Crash course in mathematics – Master SCCI

Vanessa Vitse

2013-2014

Contents

Chapter 1

Modular arithmetic over integers

1.1 Euclidean division and congruences

Theorem 1.1.1 (Euclidean division)**.** *For $a, b \in \mathbb{Z}$, $b \neq 0$, there exist a unique couple $q, r \in \mathbb{Z}$ s.t. $a = bq + r$ and $0 \leq r < |b|$. The integer r is the* remainder *in the division of a by b, and q is the* quotient*.*

Definition 1.1.2 (Divisibility)**.** *Let a and b two integers. Then a* divides *b (or b is a* multiple *of a) if there exists an integer c such that $b = a \cdot c$. This is denoted $a|b$.*

Definition 1.1.3 (Congruence)**.** *Let $x, y, n \in \mathbb{Z}$. Then x is* congruent *to y* modulo *n if their remainders in the division by n are the same.*

In particular

$$\begin{aligned} x = y \bmod n \quad &\Leftrightarrow \quad n|(x-y) \\ &\Leftrightarrow \quad \exists k \in \mathbb{Z}, x = kn + y \end{aligned}$$

Property 1.1.4.

1. *This is an equivalence relation (reflexive, transitive and symmetric)*
2. *Compatibility with addition and multiplication mod n: for all integers a, b, a', b' s.t. $a = a' \bmod n$ and $b = b' \bmod n$, then $a + b = a' + b' \bmod n$ and $ab = a'b' \bmod n$.*
3. *Other interesting properties :*
   - $a = b \bmod n \Leftrightarrow ac = bc \bmod nc$
   - $a = b \bmod mn \Rightarrow (a = b \bmod m$ *and* $a = b \bmod n)$

The congruence equivalence relation partitions the set $\mathbb{Z}$ into equivalence classes:

Definition 1.1.5 (Residue classes modulo n)**.** *$\mathbb{Z}/n\mathbb{Z}$ is the set of equivalence classes or* residue classes *modulo n for the congruence relation. For any integer m in a residue class, we call m a* representative *of that class.*

Note that there are precisely n distinct residue classes modulo n, given for example by $0, \ldots, n-1$ (corresponding to the remainders in the Euclidean division by n).

Property 1.1.6. *$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is a (commutative and unit) ring. See next chapter.*

Modular exponentiation

Question: given $x \in \mathbb{Z}/n\mathbb{Z}$ and $e \in \mathbb{N}^*$, how to compute $x^e \bmod n$?

An obvious way is to iteratively multiply by x a total of e times, reducing modulo n at each step. The complexity is then in $O(e\log(n)^2)$. Another (much faster) way is to apply the "square-and-multiply" algorithm; the idea is based on the following mathematical property:

Property 1.1.7. *Let $e = (e_{\ell-1}\dots e_0)_2$ be the binary expansion of e, that is $e = \sum_{i=0}^{\ell-1} e_i 2^i$. Then*

$$x^e = \prod_{i=0}^{\ell-1}(x^{2^i} \bmod n)^{e_i} = \prod_{i=0,e_i\neq 0}^{\ell-1}(x^{2^i} \bmod n).$$

This yields the following algorithm:

Algorithm 1: "Right-to-left" algorithm for modular exponentiation

```
Input  : $x \in \mathbb{Z}/n\mathbb{Z}$, $e, n \in \mathbb{N}^*$
Output: $y = x^e \bmod n$
$y \leftarrow 1$
$t \leftarrow x$
while $e \neq 0$ do
    if $e\%2 = 1$ then
        $y \leftarrow y \cdot t \bmod n$
    $e \leftarrow e \gg 1$
    $t \leftarrow t^2 \bmod n$
return $y$
```

Exercise 1. Propose another algorithm which reads the bits of e from "left-to-right". Show that all these algorithms have polynomial complexity.

Remark. Given $n \in \mathbb{N}^*$, $g \in \mathbb{Z}/n\mathbb{Z}$ and $x \in \mathbb{Z}$, it is easy to compute $g^x \bmod n$ (there exist algorithms with polynomial complexity). However, there is no efficient algorithm which computes x given $n, g, g^x \bmod n$: this problem is called *discrete logarithm problem* and is useful for many asymmetric cryptographic protocols.

1.2 Extended Euclid algorithm

Definition 1.2.1 (gcd, lcm, coprimality)**.** *For $a, b \in \mathbb{Z}$, we note* $\gcd(a,b)$ *or $a \wedge b$ the greatest common divisor of a and b and* $\operatorname{lcm}(a,b)$ *or $a \vee b$ their least common multiple. We say that a and b are* coprime *if* $\gcd(a,b) = 1$.
More generally, the gcd of $\{a_1,\dots,a_n\} \subset \mathbb{Z}$ is the greatest common divisor of $a_1,\dots,a_n$.

The gcd of two integers can be expressed as a linear combination of these integers:

Lemma 1.2.2 (Bézout lemma)**.** *For $a, b \in \mathbb{Z}$, there exist $u, v \in \mathbb{Z}$ such that $au + bv = \gcd(a,b)$.*

Proof. Consider the non zero element of $S = \{au + bv : u, v \in \mathbb{Z}\}$ with minimal absolute value and show that this element is necessarily the gcd of a and b □

Obviously, this proof is not very helpful for the computation of gcd. Euclid's algorithm will remedy this and give a constructive proof. We use the fact that if r is the remainder in the Euclidean division of a by b, then

$$a \wedge b = b \wedge r.$$

Now let $r_0 := a$ and $r_1 := b$. We compute iteratively

$$\begin{array}{rclll}
r_0 & = & r_1\,q_1 + r_2 & \text{with} \quad 0 \le r_2 < |r_1| & \rightarrow \quad a \wedge b = r_0 \wedge r_1 = r_1 \wedge r_2 \\
r_1 & = & r_2\,q_2 + r_3 & \text{with} \quad 0 \le r_3 < r_2 & \rightarrow \quad r_1 \wedge r_2 = r_2 \wedge r_3 \\
 & \vdots & & \quad\quad\; \vdots & \\
r_{n-2} & = & r_{n-1}\,q_{n-1} + r_n & \text{with} \quad 0 \le r_n < r_{n-1} & \rightarrow \quad r_{n-2} \wedge r_{n-1} = r_{n-1} \wedge r_n \\
r_{n-1} & = & r_n\,q_n + r_{n+1} & \text{with} \quad r_{n+1} = 0 & \rightarrow \quad r_{n-1} \wedge r_n = r_n
\end{array}$$

In particular, $a \wedge b$ is equal to the last non-zero remainder r_n. To get u and v we explicitly introduce the sequences $(u_i), (v_i)$ such that $r_n = u_i\,r_i + v_i\,r_{i+1}$, given by (backward) induction :

- $r_n = 0 \cdot r_{n-1} + 1 \cdot r_n$, so $\begin{cases} u_{n-1} = 0 \\ v_{n-1} = 1 \end{cases}$
- if $r_n = u_i\,r_i + v_i\,r_{i+1}$, we use that $r_{i-1} = r_i\,q_i + r_{i+1}$. Then $r_n = u_i\,r_i + v_i\,(r_{i-1} - r_i\,q_i) = v_i\,r_{i-1} + (u_i - v_i\,q_i)\,r_i$, so that we take $\begin{cases} u_{i-1} = v_i \\ v_{i-1} = u_i - v_i\,q_i \end{cases}$

Note that you can also write it directly by introducing the sequences $(s_i), (t_i)$ such that $s_i a + t_i b = r_i$.

- Initialisation: $\begin{cases} s_0 = 1 \quad t_0 = 0 \\ s_1 = 0 \quad t_1 = 1 \end{cases}$
- Induction hypothesis: $\begin{cases} s_{i-1}a + t_{i-1}b = r_{i-1} \\ s_i a + t_i b = r_i \end{cases}$

Writing $r_{i+1} = r_{i-1} - r_i q_i = s_{i-1}a + t_{i-1} - (s_i a + t_i b)q_i = (s_{i-1} - q_i s_i)a + (t_{i-1} - q_i t_i)b$, you get

$$\begin{cases} s_{i+1} = s_{i-1} - q_i s_i \\ t_{i+1} = t_{i-1} - q_i t_i \end{cases}$$

1.3 Modular inverse

Definition 1.3.1. *Let $x, n > 0$ two integers. We say that x admits a* multiplicative inverse *modulo n if there exists $y \in \mathbb{Z}$ such that $x \cdot y = 1 \bmod n$; this is denoted by $y = x^{-1} \bmod n$.*
Similarly, $x \in \mathbb{Z}/n\mathbb{Z}$ is invertible *if there exists $y \in \mathbb{Z}/n\mathbb{Z}$ such that $xy = 1 \bmod n$.*

Remark. If $a \in \mathbb{Z}$ is invertible modulo n and if $a' = a \bmod n$ then a' is also invertible modulo n.

Theorem 1.3.2. *An integer a is invertible modulo n iff a and n are coprime.*

Proof. Direct application from Bézout: $ua + vn = 1 \Rightarrow u = a^{-1} \bmod n$. □

Remark. If p is prime, then every element of $(\mathbb{Z}/p\mathbb{Z})^*$ is invertible. In particular, $\mathbb{Z}/p\mathbb{Z}$ is a field ; it is in fact the unique field (up to isomorphism) with p elements, and will be denoted GF_p.

Algorithm 2: Computation of inverse modulo n

```
Input  : $a \in \mathbb{Z}$, $n \in \mathbb{N}^*$
Output: $a^{-1} \bmod n$
$s_0 \leftarrow 1$   $s_1 \leftarrow 0$; while $b \neq 0$ do
    $tmp \leftarrow a$
    $a \leftarrow b$
    $b \leftarrow tmp\%a$
    $q \leftarrow tmp/a$
    $tmp \leftarrow s_0 - qs_1$   $s_0 \leftarrow s_1$   $s_1 \leftarrow tmp$
return $s_0$
```

Exercise 2. Solve $35x = 7[43]$.

1.4 Prime numbers

Definition 1.4.1 (Prime numbers)**.** *A* prime number *is a positive integer $p \neq 1$ that is only divisible by ± 1 and $\pm p$. The set of prime numbers is denoted $\mathcal{P}$; $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$. A positive integer that is not a prime is called* composite*.*

The largest known prime number (last record of 2013) is $2^{57885161} - 1$ (with almost 17 millions of digits).

Theorem 1.4.2 (Fundamental theorem of arithmetic)**.**
Every nonzero integer n can be written as a product of primes:

$$n = \pm 1 \,.\, p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \quad p_i \in \mathcal{P}, \quad \alpha_i \in \mathbb{N}.$$

This decomposition is unique if $p_1 < p_2 < \cdots < p_k$ and $\alpha_i > 0$ for all i.

The uniqueness of decomposition relies on the following Lemma:

Lemma 1.4.3 (Euclid's lemma)**.** *Let p be a prime number and a, b two integers. Then $p|ab \Rightarrow p|a$ or $p|b$.*

Existence can be obtained by considering non trivial divisors of n and using induction. Note that you can obtain the decomposition by trial division by the prime numbers lower than $\sqrt{n}$, which in turn can be obtained using Eratosthenes sieve.

The fundamental theorem of arithmetic gives a naive algorithm for computing gcd /lcm of two numbers.

