ker d_n$, and call H_n the quotient group $\ker d_n / \operatorname{im} d_{n+1}$. H_n is called the n-th homology group of A.

Consider $X = \mathbb{R}^3$, on which we can define the operators "gradient", "divergence", and "curl":

$$\operatorname{grad} f = \nabla f, \qquad \operatorname{div} f = \nabla \cdot f, \qquad \operatorname{curl} f = \nabla \times f$$

1. Let F_1 be the space of smooth functions on X with values in $\mathbb{R}$, and F_3 be the space of smooth functions on X with values in $\mathbb{R}^3$. Show that these are Abelian groups, and in fact, $\mathbb{R}$-vector spaces.
2. Show that each of the three operations above are group morphisms, and in fact, linear operations.
3. Show that for any $f \in F_1$, $\operatorname{curl}\operatorname{grad} f = 0$
4. Show that for any $f \in F_3$, $\operatorname{grad}\operatorname{div} f = 0$
5. Show that for any $f \in F_3$, $\operatorname{div}\operatorname{curl} f = 0$
6. Write down a chain complex using F_1, F_3, and the above operations.

The above was the starting point of the development of de Rham (co)homology, one of the most important examples of a (co)homology theory.

Exercise 16. Let $n \in \mathbb{N}$, define the set

$$E_n = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x^2 + y^2 = 5^n\}.$$

1. Compute E_0.
2. Let $a \in E_0$. For any b such that $0 \leq a \leq n$, define

   $$Z_{a,b} = a(2+i)^b(2-i)^{n-b},$$

   where $i^2 = -1$. Show that $|Z_{a,b}|^2 = 5^n$, and that the application

   $$(a, b) \mapsto Z_{a,b}$$

   is an injective map from $E_0 \times \{0, \ldots, n\}$ to E_n.
3. Let $(x, y) \in E_n$. Show that either

   $$\begin{cases} 2x - y \equiv 0 \bmod 5 \\ x + 2y \equiv 0 \bmod 5 \end{cases}$$

   or

   $$\begin{cases} 2x + y \equiv 0 \bmod 5 \\ -x + 2y \equiv 0 \bmod 5 \end{cases}$$

4. Deduce from the above that either $z/(2+i)$ or $z/(2-i)$ gives an element of E_{n-1} (taking its real and imaginary parts).
5. Show that $(a, b) \mapsto Z_{a,b}$ is in fact bijective, and deduce the number of elements in E_n, i.e., the number of solutions to the Diophantine equation

   $$x^2 + y^2 = 5^n.$$

Chapter 3

Rings

3.1 Basic definitions

Definition 19 (Ring) A ring is a set R, together with two binary operations (denoted $+$ and $\cdot$ respectively) such that

1. $(R, +)$ is an abelian group; the neutral element for $+$ is denoted 0.
2. For every $x, y, z \in R$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
3. There exists a neutral element for $\cdot$ which is denoted 1, and $1 \neq 0$.[1]
4. For every $x, y, z \in R$,

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

Example 9

- $\mathbb{Z}/(2) = \{0, 1\}$ is the smallest possible ring.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ have a ring structure, given by the usual addition and multiplication operations, and the usual neutral elements 0 and 1. However, $\mathbb{N}$ is not a ring, as $(\mathbb{N}, +)$ is not a group.
- Let R be a ring, then $n \times n$ matrices together with matrix addition and multiplication form the ring of matrices, denoted $M_n(R)$.

Definition 20 (Characteristic) Let R be a ring and $r \in R$. Let $n \in \mathbb{N}$, $n > 1$. We write $r + \cdots + r$ (n times) as nr. The characteristic of R, denoted $\operatorname{char} R$ is the least positive integer n such that $nr = 0$ for all $r \in R$. If no such integer exists, we say that the characteristic is zero.

[1] Some authors leave out the requirement that $1 \neq 0$ and distinguish "rings with identity" from "rings (without identity)"; we will always assume rings "with identity".

Definition 21 (Group of units) Let R be a ring. The group of units of R, denoted $R^\times$, is the group of elements that have a multiplicative inverse in R.

Definition 22 (Subring) A subset $S \subset R$ such that $1 \in S$, that is closed under addition, additive inverses, and multiplication is called a subring of R.

Example 10

- $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ forms a tower of subrings.
- The set $A = \{a/b \mid a \in \mathbb{Z}, b \in 2\mathbb{Z} - \{0\}\}$ is a subring of $\mathbb{Q}$.
- For every integer $n > 1$, the group $Z/(n)$ is in fact a ring.
- The set of functions from a set X to a ring Y is itself a ring called the ring of functions from X to Y.
- The set $M_n(R)$ of $n \times n$ matrices with coefficients in a ring R is itself a ring, called the ring of matrices with coefficients in R.

Definition 23 (Commutative ring) We say that a ring $(R, +, \cdot)$ is commutative if the operation $\cdot$ is commutative.

Definition 24 (Field) Let R be a commutative ring. If $R - \{0\}$ is a group under multiplication, then we say that R is a field.

Example 11

- If K is a field, then $K^\times = K - \{0\} = K^*$.
- $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ is a tower of fields.
- However $\mathbb{Z}$ is not a field, as some integers do not have integer multiplicative inverses.
- $M_n(\mathbb{R})$ is not a field for $n \geq 2$, as some matrices are singular and thus do not have multiplicative inverses.
- Let
$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$
where $i^2 = -1$. These matrices satisfy the following relations:
$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1},$$
$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j}$$
$$\mathbf{ji} = -\mathbf{k}, \quad \mathbf{kj} = -\mathbf{i}, \quad \mathbf{ik} = -\mathbf{j}$$

Let $\mathbb{H}$ consist of matrices of the form $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, where $a, b, c, d \in \mathbb{R}$. Observe that if $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$, then

$$(a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = a^2 + b^2 + c^2 + d^2$$

which is zero if and only if $a = b = c = d = 0$. Thus, if $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \neq 0$, we can define

$$(a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^{-1} = \frac{a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}.$$

The ring $\mathbb{H}$, called the quaternions, is however not a field because it is not commutative (it is a "division ring").

- Let M be a finite set, and K a field, then the set of all invertible functions form a field, the function field of M in K.

Theorem 21 (Finite fields of prime order) *Let $p \in \mathfrak{P}$, then $\mathbb{Z}/(p)$ is a field. It is called the finite field of order p, and denoted $\mathbb{F}_p$.*

Proof: The only point to check is that every non-zero element of $\mathbb{Z}/(p)$ has a multiplicative inverse. Let $a \in \mathbb{Z}/(p)$, $a \neq 0$. In particular, $\gcd(a, p) = 1$ so by Theorem 7 there exists $r, s \in \mathbb{Z}$ such that $ar + ps = 1$. Since $ps = 1 - ar$, we have $ar = 1 \bmod p$, i.e., r is the inverse of a in $\mathbb{Z}/(p)$. □

Lemma 7 *Let R be a ring, and $a \in R$. If $a^{-1} \in R$, then a is not a zero divisor, i.e., $a \neq 0$ and there is no $b \in R$, $b \neq 0$ satisfying $ab = 0$ nor $ba = 0$.*

Definition 25 (Integral domain) A commutative ring that has no zero divisor is called an integral domain.

In other words, R is an integral domain if and only if $ab = 0$ implies either $a = 0$ or $b = 0$, where $a, b \in R$.

Example 12

- $\mathbb{Z}$ is an integral domain.
- $M_n(\mathbb{R})$ is an integral domain for $n = 1$, but is not an integral domain for $n \geq 2$.

Lemma 8 (Cancellation in integral domains) *Let R be a commutative ring. Then R is an integral domain if and only if, for every $a \in R - \{0\}$, $ab = ac$ implies $b = c$.*

Theorem 22 (Wedderburn) *Every finite integral domain is a field.*

Proof: Let R be a finite integral domain, and R^* be the set of non-zero elements of R. Let $a \in R^*$, define the map $\phi_a : R^* \to R^*$ by $\phi_a(r) = ar$; this makes sense because there are no zero divisors in R^*, so $ar \neq 0$. For every $r_1, r_2 \in R^*$, $\phi_a(r_1) = \phi_a(r_2)$ implies $ar_1 = ar_2$, which implies $r_1 = r_2$ by Lemma 8; hence ϕ_a is injective. Since R^* is finite and ϕ_a is injective, it is bijective, and in particular surjective. Therefore, there exists $b \in R^*$ such that $\phi_a(b) = 1 = ab$. Thus a has a left inverse, and since R is commutative, a right inverse. This being true of every non-zero element $a \in R$, we have shown that R is a field. □

Theorem 23 (Newton) *Let R be a ring, $a, b \in R$ such that $[a, b] = ab - ba = 0$. Then for any integer $n > 0$,*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

3.2 Ring morphisms and ideals

Definition 26 (Ring morphism) Let $\phi : R \to S$ be a function between two rings R and S, such that $\phi(1_R) = 1_S$ and for every $a, b \in R$,

$$\phi(a+b) = \phi(a) + \phi(b)$$
$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

Then ϕ is called a ring morphism. The kernel of ϕ is the inverse image of 0.

Example 13

- The map $R[X] \to R[X]$ that sends $f(X)$ to $f(X+1)$ is a ring morphism.
- The map $\sigma : \mathbb{C} \to \mathbb{C}$ that sends a complex number to its conjugate is a ring morphism.

Definition 27 (Ideal) Let R be a ring, and $I \subset R$. We say that I is an ideal of R if I is an additive subgroup of R such that for all $a \in I, r \in R$,

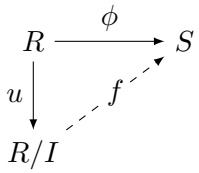
$$ar \in I \qquad \text{and} \qquad ra \in I.$$

Lemma 9 *Let $\phi : R \to S$ be a ring morphism. Then $\ker \phi$ is an ideal of R.*

Proposition 4 (Quotient ring) *Let R be a ring and $I \neq R$ be an ideal of R. Then R/I is a ring, and there is a natural morphism $R \to R/I$ that maps $r \mapsto r + I$.*

Theorem 24 (Universality) *Let R be a ring, $I \neq R$ be an ideal of R, and $u : R \to R/I$ as above. Then u is universal amongst all ring morphisms whose kernel contains I, in the following sense.*

Let $\phi : R \to S$ such that $I \subset \ker \phi$, then there exists a unique morphism f that makes the following diagram commute:



Definition 28 (Principal ideal) Let R be a commutative ring and $a \in R$. The set $(a) = aR$ is an ideal of R, and any ideal of this form is called a principal ideal.

Example 14

- Let R be a ring. Then $\{0\}$ and R are ideals of R, called the trivial ideals.
- The additive subgroup $(n) = n\mathbb{Z}$ is a principal ideal of $\mathbb{Z}$. The corresponding quotient ring is $\mathbb{Z}/(n)$.
- Let X be a set, $Y \subset X$, and R be a ring. The set of functions $X \to R$ forms a ring C, and the subset of functions that vanish on Y form an ideal V of this ring. Furthermore, the ring C/V is isomorphic to the ring of functions $Y \to R$.
- $\mathbb{Z}$ is not an ideal of $\mathbb{Q}$.
- Let R and S be rings. Then the ideals of the ring $R \times S$ are exactly the ideals $I \times J$, where I is an ideal of R and J an ideal of S respectively.

Lemma 10 *Let R be a ring, and I an ideal of R. If I contains a unit, then $I = R$.*

Proof: Suppose that $u \in R^\times \cap I$. Then $uv = 1$ for some $v \in R$, therefore $1 = uv \in I$. Then for any $a \in R$, $a = a \cdot 1 \in I$. □

Corollary 13 *Let K be a field, then the only ideals of K are (0) and K.*

Definition 29 (Maximal ideal) Let R be a ring, and M be an ideal of R. If for every ideal $I \neq M$ such that $M \subset I$, we have $I = R$ we say that M is a maximal ideal of R.

Theorem 25 (Maximal ideals and fields) *Let M be a commutative ring and M an ideal of R. Then M is a maximal ideal of R if and only if R/M is a field.*

Proof: Let M be a maximal ideal of R. In particular R/M is commutative and $1+M$ acts as the identity of R/M. We must show that every non-zero element of R/M has a multiplicative inverse. If $a+M \in R/M$ is non-zero, then $a \notin M$; let $I = \{ra+m \mid r \in R, m \in M\}$, which is non-empty since $0 \in I$. If r_1a+m_1 and r_2a+m_2 are in I, then

$$(r_1a+m_1)-(r_2a+m_1) = (r_1-r_2)a+(m_1-m_2)$$

also belongs to I. Also, for every $r \in R$, $rI \subset I$. Therefore, I is an ideal of R; furthermore $I \neq M$, and $M \subset I$. Since M is maximal, this implies $I = R$. Therefore there exists $m \in M$ and $b \in R$ such that $1 = ab+m$, and

$$1+M = ab+M = (a+M)(b+M)$$

Conversely, suppose that R/M is a field; then it contains at least $0+M = M$ and $1+M$, and therefore $M \neq R$. Let I be an ideal of R such that $M \subset I$, and let $a \in I$, $a \notin M$. Since $a+M$ is non-zero, there exists an inverse $b+M$ in R/M such that $(a+M)(b+M) = ab+M = 1+M$. Thus there exists an element $m \in M$ such that $ab+m = 1$; and $1 \in I$. Since 1 is a unit of R, this entails $I = R$. Hence M is maximal. □

Remark 14 Since $\mathbb{Z}/(p)$ is a field, we have that (p) is a maximal ideal of $\mathbb{Z}$.

Definition 30 (Prime ideal) Let R be a commutative ring. Let I be a proper ideal of R. We say that I is a prime ideal if whenever $ab \in I$, then either $a \in I$ or $b \in I$.