Property 1.4.4. *If $a = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ and $b = p_1^{\beta_1} \dots p_n^{\beta_n}$, then*

$$\begin{cases} a \wedge b = p_1^{\min(\alpha_1,\beta_1)} \dots p_n^{\min(\alpha_n,\beta_n)} \\ a \vee b = p_1^{\max(\alpha_1,\beta_1)} \dots p_n^{\max(\alpha_n,\beta_n)} \end{cases}$$

In particular,

$$(a \wedge b) \times (a \vee b) = ab$$

Exercise 3. Write algorithms that compute gcd's and Bézout coefficients.

In particular,

$$x|a \text{ and } x|b \Leftrightarrow x|(a \wedge b),$$
$$a|m \text{ and } b|m \Leftrightarrow (a \vee b)|m.$$

We easily deduce from the fundamental theorem another interesting result:

Property 1.4.5 (Gauss lemma)**.** *If p, q are coprime and x is an integer s.t. $p|qx$, then $p|x$.*

As a last application of the extended Euclid's algorithm, we give a method to solve congruential systems using the famous Chinese Remainder theorem.

Theorem 1.4.6 (Chinese Remainder Theorem – CRT)**.** *Let n, m be two coprime integers and a, b two integers. Then the system*

$$\begin{cases} x = a \bmod n \\ x = b \bmod n \end{cases}$$

admits a unique solution $x \bmod mn$.

Proof. From Bézout, there exist u, v s.t. $un + vm = 1$ and $x_0 = bun + avm$ is a particular solution. If x_1 is another solution of the previous system then $\begin{cases} x_1 - x_0 = 0 \bmod n \\ x_1 - x_0 = 0 \bmod m \end{cases}$. From Gauss lemma, we deduce that $x_0 = x_1 \bmod mn$. □

Exercise 4. Solve the following system

$$\begin{cases} 35x = 7\ [4] \\ 22x = 33\ [5] \end{cases}$$

Exercise 5.

1. Let $a, b, c \in \mathbb{Z}$ such that $(a, b) \neq (0, 0)$. Show that the equation
$$ax + by = c \tag{1.1}$$
has a solution iff $a \wedge b$ divides c.
2. Find all the integer solutions of the following equations: $7x - 9y = 6$, $11x + 17y = 5$.

Exercise 6. In a country named ASU where the currency is the rallod, the national bank issues banknotes of 95 rallods and coins of 14 rallods.

1. Show that it is possible to pay any integer amount (provided that each participant has access to as many coins and banknotes as needed).

2. Suppose that you need to pay an amount S and that you have access to as many coins and banknotes as needed, but that your creditor cannot give the change. Thus it is possible for example to pay $S = 14$ rallods but impossible to pay 13 or 15 rallods. Show that it is always possible to pay any large enough amount.

Exercise 7. A rooster costs 5 silver coins, a hen 3 coins and a set of 4 chicks 1 coin. Someone bought 100 chickens for 100 coins. How many pieces of each kind has he bought?

The end of this section is devoted to some results about the repartition of prime numbers.

Theorem 1.4.7. *There are infinitely many prime numbers. Let $\pi(n)$ be the number of primes smaller than n, then $\pi(n) \sim n/\log n$.*

Remark. So informally, the probability that a random integer n is prime is about $1/\log n$. More precisely,

$$\pi(x) \underset{x\to\infty}{\sim} \int_2^x \frac{dt}{\ln(t)}.$$

For example, about one number among 21 is prime near $x = 1\,000\,000\,000$.

1.5 Euler-Fermat theorem and non-primality test

Euler-Fermat theorem is at the heart of the RSA cryptosystem. Let us first recall some notions:

Definition 1.5.1 (Euler's totient function)**.** *Euler's totient function (or Euler's phi function) is defined by*

$$\forall n \in \mathbb{N}^*,\ \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

This equivalent to say that $\varphi(n)$ is the number of integers between 0 and $n-1$ that are coprime with n.

Examples. $\varphi(1) = 1; \varphi(2) = 1; \varphi(3) = 2; \varphi(4) = 2...$

Computation of Euler's totient function

Property 1.5.2.

- *$\varphi(mn) = \varphi(m)\varphi(n)$ for all coprime positive integers n, m.*
- *$\varphi(p^e) = p^e - p^{e-1} = p^e(1 - 1/p)$ for all prime p and positive integer e.*
- *$\varphi(n) = n\prod_{i=1}^r(1 - 1/p_i)$ where $n = p_1^{e_1} \dots p_k^{e_k}$ is the factorisation of n into primes.*

Proof.

- Consider the map $a \in \mathbb{Z}/nm\mathbb{Z} \mapsto (a \bmod n, a \bmod m) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ which is well-defined and a bijection according to CRT. Moreover $a \wedge mn = 1$ iff ($a \wedge m = 1$ and $a \wedge n = 1$), so that the previous application gives a bijection between $(\mathbb{Z}/mn\mathbb{Z})^*$ and $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$.
- Among the p^e elements between 0 and $p^e - 1$, the only elements which are multiples of p are not invertible; these are $0 \cdot p, 1 \cdot p, \dots, (p^{e-1} - 1) \cdot p$ and there are precisely p^{e-1}.

- Direct from the previous items.

□

Examples : $\varphi(36) = \varphi(2^2 3^2) = 36\left(1-\frac{1}{3}\right)\left(1-\frac{1}{2}\right) = 36 \times \dfrac{2}{3} \times \dfrac{1}{2} = 12.$

Theorem 1.5.3 (Euler-Fermat theorem)**.** *Let a, n ($n \geq 0$) be two* coprime *integers, then*

$$a^{\varphi(n)} = 1 \ [n]$$

Among other things, this theorem means that if $a \wedge n = 1$ and $\varphi(n)$ is known, then it is possible to simplify modular exponentiations: $a^x = a^{x_0} \ [n]$, where x_0 is the remainder in the Euclidean division x par $\varphi(n)$.

In practice however, the computation of $\varphi(n)$ is difficult. For instance, if n is the product of two distinct primes p and q, then the computation of $\varphi(n)$ is as difficult as the factorization of n, and we have mentioned that this is a hard problem. The proof will be seen in the exercises.

When p is prime, Euler-Fermat theorem (known as "Fermat's little theorem" in this case) yields a *pseudo-primality* test. The statement becomes:

Theorem 1.5.4.
- *If p is prime and $a \in \mathbb{Z}/p\mathbb{Z}$ is such that $p \nmid a$ (i.e. $a \wedge p = 1$), then*
$$a^{p-1} = 1 \ [p]$$
- *If p is prime and $a \in \mathbb{Z}$, then $a^p = a \ [p]$*

Proof. The first part is a direct application of Euler-Fermat for $n = p$. The second part is an obvious consequence if $a \wedge n = 1$; otherwise, a is a multiple of p : the equality then can be rewritten as $0 = 0 \ [p]$... □

The converse of this theorem gives the following probabilistic primality test:

1. choose a at random between 1 and $n - 1$
2. n satisfies the test if $a^{n-1} = 1 \ [n]$

If the test is satisfied for n, then n has a good probability of being prime. But if n does not satisfy the test, then we know for sure that n is not prime:

$$2^{25009996} = 13697276 \ [25009997] \Rightarrow 25009997 \text{ is not prime.}$$

Chapter 2

Fundamental structures

2.1 Groups

Let G be a set. A *binary operation* (or *composition law*) is a map $f : G \times G \to G$. Binary operations are usually written in infix notations, i.e. $a + b$, $a \times b$, $a \cdot b$, ... or simply by juxtaposition, i.e. ab, instead of $f(a, b)$.

Example. On the set $\mathbb{N}$ of natural integers $+$ and $\times$ are binary operations, but $-$ is not.

Definition 2.1.1. *Let G be a set and $\cdot$ a binary operation on G. Then $(G, \cdot)$ is a* group *if*

1. *the binary operation is* associative*: for all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*
2. *there exists a (necessarily unique) element $e \in G$, called the* neutral element *or the identity, such that for all $a \in G$, $a \cdot e = e \cdot a = a$*
3. *for each $a \in G$, there exists a (necessarily unique) element $b \in G$, called the* group inverse *of a, such that $a \cdot b = b \cdot a = e$*

A group is called abelian *or commutative if its group law is commutative, i.e. $a \cdot b = b \cdot a$ for all $a, b \in G$.*

The inverse of an element a is often denoted by a^{-1}; similarly, the element $a \cdot a \cdot a \cdot \ldots \cdot a$ (n times) is denoted by a^n. This notation can be extended to $\mathbb{Z}$ by setting $a^{-n} = (a^{-1})^n$ and $a^0 = e$.

Exercise 8. Which of the followings are groups ? abelian groups ?

- $(\mathbb{Z}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{Z}, \times)$
- $(\mathbb{R}, +)$, $(\mathbb{R}, \times)$, $(\mathbb{R}^*, \times)$, $(\mathbb{R}^*_+, \times)$
- $(GL_n(\mathbb{R}), \cdot)$, $(Bij(E), \circ)$, $(\mathbb{R}^3, \times)$ where × is the vector cross-product
- $(\mathbb{Z}/n\mathbb{Z}, +)$, $(\mathbb{Z}/n\mathbb{Z}, \times)$
- $\emptyset$, $\{e\}$ (with their only possible composition law), $(\{\texttt{True}, \texttt{False}\}, XOR)$

Definition 2.1.2 (Subgroup)**.** *Let $(G, \cdot)$ be a group. A subset H of G is a* subgroup *of G, denoted $H < G$, if $\cdot$ is a binary operation on H (i.e. $a \cdot b \in H$ for all $a, b \in H$) and $(H, \cdot)$ is a group.*

Exercise 9. Show that $H < G$ if and only if $H \neq \emptyset$ and $h_1 \cdot h_2^{-1} \in H$ for all $h_1, h_2 \in H$. Show that the intersection of a family of subgroups is a subgroup.

Example.
- Every group G admits $\{e\}$ and G as subgroups.
- $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$
- $(\{1, -1\}, \times) < (\mathbb{Q}^*, \times) < (\mathbb{R}^*, \times) < (\mathbb{C}^*, \times)$
- The subgroups of $(\mathbb{Z}, +)$ are $\{0\}$, $\mathbb{Z}$, and $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$ for all $n \in \mathbb{N}^*$.

Definition 2.1.3. *Let $(G_1, \cdot)$ and $(G_2, *)$ be two groups. A map $\phi : G_1 \to G_2$ is a* homomorphism *(or group morphism) if for all $a, b \in G_1$, $\phi(a \cdot b) = \phi(a) * \phi(b)$. The* kernel *of ϕ is the set $\ker \phi = \{a \in G_1 : \phi(a) = e_{G_2}\}$; it is a subset of G_1. The* image *of ϕ is the set $\mathrm{Im}\phi = \{\phi(a) : a \in G_1\}$; it is a subset of G_2. A bijective homomorphism is called an* isomorphism. *Two groups G_1 and G_2 are called* isomorphic *if there exists an isomorphism $G_1 \to G_2$; this is denoted $G_1 \simeq G_2$.*

Example.
- The natural logarithm is an isomorphism from $(\mathbb{R}_+^*, \times)$ to $(\mathbb{R}, +)$.
- If $H < G$, then the inclusion map $\imath : H \to G$ is a morphism, with $\ker \imath = \{e\}$ and $\mathrm{Im}\imath = H$.
- Let G be a group and g a fixed element of G. Then the map $n \mapsto g^n$ is a homomorphism from $(\mathbb{Z}, +)$ to G. The conjugacy map $x \mapsto g \cdot x \cdot g^{-1}$ is homomorphism from G to G, equal to the identity if G is abelian. The maps $x \mapsto x^2$ and $x \mapsto x^{-1}$ are homomorphisms from G to G iff G is abelian.
- Let $\phi : \mathbb{R}^* \to \mathbb{R}^*,\ x \mapsto x^2$. Then $\ker \phi = \{1, -1\}$ and $\mathrm{Im}\phi = \mathbb{R}_+^*$.