Theorem 26 (Prime ideals and integral domains) *Let R be a commutative ring, and I be a proper ideal of R. Then I is a prime ideal of R if and only if R/P is an integral domain.*

Corollary 14 *Every maximal ideal in a commutative ring is prime.*

Definition 31 (Spectrum of a ring) The set of all prime ideals of a ring R is called the spectrum of R and denoted $\operatorname{Spec} R$.

Example 15 $\operatorname{Spec}\mathbb{Z} = \{0\} \cup \{(p) \mid p \in \mathfrak{P}\}$.

Definition 32 (Finite field) Let $p \in \mathfrak{P}$. The quotient $\mathbb{Z}/(p)$ is a field called the finite field of order p, and denoted $\mathbb{F}_p$.

Remark 15 The spectrum of a ring can be endowed with a topology, making it a scheme, one of the central objects of interest in algebraic geometry.

Definition 33 (Radical of an ideal) Let R be a commutative ring and I be an ideal of R. The radical of I, denoted $\operatorname{rad} I$, is the ideal defined by

$$\operatorname{rad} I = \{r \in R \mid r^n \in I \text{ for some } n > 0\}$$

Definition 34 (Reduced ring) A ring R is reduced if it has no nilpotent elements.

Theorem 27 (Reduced rings and radical ideals) *The following statements are equivalent:*

1. *An ideal I in R is radical;*
2. *The quotient ring R/I is reduced;*
3. *The nilradical of R is zero;*
4. $\bigcap_{I \in \operatorname{Spec} R} I = (0)$.

Example 16

- Every integral domain is a reduced ring since a nilpotent element is a fortiori a zero divisor, and integral domains do not have any zero divisor.
- $\mathbb{Z}/(n)$ is reduced if and only if $n = 0$ or n is a square-free integer.

3.3 Field extensions, trace and norm

Definition 35 (Field extension) Let L a field and K be a subfield of L (we say that L is an extension of K). Then L can be considered as K-vector space, and the dimension $\dim_K L$ is called the degree of the extension. An extension is finite if its degree is finite.

Example 17

- The field $\mathbb{C}$ of complex numbers is a field extension of $\mathbb{R}$ of degree 2 — such extensions are called quadratic. As a particular consequence, there are no non-trivial fields between $\mathbb{R}$ and $\mathbb{C}$.
- The ring $\mathbb{Q}[\sqrt{2}]$ of numbers of the form $a + b\sqrt{2}$ is actually a field. As such, it is a quadratic extension of $\mathbb{Q}$, denoted $\mathbb{Q}(\sqrt{2})$. Such finite extensions of $\mathbb{Q}$ are called number fields.
- The ring $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ can also be turned into a field; it is made of numbers of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ and is therefore of degree 4 over $\mathbb{Q}$.

Definition 36 (Field trace and norm) Let L be a finite extension of a field K. For every $a \in L$, the application $m_a : L \to L$ defined by

$$m_a : \ell \mapsto a\ell$$

is a K-linear transformation. Let $\Delta_{L/K}(a)$ be the matrix of this transformation. The field trace of a on L over K is the trace of $\Delta_{L/K}(a)$ and denoted $\operatorname{Tr}_{L/K}(a)$. The field norm of a on L over K is the determinant of $\Delta_{L/K}(a)$ and denoted $N_{L/K}(a)$.

Example 18

- A basis of $\mathbb{Q}(\sqrt{2})$ as a quadratic extension of $\mathbb{Q}$ is $\{1, \sqrt{2}\}$. Let $a \in Q(\sqrt{2})$, $a = \alpha + \beta\sqrt{2}$. Multiplication by a sends 1 to a, and $\sqrt{2}$ to $2\beta + \alpha\sqrt{2}$; the matrix of $\ell \mapsto a\ell$ is thus
$$\Delta_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}} = \begin{pmatrix} \alpha & 2\beta \\ \beta & \alpha \end{pmatrix}$$
thus $N_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(a) = \alpha^2 - 2\beta^2$ and $\mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(a) = 2\alpha$.
- The same reasoning with $\mathbb{C}$ as an extension of $\mathbb{R}$ gives, for any $z = x + iy \in \mathbb{C}$,
$$N_{\mathbb{C}/\mathbb{R}}(z) = x^2 + y^2, \qquad \mathrm{Tr}_{\mathbb{C}/\mathbb{R}} = 2x.$$

Remark 16 Note that the field norm is not a norm in the usual sense (that of normed vector spaces); for instance, the element $1 + \sqrt{2}$ has norm -1 in $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.

3.4 Field of fractions

Let R be an integral domain. There is a generic construction of a field from R, obtained as follows. Let $\sim$ be the relation defined on $R \times R$ by $(a, b) \sim (c, d) \Leftrightarrow ad = bc$.

Lemma 11 *The relation $\sim$ is an equivalence.*

Lemma 12 *Let (a_i, b_i) be couples of $R \times R$ for $i = 1, 2, 3, 4$, such that*
$$(a_1, b_1) \sim (a_2, b_2) \quad \textit{and} (a_3, b_3) \sim (a_4, b_4).$$
Then
$$(a_1 b_3 + a_3 b1, b_1 b_3) \sim (a_2 b_4 + a_4 b_2, b_2 b_4) \quad \textit{and} \quad (a_1 a_3, b_1 b_3) \simeq (a_2 a_4, b_2 b_4).$$

Corollary 15 *Let $K = (R \times R)/\sim$. Define the (equivalence class of the) product as*
$$[(a, b)][(c, d)] = [(ac, bd)]$$
and the (equivalence class of the) sum as
$$[(a, b)] + [(c, d)] = [(ad + bc, bd)].$$
This makes K into a ring, and in fact a field, since for any non-zero $[(a, b)]$, $[(a, b)]^{-1} = [(b, a)]$. We call this field the field of fractions of R, denoted $\mathrm{Frac}\, R$.

Remark 17 There is a natural injective ring morphism $\iota : R \hookrightarrow \mathrm{Frac}\, R$ ('fractions with denominator 1').

Example 19

- $\mathrm{Frac}\, \mathbb{Z} \simeq \mathbb{Q}$
- $\mathrm{Frac}\, \mathbb{Z}[i] \simeq \mathbb{Q}[i]$
- For any field K, $\mathrm{Frac}\, K \simeq K$.

3.5 Exercice set.

Exercise 1. A ring R is called Boolean if for every $r \in R$, we have $r^2 = r$. Prove that such a ring is commutative. Let X be a set, and 2^X be the set of subsets of X (the 'power set'); using symmetric difference as addition, and set intersection as multiplication, show that 2^X is a ring, and in fact a Boolean ring.

Exercise 2. Let R be a ring, such that $r^3 = r$ for all $r \in R$. Show that R is commutative.

Exercise 3. Find two non-zero matrices A and B with coefficients in $\mathbb{Z}$ such that $AB = 0$.

Exercise 4. Let $p \in \mathfrak{P}$ and define

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } \gcd(b, p) = 1 \right\}.$$

Prove that $\mathbb{Z}_{(p)}$ is a ring. It is called the ring of integers localised at p.

Exercise 5. Find the kernels of the morphisms given in Example 13.

Exercise 6. Let R be a ring. An element $r \in R$ is nilpotent if there exists $n > 0$ such that $r^n = 0$. Show that the set of nilpotents of R forms an ideal. It is called the nilradical of R.

Exercise 7. Using Bézout's theorem, show that (p) is a maximal ideal of $\mathbb{Z}$ when p is prime.

Exercise 8. Let i be a square root of -1, and $\mathbb{Z}[i]$ be the set of numbers of the form $a + ib$, where $a, b \in \mathbb{Z}$. Show that $\mathbb{Z}[i]$ is a ring. It is referred to as the ring of Gaussian integers.

Exercise 9. Let X be a set, and R be a ring. Let $f : X \to A$ be a function. Show that f is invertible if and only if $f(X) \subset A^\times$.

Exercise 10. Let R and S be rings. Show that $(R \times S)^\times \simeq R^\times \times S^\times$.

Exercise 11. Show that a ring morphism $R \to S$ induces a morphism of spectra in the reverse direction: $\operatorname{Spec} S \to \operatorname{Spec} R$.

Exercise 12. Equations of the form $X^2 - DY^2 = 1$, where D is a square-free integer, are called Pell–Fermat equations.[2] Show that a solution to such an equation is, in a precise sense, 'just' a unit of $\mathbb{Z}[\sqrt{D}]$. From there, show that solutions form a group and make the group law explicit.

[2] The attribution to Pell, due to Euler, is a mistake. But the name is now standard.

Chapter 4

Polynomial rings

4.1 Basic definitions

Definition 37 (Polynomial ring) Let R be a ring. The polynomial ring $R[X]$ is defined to be the set of all formal sums

$$\sum a_i X^i$$

where $a_i \in R$ and all the a_i are zero, except maybe for a finite number of them. Elements of $R[X]$ are called polynomials.

Definition 38 (Degree of a polynomial) Let $P \in [X]$, $P = a_0 + \cdots + a_k X^k$. The degree of P, denoted $\deg P$, is the largest k such that $a_k \neq 0$; the degree of the zero polynomial is $-\infty$.

Remark 18 We can define an ordered set $\underline{\mathbb{N}} = \mathbb{N} \cup \{-\infty\}$, by setting $-\infty \leq n$ for all $n \in \mathbb{N}$, $(-\infty) + n = n + (-\infty) = -\infty$, and $(-\infty) + (-\infty) = -\infty$. Then the degree is an application

$$\deg : K[X] \to \underline{\mathbb{N}}.$$

Proposition 5 *Let $P, Q \in R[X]$, we have*

- $\deg(P + Q) \leq \max(\deg P, \deg Q)$, *with equality if* $\deg P \neq \deg Q$;
- $\deg(PQ) = \deg P + \deg Q$.

Definition 39 (Monic polynomial) A polynomial $P = a_0 + \cdots + a_k X^k$ of degree k is monic if $a_k = 1$.

Corollary 16 (Units of a polynomial ring) *The ring $R[X]$ is an integral domain, and $R[X]^\times = R^\times$.*

Proof: $R[X]$ is a non-empty commutative ring. By Proposition 5, $PQ = 0$ implies either $\deg P = -\infty$ or $\deg Q = -\infty$, i.e., $P = 0$ or $Q = 0$. Hence $R[X]$ has no zero divisor. Furthermore, if $PQ = 1$, then $\deg P + \deg Q = 0$, but since these are non-negative integers, $\deg P = \deg Q = 0$. □

Theorem 28 (Euclidean division of polynomials) *Let $A, B \in S[X]$, $B \neq 0$. Then there exists a a unique couple (Q, R) of polynomials in $S[X]$ such that*

$$A = BQ + R \qquad \textit{and} \qquad \deg R < \deg B.$$

We say that Q is the quotient, and R is the remainder of the Euclidean division of A by B. If $R = 0$, we say that B divides A, and write $B|A$.

Proposition 6 *Let $A, B \in R[X]$, $A, B \neq 0$, such that $A|B$ and $B|A$. Then there exists $\lambda \in R$, $\lambda \neq 0$, such that $A = \lambda B$.*

Proof: By Theorem 28, there exists $Q_1, Q_2 \in R[X]$ such that $A = BQ_1$ and $B = AQ_2$. Therefore $A(1 - Q_1Q_2) = 0$. Since $R[X]$ is an integral domain and $A \neq 0$, this implies $Q_1Q_2 = 1$, i.e., Q_1 is invertible (Corollary 16). □

Remark 19 The notion of irreducibility is profoundly dependent on the underlying ring R, and the following example shows: Let $R_1 = \mathbb{Z}$ and $R_2 = \mathbb{Z}[\sqrt{2}]$. The polynomial $X^2 - 2$ is irreducible in $R_1[X]$, but it can be decomposed as $(X - \sqrt{2})(X + \sqrt{2})$ in $R_2[X]$.

4.2 Spectrum of a polynomial ring

Remark 20 In this section, we assume that R is a field.

Theorem 29 (Ideals of a polynomial ring) *Let R be a field, and I be a non-zero ideal of $R[X]$. Then there exists a unique monic polynomial $P \in R[X]$ such that $I = (P)$. As a consequence, all the ideals of $R[X]$ are principal.*

Proof: Since $I \neq 0$, there exists a non-zero $P \in I$ of minimal degree. Up to multiplication by a unit, we may assume P is monic. By definition, P and all its multiples belong to I. Conversely, if $Q \in I$, then by Theorem 28 there are unique A, B such that $Q = AP + B$ with $\deg B < \deg P$. But then $B \in I$, and if $B \neq 0$ then this contradicts that P is minimal. Hence $B = 0$, and $P|Q$, which means that $Q \in (P)$.

Now if there are polynomials $P_1, P_2 \in R[X]$ such that $I = (P_1) = (P_2)$, we have $P_2|P_1$ and $P_2|P_1$, hence $P_1 = \lambda P_2$ for some $\lambda \in R^\times$ (Proposition 6). But since P_1 and P_2 are monic, $\lambda = 1$ and $P_1 = P_2$. □

Corollary 17 (Greatest common divisor) *Let $A, B \in R[X]$, $A, B \neq 0$. Then*

$$I = \{AU + BV \mid U, V \in R[X]\}$$

is an ideal of $R[X]$, that is non-empty. Then by Theorem 29 there exists a unique monic polynomial $D \in R[X]$ such that $I = (D)$. We say that D is the greatest common divisor of A and B, and write $D = \gcd(A, B)$.

Definition 40 (Coprime polynomials) Two polynomials $A, B \in R[X]$ are coprime if $\gcd(A, B) = 1$, or equivalently, if there exist $U, V \in R[X]$ such that $AU + BV = 1$.