Property 2.1.4.
- *Let $\phi : G_1 \to G_2$ a group morphism. Then $\ker \phi$ is a subgroup of G_1 and $\mathrm{Im}\phi$ is a subgroup of G_2.*
- *ϕ is injective $\Leftrightarrow \ker \phi = \{e_{G_1}\}$*
- *The composition of two group morphisms $\phi : G_1 \to G_2$ and $\psi : G_2 \to G_3$ is also a group morphism $\psi \circ \phi : G_1 \to G_3$*
- *The inverse function of an isomorphism $G_1 \to G_2$ is an isomorphism $G_2 \to G_1$.*

Definition 2.1.5 (Product of group)**.** *Let $(G_1, \cdot)$ and $(G_2, *)$ be two groups. The* direct product *of G_1 and G_2 is defined as the set $G_1 \times G_2$ endowed with the binary operation*

$$(g_1, g_2) \star (g_1', g_2') = (g_1 \cdot g_1', g_2 * g_2').$$

One can check that $(G_1 \times G_2, \star)$ is a group with neutral element (e_{G_1}, e_{G_2}).

Exercise 10.

1. Show that $(\mathbb{C}, +)$ is isomorphic to the direct product of $(\mathbb{R}, +)$ with itself.
2. Write down a table for the group law of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Is it isomorphic to $\mathbb{Z}/4\mathbb{Z}$?
3. Let p, q be two coprime numbers. Show that there is a isomorphism between $\mathbb{Z}/pq\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Definition 2.1.6 (Quotient by a subgoup)**.** *Let G a group and H a subgroup of G. We define on G the binary relation*

$$g \sim_H g' \Leftrightarrow g^{-1}g' \in H.$$

This is an equivalence relation (exercise). The equivalence class, or coset*, of an element $g \in G$ is the set $gH = \{g\,h : h \in H\}$. The quotient G/H is defined as the set of equivalence classes for $\sim_H$; its cardinality is called the* index *of H in G.*

Theorem 2.1.7 (Lagrange's theorem)**.** *Let H be a subgroup of a finite group G, then*

$$|G| = |G/H| \times |H|.$$

In particular, the cardinality of a subgroup always divides the cardinality of the group.

Example. If p is prime, then $\mathbb{Z}/p\mathbb{Z}$ has no non-trivial subgroup.

Definition 2.1.8 (Normal subgroup)**.** *Let G a group. A subgroup H of G is called* normal*, denoted by $H \lhd G$, if*

$$\forall g \in G, \forall h \in H, g^{-1}hg \in H.$$

Exercise 11. Let $\phi : G_1 \to G_2$ a group morphism. Show that $\ker\phi$ is a normal subgroup of G_1.

Proposition 2.1.9 (Quotient group)**.** *Let H be a normal subgroup of G. Then on the quotient G/H, the binary operation*

$$\begin{array}{rcl} G/H \times G/H & \to & G/H \\ (gH, g'H) & \mapsto & (gg')H \end{array}$$

is well-defined and is a group law. The canonical projection map $\pi : G \to G/H,\ g \mapsto gH$ *is a group morphism, whose kernel is precisely H.*

Exercise 12. Show that $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. What is the quotient group ?

Theorem 2.1.10 (Isomorphism theorem)**.** *Let $\phi : G_1 \to G_2$ a surjective group morphism. Then there exists a unique homomorphism $\hat{\phi} : G_1/\ker\phi \to g_2$, such that the following diagram is commutative:*

$$\begin{tikzcd} G_1 \arrow[r, "\phi"] \arrow[d, "\pi"'] & G_2 \\ G_1/\ker\phi \arrow[ur, "\hat{\phi}"'] & \end{tikzcd}$$

i.e. $\phi = \hat{\phi} \circ \pi$; furthermore $\hat{\phi}$ is an isomorphism.

Example. Let $f : \mathbb{R} \to \mathbb{C}^*$, $x \mapsto e^{2i\pi x}$, this is a morphism (from $(\mathbb{R}, +)$ to $(\mathbb{C}^*, \times)$). One has $\ker f = \mathbb{Z}$; the above theorem implies that $\mathbb{R}/\mathbb{Z}$ is isomorphic to $\mathrm{Im} f = \mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$.

Definition 2.1.11. *Let $(G, \cdot)$ be a group and S a subset of G. The subgroup* generated *by S, denoted $\langle S\rangle$, is the smallest subgroup of G containing S, and one has*

$$\langle S\rangle = \{a_1^{n_1} \cdot a_2^{n_2} \cdot \ldots \cdot a_k^{n_k} : k \in \mathbb{N}, a_i \in S, n_i \in \mathbb{Z}\}.$$

If $G = \langle S\rangle$ we say that S is a set of generators of G. If $G = \langle S\rangle$ and S is finite then G is called finitely generated.
A group generated by a unique element is called cyclic*. The* order *of an element g in a group is the cardinality of the cyclic subgroup $\langle g\rangle$ it generates.*

Property 2.1.12. *1. Let G be a group and $g \in G$ an element of finite order d. Then d is the smallest positive integer such that $g^d = e$.*

2. Let G be a finite group. Then for all $g \in G$, $g^{|G|} = e$.

Exercise 13.

1. Show that every cyclic group is isomorphic either to $\mathbb{Z}$ or to $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$ (hint: apply the isomorphism theorem to the map $\mathbb{Z} \to \langle g \rangle$, $k \mapsto g^k$).
2. Let p be a prime number. Show that up to isomorphism, there is a unique group of cardinality p.

Proposition 2.1.13. *Let G be a cyclic group of cardinality n. Then for any divisor d of n, there exists a unique subgroup $H_d < G$ of cardinality d, given by $H_d = \{x \in G : x^d = e\}$; this subgroup is cyclic. The quotient G/H_d is also a cyclic group, of cardinality n/d.*

Proof. (Sketch). Let g a generator of G. Then $H_d = \langle g^q \rangle$ where $q = n/d$. For the quotient, use the isomorphism theorem with the map $G \to \langle g^d \rangle$, $x \mapsto x^d$. □

Theorem 2.1.14 (Structure of finitely generated abelian groups)**.** *Let G be a finitely generated abelian group. Then there exist integers $r, n_1, n_2, \dots, n_k$, $n_1 | n_2 | \dots | n_k$, such that*

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z},$$

and this decomposition is unique (if $n_1 > 1$).

Exercise 14.

1. Show that $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ is a group.
2. Prove Euler's theorem: for any positive integer n and any integer a coprime to n

$$a^{\varphi(n)} = 1 \bmod n.$$

(In other words, the order of a mod n divides $\varphi(n)$).

3. Deduce Fermats's little theorem:

$$\forall a \in \mathbb{Z},\ p \text{ prime},\ a^p = a \bmod p.$$

4. Application: show that 1763 is not a prime number.

2.2 Commutative ring

We suppose that all rings are unitary and commutative.

Definition 2.2.1. *Let A be a set with two binary operations $+$ and $\cdot$. Then $(A, +, \cdot)$ is a* ring *if*

1. $(A, +)$ is a abelian group, with neutral element 0_A;

2. *$\cdot$ is associative, i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in A$;*

3. *$\cdot$ is distributive over $+$, i.e. $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in A$;*

4. *there exists a unit element 1_A such that $a \cdot 1_A = 1_A \cdot a$ for all $a \in A$;*

5. *$\cdot$ is commutative, i.e. $a \cdot b = b \cdot a$ for all $a, b \in A$.*

Example. $(\mathbb{Z}, +, \times)$ is a ring, as is $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ for any $n \in \mathbb{N}^*$. The set $\mathbb{R}[X]$ of polynomials with real coefficients is a ring for the usual addition and multiplication laws. $(\{0\}, +, \times)$ is also a ring, called the zero ring: it is the only ring for which $1 = 0$.

Remark. If A is a ring, then $0 \cdot a = 0$ for all $a \in A$

Definition 2.2.2.

- *A is a* domain *if $A \neq \{0\}$ and $\forall x, y \in A$, $x \cdot y = 0 \Rightarrow x = 0$ or $y = 0$.*
- *a is called a* zero divisor *if $a \neq 0$ and there exist a non-zero element $b \in A$ such that $ab = 0$. In particular, A is a domain if it has no zero divisors. A non-zero element a which is not a zero divisor is called* regular*.*

Example.

- $\mathbb{Z}$ is a domain. $\mathbb{Z}/n\mathbb{Z}$ is a domain if and only if n is prime.
- If A and B are two rings, the cartesian product $A \times B$ is a ring for the operations $(a, b) + (a', b') = (a + a', b + b')$ and $(a, b) \cdot (a', b') = (aa', bb')$. It is however never a domain since $(1_A, 0_B) \cdot (0_A, 1_B) = (0_A, 0_B)$.

Definition 2.2.3. *An element $x \in A$ is called* invertible *if there exists $y \in A$ s.t. $x \cdot y = 1$.*
The set of all invertible elements of A is denoted by $A^\times$ and is a group for the binary operation $\cdot$.

Exercise 15.

1. Show that if $a \in A$ is regular, then $ab = ab' \Leftrightarrow b = b'$.
2. Show that $a \in \mathbb{Z}/n\mathbb{Z}$ is regular if and only if it is invertible.

Definition 2.2.4. *Let A and B two rings. A map $f : A \to B$ is a* ring morphism *if $f(1_A) = 1_B$ and for all $a_1, a_2 \in A$, $f(a_1 + a_2) = f(a_1) + f(a_2)$ and $f(a_1 a_2) = f(a_1) f(a_2)$. Ring morphisms are stable under composition.*

Example. For any ring A, there exists a morphism $f : \mathbb{Z} \to A$ defined by setting $f(n) = 1 + 1 + \cdots + 1$ (n times).

Definition 2.2.5. *A ring $(A, +, \cdot)$ is a* field *if $0 \neq 1$ and every non-zero element is invertible, i.e. $A^\times = A^* \neq \emptyset$.*

Example. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields, but $\mathbb{Z}$ is not. For any prime p, $\mathbb{Z}/p\mathbb{Z}$ is a field. The set $\mathbb{R}(X)$ of real rational fractions is a field for the usual laws.

Definition 2.2.6 (Field of fractions)**.** *Let A be a domain. The* field of fractions *of A, denoted $Frac(A)$, is the set of equivalence classes of pairs $A \times A^*$ for the relation $(a, b) \sim (a', b')$ iff $ab' = a'b$. The class of a pair (a, b) is usually denoted by a/b or $\frac{a}{b}$. The sum and product of two elements of $Frac(A)$ are defined by $\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + ba'}{bb'}$ and $\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$. Then $(Frac(A), +, \cdot)$ is a field and there is a canonical injective ring morphism $A \to Frac(A)$ which sends a to $\frac{a}{1}$.*

Example. $Frac(\mathbb{Z}) = \mathbb{Q}$. If K is already a field then $Frac(K) = K$. The field of fractions of $\mathbb{R}[X]$ is $\mathbb{R}(X)$, the field of real rational fractions.

Definition 2.2.7. *A subset I of a ring $(A, +, \cdot)$ is an* ideal *if*

1. *$(I, +)$ is a subgroup of $(A, +)$,*
2. *for all $x \in I$ and $a \in A$, $ax \in I$.*

Example.