Remark 21 Theorem 29 relies critically on the assumption that R is not only a ring, but a field.

Definition 41 (Irreducible polynomial) A polynomial $P \in R[X]$ is said to be irreducible if $P \notin R^\times$, and if $Q|P$, $Q \neq P$ implies $Q \in R^\times$.

Example 20

- The polynomial $X^2 - 1$ is reducible in any ring, since it equals $(X - 1)(X + 1)$
- The polynomial $X^2 - 2$ is irreducible in $\mathbb{Z}[X]$ or $\mathbb{Q}[X]$, as otherwise there would be a rational (or integer!) square root of 2.
- The polynomial $X^p - 1$, where $p > 2$ is prime, is reducible since it has an obvious root. But it we remove this factor, we get

  $$\Phi_p = \frac{X^p - 1}{X - 1} = 1 + X + \cdots + X^{p-1}$$

  which is irreducible in $K[X]$ if K doesn't have roots of unity besides 1. Φ_p is known as the p-th cyclotomic polynomial.

Theorem 30 (Prime decomposition) *Let $P \in R[X]$, $P \neq 0$. Then P can be uniquely written (up to reordering) as*

$$P = u \prod_{P_i \text{ monic irred.}} P_i^{n_i}$$

where all but a finite number of the integers n_i are zero, and $u \in R^\times$.

Remark 22 A ring in which all the ideals are principal and there are no zero divisors is called a principal ideal domain. In particular, elements of such rings always admit a unique factorisation into "irreducible" elements, and a notion of GCD, similar to the situation in $\mathbb{Z}$.

Remark 23 The spectrum of $R[X]$, i.e., the prime ideals of $R[X]$, are (0) and (P_i), where P_i are the monic irreducible polynomials of $R[X]$.

Remark 24 If R is not a field, there can be other ideals. For instance, $\mathbb{Z}[X]$ is not a principal ideal domain. Its spectrum is composed of

- (0);
- (p) for each $p \in \mathfrak{P}$;
- (P) for each monic polynomial P irreducible in $\mathbb{Q}$ (hence, in $\mathbb{Z}$);
- (q, Q) for $q \in \mathfrak{P}$ and Q a monic polynomial irreducible in $\mathbb{F}_q$.

The following result is remarkably useful:

Theorem 31 (Eisenstein's criterion) *Let $P \in \mathbb{Z}[X]$, $P = c_n X^n + c_{n-1} X^{n-1} + \cdots + c_1 X + c_0$. If there exists a prime p such that all the three following conditions hold:*

1. $p \nmid c_n$;
2. $p \mid c_{n-1}, c_{n-2}, \ldots, c_0$;
3. $p^2 \nmid c_0$;

then P is irreducible in $\mathbb{Q}[X]$, hence in $\mathbb{Z}[X]$.

Example 21 Let $X^3 - 6X + 3$. By Eisenstein's criterion (using $p = 3$) this polynomial is irreducible in $\mathbb{Q}$.

Proof: Assume that P is reducible, and write $P = gh$ with $\deg g$ and $\deg h$ strictly smaller than $\deg P$. Let $g = a_0 + \cdots + a_k X^k$ and $h = b_0 + \cdots + b_\ell X^\ell$.

Since $c_n = a_k b_\ell$, and $p \nmid c_n$, we have that $p \nmid a_k$ and $p \nmid b_\ell$. Similarly, p divides one of a_0 or b_0, but not both, since $p^2 \nmid c_0$; without loss of generality assume $p | a_0$.

Finally, $P = fg$ holds modulo p, i.e.,

$$c_n X^n \equiv P \equiv (a_0 + \cdots + a_k X^k)(b_0 + \cdots + b_\ell X^\ell) \bmod p$$

(we work in the ring $(\mathbb{Z}/(p))[X]$). The right-hand side of this equation would imply that, for any $m < n$, the coefficient of X^m is $a_m b_0 \not\equiv 0 \bmod p$. This contradicts the left-hand side. □

4.3 Roots of a polynomial

Definition 42 (Polynomial function) Let $P \in R[X]$, $P = a_0 + \cdots + a_k X^k$, and $x \in K$. The map $\mathrm{eval}_x : K[X] \to K$, defined by

$$\mathrm{eval}_x(P) = \sum_{k=0}^{\deg P} a_k x^k$$

is a ring morphism (the evaluation morphism). This defines an application $K \to K$ that we (abusively, but conventionally) denote P, and that we call the polynomial function associated to P.

Remark 25 Many polynomials will in often determine the same function. As an example, there are exactly 4 functions from $\mathbb{Z}/(2)$ to itself, while there are infinitely many polynomials in $(\mathbb{Z}/(2))[X]$.

Definition 43 (Root) Let $P \in R[X]$. An element $a \in R$ such that $P(a)$ is a root of P.

Lemma 13 *Let $P \in R[X]$ and $a \in R$. Then a is a root of P if an only if $(X-a)|P$.*

Remark 26 An irreducible polynomial may have no root: consider for instance $(X^1+1)^2$ which is reducible but has no real roots in $\mathbb{R}$.

Definition 44 (Derived polynomial) Let $P \in R[X]$, $P = a_0 + \cdots + a_k X^k$. The derived polynomial of P is

$$P' = \sum_{k=1}^{\deg P} k a_k X^{k-1}.$$

Remark 27 If $a \in R$ is a root of P but not a root of P', then a is called a simple root of P; in particular, $(X-a)^2 \nmid P$.

Lemma 14 *Let $P \in R[X]$, $\deg P = n$. Then P has at most n distinct roots.*

Proposition 7 *Let $p \in \mathfrak{P}$. Then every $a \in \{1, 2, \ldots, p-1\}$ is a root of the polynomial $X^{p-1} - 1 \in (\mathbb{Z}/(p))[X]$.*

Proof: This is a consequence of Fermat's little theorem. □

Corollary 18 (Wilson's theorem) *Let $p \in \mathbb{Z}$, $p > 1$. Then $p \in \mathfrak{P}$ if and only if $p|((p-1)!+1)$.*

Proof: Using the previous lemma, and the fact that $P = X^{p-1} - 1$ has degree $p-1$, we can write it as

$$P = \prod_{a=1}^{p-1} (X - a).$$

In particular, $P(0) = -1$ (left hand side) and $P(0) = \prod_{a=1}^{p-1}(-a)$ (right hand side), which gives the result.

Conversely, assume $p|((p-1)!+1)$. If $q|p$ and $q \neq p$, then $q|(p-1)!$ which gives $q = 1$; therefore p is prime. □

4.4 Quotients

Definition 45 (Module) Let R be a ring. A set E endowed with

- An Abelian group structure on E (denoted additively);
- An external law ("scalar multiplication") $\times : R \times E \to E$ such that for all $a, b \in R$ and all $x, y \in E$,

$$\begin{aligned} a \times (x + y) &= a \times x + a \times y \\ (a + b) \times x &= a \times x + b \times x \\ a \times (b \times x) &= (ab) \times x \\ 1 \times x &= x \end{aligned}$$

is called an R-module. Since there is no ambiguity, we omit the symbol $\times$ for scalar multiplication.

Remark 28 If R is a field, then R-modules are typically called R-vector spaces.

Remark 29 If E is a ring and an R-module, it is called an R-algebra.

Example 22

- An Abelian group is exactly the same thing as a $\mathbb{Z}$-module.
- A commutative ring is exactly the same thing as a $\mathbb{Z}$-algebra.
- A polynomial ring $R[X]$ has a natural R-algebra structure, with scalar multiplication by "constants". As a result, we may refer to $R[X]$ as the polynomial algebra on R. It is an associative and commutative algebra.
- The ring of square $n \times n$ matrices with coefficients in R, $M_n(R)$, has a natural R-algebra structure.
- Let R be a ring and $Z(R)$ be its center, then R is an $Z(R)$-module.

Theorem 32 *Let R be a ring, and I be an ideal of $R[X]$. Then $R[X]/I$ is an R-algebra.*

Proof: As a ring quotient, $R[X]/I$ is a ring. Multiplication by an element of R gives it an R-algebra structure, as it it easily checked that this operation is compatible with the quotient. □

Theorem 33 (Units of a polynomial ring) *Let R be a field and $P \in R[X]$, $\deg P \geq 0$. Then $(R[X]/(P))^\times$ is made of the (classes of) polynomials coprime with P.*

Corollary 19 (Prime ideals of a polynomial ring) *The prime ideals of $R[X]$ are its irreducible polynomials.*

Theorem 34 *If P is irreducible, then $R[X]/(P)$ is an integral domain, and in fact, a field.*

Proof: We already know that the quotient of a ring by a prime ideal is an integral domain. Let show that any non-zero polynomial in $Q \in R[X]/(P)$ is invertible. Since P is irreductible and $P \nmid Q$ (otherwise Q would be zero in the quotient ring) P and Q are coprime polynomials. By Theorem 33 Q is therefore invertible. □

Theorem 35 *Let R be a field, and $P \in \operatorname{Spec} R[X]$. There exists a field K, such that*

- *R is a subfield of K;*
- *There is a root of P in K;*
- *K is an R-vector space*
- *As a vector space, K has finite dimension, and $\dim K = \deg P$.*

Proof: Denote $A = R[X]/(P)$; by Theorem 34, A is a field. Define

$$Z = \{a \in A \mid a \notin R + (P)\}$$

and $K = Z + R$. Then the application $f : A \to L$ defined for all $x \in R$ by

$$f(x) = x \bmod (P)$$

and for all $z \in Z$ by $f(z) = z$ is a bijection from A to K. This allows us to define the following operations on K: for every $u, v \in K$ and every $r \in R$, define

$$\begin{aligned} u + v &= f\left(f^{-1}(u) + f^{-1}(v)\right) \\ u \cdot v &= f\left(f^{-1}(u) \cdot f^{-1}(v)\right) \\ ru &= f(rf^{-1}(u)) \end{aligned}$$

which makes K an R-algebra; in particular, $A \simeq K$ as R-algebras. We conclude by showing that A, hence K, is an R-vector space of dimension $\deg P$.

Let $\beta = X + (P)$, and define the family $B = \left\{\beta^0, \beta^1, \ldots, \beta^{\deg P - 1}\right\}$. Let $\lambda_0, \ldots, \lambda_{\deg P - 1} \in R$ such that

$$\sum_{i=0}^{\deg P - 1} \lambda_i \beta^i = 0,$$

which in particular implies

$$\sum_{i=0}^{\deg P - 1} \lambda_i X^i \in (P).$$

But P is of degree $\deg P$, so the λ_i are necessarily zero, therefore the elements of B are linearly independent.

Now let $Q \in R[X]/(P)$, there exists $S \in R[X]$ such that $Q = S + R$. Since P is non-zero, there exists by Theorem 28 $U, V \in R[X]$ such that $Q = PU + V$ and $\deg V < \deg P$. As a result, $Q = V \bmod (P)$, which shows that B is a generating family. □

Remark 30 The notion of polynomial ring extends the base ring. Then taking a quotient restricts the polynomial ring. For well chosen quotients, this enables us to build precisely controlled extensions. The process is usually as follows:

1. Start from some base ring or field K which you want to build an extension of.
2. Consider the corresponding polynomial ring $K[X]$
3. Choose an irreducible polynomial of $K[X]$, and consider the quotient $K[X]/(P)$.

Remark 31 Taking quotients is not a harmless operation. For instance, in the ring $\mathbb{Z}[\sqrt{-5}] \simeq \mathbb{Z}[X]/(X^2+5)$,

$$(1-\sqrt{-5})(1+\sqrt{-5}) = 6 = 2 \cdot 3$$

and both $2, 3, (1-\sqrt{-5})$, and $(1+\sqrt{-5})$ are irreducible; so this means we do not have unique factorisation! That being said, the ideal (6) can be uniquely decomposed as a product of prime ideals (which ones?). This remarkable feature was Kummer's motivation for introducing ideals in the first place.

Example 23

- $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{R}[i] \simeq \mathbb{C}$ is a possible definition of the field of complex numbers, and $\dim_{\mathbb{R}} \mathbb{C} = \deg(X^2+1) = 2$. (Which tells us, for instance, that any complex number is entirely described by a couple (x, y) of reals).
- Every polynomial is reducible over $\mathbb{C}$, so we cannot construct algebraic extensions of $\mathbb{C}$ that are not $\mathbb{C}$ itself.
- If P is an irreducible polynomial of degree n in some polynomial ring $K[X]$, then it is often practical to introduce a formal root α of P and think of $K[X]/(P)$ as an extention $K[\alpha, \alpha^2, \ldots, \alpha^{n-1}]$ which is a concrete realisation of the corresponding K-algebra. For instance, $\mathbb{Z}[X]/(X^2+D) \simeq \mathbb{Z}[\sqrt{-D}]$, where $\sqrt{-D}^2 = -D$.
- It is possible to construct extensions of extensions. For instance, X^2-2 is irreducible in $\mathbb{Q}[X]$, and we construct from it $\mathbb{Q}(\sqrt{2}) \simeq \mathbb{Q}[X]/(X^2-2)$. Now X^2-3 is irreducible in that new field, and we can get $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})[\sqrt{3}] \simeq \mathbb{Q}(\sqrt{2})[X]/(X^2-3)$. In particular, this shows that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ has dimension 4 over $\mathbb{Q}$.
- Let $p \in \mathfrak{P}$, $p \neq 2$, then the p-th cyclotomic polynomial is monic and irreducible in $\mathbb{Q}[X]$. Therefore $\mathbb{Q}[X]/(\Phi_p)$ is a field, called the p-th cyclotomic field. If we introduce a formal p-th root of unity $\zeta \neq 1$, then $\mathbb{Q}[X]/(\Phi_p) \simeq \mathbb{Q}[\zeta]$, which we write $\mathbb{Q}(\zeta)$ to insist that it is a field. We can similarly define $\mathbb{Z}[\zeta]$.