- Every ring A admits $\{0\}$ and A as ideals; they are called the trivial ideals.
- For any $x \in A$, the set $xA = \{x \cdot a : a \in A\}$ is an ideal.
- Let I be an ideal of A such that I contains an invertible element, then $I = A$.
- Let $f : A \to B$ be a ring morphism. Then $\ker f = \{a \in A : f(a) = 0_B\}$ is an ideal of A.

Property 2.2.8 (Operations on ideals)**.** *Let I, J two ideals of A, then*

- *$I \cap J$ is an ideal,*
- *$I + J := \{f + g : f \in I, g \in J\}$ is an ideal. It is the smallest ideal containing I and J.*
- *$I \cdot J := \{f_1 g_1 + \cdots + f_k g_k : f_i \in I, g_i \in J\}$ is an ideal, included in $I \cap J$.*

Definition 2.2.9.

- *The ideal generated by $x_1, \ldots, x_n \in A$ is*

$$(x_1, \ldots, x_n) := x_1 A + \cdots + x_n A = \{x_1 a_1 + \cdots + x_n a_n : a_1, \ldots, a_n \in A\}.$$

  An ideal is called principal *if it is generated by one element.*
- *A ring is* principal *if all its ideals are principal.*

Proposition 2.2.10 (Ideals of a field)**.** *A non-zero ring A is a field if and only if A has no non-trivial ideals.*

Definition 2.2.11 (Quotient ring)**.** *Let I an ideal of $(A, +, \cdot)$. The quotient ring of A by I is $(A/I, +, \cdot)$, where $(A/I, +)$ is the quotient subgroup of $(A, +)$ by $(I, +)$ and the binary operation $\cdot$, given by $(a + I) \cdot (a' + I) = (a \cdot a' + I)$ is well defined.*
The canonical projection map $\pi : A \to A/I$ is a ring morphism, whose kernel is precisely I.

Property 2.2.12 (Ideals of a quotient)**.** *There is one-to-one correspondence between the ideals of A/I and the ideals of A containing I:*

$$\begin{array}{rcl} \{\textit{Ideals of } A/I\} & \simeq & \{J \textit{ ideal of } A : I \subset J\} \\ \mathcal{I} & \mapsto & \pi^{-1}(\mathcal{I}) \\ \pi(J) & \leftarrow\!\shortmid & J \end{array}$$

Theorem 2.2.13 (Isomorphism theorem)**.** *Let $\phi : A_1 \to A_2$ a surjective ring morphism. Then there exists a unique homomorphism $\hat{\phi} : A_1/\ker\phi \to A_2$, such that the following diagram is commutative:*

$$\begin{tikzcd} A_1 \arrow[r, "\phi"] \arrow[d, "\pi"'] & A_2 \\ A_1/\ker\phi \arrow[ru, "\hat{\phi}"'] & \end{tikzcd}$$

i.e. $\phi = \hat{\phi} \circ \pi$; furthermore $\hat{\phi}$ is an isomorphism.

Example. Let $f : P(X) \in \mathbb{R}[X] \mapsto P(i) \in \mathbb{C}$. Then $\ker(f)$ is the ideal generated by $X^2 + 1$ and one has the isomorphism $\mathbb{R}[X]/(X^2 + 1) = \mathbb{C}$.

Definition 2.2.14. *An ideal I of a ring A is called* prime *if $I \neq A$ and for all $a, b \in I$*

$$ab \in I \Rightarrow a \in I \text{ or } b \in I.$$

An ideal I is called maximal *if $I \neq A$ and for all ideal J s.t. $I \subset J$, either $I = J$ or $J = A$.*

Exercise 16.

1. Show that I is a prime ideal of A iff A/I is a domain.
2. Show that I is a maximal ideal of A iff A/I is a field.
3. Deduce that a maximal ideal is necessarily prime.

2.2.1 The rings $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$

1. $\mathbb{Z}$ is principal (from Euclidean division)
2. prime ideals are $p\mathbb{Z}$ (and so maximal since the quotient is a field)
3. $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$
4. $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$

If $n = \prod (p_i)^{\alpha_i}$, then

1. $\mathbb{Z}/n\mathbb{Z} \simeq \prod \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$
2. $\mathbb{Z}/n\mathbb{Z}^\times \simeq \prod (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$
3. $\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z}^\times) = \prod \varphi(p_i^{\alpha_i}) = n \prod (1 - 1/p_i)$

2.2.2 Polynomial rings

Definition 2.2.15. *Let A be a ring. The ring of polynomials in n variables and coefficients in A is*

$$A[X_1, \ldots, X_n] = \left\{ \sum_{\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n} c_\alpha X_1^{\alpha_1} \ldots X_n^{\alpha_n} \right\},$$

where there are only finitely many non-zero coefficients $c_\alpha \in A$.

Property 2.2.16. *1. There is a canonical isomorphism $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$.*

2. The ring $A[X_1, \ldots, X_n]$ is a domain if and only if A is a domain.

3. If A is a domain then $A[X_1, \ldots, X_n]^\times = A^\times$.

Proof. 2. Using 1., by induction on the number of variables it suffices to show that $A[X]$ is a domain if A is a domain (the "only if" part is clear since $A \subset A[X]$). So let P and Q be two non-zero elements of $A[X]$, A domain. Then the leading coefficient of the product PQ is the product of the leading coefficients of P and Q, which cannot vanishes since A is a domain; in particular $PQ \neq 0$.

3. By induction it suffices again to consider the case of $A[X]$, which is settled by looking at the leading coefficients.

□

Euclidean division : The Euclidean division algorithm in $A[X]$ is similar to the algorithm in $\mathbb{Z}$: at each step, one tries to cancel out the highest order term of the dividend. For instance in $\mathbb{Z}[X]$, the division of $3X^5 + 2X^4 - X^3 - 7X + 5$ by $X^2 - X + 2$ is carried out as follows:

$$\begin{array}{rrrrrr|l}
3X^5 & +2X^4 & -X^3 & & -7X & +5 & X^2 - X + 2 \\ \hline
3X^5 & -3X^4 & +6X^3 & & & & 3X^3 + 5X^2 - 2X - 12 \\
 & 5X^4 & -7X^3 & & -7X & +5 & \\
 & 5X^4 & -5X^3 & +10X^2 & & & \\
 & & -2X^3 & -10X^2 & -7X & +5 & \\
 & & -2X^3 & +2X^2 & -4X & & \\
 & & & -12X^2 & -3X & +5 & \\
 & & & -12X^2 & +12X & -24 & \\
 & & & & -15X & +29 &
\end{array}$$

$\Rightarrow 3X^5 + 2X^4 - X^3 - 7X + 5 = (X^2 - X + 2)(3X^3 + 5X^2 - 2X - 12) - 15X + 29$.
This algorithm may fail when the leading coefficient of the divisor is not invertible: for instance in $\mathbb{Z}[X]$ it does not work for the division of $3X^2 + 1$ by $2X$. This is not an issue if A is a field.

Theorem 2.2.17. *Let K a field.*

1. *Euclidean division: for all $P_1, P_2 \in K[X]$, $P_2 \neq 0$, there exist unique $Q, R \in K[X]$ s.t. $P_1 = P_2Q + R$ with $\deg R < \deg P_2$.*
2. *$K[X]$ is principal.*

Proof. (Principality of $K[X]$). Let $\mathcal{I} \neq \{0\}$ be an ideal of $K[X]$. Let P_m be a polynomial in $\mathcal{I}$ such that $\deg P_m = \min\{\deg P : P \in \mathcal{I}, P \neq 0\}$; we want to show that $\mathcal{I} = (P_m)$. Let P be a polynomial in $\mathcal{I}$, then there exist Q, R such that $P = P_mQ + R$, $\deg R < \deg P_m$. Since P_m and P are in $\mathcal{I}$, $P - P_mQ = R$ is also in $\mathcal{I}$. But $\deg R < \deg P_m = \min\{\deg P : P \in \mathcal{I}, P \neq 0\}$, so $R = 0$ and $P = P_mQ$, i.e. $P \in (P_m)$. □

The polynomial P_m is called the *minimal polynomial* of $\mathcal{I}$; it is unique if it is required to be monic (i.e. its leading coefficient equals 1).

Remark. $A[X]$ is never principal if A is not a field. In particular $K[X_1, \ldots, X_n]$ is not principal if $n \geq 2$ (consider the ideal (X_1, X_2)).

Since $K[X]$ is principal, we can define gcd's and lcm's as in the integer case. These notions are only well-defined up to multiplication by a non-zero constant, so we will require polynomials to be monic. We will not develop here the theory in several variables.

Definition 2.2.18 (Gcd and lcm)**.** *Let P_1, P_2 be two polynomials in $K[X]$. The gcd of P_1 and P_2 is the monic polynomial $G = P_1 \wedge P_2$ such that $(G) = (P_1) + (P_2)$. The lcm of P_1 and P_2 is the monic polynomial $L = P_1 \vee P_2$ such that $(L) = (P_1) \cap (P_2)$. The polynomials P_1 and P_2 are coprime if $P_1 \wedge P_2 = 1$.*

Property 2.2.19.

- *$Q|P_1$ and $Q|P_2 \Leftrightarrow Q|(P_1 \wedge P_2)$.*
- *$P_1|Q$ and $P_2|Q \Leftrightarrow (P_1 \vee P_2)|Q$.*
- *Gauss: if P and Q are coprime and $P|QR$, then $P|R$.*
- *Bézout: there exist $U, V \in K[X]$ such that $UP_1 + VP_2 = (P_1 \wedge P_2)$*

Gcd's and Bézout coefficients can be computed with the extended Euclid algorithm, as in the integer case.

Exercise 17.

1. Compute the gcd of $X^5+2X^4+2X^3+3X^2+4X+4 \in \mathbb{Z}/7\mathbb{Z}[X]$ and $X^4+3X^3+5X^2+3X+1 \in \mathbb{Z}/7\mathbb{Z}[X]$. (Answer: X^2+4X+1).
2. Compute the Bézout coefficients of $P_1 = X^3+2X^2+2X+1 \in \mathbb{Z}/3\mathbb{Z}[X]$ and $P_2 = X^3+X^2+2 \in \mathbb{Z}/3\mathbb{Z}[X]$. (Answer: $(2X+1)P_1 + XP_2 = 1$).

We can also define a congruence relation for polynomials in an obvious fashion, so that working modulo a polynomial $P \in K[X]$ is equivalent to working in $K[X]/(P)$. In particular, using the Euclidean division we see that the elements of $K[X]/(P)$ (i.e. the residue classes modulo P) are in one-to-one correspondence with the set of polynomials of $K[X]$ of degree strictly smaller than $\deg P$.

Property 2.2.20.

- *Chinese remainder theorem: let P_1 and P_2 two coprime polynomials in $K[X]$, then for any polynomials Q_1, Q_2, the equations $\begin{cases} P = Q_1 \bmod P_1 \\ P = Q_2 \bmod P_2 \end{cases}$ have a solution, unique modulo P_1P_2.*
- *Modular inverse: a polynomial $Q \in K[X]$ is invertible modulo P (i.e. there exists R s.t. $QR = 1 \bmod P$) iff Q and P are coprime.*

Exercise 18.

1. Find a polynomial P in $\mathbb{Z}/3\mathbb{Z}[X]$ such that $\begin{cases} P = X^2+X \bmod X^3+2X^2+2X+1 \\ P = 2X+1 \bmod X^3+X^2+2 \end{cases}$
2. In $\mathbb{Z}/2\mathbb{Z}[X]$, is X^3+X+1 invertible modulo X^4+X^2+1 ? If so, compute its modular inverse. (Answer: yes, X^3+X^2+1).