4.5 Exercise set

Exercise 1. Let $\mathbb{F}_2 = \mathbb{Z}/(2)$. Compute the Euclidean division of $X^3 + X^2 + 1$ by $X^2 + X + 1$ in $\mathbb{F}_2[X]$.

Exercise 2. Let $m, n \in \mathbb{N}$, $m, n > 0$. Show that $\gcd(X^n - 1, X^m - 1) = X^{\gcd(n,m)} - 1$.

Exercise 3. Let $p \in \mathfrak{P}$ and $\mathbb{F}_p = \mathbb{Z}/(p)$. How many monic polynomials are there in $\mathbb{F}_p[X]$? Show that there are $p(p-1)/2$ irreducible monic polynomials of degree 2 in that ring.

Exercise 4. Compute $\operatorname{Spec} \mathbb{R}[X]$, $\operatorname{Spec} \mathbb{C}[X]$, $\operatorname{Spec} \mathbb{F}_q[X]$.

Exercise 5. Show that if $p \in \mathfrak{P}$, $W(p) = ((p-1)! + 1)/p$ is an integer. If $p|W(p)$ then p is called a Wilson prime.

Open question (2018): Are there other Wilson primes besides 5, 13, and 563?

Exercise 6. Let $\mathbb{F}_2 = \mathbb{Z}/(2)$, and $P = X^3 + X + 1 \in \mathbb{F}_2[X]$.

1. Show that P is irreducible.
2. What is the dimension of the the field $\mathbb{F}_2[X]/(P)$?
3. How many elements does the field $\mathbb{F}_2[X]/(P)$ contain?
4. Let α be the class of X modulo (P), show that
   a) $P(\alpha) = 0$
   b) $\alpha^4 = \alpha^2 + \alpha$
   c) α^2 is a root of $X^2 + \alpha X + 1 + \alpha^2$
   d) α^4 is a root of $X^2 + \alpha X + 1 + \alpha^2$

   Conclude that
   $$P = (X + \alpha)(X + \alpha^2)(X + \alpha + \alpha^2)$$

Exercise 7. The sequence of Fibonacci numbers is defined by $F_0 = F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$.

1. Show that there is a closed-form formula for F_n, given by
   $$F_n = \frac{\phi^n - \overline{\phi}^n}{\sqrt{5}},$$
   where $\phi = (1 + \sqrt{5})/2$ is the golden ratio, and $\overline{\phi} = (1 - \sqrt{5})/2 = -1/\phi$.

2. What is the approximate binary length of F_n?
3. Write a program computing F_n using this formula. What is a concrete issue with this approach? What happens for large values of n?
4. Show that
$$\begin{pmatrix} F_{n+2} \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} F_{n+1} \\ F_n \end{pmatrix}.$$
and therefore that
$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$
Write a program that uses this equality to compute the exact value of F_n.
5. Use the above equation to prove Cassini's identity:
$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$
6. Show that for all $n \geq 1$,
$$\begin{aligned} F_{2n-1} &= F_n^2 + F_{n-1}^2 \\ F_{2n} &= (F_{n-1} + F_{n+1})F_n = (2F_{n-1} + F_n)F_n = 2F_{n-1}F_n + F_n^2. \end{aligned}$$
Use this to write a program computing the exact value of F_n. Using memoization (i.e., keeping track of already-computed values), this is faster than computing F_n using the matrix formula, and much faster than using the definition.
7. Let $n \in \mathbb{N}$, $n > 1$. Show that $F_k \bmod n$ is a periodic sequence. The period of $F_k \bmod n$ is known as the Pisano period. Write a program that computes the Pisano period for small values of n; this gives: $1, 3, 8, 6, 20, 24, \ldots$ Observe (or better, prove) that the period mod mn is the least common multiple of the period mod m and the period mod n (Hint: it suffices to consider prime powers, and invoke the CRT).

Exercise 8. The goal of this exercise is to prove Mason's theorem. For any polynomial $P \in \mathbb{C}[X]$, define its radical as
$$\operatorname{rad} P(X) = \prod_{\alpha \text{ s.t. } P(\alpha)=0} (X - \alpha) \in \mathbb{C}[X].$$

1. Show that if $P \in \mathbb{C}^*$, then $\operatorname{rad} P = 1$.
2. Let $A, B, C \in \mathbb{C}[X]$ non zero and pairwise coprime polynomials, satisfying
$$A + B + C = 0.$$
Show that
$$\begin{vmatrix} A' & B' \\ A & B \end{vmatrix} = \begin{vmatrix} B' & C' \\ B & C \end{vmatrix} = \begin{vmatrix} C' & A' \\ C & A \end{vmatrix}.$$

3. Deduce from this that if $AB \neq C$, then
$$\deg\left(\frac{ABC}{\operatorname{rad} ABC}\right) < \deg(AB).$$

4. Show that if $\deg(ABC) > 0$ then
$$\max(\deg A, \deg B, \deg C) < \deg \operatorname{rad} ABC.$$

5. Conclude that for $n \geq 3$, the curve $x^n + y^n + z^n = 0$ cannot be parametrised by elements of $C[X]$

Exercise 9. A party trick consists in the following: ask a challenger to choose a polynomial $P \in \mathbb{Z}[X]$, and keep it secret from you. Your goal is to guess P, by querying your challenger with values x, and having her reply with the value $P(x)$. Show that you only need two queries. What if she had chosen a polynomial in $\mathbb{Q}$? In $\mathbb{F}_p$ for given p?

Exercise 10. Let $P \in \mathbb{Z}[X]$ of degree n, $P = a_n X^n + \cdots + a_1 X + a_0$, and $H = \max_{i \neq n} |a_i/a_n|$. We want to show the following result:

> *If there exists $N \in \mathbb{N}$, $N > H + 1$ such that $P(N) \in \mathfrak{P}$, then P is irreducible in $\mathbb{Z}[X]$.*

1. Assume that P has a root α (one may consider working in $\mathbb{C}[X]$). Show that $|\alpha| < H + 1$.

2. Assume that P is reducible. Show that therefore $P = QR$ satisfies $R(N) = \pm 1$ and write
$$R = c \prod_i (X - \alpha_i)$$
with $\alpha_i \in \mathbb{Z}$ and c is the leading coefficient of R. Use the previous result to show that $|R(N)| > 1$. Conclude.

3. Consider the polynomial $P = X^4 + 6X^2 + 1$. Show that one cannot use Eisenstein's criterion on P; show that $P(8)$ is prime, and therefore that P is irreducible in $\mathbb{Z}[X]$.

4. Consider the polynomial $P = (X - 9)(X^2 + 1)$, show that $P(10) = 101 \in \mathfrak{P}$. P is clearly reducible, what does this say about the statement at hand?

5. There exists a slightly stronger version of this result, known as Cohn's theorem: if P is constructed from that base 10 representation of a prime, such as
$$p = 65537 \in \mathfrak{P} \mapsto P_p = 6X^4 + 5X^3 + 5X^2 + 3X + 7$$
then P_p is irreducible in $\mathbb{Z}[X]$. Show that there exist at least a number $q \notin \mathfrak{P}$ such that P_q is irreducible.

Chapter 5

Finite fields

5.1 Finite fields of prime order

Theorem 36 (Wedderburn) *Every finite field is commutative.*

Lemma 15 (Characteristic of an integral domain) *Let A be an integral domain, then either* $\operatorname{char} A = 0$ *or* $\operatorname{char} A \in \mathfrak{P}$.

Proof: Let $f : \mathbb{Z} \to A$ the application defined by $f(m) = 1m$. It is a ring morphism, and therefore its kernel is an ideal of $\mathbb{Z}$. Since $\mathbb{Z}$ is a principal ideal domain, this means that there exists a unique $n \in \mathbb{Z}$ such that $\ker f = (n)$ — by definition, $n = \operatorname{char} A$.

As a result, $\mathbb{Z}/(n)$ is isomorphic to a subring of A, and is therefore an integral domain.

If n is non-zero, $\mathbb{Z}/(n)$ is a finite integral domain, hence it is a field (Theorem 22). Therefore $n \in \mathfrak{P}$. □

Lemma 16 *If K is a field of characteristic zero, then it contains a subfield that is isomorphic to $\mathbb{Q}$ (which is infinite).*

Proof: If K is of characteristic zero, then the map $\mathbb{Q} \to K$ defined by $a/b \mapsto a1(b1)^{-1}$ is a field morphism. Thus its image is a subfield of K which is isomorphic to $\mathbb{Q}$. □

Lemma 17 *If K is a field of characteristic p, then it contains a subfield that is isomorphic to $\mathbb{F}_p = \mathbb{Z}/(p)$.*

Proof: We have $m1 = 0$ if and only if $p|m$; the image of the map $m \mapsto m1$ is thus a subfield of K, isomorphic to $\mathbb{F}_p$. □

Corollary 20 (Characteristic of finite fields) *A finite field has prime characteristic.*

Corollary 21 (Order of finite fields) *Let K be a finite field. There exists an integer $n > 0$ and a prime $p \in \mathfrak{P}$ such that K has p^n elements.*

Proof: Let $p = \operatorname{char} K$. By the above lemma, K contains a subfield isomorphic to $\mathbb{F}_p$. This gives K a natural $\mathbb{F}_p$-vector space structure, and since K is finite, its dimension n as a vector space is also finite. Therefore as vector spaces $K \simeq \mathbb{F}_p^n$, and $|K| = p^n$. □

5.2 Finite fields of prime power order

Theorem 37 (Constructing finite fields of prime power order) *Let K be a finite field with p^n elements. Then there exists an irreductible polynomial $F \in \mathbb{F}_p[X]$ of degree n such that $K \simeq \mathbb{F}_p[X]/(P)$.*

Proof: Let α be a generator of $K^\times$, and define the application $f : \mathbb{F}_p[X] \to K$ by

$$f\left(\sum a_i X^i\right) = \sum a_i \alpha^i.$$

Then f is a ring morphism, and it is surjective because $\langle \alpha \rangle = K^\times$. The kernel of f is an ideal I of $\mathbb{F}_p[X]$, and therefore $\mathbb{F}_p[X]/I \simeq K$ as rings. Note that I is non-zero, because this would imply $K \simeq F_p[X]$ which is not a field. Therefore there exists $F \in \mathbb{F}_p[X]$ such that $I = (F)$; since $\mathbb{F}_p[X]/(P)$ is a field, the polynomial P is irreducible. Finally, the degree of P must be n so that the size of K matches p^n. □

Remark 32 What the above entails is that there exists a finite field with p^n elements if, and only if, there exists an irreducible polynomial of degree n in $\mathbb{F}_p[X]$. We will admit the following result.

Theorem 38 (Möbius) *Let $\mu : \mathbb{Z} \to \{-1, 0, 1\}$ be defined as*

$$\mu(n) = \begin{cases} (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct prime numbers} \\ 0 & \text{otherwise} \end{cases}$$

then the number of irreductible polynomials of degree d in $\mathbb{F}_p[X]$ is

$$\frac{1}{n} \sum_{d|n} \mu(d) p^{\frac{n}{d}}.$$

In particular, for every $n \geq 1$ and every $p \in \mathfrak{P}$, this quantity is strictly positive.

Corollary 22 *For every $n > 0$ and $p \in \mathfrak{P}$, there exists a finite field with p^n elements.*

Remark 33 Using the formula from Theorem 38, we see that there are 22517997465744 ways to construct a field of size 2^{50}. As we will now see, they are all isomorphic to one another.

Theorem 39 (Fields of same order are isomorphic) *If K and L are finite fields and $|K| = |L|$, then $K \simeq L$.*

Proof: We have $|K| = p^n$ with $p \in \mathfrak{P}$ by Corollary 21. Let $\alpha \in K^\times$ of order $p^n - 1$ (such an element necessarily exists) and consider the evaluation morphism a which maps polynomials in $\mathbb{F}_p[X]$ to K by mapping X to α. This is a surjective morphism, and its kernel is an ideal, which can be generated by a monic irreducible polynomial $P \in \mathbb{F}_p[X]$. Then $P|(X^{p^n} - X)$.

Now if $|L| = |K| = p^n$, we have for every $\ell \in L$, $\ell^{p^n} = \ell$, i.e., the sets of roots of the polynomial $X^{p^n} - X$ is exactly L. If r is any root of P, the evaluation morphism at r factors through $\mathbb{F}_p[X]/(P)$ and induces an isomorphism $K \simeq L$. □

Remark 34 We will henceforth talk of "the" finite field of size p^n, and write $\mathbb{F}_{p^n}$ to denote any construction of this field. The finite fields $\mathbb{F}_q$ are sometimes referred to as Galois fields, and denoted $GF(q)$.

Remark 35 Beware! The field $\mathbb{F}_2$ is isomorphic to $\mathbb{Z}/(2)$, but the field $\mathbb{F}_8 = \mathbb{F}_{2^3}$ is not isomorphic to $\mathbb{Z}/(8)$, which is not a field!

Remark 36 Although all finite fields are isomorphic to some $\mathbb{F}_q$, this isomorphism is not unique!

Example 24

- $\mathbb{F}_2 \simeq \mathbb{Z}/(2)$
- $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$
- $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1)$
- $\mathbb{F}_{16} \simeq \mathbb{F}_2[X]/(X^4 + X + 1)$; the polynomial $X + 2 + X$ generates a subfield of order 4.
- $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2 + X - 1)$

Remark 37 It is typical to represent a finite field element in $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P)$ by introducing a formal root α of P. This in turn allows for a compact machine representation of finite field elements as sequence of elements of $\mathbb{F}_p$. For instance, in $\mathbb{F}_4$ using the isomorphism $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$,

Element	With a formal root	Implemented as
0	0	$(0,0)$
1	1	$(0,1)$
X	α	$(1,0)$
$X+1$	$\alpha+1$	$(1,1)$

This representation is practical, but care should be taken when performing operations; as an example, $X \times X = X^2 = -X - 1 = X + 1$, which means $(1,0) \times (1,0) = (1,1)$. In the common case that $p = 2$, one can represent elements directly in binary, e.g., $1 + X$ will be represented as 11.

Theorem 40 (Subfields of $\mathbb{F}_{p^n}$) *Let $p \in \mathfrak{P}$ and $n > 0$. If K is a subfield of $\mathbb{F}_{p^n}$ then $K \simeq \mathbb{F}_{p^k}$ with $k|n$.*

Proof: Since K is a subfield of a finite field, it is finite, and therefore it is of order p^k for some k. By Lagrange's theorem (Theorem 11) if $\mathbb{F}_{p^k}$ is a subfield of $\mathbb{F}_{p^n}$, then $p^n = (p^k)^r$ for some integer r, and thus $k|n$.

Conversely, assume $k|n$, i.e. $n = kr$ for some integer r, then $p^n - 1 = (p^r - 1)\left(1 + \cdots + (p^r)^{k-1}\right) = (p^r - 1)N$. Now

$$\begin{aligned} X^{p^n} - X &= X\left(X^{p^{rk}-1} - 1\right) \\ &= X\left(X^{p^r-1} - 1\right)\left(1 + \cdots + X^{(p^r-1)(N-1)}\right). \end{aligned}$$

But since the roots of $X^{p^r} - X$ is exactly $\mathbb{F}_{p^r}$, it is contained in the field $\mathbb{F}_{p^n}$. □

Theorem 41 (Multiplicative groups of finite fields) *The group $\mathbb{F}_q^\times$ is cyclic, of order $q - 1$.*

Definition 46 (Primitive element) There are $\varphi(q-1)$ many choices for the generator of the group $\mathbb{F}_q^\times$. Such a generator is called a primitive element of $\mathbb{F}_q$.

Example 25 The field $\mathbb{F}_{2^5}$ has 32 elements, and the group $\mathbb{F}_{2^5}^\times$ is cyclic of order $2^5 - 1 = 31 \in \mathfrak{P}$ elements (this is a Mersenne prime); it is therefore isomorphic to $\mathbb{Z}/(31)$, and has 30 generators.

Remark 38 If α is a primitive element of $\mathbb{F}_q^\times$, then $\{\alpha, \alpha^2, \ldots, \alpha^{q-1}\}$ is a permutation of the elements in $\mathbb{F}_q^\times$. Given an element $x \in \mathbb{F}_q^\times$, an integer y such that $\alpha^y = x$ is called a discrete logarithm of x in base α.

Example 26 Let $p \in \mathfrak{P}$ and g be a primitive element of $\mathbb{F}_p^\times$. Consider the following game, played between Alice and Bob:

1. Alice picks a number $a \in \mathbb{F}_p^\times$ and computes $A = g^a$;

2. Bob picks a number $b \in \mathbb{F}_p^\times$ and computes $B = g^b$;
3. Alice send A to Bob ; Bob sends A to Alice; (over a possibly insecure channel)
4. Alice computes $K_A = B^a$;
5. Bob computes $K_B = A^b$.

Observe that $K_A = B^a = (g^b)^a = g^{b+a} = g^{a+b} = (g^a)^b = A^b = K_B$. Hence, Alice and Bob both know $K = K_A = K_B$. This is the principle of the Diffie–Hellman key exchange protocol (DHE).

If an eavesdropper captures the conversation between Alice and Bob, i.e., if A and B are known to the adversary, then computing K from this information is challenging — in fact, it seems there is no substantially faster way than solving the discrete logarithm problem in base g in $\mathbb{F}_p^\times$. The security of Diffie–Hellman key exchange, as employed today to secure Internet connections, relies on the assumption that this is intractable for well-chosen groups.

5.3 Exercise set

Exercise 1. Let $P = X^4 + X + 1$ in $\mathbb{F}_2[X]$.

1. Show that P is irreducible, and therefore that $\mathbb{F}_{16} \simeq \mathbb{F}_2[X]/(P)$. Can you find another irreducible polynomial of degree 4 in $\mathbb{F}_2[X]$?
2. Denote by α a formal root of P in $\mathbb{F}_{16}$. Write the multiplication table of $\mathbb{F}_{16}$.
3. The Galois counter mode (GCM) is an efficient and provably secure mode of operation for cryptographic block ciphers for use in authenticated encryption. It relies on multiplications in the finite field $\mathbb{F}_{2^{128}} \simeq \mathbb{F}_2[X]/(X^{128} + X^7 + X^2 + X + 1)$.
   a) Compute 2^{128}.
   b) Write a program that computes multiplications in $\mathbb{F}_{2^{128}}$. You may represent the field elements as hexadecimal numbers.
   c) Show that multiplication in $\mathbb{F}_{2^{128}}$ can be computed in parallel.

   Since 2010, Intel and AMD microprocessors include a dedicated `PCLMULQDQ` for fast operations of this kind.

Exercise 2. Let $R = X^8 + X^4 + X^3 + X + 1 \in \mathbb{F}_2[X]$ (also known as the Rijndael polynomial, as it appears in the design of the cryptographic block cipher of the same name, better known as the AES). Show that $\mathbb{F}_2[X]/(R) \simeq \mathbb{F}_{256}$. Let $X = \texttt{53}$ and $Y = \texttt{CA}$ where X and Y are written in hexadecimal (base 16) representation. Show that $XY = \texttt{01} = 1$, i.e., Y is the inverse of X.

Exercise 3. Let $p \in \mathfrak{P}$, $q = p^k$ for some integer $k > 0$, and an integer $m > 0$. Let $\alpha \in \mathbb{F}_{q^m}$. Show that the trace and norm of α are given by

$$\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \sum_{i=1}^{m} \alpha^{q^i} \quad \text{and} \quad N_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha) = \prod_{i=1}^{m} \alpha^{q^i}.$$

Chapter 6

Quadratic residues and reciprocity

This chapter is concerned with the computation of "square roots" in finite fields and rings. Such roots do not always exist, but when they do there are algorithms to compute them. There are abundant uses of the notions introduced in this chapter, both theoretical and practical.

6.1 Basic definitions

Definition 47 (Legendre symbol) Let $p \in \mathfrak{P}$, $p \geq 3$, and $n \in \mathbb{Z}$. The Legendre symbol of n by p is defined as

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{if } p|n \\ 1 & \text{if there exists } b \text{ such that } a \equiv b^2 \bmod n \\ -1 & \text{otherwise} \end{cases}$$

Example 27 We have $\left(\frac{2}{7}\right) = 1$, since $3^2 \equiv 2 \bmod 7$. However, $\left(\frac{3}{7}\right) = 0$.

Remark 39 Elements a of $\mathbb{F}_p$ such that $\left(\frac{a}{p}\right) = 1$ are called quadratic residues modulo p.

Proposition 8 (Multiplicative property) *Let $p \in \mathfrak{P}$ and $a, b \in \mathbb{Z}$, then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Remark 40 As a result, multiplying a quadratic residue with a quadratic residue is again a quadratic residue; multiplying non-quadratic residues together gives a quadratic residue; multiplying a quadratic residue together with a non-quadratic residue yields a non-quadratic residue.

Remark 41 The Legendre symbol can be defined on finite extensions: for instance $\mathbb{F}_q[X] \simeq F_p[X]/(P)$, by defining for every $Q \in \mathbb{F}_p[X]$

$$\left(\frac{Q}{P}\right) = \begin{cases} 0 & \text{if } P|Q \\ 1 & \text{if } Q \text{ is a non-zero square modulo } P \\ -1 & \text{otherwise} \end{cases}$$

Definition 48 (Character) Let G be a group. A character of G is a group morphism $G \to \mathbb{C}^*$.

Remark 42 This notion is extended to fields as follows: the character of a field K is the character of its multiplicative subgroup $K^\times$. The Legendre symbol is a character of $\mathbb{F}_p$ in that sense.

Lemma 18 (Roots of 1 in $\mathbb{F}_p$) *Let $p \in \mathfrak{P}$, $p > 2$, and $\beta \in \mathbb{F}_p$. Then $\beta^2 = 1$ if and only if $\beta \in \{-1, 1\}$.*

Proof: Only the reverse direction is not trivial. Assume $\beta^2 = 1$, and lift to $\mathbb{Z}$ as $b \equiv \beta \bmod p$. Then $b^2 \equiv 1 \bmod p$ which means that $p|(b^2-1)$; but $b^2-1 = (b-1)(b+1)$ and p is prime, therefore it divides one or the other of these factors. Hence $b \equiv \pm 1 \bmod p$, and the result follows. □

Corollary 23 *Let $p \in \mathfrak{P}$, $p > 2$, and $a, b \in \mathbb{F}_p^\times$. Then $a^2 = b^2$ if and only if $a = \pm b$.*

Corollary 24 (Number of quadratic residues) *There are $(p-1)/2$ squares in $\mathbb{F}_p^\times$.*

Remark 43 In other words, for every odd prime p, exactly half the elements of $\mathbb{F}_p^\times$ are squares, and half are non-squares.

6.2 Euler's criterion

A natural question is to find efficient ways to compute the Legendre symbol. Euler's criterion provides a first tool in that direction.

Theorem 42 (Euler's criterion) *Let $p \in \mathfrak{P}$, $p > 2$, and $a \in \mathbb{F}_p^\times$. Then*

$$a^{(p-1)/2} = \left(\frac{a}{p}\right).$$

Example 28 We have $3^{(7-1)/2} = 3^3 = -1 \bmod 7$ and $4^{(7-1)/2} = 4^3 = 1 \bmod 7$. This is a more systematic way to address Example 27.

Proof: First note that, by Euler's theorem (Theorem 16), $a^{p-1} \equiv \left(a^{(p-1)/2}\right)^2 = 1 \bmod p$, which by Lemma 18 shows $a^{(p-1)/2} \equiv \pm 1 \bmod p$. If a is a quadratic residue modulo p, then there exists $b \in \mathbb{F}_p^\times$ such that $a = b^2$; using Euler's theorem again we have $a^{(p-1)/2} \equiv b^{p-1} \equiv 1 \bmod p$.

Now assume that a is not a quadratic residue. Wilson's theorem (Corollary 18) gives $\prod_{b \in \mathbb{F}_p^\times} b \equiv -1 \bmod p$. Now we will see that this product is in fact equal to $a^{(p-1)/2}$: indeed, let C be the set of pairs $(u, v) \in (\mathbb{F}_p)^2$ such that $uv = a$. Note that for any given u the corresponding v is uniquely determined, and $u \neq v$ (otherwise a would be a square, which would be a contradiction). Therefore every element of $\mathbb{F}_p^\times$ belongs to exactly one pair in C; as a result

$$\prod_{b \in \mathbb{F}_p^\times} b = \prod_{(u,v) \in C} uv = \prod_{(u,v) \in C} a = a^{(p-1)/2}$$

which finishes the proof. □

Remark 44 All the above results apply to $\mathbb{F}_q$, where $q = p^k$, by replacing $p - 1$ in the exponents with $\varphi(q)$.[1]

Lemma 19 *A number a is a quadratic residue modulo $q = p^k$ if and only if it is a quadratic residue modulo p.*

Proof: Suppose that a is a quadratic residue modulo q, then $p \nmid a$ and $a \equiv b^2 \bmod q$ for some integer b. It follows that $a \equiv b^2 \bmod p$, and therefore a is a quadratic residue modulo p.

Suppose now that a is not a quadratic residue modulo q, and assume that $p \nmid a$. Then Euler's criterion gives

$$a^{\varphi(q)/2} \equiv -1 \bmod q$$

which also holds modulo p since $p|q$; by applying several times Fermat's little theorem we get

$$a \equiv a^p \equiv a^{p^2} \equiv \cdots \equiv a^{p^k - 1} \bmod p$$

which gives

$$-1 \equiv a^{p^{k-1}(p-1)/2} \equiv a^{(p-1)/2} \bmod p.$$

Thus, by Euler's criterion again, a is not a quadratic residue modulo p. □

[1] However, the proof of Lemma 18 must be completed by explaining that q, while not prime, cannot divide both $(b-1)$ and $(b+1)$, as otherwise it would divide their difference, which is impossible since p is odd.

Theorem 43 (Roots of -1 in $\mathbb{F}_p$) *Let $p \in \mathfrak{P}$, $p > 2$. Then -1 is a quadratic residue modulo p if and only if $p \equiv 1 \bmod 4$.*

Proof: By Euler's criterion,

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \bmod p.$$

If $p \equiv 1 \bmod 4$ then the power on the right-hand side is even, and therefore -1 is a quadratic residue. Otherwise, $p \equiv 3 \bmod 4$ and the power is odd, which shows that -1 is not a quadratic residue.

□

Corollary 25 (Congruence of primes) *There are infinitely many primes p such that $p \equiv 1 \bmod 4$; and infinitely many primes such that $p \equiv 3 \bmod 4$.*

Proof: Suppose that there are only finitely such primes and call M their product. Let $N = 4M^2 + 1$, and consider a prime p dividing N. Now p cannot satisfy $p \equiv 1 \bmod 4$, as it would otherwise divide both $4M^2$ and N, and therefore their difference $N - 4M^2 = 1$, which is impossible. Furthermore, p is odd because N is odd. Moreover, $(2M)^2 \equiv -1 \bmod p$, i.e., -1 is a quadratic residue modulo p, and by Theorem 43 this implies $p \bmod 1 \bmod 4$. Therefore there are infinitely many primes of the form $4k + 1$.