Definition 2.2.21. *A polynomial $P \in K[X_1, \ldots, X_n]$ is* irreducible *if $\deg P > 0$ and P is not a product of two non-invertible polynomials, i.e.*

$$P = P_1P_2 \quad \Rightarrow \quad P_1 \in K^* \text{ or } P_2 \in K^*.$$

Example. The irreducible polynomials of $\mathbb{C}[X]$ (or more generally $K[X]$ where K is algebraically closed) are exactly the degree one polynomials. In $\mathbb{R}[X]$, the irreducible polynomials are the degree one polynomials and the degree 2 polynomials of negative discriminant.

Theorem 2.2.22 (Unique factorization)**.** *Any non-zero polynomial $P \in K[X]$ can be written as*

$$P = c\,P_1^{\alpha_1} \dots P_k^{\alpha_k},$$

where $c = LC(P) \in K^*$, $\alpha_i \in \mathbb{N}$, and the polynomials P_i are monic irreducible. This decomposition is unique up to permutation and terms with exponent zero.

Remark. This theorem is also true for polynomials in several variables. The gcd and lcm of two polynomials can be recovered from this factorization as in the integer case.

Exercise 19.

1. List all the irreducible polynomials of $\mathbb{Z}/2\mathbb{Z}[X]$ of degree up to 4.
2. Factorize $X^7 + 1 \in \mathbb{Z}/2\mathbb{Z}[X]$.

Proposition 2.2.23. *The following are equivalent:*

1. *$\mathcal{I}$ is a prime ideal of $K[X]$;*
2. *$\mathcal{I}$ is a maximal ideal of $K[X]$;*
3. *$\mathcal{I} = (P)$ where $P \in K[X]$ is irreducible.*

Proposition 2.2.24 (Roots)**.**

- *Let A be a ring and $P \in A[X]$. Then $(X - a)|P$ if and only if $P(a) = 0$.*
- *Let A be a domain. Then a polynomial $P \in A[X]$ has at most $\deg P$ distinct roots.*

Proof. For the first statement, we write the Euclidean division of P by $X - a$ (which is possible since $LC(X - a) = 1$): $P = (X - a)Q + c$, where $c \in A$ since $\deg c < 1$. Then $P(a) = (a - a)Q(a) + c = c$, so $P(a) = 0$ iff $P = (X - a)Q$.
In the case A is a field, the second part follows from the unique factorization of P. To prove the general case it suffices to work in the field of fractions of A. □

Remark. Things can go quite wrong when A is not a domain. For instance in $\mathbb{Z}/12\mathbb{Z}[X]$, $X^2 - 1 = (X + 1)(X - 1) = (X - 5)(X - 7)$.

2.2.3 Vector spaces

Definition 2.2.25. *Let K be a field. Let E be a set endowed with a binary operation $+$ and a* scalar multiplication, *i.e. a map $K \times E \to E$, $(a, x) \mapsto a \cdot x$. Then E, together with this two operations, is a* K-vector space *if:*

1. *$(E, +)$ is an abelian group;*
2. *for all $a \in K$ and $x, y \in E$, $a \cdot (x + y) = a \cdot x + a \cdot y$;*
3. *for all $a, b \in K$ and $x \in E$, $(a + b) \cdot x = a \cdot x + b \cdot x$;*
4. *for all $a, b \in K$ and $x \in E$, $(ab) \cdot x = a \cdot (b \cdot x)$;*

5. *for all $x \in E$, $1 \cdot x = x$.*

Example. For $n \geq 1$, the set of n-tuples K^n has a natural K-v.s. structure, for the operations $(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$ and $a \cdot (a_1, \dots, a_n) = (a\,a_1, \dots, a\,a_n)$.

Definition 2.2.26. *Let E be a K-vector space. A family $\{u_1, \dots, u_n\}$ of elements of K is* linearly independent *if*

$$\forall a_1, \dots, a_n \in K, \quad a_1 u_1 + \dots a_n u_n = 0 \;\Rightarrow\; a_1 = \dots = a_n = 0.$$

A family that is not linearly independent is called linearly dependent; equivalently, $\{u_1, \dots, u_n\}$ is linearly dependent if there exist $a_1, \dots, a_n \in K$, at least one of which is not zero, such that $a_1 u_1 + \dots a_n u_n = 0$.

Definition 2.2.27. *A K-vector space E is called* finite-dimensional *if there exists a (finite) family $\{u_1, \dots, u_n\}$ of elements of E such that every element of E is a linear combination of the u_i, i.e.*

$$\forall v \in E,\ \exists\, a_1, \dots, a_n \in K,\ v = a_1 u_1 + \dots + a_n u_n.$$

Such a family is called a spanning set *of E.*

Definition 2.2.28. *Let E be a finite-dimensional K-vector space. A* basis *of E is a spanning set $\{u_1, \dots, u_n\}$ which is also linearly independent. Equivalently, $\{u_1, \dots, u_n\}$ is a basis of E if for any $v \in E$, there exists a* unique *tuple $(a_1, \dots, a_n) \in K^n$ s.t. $v = a_1 u_1 + \dots + a_n u_n$.*

Theorem 2.2.29. *Let E be a finite-dimensional K-vector space. Then E admits a basis. Furthermore, all bases of E contains the same number of elements, called the* dimension *of E.*

Chapter 3

Elementary field theory

3.1 Characteristic, prime fields

Lemma 3.1.1. *For any ring A, there exists a unique ring morphism $f : \mathbb{Z} \to A$.*

Proof. By definition, $f(1) = 1_A$, so for any $n \geq 0$, $f(n) = f(1+\cdots+1) = f(1)+\cdots+f(1) = 1_A+\cdots+1_A$ (n times) and $f(-n) = -f(n)$. □

Definition 3.1.2. *The* characteristic *of a ring A is the integer $char(A) \geq 0$ such that* $\ker(f) = char(A)\mathbb{Z}$.

In particular, the isomorphism theorem shows that A contains a subring isomorphic to $\mathbb{Z}/char(A)\mathbb{Z}$. If the morphism f is injective then $char(A) = 0$ and A contains a copy of $\mathbb{Z}$ as a subring.

Proposition 3.1.3. *The characteristic of a field (or of a domain) is either 0 or a prime number p. Every field K contains a subfield, called its* prime field, *either isomorphic to $\mathbb{Q}$ if $char(K) = 0$ or isomorphic to $\mathbb{Z}/char(K)\mathbb{Z}$ otherwise.*

Proof. If the characteristic of a ring A is equal to a composite number $n = n_1 n_2$, then $f(n_1) \cdot f(n_2) = f(n_1 n_2) = f(n) = 0$ but $f(n_1) \neq 0$ and $f(n_2) \neq 0$, so that A is not a domain. For the second part, the positive characteristic case has already been discussed. If $char(K) = 0$ then K contains a subring isomorphic to $\mathbb{Z}$, but it must also contains the inverses of all the elements of this subring and finally all fractions of $\mathbb{Q}$. □

Example. The characteristic of the fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}(X)$ is zero. Examples of characteristic p fields are $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z}(X)$ (the field of rational fractions with coefficients in $\mathbb{Z}/p\mathbb{Z}$).

3.2 Field extension

Lemma 3.2.1. *Let K, L be two fields and $f : K \to L$ a ring morphism. Then f is injective.*

Proof. We know that $\ker f = \{x \in K : f(x) = 0_L\}$ is an ideal of K. But K is a field, so its only ideals are the trivial ones $\{0\}$ and K. Since $f(1_K) = 1_L$, $\ker f$ is strictly smaller than K and so is equal to $\{0\}$: f is injective. □

Definition 3.2.2. *Let K be a subfield of a field L. Then L is called an* extension *of K, which is denoted by L/K.*
If K_1 and K_2 are two fields and there exists a ring morphism $K_1 \to K_2$, then we can identify K_1 with its image in K_2 and consider the extension $K_2/f(K_1)$; when the context is clear this will also be simply denoted by K_2/K_1 and we will also say that K_2 is an extension of K_1.

Proposition 3.2.3. *Let L/K be a field extension. Then L has a natural K-vector space structure. The dimension of L as a K-vector space is denoted $[L : K]$ and is called the* degree *of this extension.*

Indeed, the scalar multiplication of $l \in L$ by $k \in K \subset L$ is just the field product $k \cdot l$ in L.

Corollary 3.2.4. *Every finite field has a cardinality of the form p^n where p is prime and $n \in \mathbb{N}$.*

Proof. Let K be a field whose cardinality is finite. It cannot contain a subfield isomorphic to $\mathbb{Q}$, which is infinite, so its characteristic is a prime number p and its prime field K_0 is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Obviously K is an extension of K_0. Let n be the degree of the extension K/K_0; n is finite since otherwise K would be infinite. So K is a dimension n vector space over $K_0 \simeq \mathbb{Z}/p\mathbb{Z}$; in particular its cardinality is p^n. □

We will see later that in fact, for any p and n, there exists up to isomorphism a unique field with p^n elements.

Theorem 3.2.5 (Multiplicative formula for degrees)**.** *Let M/L and L/K two field extensions, then M/K is an extension field and*

$$[M : K] = [M : L] \cdot [L : K].$$

Proof. Check that if $\{e_1, \ldots, e_n\}$ is a basis of M over L and $\{f_1, \ldots, f_m\}$ is a basis of L aver K then $\{e_i f_j : 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis of M over K. □

Definition 3.2.6. *Let L/K be an extension and $A \subset L$. We define $K(A)$ (resp. $K[A]$) as the smallest subfield (resp. subring) of L containing K and A; the field $K(A)$ is of course an extension of K. If A is a finite set $\{a_1, \ldots, a_n\}$ then $K(A)$ (resp. $K[A]$) is more usually denoted by $K(a_1, \ldots, a_n)$ (resp. $K[a_1, \ldots, a_n]$).*

Remark. Let L/K be a field extension and $a \in L$. Then

$$K[a] = \{P(a) : P \in K[X]\} \text{ and } K(a) = \{P(a)/Q(a) : P, Q \in K[X], Q(a) \neq 0\}.$$

Definition 3.2.7. *Let L/K be a field extension and $a \in L$. Let $\phi : K[X] \to L$ the map that sends a polynomial P to $P(a)$; it is a ring morphism.*

- *If ϕ is injective (i.e. $\ker \phi = \{0\}$) then a is called* transcendental *over K.*
- *If ϕ is not injective then a is called* algebraic *over K. The minimal polynomial of the (principal) ideal $\ker \phi$ is called the minimal polynomial of a over K; by definition, it is the smallest degree monic polynomial $P_m \in K[X]$ such that $P_m(a) = 0$.*

Example. The real numbers π and e are transcendental over $\mathbb{Q}$. For any field K, the element X of $K(X)$ is transcendental over K. The real numbers $\sqrt{3}, i, \sqrt[3]{2}$ are algebraic over $\mathbb{Q}$: their minimal polynomials are respectively $X^2 - 3$, $X^2 + 1$ and $X^3 - 2$.