A similar argument (using $N = 4M - 1$) shows that there are infinitely many primes of the form $4k + 3$. □

Remark 45 An easy but very useful result is that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \bmod 8 \\ -1 & \text{if } p \equiv \pm 3 \bmod 8 \end{cases} = (-1)^{(p^2-1)/8}.$$

Together with Theorem 43 and the next section's key theorem, this enables the efficient computation of any Legengre symbol.

Remark 46 Using the Chinese remainder theorem (Theorem 14), it is easy to see that if $n = p_1^{e_1} \cdot p_k^{e_k}$, a number a is a quadratic residue modulo n if an only if it is a quadratic residue modulo $p_i^{e_i}$ for each $i = 1, \ldots, k$. In particular, when this is the case, a has 2^k square roots modulo n.

Remark 47 The above remark motivates the definition of a Legendre-like symbol, defined for arbitrary moduli n. This is the Jacobi symbol defined as

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \times \cdots \times \left(\frac{a}{p_k}\right)^{e_k}$$

for non-zero $n = p_1^{e_1} \cdots p_k^{e_k}$. Note however that in general, $\left(\frac{a}{n}\right) = 1$ does not imply that a is a quadratic residue! Indeed, it may happen that $\left(\frac{a}{p_i}\right) = -1$ for a pair of indices i, so that $-1 \times -1 = 1$ in the above expression.

6.3 Quadratic reciprocity

Gauss is famous for producing the first (six!) rigorous proofs of the following result

Theorem 44 (Law of quadratic reciprocity) *Let p, q be odd primes. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

In other terms, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if and only if at least one of p and q is congruent to 1 modulo 4.

To prove the theorem, following an idea of Eisenstein, we use the following easy lemma:

Lemma 20 *For any positive odd integer m,*

$$\frac{\sin mx}{\sin x} = (-4)^{(m-1)/2} \prod_{t=1}^{(m-1)/2} \left(\sin^2 x - \sin^2 \frac{2\pi t}{m}\right).$$

There are several ways to check this identity, which we leave as a rather easy exercise for the reader.

Proof: Now let $S = \{0, 1, \ldots, (p-1)/2\}$, and for any $s \in S, x \in \mathbb{F}_p^\times$, define $\epsilon_s(x) \in \{\pm 1\}$ so that $\epsilon_s(x)sx \in S$. The map $\sigma : s_x \mapsto \epsilon_s(x)sx$ from S to S is injective, and therefore bijective because S is finite. Thus for any $a \in \mathbb{F}_p^\times$, $as = \epsilon_s(a)\sigma_a(s)$. Therefore

$$\prod_{s\in S} as = \prod_{s\in S} \epsilon_s(a)\sigma_a(s)$$
$$a^{(p-1)/2} \prod_{s\in S} s = \prod_{s\in S} \epsilon_s(a) \prod_{s\in S} \sigma_a(s)$$

which gives, by Euler's criterion (Theorem 16)

$$\left(\frac{a}{p}\right) = \prod_{s\in S} \epsilon_s(a).$$

Now, since $qs = \epsilon_s(q)\sigma(q)$, we have

$$\sin\left(\frac{2\pi s}{p} q\right) = \epsilon_s(q) \sin\left(\frac{2\pi}{p}\sigma(q)\right),$$

therefore,

$$\begin{aligned}
\left(\frac{q}{p}\right) &= \prod_{s\in S} \epsilon_s(q) \\
&= \frac{\prod_{s\in S} \sin\left(\frac{2\pi s}{p} q\right)}{\prod_{s\in S} \sin\left(\frac{2\pi}{p}\sigma(q)\right)} \\
&= \prod_{s\in S} \frac{\sin\left(\frac{2\pi s}{p} q\right)}{\sin\left(\frac{2\pi}{p}\sigma(q)\right)} \\
&= \prod_{s\in S} (-4)^{(q-1)/2} \prod_{t=1}^{(q-1)/2} \left(\sin^2\frac{2\pi s}{p} - \sin^2\frac{2\pi t}{q}\right)
\end{aligned}$$

where in the last line we used the identity discussed at the beginning of this proof, with $m = q$ and $x = 2\pi s/p$. Introducing $T = \{0, 1, \ldots, (q-1)/2\}$, we see that

$$\left(\frac{q}{p}\right) = (-4)^{(p-1)(q-1)/4} \prod_{s\in S} \prod_{t\in T} \left(\sin^2\frac{2\pi s}{p} - \sin^2\frac{2\pi t}{q}\right).$$

Swapping p and q and following the same steps, we obtain

$$\left(\frac{p}{q}\right) = (-4)^{(p-1)(q-1)/4} \prod_{s\in S} \prod_{t\in T} \left(\sin^2\frac{2\pi t}{q} - \sin^2\frac{2\pi s}{p}\right),$$

or in other words,

$$\left(\frac{p}{q}\right) = (-1)^{|S|\cdot|T|} \left(\frac{q}{p}\right).$$

Since $|S| \cdot |T| = (p-1)(q-1)/4$, this concludes the proof. □

Algorithm 5 (Computing Legendre and Jacobi symbols) *The law of quadratic residuosity (LQR for short) makes it very practical to compute Legendre and Jacobi symbols, in a way reminiscent of Euclid's algorithm for the* gcd*:*

1. *Input a, n two integers.*
2. *Set $\sigma \leftarrow 1$*
3. *Repeat forever*
   a) $a \leftarrow a \bmod n$
   b) *If $a = 0$ then*
      - *If $n = 1$ then return σ otherwise return 0*
   c) *Compute a' such that $a = 2^h a'$ and a' is odd.*
   d) *If $h \not\equiv 0 \bmod 2$ and $n \not\equiv \pm 1 \bmod 8$ then $\sigma \leftarrow -\sigma$*
   e) *If $a' \not\equiv 1 \bmod 4$ and $n \not\equiv 1 \bmod 4$ then $\sigma \leftarrow -\sigma$*
   f) *Swap: $(a, n) \leftarrow (n, a')$*

Example 29 Let's compute the following Legendre symbol, step by step:

$$\begin{aligned}
\left(\frac{29}{43}\right) &\overset{\text{LQR}}{=} \left(\frac{43}{29}\right) \\
&\overset{\text{mod } 29}{=} \left(\frac{14}{29}\right) \\
&\overset{\text{Prop. } 8}{=} \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) \\
&\overset{\text{Rem. } 45}{=} -\left(\frac{7}{29}\right) \\
&\overset{\text{LQR}}{=} -\left(\frac{-29}{7}\right) \\
&\overset{\text{mod } 7}{=} -\left(\frac{-1}{7}\right) \\
&= -1.
\end{aligned}$$

Remark 48 For odd, composite n, if we know the factorization of n, then we can also determine if a is a quadratic residue modulo n by determining if it is a quadratic residue modulo each prime divisor p of n. If we do not know the factorisation of n, in general not much can be said.

Open question (2018): Let $a_i = \left(\frac{x}{p_i}\right)$ where $p_1 = 2, p_2, \ldots \in \mathfrak{P}$ and x is some integer. Given the sequence $(a_i)_{i \geq 1}$, can one efficiently recover x?

Remark 49 The proof given here of the LQR seems unnecessarily contrived and doesn't shed must light on what's happening. Finding simpler proofs, and generalising this result to moge settings (cubic, quartic reciprocity, etc.) was one of the driving forces behind algebraic number theory.

6.4 Modular square roots

Let p be an odd prime, and a be a quadratic residue modulo p.

Proposition 9 *Assume $p \equiv 3 \bmod 4$, then $b = a^{(p+1)/4}$ is a square root of a.*

Proof: It suffices to check that $4 \mid p+1$ and use Fermat's little theorem. □

Remark 50 It is also possible to compute a square root in the case $p \equiv 1 \bmod 4$, but the corresponding algorithm is less straightforward. For details see (TODOdetails or reference)

Remark 51 Let $P = aX^2 + bX + c$ be a polynomial of degree 2 defined on $\mathbb{F}_q[X]$, where $2 \nmid q$. Let $\Delta = b^2 - 4ac$. Then P has roots in $\mathbb{F}_q$ if and only if Δ is a quadratic residue modulo q; in that case let e be a root of Δ, and we can express the roots as $\alpha_1 \pm = (-b \pm e)2^{-1}a^{-1}$.

(TODO: maybe explain Hensel lifting to compute sqroots in $q = p^k$)
(TODO: finding whether a is a QR mod n is equivalent to factoring n)

6.5 Exercise set

Exercise 1. Let $\mathbb{F}_q$ be a finite field, the Jacobsthal matrix of $\mathbb{F}_q$ is defined as

$$Q = \left(\left(\frac{i-j}{q}\right)\right)_{i,j\in\mathbb{F}_q}$$

i.e., the matrix that indicates on row i and column j whether $i-j$ is a quadratic residue modulo q.

1. Show that Q is symmetric if $q \equiv 1 \bmod 4$. Show that Q is skew-symmetric if $q \equiv 3 \bmod 4$.
2. Write a program that computes Q for a given $q = p^k$.
3. Show that each row of Q sums to zero, i.e., $QJ = 0$, where J is the $q \times q$ matrix with all entries set to 1. Show that $JQ = 0$. Show that $QQ^\top + J \equiv 0 \bmod q$.
4. Assume that $q \equiv 3 \bmod 4$, and define the matrix

$$H = I_{q+1} + \begin{pmatrix} 0 & \mathbf{1}^\top \\ -\mathbf{1} & Q \end{pmatrix}$$

where I_k is the $k \times k$ identity matrix, and $\mathbf{1}$ is the all-one column vector of size q. Show that $H + H^\top = 2I_{q+1}$. This makes H a (skew) Hadamard matrix of order $2(q+1)$, which can be used to design error-correcting codes. The above construction is due to Raymond Paley (1933), and was a breakthrough in the following problem:

> **Open question (2018)**: Are there Hadamard matrices of size m, for all m divisible by 4?

This is known as the Hadamard conjecture. Paley's construction found Hadamard matrices of all possible sizes up to 100, except 92 (which was later found using other methods). As of 2018, it is unknown whether there is a Hadamard matrix of size $m = 668$.

Exercise 2. The point of this exercise is to show two easy corollaries of the following result (due to Gauss):

> *A positive integer is the sum of three squares if and only if it is not of the form* $4^a(8b-1)$ *for integers* a, b.

1. Let $n \in \mathbb{N}$, $n > 0$. Show that the above statement implies

$$x_1^2 + x_2^2 + x_3^2 = 8n + 3$$

has integer solutions x_1, x_2, x_3.

2. Compute the set of quadratic residues modulo 8, and show that the x_i are odd.

3. A triangular number is of the form $1 + 2 + 3 + \cdots + k$ for some k. Prove the following statement (originally due to Gauss):

   Every positive integer is the sum of three triangular numbers.

4. Let $n \in \mathbb{Z}$, $n > 0$. Write $n = 4^k m$ with $4 \nmid m$. Prove the following statement (originally due to Lagrange):

   Every positive integer is the sum of four squares.

Exercise 3. Consider the equation $E : y^2 = x^3 + x + 3$. If K is a field, we denote by $E(K)$ the set of solutions to E in $K \times K$.

1. Show that $E(\mathbb{R})$ is infinite. Plot this curve in the range $(-10, 10) \times (-10, 10)$.
2. Let $p \in \mathfrak{P}$. Show that $|E(\mathbb{F}_p)| \leq p - 1$. Write a computer program that outputs $|E(\mathbb{F}_p)|$.
3. Let $p \in \mathfrak{P}$. Show that if $P = (x, y) \in E(\mathbb{F}_p)$, then $-P = (x, -y)$ is also a solution.
4. Assume $\operatorname{char} K \neq 2, 3$. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points of K, $P \neq Q$ and $P \neq -Q$. Write the equation for the line through P and Q.
5. Assume $P \in E(K)$. Write the equation for the tangent line at P.
6. Assume $P, Q \in E(K)$, $P \neq Q$ and $P \neq -Q$. Show that the line through P and Q intersects with $E(K)$ at a third point R.
7. Assume $P \in E(K)$. Show that the tangent line at P intersects with $E(K)$ at a second point, which we call by convention $2P$.
8. We introduce the following notation: if $P, Q, R \in E(K)$ are distinct aligned points, we write $P + Q + R = 0$. By convention we also set $P + (-P) = 0$, and $P + P = 2P$, with $2P$ defined as in the previous point.

   a) Show that 0 is the neutral element for operation $+$ on E.

   b) Show that for any $P, Q \in E(K) \cup \{0\}$, $P + Q = Q + P$.

   c) Show that for any $P, Q, R \in E(K) \cup \{0\}$, $(P + Q) + R = P + (Q + R)$ (you may want to show this graphically).

   All these properties turn $E(K) \cup \{0\}$ into an Abelian group, called the group of rational points of the elliptic curve E.

9. Show that if $K = \mathbb{F}_q$ then this group is cyclic. How can one find a generator for it?
10. The integer $2^{1279} - 1$ is a Mersenne prime. Implement elliptic curve operations in the field $\mathbb{F}_{2^{1279}-1}$.

Part II

Applications

Chapter 7

Primality testing and factorisation

7.1 Introduction

We have highlighted the relevance of prime numbers in algebra. In this chapter we develop algorithmic tools to tell whether a number is prime. This is especially important to cryptographic applications; we will also quickly discuss algorithms to find the factorisation of a composite number.