Proposition 3.2.8. *Let a be a transcendental element over K. Then $K[a] \simeq K[X]$ and $K(a) \simeq K(X)$; in particular, $K[a] \neq K(a)$.*

Theorem 3.2.9. *Let L/K be a field extension and $a \in L$. The following are equivalent:*

1. *a is algebraic over K;*
2. *$K[a] = K(a)$;*
3. *$[K(a) : K] < \infty$.*

Proof. $3 \Rightarrow 1$ and $2 \Rightarrow 1$: we have seen that if a is not algebraic over K then $K[a] \neq K(a)$ and $K(a) \simeq K(X)$, which is infinite-dimensional as a K-vector space.
$1 \Rightarrow 2$ and $1 \Rightarrow 3$: let P_m be the minimal polynomial of a over K. Then P_m is irreducible; indeed, if $P_m = P_1 P_2$ where P_1 and P_2 are non-constant polynomials, then $P_m(a) = 0 = P_1(a)P_2(a)$, so either $P_1(a) = 0$ or $P_2(a) = 0$, which contradicts the minimality of P_m. Now the isomorphism theorem shows that $K[a] \simeq K[X]/(P_m)$. Since P_m is irreducible the ideal (P_m) is maximal, so $K[X]/(P_m) \simeq K[a]$ is a field, and thus $K[a]$ is equal to $K(a)$. In particular, every element of $K(a)$ is of the form $P(a)$ for some $P \in K[X]$. But the Euclidean division of P by P_m shows that $P(a) = Q(a)P_m(a) + R(a) = R(a)$, so in fact every element of $K(a)$ is of the form $R(a) = \sum_{i=1}^{\deg R} c_i a^i$ for some $R \in K[X]$ of degree strictly smaller than $\deg P_m$. This implies that $\{1, a, a^2, \ldots, a^{\deg P_m - 1}\}$ is a spanning set of the K-vector space $K(a)$, which is thus finite-dimensional. □

Remark. It is actually not difficult to show that if a is algebraic over K, then $\deg P_m = [K(a) : K]$ and $\{1, a, \ldots, a^{\deg P_m - 1}\}$ is a K-basis of $K(a)$. If $n = [K(a) : K]$ we say that a is algebraic of degree n.

Exercise 20. Let a be an algebraic element of minimal polynomial $P_m \in K[X]$ and P an element of $K[X]$ such that $P(a) \in K(a)$ is different from 0. How can one compute a polynomial $Q \in K[X]$ such that $Q(a) = (P(a))^{-1}$?

Definition 3.2.10. *An extension L/K is called* finite *if $[L : K] < \infty$.*
An extension L/K is called algebraic *if every element of L is algebraic over K.*

A finite extension cannot contain transcendental elements and so is algebraic. The converse is not true: an algebraic extension of K may not be finite (if it is generated by an infinite number of elements).

Exercise 21 . Show that if L/K is finite then there exist elements $a_1, \ldots, a_n \in K$ such that $L = K(a_1, \ldots, a_n)$.

Proposition 3.2.11. *Let K be a field. The following are equivalent:*

1. *every non-constant polynomial $P \in K[X]$ admits a root in K;*
2. *every non-constant polynomial $P \in K[X]$ is a product of degree 1 polynomials;*
3. *the irreducible polynomials of $K[X]$ are the $X - a$, $a \in K$;*
4. *if L/K is an algebraic extension then $L = K$.*

A field K is called algebraically closed *if it satisfies these properties.*

Exercise 22. Show the equivalence of the four points above.

Example. The field $\mathbb{C}$ is algebraically closed (fundamental theorem of algebra). For any prime p, the field $\mathbb{Z}/p\mathbb{Z}$ is not algebraically closed: the polynomial $\prod_{a=0}^{p-1}(X-a)+1$ has no roots.

Theorem 3.2.12. *Let K be a field. Then there exists an algebraically closed field $\bar{K}$ containing K and such that the extension $\bar{K}/K$ is algebraic. Such a field $\bar{K}$ is called an* algebraic closure *of K.*

Example. $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. It is however not an algebraic closure of $\mathbb{Q}$ since the extension $\mathbb{C}/\mathbb{Q}$ is not algebraic (the algebraic closure of $\mathbb{Q}$ is strictly contained in $\mathbb{C}$).

Definition 3.2.13. *Let L/K a field extension and $a_1,\dots,a_n \in L$. The family $\{a_1,\dots,a_n\}$ is called* algebraically independent *(over K) if there is no non-trivial polynomial relation over K between its elements, i.e.*

$$\forall P \in K[X_1,\dots,X_n], \quad P(a_1,\dots,a_n)=0 \;\Rightarrow\; P=0.$$

The transcendence degree *of the extension L/K is the largest cardinality of an algebraically independent family in L.*

Example.

- An element $a \in L$ is transcendental over K iff the family $\{a\}$ is algebraically independent. The transcendence degree of an extension is zero iff the extension is algebraic.
- It is not known if the family $\{\pi, e\}$ is algebraically independent over $\mathbb{Q}$. It is however possible to show that the transcendence degree of $\mathbb{R}/\mathbb{Q}$ is infinite (otherwise $\mathbb{R}$ would be countable).
- The family $\{X_1,\dots,X_n\}$ in $K(X_1,\dots,X_n)$ is algebraically independent over K, and the transcendence degree of this extension is n.

Property 3.2.14. *The transcendence degree of an extension L/K is n if and only if there exists a subfield M, $K \subset M \subset L$, such that the extension L/M is algebraic and M is isomorphic to $K(X_1,\dots,X_n)$.*

Definition 3.2.15. *An* automorphism *of a field K is a bijective ring morphism $K \to K$. If L/K is an extension, then a map $f: L \to L$ is K-automorphism of L if it is an automorphism of L and $f(k)=k$ for all $k \in K$.*
If L/K and M/K are two extensions, a ring morphism $f: L \to M$ is called a K-morphism if it fixes every element of K, i.e. $f(k)=k$ for all $k \in K$.

Exercise 23.

1. Show that the only $\mathbb{R}$-automorphisms of $\mathbb{C}$ are the identity and the complex conjugation. (There exist however many more automorphisms of $\mathbb{C}$.)
2. Let K be a field and K_0 its prime field. Show that every automorphism of K is a K_0-automorphism.
3. Let f be an automorphism of $\mathbb{R}$, show that f is the identity (hint: show that f is strictly increasing).

Definition 3.2.16. *Let L be a field and $P=\sum_{i=0}^{d} c_i X^i$ a polynomial in $L[X]$. Let σ be an automorphism of L. Then the image of P by σ is the polynomial*

$$P^\sigma = \sum_{i=0}^{d} \sigma(c_i) X^i \in L[X].$$

In particular, for any $a \in L$ one has $\sigma(P(a)) = P^\sigma(\sigma(a))$.

Definition 3.2.17. *The* Galois group *of an extension L/K is the set $Gal(L/K)$ of K-automorphisms of L; it is a group for the composition law. The* absolute *Galois group of a field K is the Galois group of the extension $\bar{K}/K$ where $\bar{K}$ is the algebraic closure of K.*

Remark. Sometimes the term "Galois group" is restricted to a specific kind of extensions (Galois extensions) and the more general term "K-automorphism group", denoted $Aut_K(L)$, is used. The aim of Galois theory is to relate the subgroups of the Galois group with the sub-extensions of L/K, but this will not be discussed in these lectures.

Theorem 3.2.18. *Let L/K be a finite field extension, then $|Gal(L/K)| \leq [L : K]$.*

Proof. We will only show this for extensions generated by a unique element, i.e. for $L = K(a)$ for some $a \in L$. Let P_m be the minimal polynomial of a and $n = [K(a) : K]$ its degree; we know that every element $x \in K(a)$ can be written as $x = \sum_{i=0}^{n-1} c_i a^i$ where $c_0, \dots, c_{n-1}$ are in K. Let σ be a K-automorphism of $K(a)$. Then $\sigma(x) = \sigma(\sum_{i=0}^{n-1} c_i a^i) = \sum_{i=0}^{n-1} \sigma(c_i)\sigma(a)^i = \sum_{i=0}^{n-1} c_i \sigma(a)^i$. This shows that a K-automorphism of $K(a)$ is completely determined by the image of a, namely, if σ and τ are two K-automorphisms such that $\sigma(a) = \tau(a)$ then $\sigma = \tau$. But the value of $\sigma(a)$ cannot be arbitrary. Indeed, since $P_m(a) = 0$, one must have $\sigma(P_m(a)) = P_m^\sigma(\sigma(a)) = \sigma(0) = 0$. But $P_m^\sigma = P_m$ because P_m has coefficients in K, so $P_m(\sigma(a))$ must be zero. Since P_m has at most n distinct roots, this implies that there are at most n distinct K-automorphisms of $K(a)$. □

Definition 3.2.19. *Let K be a field and S a set of automorphisms of K. Then the* fixed field *of S is the set*

$$K^S = \{k \in K : \sigma(k) = k \text{ for all } \sigma \in S\}.$$

Remark. It is immediate to show that K^S is indeed a field. It is also clear that if G is the group of automorphisms generated by S then $K^S = K^G$.

3.3 Rupture field and splitting field

Definition 3.3.1. *Let $P = \sum_{i=0}^{d} a_i X^i$ be a polynomial of $K[X]$. Its* (formal) derivative *is the polynomial $P' = \sum_{i=0}^{d} (i.a_i) X^{i-1}$, where $i.a_i$ is a shorthand for $a_i + \dots + a_i$ (i times).*

Property 3.3.2. *The formal derivative satisfies the usual derivative properties: for all $P, Q \in K[X]$ and $a \in K$, $(P+Q)' = P' + Q'$, $(aP)' = a(P')$, and $(PQ)' = P'Q + Q'P$.*

Exercise 24. Determine all the polynomials whose derivatives is zero.

Proposition 3.3.3. *Let K be a field and $\bar{K}$ its algebraic closure. Let P be a non-zero polynomial in $K[X]$ and $\alpha \in \bar{K}$ a root of P. Then α is a multiple root of P if and only if $P'(\alpha) = 0$. In particular, P has no multiple root in $\bar{K}$ if and only if $gcd(P, P') = 1$.*

Definition 3.3.4. *Let P be a polynomial in $K[X]$ and L/K a field extension. The field L is called a* rupture field *of P if there exists an element $\alpha \in L$ such that $P(\alpha) = 0$ and $L = K(\alpha)$. The field L is called a* splitting field *of P if there exist $\alpha_1, \dots, \alpha_{\deg P} \in L$ such that $P = c\prod(X - \alpha_i)$ and $L = K(\alpha_1, \dots, \alpha_{\deg P})$*

In other words, a rupture field for P is obtained by adjoining to the base field a root of P, while a splitting field is obtained by adjoining all the roots of P. Note that rupture fields are usually defined only for irreducible polynomials since otherwise there is an ambiguity on the irreducible factor whose root is adjoined.

Theorem 3.3.5. *Let $P \in K[X]$ be an irreducible polynomial. There exists a rupture field L for P. Furthermore, if L and L' are two rupture fields for P then there exists a K-isomorphism $L' \to L$, i.e. the rupture field is unique up to isomorphism.*

Proof. Existence: if d is the degree of P we can write P as $\sum_{i=0}^{d} c_i X^i$. We start by considering the polynomial $P(T) = \sum_{i=0}^{d} c_i T^i \in K[T]$ and the quotient ring $L = K[T]/(P(T))$. Since P is irreducible, the ideal $(P(T))$ is maximal so L is a field. Furthermore L contains K as the residue classes of the constant polynomials, thus it is an extension of K. Let t be the residue class of T, i.e. its equivalence class in the quotient; it is clear that $L = K(t)$. We claim that t is a root of $P \in K[X] \subset L[X]$ (note that elements of the later ring are polynomials whose coefficients are themselves residue classes of polynomials). Indeed, since t is the residue class of T, $P(t) = \sum_{i=0}^{d} c_i t^i$ is the residue class of $P(T)$, which is exactly the zero element of L.
Uniqueness: we will show that any rupture field L of P is isomorphic to $K[T]/(P(T))$. Let $\alpha \in L$ be a root of P such that $L = K(\alpha)$. Since $P(\alpha) = 0$, P is a multiple of the minimal polynomial P_m of α, and the irreducibility of P implies that $P = P_m$ (possibly up to multiplication by a constant in K^* if P is not monic). Now we have already seen in the proof of Theorem 3.2.9 that $K(\alpha)$ is isomorphic to $K[X]/(P_m) \simeq K[T]/(P(T))$. □

Remark.

- The rupture field of an irreducible polynomial may or may not be also its splitting field. For instance, the field $\mathbb{Q}(\sqrt[3]{2})$ is a rupture field for $P = X^3 - 2 \in \mathbb{Q}[X]$, but it does not contain the two other roots $j\sqrt[3]{2}$ and $j^2\sqrt[3]{2}$, and P only factorizes as $(X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + (\sqrt[3]{2})^2)$ over $\mathbb{Q}(\sqrt[3]{2})$. On the other hand, the field $\mathbb{Q}(e^{i\pi/4})$ is both a rupture field and a splitting field of the polynomial $X^4 + 1 \in \mathbb{Q}[X]$.
- The isomorphism between two rupture fields is not unique in general. For instance, as rupture fields of $X^2 + 1$ over $\mathbb{R}$, $\mathbb{R}[T]/(T^2 + 1)$ and $\mathbb{C}$ are isomorphic but there are two possible isomorphisms, depending whether the class of T is sent to i or $-i$.

Theorem 3.3.6. *Let $P \in K[X]$ a polynomial. There exists a splitting field L for P. Furthermore, if L and L' are two splitting fields for P then there exists a K-isomorphism $L' \to L$, i.e. the splitting field is unique up to isomorphism.*

Proof. The existence of a splitting field follows from the existence of rupture fields. The idea is to start with a irreducible factor (of degree > 1) of P and consider its rupture field L_1. If P splits over L_1 then $L = L_1$; otherwise we choose an irreducible factor in the decomposition of P over L_1 and consider its rupture field L_2. We go on like that, enlarging the field K until P becomes a product of degree 1 factors. Likewise, the uniqueness of the splitting field follows from the uniqueness (up to isomorphism) of rupture fields. □

Exercise 25 . Let L be the splitting field of a polynomial $P \in K[X]$. Show that $[L : K]$ divides $(\deg P)!$.

3.4 Finite fields

Proposition 3.4.1. *Let p be a prime number, K a characteristic p field and $K_0 \simeq \mathbb{Z}/p\mathbb{Z}$ its prime field. The map $\Phi_p : K \to K$, $x \mapsto x^p$ is a morphism, called the* Frobenius morphism, *and its fixed field K^{Φ_p} is exactly K_0.*

Proof. In order to show that the Frobenius map is a morphism we just have to check that $(x+y)^p = x^p + y^p$ for all $x, y \in K$. This results from the binomial formula $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$ and from the following easy lemma:

Lemma 3.4.2. *Let p be a prime number and k an integer such that $1 \leq k \leq p-1$. Then p divides $\binom{p}{k}$.*

Now $\Phi_p(x) = x$ iff x is a root of $X^p - X$. But we already know that $x^p = x$ for all elements of $K_0 \simeq \mathbb{Z}/p\mathbb{Z}$ (this is Fermat's little theorem, see exercice 14). Thus the p roots of $X^p - X$ are exactly the elements of K_0. □

Remark. As a morphism between fields, the Frobenius morphism is always injective. In particular if K is a finite field then Φ_p is a bijective map and is thus called the Frobenius automorphism. Note however that Φ_p is not always surjective, as is the case for $\mathbb{Z}/p\mathbb{Z}(X)$.

Theorem 3.4.3 (Existence and uniqueness of finite fields)**.** *Let p be a prime number and $q = p^n$, $n \in \mathbb{N}^*$. Up to isomorphism, there exists a unique field with q elements, denoted by $\mathbb{F}_q$ or $GF(q)$ (where GF stands for Galois field).*

Proof. First of all, it is clear that every field of cardinality p is isomorphic to $\mathbb{Z}/p\mathbb{Z} = GF(p)$ and that the isomorphism is unique (because it is completely determined by the fact that 1 is mapped to 1).
Existence: let L be the splitting field of the polynomial $P_q = X^q - X$ over $GF(p)$. Since $(X^q - X)' = -1$, P_q has no multiple roots and thus exactly q distinct roots in L. Let $K = \{x \in L : x \text{ is a root of } P_q\} = \{x \in L : x^q = x\}$. But the map $\Phi_q : x \mapsto x^q$ is just the Frobenius automorphism iterated n times: $\Phi_q = (\Phi_p)^n$. So Φ_q is an automorphism of L and its fixed field is $L^{\Phi_q} = K$. This shows that K is actually a field, containing exactly q elements which are the q roots of $X^q - X$ (so K is in fact the splitting field of $X^q - X$, i.e. $K = L$).
Uniqueness: let K be a field with q elements. Then K^* is a multiplicative group of order $q-1$, and in particular $x^{q-1} = 1$ for all $x \in K^*$ (see Property 2.1.12). In other words $x^q = x$ for all $x \in K^*$, and in fact for all $x \in K$. The polynomial $X^q - X \in GF(p)[X]$ is thus split over K, and obviously K is a splitting field for this polynomial. Uniqueness follows from the uniqueness of the splitting field of $X^q - X$ up to isomorphism. □

We have already seen the converse in Corollary 3.2.4, namely that the cardinality of a finite field is necessarily of the form p^n. In the following of these lectures q will always denote a prime power.

Theorem 3.4.4. *If K is a field, any finite subgroup of K^* is cyclic. In particular, the multiplicative group $GF(q)^*$ is cyclic.*

Proof. Let G be a finite subgroup of K^* and m its order. The structure theorem for finitely generated abelian group (Theorem 2.1.14) shows that there exist $n_1, \ldots, n_k$ such that $n_1 | n_2 | \ldots | n_k$, $m = n_1 n_2 \ldots n_k$ and $G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ (beware that the group law is the multiplication on the left hand side and the addition on the right hand side). In particular, the order of every element of G divides n_k, i.e. $x^{n_k} = 1$ for all $x \in G$. But the polynomial $X^{n_k} - 1$ has at most n_k roots in K whereas G has $m = n_1 \ldots n_k$ elements. This implies that $n_k = m$ and $k = 1$, and so $G \simeq \mathbb{Z}/m\mathbb{Z}$.
Note that it is possible to prove this theorem without relying on the structure theorem of abelian groups; the key observation is still that because $X^d - 1$ has at most d roots, there are at most d elements in G whose order divides d. □

Corollary 3.4.5. *For any p prime and $n \geq 1$, there exists $\alpha \in GF(p^n)$ such that $GF(p^n) = GF(p)(\alpha)$. In particular, there exist irreducible polynomials of degree n in $GF(p)[X]$ for any n. Furthermore, for any irreducible polynomial $P \in GF(p)[X]$ of degree n, the field $GF(p^n)$ is isomorphic to $GF(p)[X]/(P)$.*

Proof. Let α be a generator of $GF(p^n)^*$, then it is clear that $GF(p)(\alpha) = GF(p^n)$; its minimal polynomial is irreducible and has degree $[GF(p^n) : GF(p)] = n$. If $P \in GF(p)[X]$ is an arbitrary irreducible polynomial of degree n, then $GF(p)[X]/(P)$ is a field and a degree n extension of $GF(p)$, so it is actually $GF(p^n)$. □

Remark. This corollary has several important consequences:

- In order to compute in $GF(q)$ it is always possible to consider residue classes of polynomials of $GF(p)[X]$. Thus working in $GF(q)$ is no more difficult that working modulo an irreducible polynomial and allows for efficient implementations.
- Any degree n irreducible polynomial can be used to define $GF(p^n)$. Of course, some of them may be preferable for efficiency reasons.

Note also that in order to have $GF(q) = GF(p)(\alpha)$ it is not necessary that α is a generator of $GF(q)^*$.

Exercise 26.

1. Describe the fields $GF(4)$, $GF(8)$ and $GF(9)$. Give the multiplicative order and the minimal polynomial (over the prime field) of all the elements.
2. Let $P \in GF(p)[X]$ be a degree n irreducible polynomial so that $GF(p^n) = GF(p)[X]/(P)$. In particular, any element of $GF(p^n)$ is the equivalence class of a polynomial of degree $< n$. Give two different methods to compute the inverse of an element in this representation. Which one is faster ?

Remark. Working in $GF(p^n)$ is **not** the same as working modulo p^n! $\mathbb{Z}/p^n\mathbb{Z}$ is **not** equal to $GF(p^n)$ when $n > 1$.

Proposition 3.4.6. *The group $Aut(GF(p^n))$ of automorphisms of $GF(p^n)$ is cyclic of order n and is generated by the Frobenius automorphism Φ_p.*

Proof. We have seen that any automorphism of $GF(p^n)$ fixes $GF(p)$ (see Exercise 23), so that $Aut(GF(p^n)) = Gal(GF(p^n)/GF(p))$, and Theorem 3.2.18 shows that the cardinality of this group is bounded by n. Thus it is sufficient to prove that $\Phi_{p^k} = (\Phi_p)^k$ is different from the identity for any $1 \leq k < n$. So suppose that Φ_{p^k} is the identity map. Then $\Phi_{p^k}(x) = x^{p^k} = x$ for all $x \in GF(p^n)$, i.e. every element of $GF(p^n)$ is a root of $X^{p^k} - X$. But this polynomial has at most $p^k < p^n$ roots, which is a contradiction. □

Proposition 3.4.7. *Let p be a prime and m, n two positive integers. Then $GF(p^n)$ contains a subfield isomorphic to $GF(p^m)$ if and only if $m|n$. Furthermore if $m|n$ then $GF(p^n)$ has only one subfield isomorphic to $GF(p^m)$, which is the fixed field of Φ_{p^m}, and $Gal(GF(p^n)/GF(p^m)) = \langle \Phi_{p^m} \rangle \simeq \mathbb{Z}/\frac{n}{m}\mathbb{Z}$.*

Proof. If $GF(p^m)$ is a subfield of $GF(p^n)$ then $GF(p^n)$ is a $GF(p^m)$-vector space of dimension $d = [GF(p^n) : GF(p^m)]$, so $p^n = (p^m)^d = p^{md}$ and thus $n = md$.
Reciprocally, suppose that $n = md$, and consider the field $K = GF(p^n)^{\Phi_{p^m}}$. Its elements are exactly the roots in $GF(p^n)$ of $X^{p^m} - X$; in other words K consists of 0 and the roots of $X^{p^m-1} - 1$, i.e. the elements of $GF(p^n)^*$ whose order divides $p^m - 1$. Now it is easy to check that $p^m - 1$ is a divisor of $p^n - 1 = p^{md} - 1$, which is the cardinality of $GF(p^n)^*$. Since $GF(p^n)^*$ is a cyclic group, it has exactly one subgroup of cardinality $p^m - 1$, whose elements are precisely those of order dividing $p^m - 1$ (see Proposition 2.1.13). This shows that the finite field K has indeed p^m elements, and also that it is the only such subfield of $GF(p^n)$.
Finally, the proof that $Gal(GF(p^n)/GF(p^m)) = \langle \Phi_{p^m} \rangle \simeq \mathbb{Z}/d\mathbb{Z}$ is similar to the proof of Proposition 3.4.6. □

Property 3.4.8. *Let $q = p^n$ be a prime power and m a positive integer. There exists $\alpha \in GF(q^m)$ which generates the extension $GF(q^m)/GF(q)$, i.e. $GF(q^m) = GF(q)(\alpha)$. In particular, there exist irreducible polynomials of degree m in $GF(q)[X]$ for any m.*

Proof. As in the proof of Corollary 3.4.5, one can choose for α any generator of the cyclic group $GF(q^m)$, and its minimal polynomial over $GF(q)$ is irreducible. □

Remark. This means that there are (at least) two different ways to represent elements in $GF(p^{mn})$. One can either work with polynomials in $GF(p)[X]$ modulo a degree mn irreducible polynomial, or with polynomials in $GF(p^n)[X]$ modulo a degree m irreducible polynomial.