7.2 Basic definitions

Definition 49 (Smooth integer) Let $B > 0$. An integer $n \in \mathbb{Z}$ is B-smooth if all the prime factors of n are smaller than B.

Remark 52 For relatively small values of B, testing for B-smoothness can be done efficiently by trial division.

Remark 53 In 1947, William H. Mills proved the existence of a number A such that, for every natural number n,

$$\left\lceil A^{3^n} \right\rceil \in \mathfrak{P}.$$

However... the value of A, called Mill's constant, is unknown! Under the Riemann hypothesis[1], its value can be estimated as

$$A \approx 1.306377883863080690468614492 6\ldots$$

Naturally, not much is known about this number (not even whether it is rational...). As of 2018, it is known that the number obtained with $n = 11$ is indeed prime

(TODOexplain the Solovay–Strassen algorithm)

[1] In particular, the Riemann hypothesis implies that there exists a prime between any two consecutive cubes.

Chapter 8

Error-correcting codes

8.1 Introduction

Communication at a distance is never a perfect process. A signal is usually corrupted on its way to the receiving end of a communication channel, the precise nature of this corruption depending on the channel's physical properties. The purpose of error-correcting codes is to send messages so that the receiving end can detect, and even maybe correct, incorrect parts of a message. Thus the physical nature of a channel can be abstracted out, and we can build protocols on top of this abstraction.

A simple, yet ineffective approach consists in repeating the message multiple times; algebraic tools provide much more effective codes, as well as important theorems about the properties of wide classes of solutions.

8.2 Basic definitions

Definition 50 (Code) A code $C = (X, Y, \mathsf{Enc} : X \to Y, \mathsf{Dec} : Y \to X)$ is the data of two sets and two algorithms, respectively called the set of words, set of codewords, encoding algorithm, and decoding algorithm, satisfying the following correctness property:

$$\forall x \in X, \quad \mathsf{Dec}\left(\mathsf{Enc}(x)\right) = x.$$

Remark 54 Some authors use a more restrictive definition of a code, sometimes confusing Y with the code itself. This makes sense when working with codes in systematic form (see below), because encoding is straightforward. We adopt here a slightly more general setting, and will therefore call "code" the 4-tuple $C = (X, Y, \mathsf{Enc} : X \to Y, \mathsf{Dec} : Y \to X)$, refering to Y itself as the "codebook" or the set of codewords.

Example 30

- The trivial code on a set of words X is $1_X = (X, X, \mathsf{id}, \mathsf{id})$.

- If $C_1 = (\mathsf{Enc}_1, \mathsf{Dec}_1, X_1, Y_1)$ and $C_2 = (\mathsf{Enc}_2, \mathsf{Dec}_2, X_2, Y_2)$ are codes, and $Y_1 \simeq X_2$, then C_3 defined by

$$\mathsf{Enc}_3 = \mathsf{Enc}_2 \circ \mathsf{Enc}_1, \qquad \mathsf{Dec}_3 = \mathsf{Dec}_1 \circ \mathsf{Dec}_2, \qquad X_3 = X_1, \qquad Y_3 = Y_2$$

  is a new code.

- Let k be an odd integer, $X = \{0,1\}$, $Y = \{0,1\}^k$, Enc being the function that takes 0 (resp. 1) to the binary string made of k zeros (resp. ones), and Dec being the majority function, which returns whichever digit is most represented in its input. This defines the k-repetition code R_k.

Remark 55 In general, the message to be transmitted will be written using a fixed number of symbols k from a fixed alphabet F, i.e., we will have $X \subseteq F^k$. Similarly, the codewords can be considered as words written from an alphabet E, i.e., $Y \subseteq E^n$. When $|E| = |F|$, as will often be the case, the ratio k/n is called the code's information rate.

Definition 51 (Hamming distance) Let $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ two elements from a set E^n. The Hamming distance between x and y is the number of indices i such that $x_i \neq y_i$. It is denoted $d_H(x, y)$.

Definition 52 (Minimal distance) Let $C = (X, Y, \dots)$ be a code. The minimal distance of C is the integer

$$d = \min_{y_1 \neq y_2 \in Y} d_H(y_1, y_2).$$

Example 31

- The k-repetition code has minimal distance k (in fact the distance between any two codewords of this code is k).

- The following code has minimal distance $d = 3$:

$$Y = \{010101, 101010, 111111, 000000\}.$$

We can now address the question we set out to deal with, namely the problem of imperfect transmission of information. The situation can be modelled as follows: the sender wishes to emit some message $m \in X$; to do so, she uses a code C and actually sends $c \in Y$ over the channel; but the channel is imperfect and therefore the recipient receives $y' \in Y$.

Theorem 45 (Correction capacity) *Let d be the minimal distance of C, then up to t errors can be corrected, where*

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

In that case C is called a t-error correcting code.

Proof: Let $B(y, \rho)$ denote the sphere of center y and radius ρ, i.e.,

$$B(y, \rho) = \left\{ y' \in F^n \mid d_H(y, y') \leq \rho \right\}.$$

By definition of d, for any $y \neq y' \in Y$, the spheres $B(y, t)$ and $B(y', t)$ are disjoint. Therefore it is not possible to have $y' \in F^n$ such that $d_H(y, y') < t$ and y, y' belong to separate spheres. □

Remark 56 A code such that $F_n = \bigcup_{y \in Y} B(y, t)$ is called a perfect code. Needless to say, this does not happen often; in general, there are elements of F^n that cannot be safely attributed to an original codeword: we know that there was a mistake, but cannot correct it.

Example 32

- The k-repetition code has correcting capacity $t = (k-1)/2$.
- The following code can detect 2 errors and correct at most 1:

$$Y = \{010101, 101010, 111111, 000000\}.$$

8.3 Linear codes

Definition 53 (Linear code) Let $p \in \mathfrak{P}$, $\ell \geq 1$, $q = p^\ell$. A (n, k, d)-linear code is a code of minimal distance d such that Y is a k-dimensional vector subspace of $\mathbb{F}_q^n$.

Remark 57 Since linear codes are very common, it is useful to recall standard names for the parameters:

- n is called the code's length
- k is called the code's dimension
- d is always the minimal distance.

In fact, linear codes are so common that some authors do not bother being explicit; they may refer to $[n, k, d]_q$ codes, which quite often corresponds to a (n, k, d)-linear code over $\mathbb{F}_q$.

Remark 58 The minimal distance of a linear code can be expressed as $d = \min_{0 \neq y \in Y} d_H(y, 0)$.

Example 33 The code defined by

$$Y = \{0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111\}$$

is a linear code of length $n = 4$ and dimension $k = 3$ over $\mathbb{F}_2$, it has minimal distance $d = 2$.

Theorem 46 (Singleton) *Let C be a (n, k, d)-linear code. Then $d \leq n - k + 1$.*

Proof: Let (e_i) be the canonical basis of $\mathbb{F}_q^n$. Let $E = \langle e_1, \ldots, e_{n-k+1} \rangle$. Since $\dim E + \dim Y > n$, $E \cap Y$ is non-empty and not reduced to 0; therefore there exists $y \in Y$ such that $d_H(y, 0) \leq n - k + 1$. □

Definition 54 (Maximum distance separable code) A (n, k, d)-linear code C that satisfies $d = n - k + 1$ is called a maximum distance separable, or MDS code.

Remark 59 A consequence of Singleton's theorem is that $d/n + k/n < 1 + 1/n$, which means that one cannot hope to have linear codes with high correction capacity (i.e., large d) and simultaneously high information rate (i.e., small n). In that regard MDS codes are the linear codes that strike the optimal balance.

Definition 55 (Generating and parity matrices) The generating matrix of C is the matrix G of a basis of Y. A parity matrix for G is a matrix H such that $GH^\top = 0$.

Remark 60 Thus for linear codes, encoding is performed by matrix multiplication, which is well-known. We will therefore not describe the Enc algorithm in detail.

Remark 61 Consider a linear code generated by G, and the corresponding parity matrix H. A message m is encoded as $c = mG$, and received with some error: $c' = mG + r$. Now by computing $cH^\top = mGH^\top + rH^\top = rH^\top \neq 0$, we already detect an error. The remainder, $s = rH^\top$ is called the syndrome. To correct the error (if possible), we have to find r such that $d_H(r, 0) \leq t$ and $rH^\top = s$. This approach is called syndrome decoding.

Example 34 Consider the following matrix:

$$lm220K, p145, ex7.8 \tag{8.1}$$

Definition 56 (Systematic form) A (n, k, d)-linear code C is systematic if there exists a matrix B with k lines and $n - k$ rows, such that $G = (I_k|B)$ is a generating matrix for C. If such a matrix exist, it is unique, and the corresponding parity matrix is equal to $H = (-B^\top|I_{n-k})$. We refer to such G and H as matrices in systematic form.

Remark 62 One interest of codes in systematic form is that one can directly "read" the codewords, as the first k components are just the original message. The remaining $n - k$ components form the "redundancy".

Example 35 Consider the following generating matrix:

$$G = \overbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}^{I_3} \begin{matrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{matrix}$$

in systematic form. To encode a message $m \in \mathbb{F}_2^3$, we simply compute mG (which is equivalent here to taking the row of G corresponding to m, when $m \neq 0$). Every codeword thus has length 5, and the code's minimal distance is $d = 2$.

Theorem 47 (Characterisation of systematic codes) *Let C be a linear code and $G = (g_{i,j})$ a generating matrix for C. Then C is systematic if and only if the matrix $\widetilde{G} = (g_{i,j})_{1 \leq i,j \leq k}$ is invertible.*

Proof: If C is systematic, and G in systematic form, then $\widetilde{G} = I_k$ is clearly invertible. If G is not in systematic form then it is related to the systematic form matrix by an invertible transformation, and is therefore invertible.

Conversely, if $\widetilde{G}$ is invertible, then using Gauss' reduction we bring G to systematic form while keeping G a generating matrix at each operation. □

Definition 57 (Equivalent codes) Two linear codes C_1 and C_2 are equivalent if there exists a permutation $\sigma \in \mathfrak{S}_n$ such that every $\sigma(Y_2) = Y_1$, where σ acts as $\sigma((x_1, \ldots, x_n)) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)})$ on each element.

Theorem 48 (Equivalence with a systematic code) *Every code is equivalent to a systematic code.*

Proof: Let C be a (n, k, d)-linear code on $\mathbb{F}_q$, with generating matrix G. There exists a $k \times k$ submatrix $\widetilde{G}$, extracted from G, which is invertible, i.e., if g_i denote the columns of G, then the columns of $\widetilde{G}$ are g_{j_i} with $j_1 < \cdots < j_k$. Let $\sigma \in \mathfrak{S}_n$ be defined by

$$\sigma(i) = \begin{cases} j_i & \text{if } 1 \leq i \leq k \\ i & \text{if } k+1 \leq i \leq n \end{cases}$$

On the one hand this generates a code that is equivalent to C, with permutation σ. On the other hand the matrix $\widetilde{G}$ is invertible and therefore the code is systematic. □

Example 36 Consider the following generating matrix

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

This matrix defines a binary linear code of length 5, dimension 3, and distance 1; but it is not systematic as the 3×3 submatrix extracted from G is not invertible. But we can construct an equivalent code by reordering the columns from G, giving

$$G' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

We can then use Gauss' reduction to put G' in systematic form

$$G'' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

In particular, the length and dimension are left unchanged, and the distance is still 1, as clearly visible from G''.

Definition 58 Let $r > 0$, α be a generator of $\mathbb{F}_{2^r}^\times$ of order $n = 2^r - 1$, and consider the map $f : \mathbb{F}_2^n \to \mathbb{F}_{2^r}$ defined by

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \alpha_i.$$

Let $Y = \ker f$, which is a vector subspace of $\mathbb{F}_2^n$. This gives a (n, k, d)-linear code C known as the binary Hamming code of length $2^r - 1$.

Proposition 10 (Minimal distance of the binary Hamming code) *The binary Hamming code of length $2^r - 1$ has minimal distance $d = 3$.*

Proof: If there was $y \in Y$ satisfying $d_H(y, 0) = 1$, then we would have $\alpha^i = 0$ for some i, which cannot be; similarly $d_H(y, 0) = 1$ would imply $\alpha^{j-i} = 1$ for some $1 \leq i < j \leq n$. Therefore the minimal distance of C is $d \geq 3$.

Let G be a generating matrix for C and H the corresponding parity matrix. Every pair of columns c_i, c_j of H is distinct, and therefore H contains each non-zero r-column vectors with coefficients in $\mathbb{F}_2$. Thus adding any two columns of H results in a column that is already in H, i.e., $d \leq 3$. □

8.4 Cyclic codes

Definition 59 (Cyclic code) A code is cyclic if any rotation of a codeword is again a codeword.

Example 37 The k-repetition code is cyclic.

Proposition 11 (Characterisation of cyclic codes) *A (n, k, d)-linear code C is cyclic if and only if its image by the isomorphism $\psi : \mathbb{F}_q^n \simeq \mathbb{F}_q[X]/(X^n - 1)$ defined by*

$$\psi(x_1, \ldots, x_n) = x_1 X^{n-1} + \cdots + x_{n-1} X + x_n$$

is an ideal.

Proof: A rotation corresponds to multiplication by X, so C is cyclic if and only if $\psi(Y)$ is stable under multiplication by X, and therefore by any element from $\mathbb{F}_q[X]$. It is, in other words, an ideal. □

Corollary 26 *The set of cyclic linear codes of length n is in bijection with monic polynomials that divide $X^n - 1$.*

Remark 63 This means that we can refer to a cyclic code C by this polynomial g_C, called the generating polynomial of C. Concretely, we can encode a message as follows: let $m = (x_1, \ldots, x_k) \in \mathbb{F}_q^k$, and define

$$p_m = c_1 X^{n-1} + \cdots + x_k X^{n-k}.$$

Compute the Euclidean division of p_m by g_C, which gives a remainder p_r. The encoding is therefore $p_m + p_r$, which is in systematic form.

(TODO: explain BCH/Reed Solomon/Golay)

8.5 Exercise set.

Exercise. Credit card numbers are encoded using the Code!Luhn code, which works as follows: a last digit is added, so that the sum of all digits (including the last one) modulo 10 gives zero. Is that a code? It is linear, cyclic? How many errors can it detect? How many can it correct?

Exercise. Let C be a linear code, with codeword matrix Y. We define

- The dual code $C^\dagger$ given by $Y^\dagger = \{y' \in \mathbb{F}_q^n \mid \forall y \in Y, y \cdot y' = 0\}$.
- The extended code C^+ given by $Y^+ = \{(x_1, \ldots, x_{n+1}) \in \mathbb{F}_q^{n+1} \mid (x_1, \ldots, x_n) \in Y, x_1 + \cdots + x_{n+1} = 0\}$.

Show that there are indeed codes. Show that $(C^\dagger)\dagger$ is equivalent to C. For each code, compute the minimal distance, then give a generating and parity matrix.

Exercise. Show that the Hamming code of length $7 = 2^3 - 1$ is perfect, has a correction capacity of 1, but is not MDS.

Exercise. The purpose of this exercise is to study a correcting code used for the French Minitel, which we will refer to as the Minitel code.

1. Let $P = X^7 + X^3 + 1$. Show that $\mathbb{F}_2[X]/(P) \simeq \mathbb{F}_{128}$, and that X is a generator of $\mathbb{F}_{128}^\times$.
2. To send a 15-byte message, i.e., 120 bits $a_0, a_1, \ldots, a_{119} \in \mathbb{F}_2$, we write

   $$c = a_0 X^{126} + \cdots + a_{119} X^7$$

   which can also be written $c = a_{120} X^6 + \cdots + a_{126}$. The codeword sent is $a_0, a_1, \ldots, a_{126}, a_{127}$, where a_{127} is a parity bit computed so that $a_0 + \cdots + a_{127} = 0$. (Thus the complete codeword fits in 16 bytes).

   a) How many errors can the parity bit detect? Correct?

   b) We receive $a'_0, \ldots, a_1 26', a_1 27'$ with a correct parity bit. Show that $a'_0 X^{126} + \cdots + a'_{126} = 0$.

   c) Assume that there is only one error, i.e., a single $a'_i \neq a_i$. Can one recover the original message?

Exercise. Show that the set of cyclic linear codes of length n is in bijection with the set

$$S_q = \{I \subseteq (\mathbb{Z}/(n))^\times \mid \forall u \in I, uq \in I\}.$$

.

Chapter 9

Digital signature schemes

9.1 Introduction

A digital signature should play the role of traditional signatures, i.e., authentify a document as being produced (or recognised as valid) by an identified person. Fundamentally, this requires this person to produce some information — some number — in a way that other people cannot. The first public solution was proposed in 1978 by Rivest, Shamir, and Adleman; with minor adjustments it is still used at the time of writing. In this chapter, we introduce a formalism to discuss digital signature schemes and their security. This is illustrated by describing three such schemes: RSA, Schnorr signatures, and DSA.

Chapter 10

Problem sets

10.1 Additive polynomials

Let $p \in \mathfrak{P}$ and K be a ring of characteristic p.

1. Let $x, y \in K$. Show that
$$(x+y)^p = x^p + y^p$$
The map $\tau_K : K \to K$ defined by $x \mapsto x^p$. The above equation can be restated as
$$\tau_K(x+y) = \tau_K(x) + \tau_K(y)$$
for all $x, y \in K$.

2. Show that τ_K is a ring morphism. It is called the Frobenius endomorphism of K.

3. Let L be a ring of characteristic p, and $\alpha : K \to L$ be a ring morphism. Show that
$$\alpha \circ \tau_K = \tau_L \circ \alpha$$
which can be restated by saying that the following diagram of rings and ring morphisms commutes:
$$\begin{array}{ccc} K & \xrightarrow{\tau_K} & K \\ {\scriptstyle\alpha}\downarrow & \circlearrowright & \downarrow{\scriptstyle\alpha} \\ L & \xrightarrow[\tau_L]{} & L \end{array}$$
(We say that the Frobenius morphism is a natural transformation.)

4. Show that if K is a field, then τ_K is injective. We will henceforth assume that K is a field, i.e., $K \simeq \mathbb{F}_p$.

5. Show that for all $x \in K$, $\tau_K(x) = x$. Deduce that the p roots of the polynomial $X^p - X$ are the elements of K

6. A polynomial $P \in K[X]$ such that for all $x, y \in K$ we have $P(x+y) = P(x) + P(y)$ is called an additive polynomial. Show that τ_K defines an additive polynomial. Show that for all $n > 0$, $\tau_K^n = \tau_K \circ \cdots \circ \tau_K$ defines an additive polynomial.

7. Show that the set $T_K = \{\mathrm{id}, \tau_K, \tau_K^2, \dots\}$, together with the usual addition and function composition (instead of usual multiplication) form a commutative ring (it is denoted $K\{\tau_K\}$).

8. Let $P \in K[X]$ of degree n having distinct roots $\{\omega_1, \dots, \omega_n\} = \Omega \subset K$. Prove that if P is additive, then Ω is an additive subgroup of K.

9. Assume $p \neq 2$, show that the polynomial $Q = X + (X^p - X)^2 k$ is additive in $\mathbb{F}_p$ for $k \geq 0$, but that its roots do not form an additive group.

The study of additive polynomials is related to that of linear codes. Indeed, there is an equivalence between the set of linear codes over $\mathbb{F}_{p^n}$ and the elements of the ring $\mathbb{F}_{p^n}\{\tau\}$ — in particular, there is a ring structure on linear codes; this ring can be studied in its own right, and the results (divisibility, etc.) can be transported back to codes. As an example, factorisation in the ring of codes shows that every k-dimensional binary code can be decomposed as a product of k one-dimensional subcodes (although not in a unique fashion).

10.2 Fermat–Wiles' theorem, case $n = 4$

In this problem we consider the equation

$$x^4 + y^4 = z^4.$$

As a preliminary, we are going to show that if a triangle has a right angle and integer sides, then its area cannot be a perfect square.

1. Let p, q be primes, with $p > q$, and let

$$\begin{aligned} a &= 2pq \\ b &= p^2 - q^2 \\ c &= p^2 + q^2. \end{aligned}$$

   Show that $a^2 + b^2 = c^2$.

2. Show that the area of a right triangle with integer sides is $A = pq(p+q)(p-q)$.

3. Show that if A is square, then there exist x, y, u, v pairwise coprime integers such that

$$\begin{aligned} p &= x^2 \\ q &= y^2 \\ p + q &= u^2 \\ p - q &= v^2 \end{aligned}$$

   And deduce that $2y^2 = (u + v)(u - v)$.

4. Show that (up to swapping u and v), there are integers r, s such that

$$\begin{aligned} u + v &= 2r^2 \\ u - v &= 4s^2 \end{aligned}$$

   and therefore $x^2 = r^4 + 4s^4$.

5. Let E be the set of integers c which correspond to the hypothenuse of a right triangle with integer sides whose area is a perfect square. Assume that E is not empty. Then it has a smallest element $c = p^2 + q^2$. Use the above to construct a strictly smaller solution and derive a contradiction.

We are now equipped to prove Fermat–Wiles' theorem for $n = 4$.

1. Show that without loss of generality, we may assume x, y, z are pairwise coprime, and x even.
2. Write the equation as $x^4 = (z^2 - y^2)(z^2 + y^2)$, and show that there is no solution by using the preliminary.
3. Show that this implies that to prove Fermat–Wiles' theorem in general, it suffices to show it for primes $p > 3$.

10.3 Fermat–Wiles' theorem, case $n = 3$

In this problem we consider the equation

$$x^3 + y^3 = z^3.$$

1. Show that without loss of generality, we may assume x, y, z pairwise coprime.
2. We assume z is even, and write $x = a + b$, $y = a - b$ with integers a, b. Show that

$$\frac{a}{4}(a^2 + 3b^2) = \left(\frac{z}{2}\right)^3$$

   and deduce from this that $a \equiv 0 \bmod 4$.

3. Assume that $3 \nmid z$.

   a) Show that there exist integers r, s such that

   $$\begin{aligned} a &= 4r^3 \\ a^2 + 3b^2 &= s^3 \end{aligned}$$

   b) Show that there exists u, v coprime integers such that

   $$\begin{aligned} a &= u(u+3v)(u-3v) \\ b &= 3v(u^2 - v^2) \end{aligned}$$

   c) Deduce from this that there are integers A, B, C such that

   $$\begin{aligned} u &= 4A^3 \\ u + 3v &= B^3 \\ u - 3v &= C^3 \end{aligned}$$

   d) Show that this implies $(-2A)^3 + B^3 + C^3 = 0$, which is a solution to Fermat's equation, with strictly smaller integers than x, y, z.

4. Now assume $3 \mid z$.

   a) Show that

   $$\frac{a}{36}\left(b^2 + 3\left(\frac{a}{3}\right)^2\right) = \left(\frac{z}{6}\right)^3.$$

   b) Show that the two left hand side multiplicands are therefore coprime cubes.

   c) Show that this implies that there exist u, v coprime such that

   $$\begin{aligned} a &= 36r^3 \\ b &= u(u+3v)(u-3v) \\ \frac{a}{3} &= 3v(u^2 - v^2) \end{aligned}$$

   d) Show that $2v$, $v+u$, and $v-u$ are cubes, and construct a solution to Fermat's equation that is strictly smaller than x, y, z.

5. Conclude.

10.4 Cryptanalysis of the DVD encryption system

In the 1980s, when designing DVDs for movie contents, it was thought that some protection should be put to protect the contents. This gave rise to the Content Scrambling System (CSS), an inexpensive but very weak cipher, in line with the previous century's export legislation (namely, less than 40-bit security). It relies on the use of linear feedback shift registers (LSFRs), and easy-to-implement primitive (see Figure 10.1):

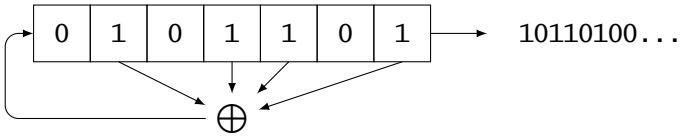


Figure 10.1: Illustration of an LSFR. Each clock cycle, a new bit is output.

1. Let $s = (b_{n-1}, \ldots, b_0) \in (\mathbb{F}_2)^n$ be the 'initial state';
2. Repeat ℓ times:
   a) Output b_0;
   b) Compute $b \leftarrow b_{v_1} + b_{v_2} + \cdots + b_{v_d}$;
   c) Set $s \leftarrow (b, b_{n-1}, \ldots, b_1)$.

The parameters n, $V = \{v_1, \ldots, v_d\}$, ℓ, and the initial state s entirely determine the output from this algorithm. We therefore refer to it as $\mathrm{LSFR}_{n,V,\ell,s}$, and by convention treat the output as a number in $\{0, \ldots, 2^\ell - 1\}$.

1. Show that is the initial state is $s = (0, \ldots, 0)$ then the output is $(0, \ldots, 0)$.
2. Show that, given n consecutive bits of the output, it is possible to find all subsequent output bits.
3. The CSS algorithm works as follows:

   a) Let $A \in (\mathbb{F}_2)^{16}$ and $B \in (\mathbb{F}_2)^{24}$ be the initial states (usually represented as a single 40-bit seed);
   b) Let $s_1 \leftarrow 1 \| A$ and $s_2 \leftarrow 1 \| B$, where $\|$ denotes concatenation[a] and initialise $L_1 = \mathrm{LSFR}_{17,V_1,8,s_1}$, $L_2 = \mathrm{LSFR}_{25,V_2,8,s_2}$.
   c) Let $c \leftarrow 0$.
   d) Repeat forever
      i. Let x be the output of L_1 and y be the output of L_2;
      ii. Output $x + y + c \bmod 2^8$;[b]
      iii. If $x + y > 255$ then $c \leftarrow 1$ else $c \leftarrow 0$.;

   [a] Following Boneh and Shoup, we present here a variant, which is identical from a security standpoint, but slightly easier to work with. In the real CSS, instead of prepending a 1 to the initial seeds, one inserts the 1 in bit position 9 for the 17-bit LFSR and in bit position 22 for the 25-bit LFSR.

   [b] The real CSS discards the first byte output by the 17-bit LFSR and the first two bytes output by the 25-bit LFSR. This is without effect for the rest of the discussion.

with $V_1 = \{0, 14\}$ and $V_2 = \{0, 3, 4, 12\}$. Implement this algorithm.

4. Guessing the seeds A, B naively requires of the order of 2^{40} trials; approximately how long would such a computation require?

5. Assume we know x_1, x_2, x_3, the first three bytes output by L_1. Let z_1, z_2, z_3 be the first three bytes output by the CSS algorithm. Show that one recovers the seed B by computing

$$\left(2^{17} + 2^{16}z_3 + 2^8 z_2 + z_1\right) - \left(2^{16}x_3 + 2^8 x_2 + x_1\right).$$

6. Since (x_1, x_2, x_3) is determined (but not uniquely!) by A, show that one recovers the full seed in at most 2^{16} operations. Approximately how long would such a computation require? Implement this algorithm.

7. Show that, as claimed, the simplifications made in our description of CSS are minor, by implementing the attack against the real CSS algorithm.

Index