Proposition 3.4.9. *Let q be a prime power and $P \in GF(q)[X]$ a degree d irreducible polynomial. Then*

1. *P has no multiple roots (in an algebraic closure);*
2. *$GF(q^d)$ is both a rupture field and a splitting field for P.*

Proof. Since P is irreducible then P and P' are coprime (and so P has no multiple roots) unless $P' = 0$. If $P' = 0$ then P is of the form $\sum_k a_k X^{kp}$, see Exercise 24. But the Frobenius map $x \mapsto x^p$ is bijective on $GF(q)$, so for any k there exists b_k such that $a_k = b_k^p$. It follows that $P = \sum_k b_k^p X^{kp} = (\sum_k b_k X^k)^p$, which contradicts the fact that P is irreducible.
We know that a rupture field for P is $GF(q)[T]/(P(T)) \simeq GF(q^d)$. Let t be the class of T; it is a root of P and generates the extension, i.e. $GF(q^d) = GF(q)(t)$. Let $\sigma = \Phi_q$ be the q-th Frobenius automorphism. Then for all i with $0 \leq i < d$, $\sigma^i(P(t)) = 0 = P^{\sigma^i}(\sigma^i(t)) = P(\sigma^i(t))$ since P has coefficients in $GF(q)$. So $t, \sigma(t), \sigma^2(t), \ldots, \sigma^{d-1}(t)$ are roots of P, and they are all distinct (because if $\sigma^i(t) = \sigma^j(t)$ then $\sigma^i = \sigma^j$ on $GF(q^d) = GF(q)(t)$ and we know that σ has order d). So P has all its roots in $GF(q^d)$, which is thus the splitting field of P. □

Exercise 27. Let $P \in GF(q)[X]$ be a polynomial of degree 5. Find all the possible extension degrees of its splitting field (compare with Exercise 25).

Exercise 28. Give the factorization of $X^q - X$ over $GF(p)$, where $q = p^n$.

Exercise 29. Let p be a prime number and q be an odd prime power.

1. Show that $a \in GF(q)^*$ is a square (i.e. there exists $x \in GF(q)^*$ such that $a = x^2$) iff $a^{(q-1)/2} = 1$. Can the algorithm that computes square roots modulo p be applied to $GF(q)$?

2. Show that the following algorithm computes square roots modulo p:

```
Algorithm 3: Computation of square roots in $\mathbb{Z}/p\mathbb{Z}^*$
  Input  : $a$ a quadratic residue modulo $p$
  Output: $x$ such that $x^2 = a \bmod p$
  Select $b$ at random until $(b^2 - 4a)^{(p-1)/2} = -1 \bmod p$
  $f \leftarrow X^2 + bX + a$
  Compute $r = X^{(p+1)/2} \bmod f$ with a square-and-multiply algorithm
  return $r$
```

What is it complexity ? Can it be applied to $GF(q)$?

Exercise 30.

1. Show that for any $a \in GF(2^m)$, the equation $x^2 = a$ has a unique solution in $GF(2^m)$.
2. Let $a \in GF(2^m)$. Show that the equation $x^2+x+a = 0$ has a solution in $GF(2^m)$ iff $\sum_{i=0}^{m-1} a^{2^i} = 0$. (Hint: show that the maps $f : x \mapsto x^2 + x$ and $g : x \mapsto \sum_{i=0}^{m-1} x^{2^i}$ are $GF(2)$-linear and that $\operatorname{Im} f = \ker g$).

Exercise 31. Let p be a prime. For n and m two integers such that $n|m$, we will consider $GF(p^n)$ as a subfield of $GF(p^m)$.

- Show that $K = \bigcup_k GF(p^{k!})$ is a field (Note that the sequence $GF(p^{k!})$ is increasing).
- Show that the extension $K/GF(p)$ is algebraic.
- Show that K is algebraically closed.
- Deduce from the previous questions that K is an algebraic closure of $GF(p)$, and in fact of $GF(p^n)$ for all positive integers n.

Chapter 4

Elliptic curves

In all this chapter, unless otherwise mentioned all fields considered are either characteristic zero fields, finite fields or algebraically closed fields. We will use without proof the following fact:

Theorem 4.0.10. *$K[X_1, \ldots, X_n]$ is noetherian, i.e. its ideals are finitely generated: for all ideal $\mathcal{I} \subset K[X_1, \ldots, X_n]$ there exist $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ such that $\mathcal{I} = (f_1, \ldots, f_s)$.*

4.1 Basic algebraic geometry

Algebraic geometry (at its basic level) studies the properties of sets defined by polynomial equations.

Definition 4.1.1. *A subset $V \subset K^n$ is an* affine algebraic set *if there exists an ideal $\mathcal{I} \subset K[X_1, \ldots, X_n]$ such that*

$$V = \{P = (x_1, \ldots, x_n) \in K^n : \forall f \in \mathcal{I},\ f(x_1, \ldots, x_n) = 0\}.$$

This is denoted by $V = \mathbb{V}(\mathcal{I})$. If $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ are a set of generators of $\mathcal{I}$, i.e. $\mathcal{I} = (f_1, \ldots, f_s)$, then V is the set of solutions of the polynomial system

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \quad\vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases}$$

Example. The unit circle in $\mathbb{R}^2$ is an algebraic set; it is $\mathbb{V}(X^2+Y^2-1)$. The algebraic set $\mathbb{V}(XZ, YZ) \subset K^3$ is the union of the plane $Z = 0$ with the line of equation $\begin{cases} X = 0 \\ Y = 0 \end{cases}$

Exercise 32. What are the algebraic sets of $K = K^1$?

Note that in general different ideals can define the same algebraic set, e.g. $\mathbb{V}(X) = \mathbb{V}(X^2)$, or in $\mathbb{R}^2$, $\mathbb{V}(1) = \mathbb{V}(X^2 + Y^2 + 1) = \emptyset$. But there is always a largest ideal defining a given algebraic set:

Proposition 4.1.2. *Let V be an affine algebraic set. The set*

$$\mathbb{I}(V) = \{f \in K[X_1, \ldots, X_n] : \forall P = (x_1, \ldots, x_n) \in V,\ f(x_1, \ldots, x_n) = 0\}$$

is an ideal of $K[X_1, \ldots, X_n]$, and $\mathbb{V}(\mathbb{I}(V)) = V$.

Definition 4.1.3. *An (affine) algebraic set V is* irreducible *if it is not a non-trivial union of two algebraic sets, i.e. for all algebraic sets V_1 and V_2 such that $V = V_1 \cup V_2$, either $V_1 = V$ or $V_2 = V$. An affine* variety *is an irreducible affine algebraic set.*

Example. The algebraic set $\mathbb{V}(XZ, YZ) \in K^3$ of the previous examples is clearly not irreducible. A point $(x_1, \ldots, x_n)$ is an algebraic set (it is $\mathbb{V}(X_1 - x_1, \ldots, X_n - x_n)$) and is irreducible.

Proposition 4.1.4. *An affine algebraic set V is irreducible if and only if $\mathbb{I}(V)$ is a prime ideal.*

Definition 4.1.5. *Let V be an affine algebraic set. Its* coordinate ring *is the quotient ring*

$$K[V] = K[X_1, \ldots, X_n]/\mathbb{I}(V).$$

If V is a variety, then $K[V]$ is a domain and its fraction ring $K(V) = Frac(K[V])$ is called the function field *of V.*

Remark. The idea behind this definition is that we want to identify two polynomials if they are equal on V, i.e. if they differ by an element of $\mathbb{I}(V)$. So the coordinate ring is in some sense the ring of polynomial functions on V.

Definition 4.1.6. *Let $f \in K[V]$ and $P \in V$, and $F \in K[X_1, \ldots, X_n]$ an element in the class of f. The* value *of f at P is $f(P) = F(P)$; this is well-defined.*
Let $\phi \in K(V)$ and $P \in V$. If there exist $f, g \in K[V]$ such that $\phi = f/g$ and $g(P) \neq 0$, then ϕ is defined *at P and its value is $\phi(P) = f(P)/g(P)$. If there exist $f, g \in K[V]$ such that $\phi = f/g$ and $f(P) \neq 0, g(P) = 0$ then ϕ has a* pole *at P. If for all $f, g \in K[V]$ such that $\phi = f/g$, one has $f(P) = g(P) = 0$ then ϕ is* undetermined *at P.*

Exercise 33. Let $\mathcal{C} = \mathbb{V}(Y^2 - X^3 - X^2)$, $\psi = Y/(X+1) \in K(V)$, and $\phi = X/Y \in K(V)$. What can be said of ψ, ϕ, and ϕ^2 at $P_1 = (0,0)$ and $P_2 = (-1,0)$?

Definition 4.1.7. *Let K be a field and $\bar{K}$ its algebraic closure. An ideal $\mathcal{I} \subset \bar{K}[X_1, \ldots, X_n]$ is* defined over *K if there exist $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ such that $\mathcal{I} = (f_1, \ldots, f_s)$. If $\mathcal{I}$ is defined over K, we set $\mathcal{I}_K = \mathcal{I} \cap K[X_1, \ldots, X_n]$; it is an ideal of $K[X_1, \ldots, X_n]$, generated by $f_1, \ldots, f_s$.*
An affine algebraic set $V \subset \bar{K}^n$ is defined over *K if $\mathbb{I}(V)$ is defined over K; this is denoted by $V_{|K}$. In that case, the set $V(K) = V \cap K^n$ is called the set of K-*rational points *of V.*

Remark.

- If $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ generates the ideal $\mathcal{I}$ defined over K, then $V(K)$ is exactly the set of solutions in K^n of the system $f_1(x_1, \ldots, x_n) = \cdots = f_s(x_1, \ldots, f_s) = 0$.
- If V is defined over K then it is also defined over any larger field L with $K \subset L \subset \bar{K}$. In particular it makes sense to speak of the set $V(L)$ of L-rational points of V.

Example. Let $n \geq 3$ an integer and $V = \mathbb{V}(X^n + Y^n - 1) \subset \bar{\mathbb{Q}}^2$. It is an affine algebraic set defined over $\mathbb{Q}$, and Fermat-Wiles theorem states that the only $\mathbb{Q}$-rational points of V are $\{(1,0),(0,1)\}$ or $\{(\pm 1, 0), (0, \pm 1)\}$.

4.2 Projective space

Introduction: the projective line. Consider in the plane the line D of equation $x = 1$. Let Δ be a line going through $(0,0)$. The ordinate of the intersection point of D and Δ is exactly the slope of Δ, so that the point of D are in one-to-one correspondence with the lines passing through the origin, except for the vertical one. However as Δ comes close to being vertical, the intersection point of D

and Δ "goes to infinity". If we add a "point at infinity" to D and call $\bar{D}$ the result, we obtain a complete one-to-one correspondence between the points of $\bar{D}$ and the lines passing through the origin. The "projective line" $\bar{D}$ can thus also be defined as the set of lines of the plane passing through $(0, 0)$. With this definition, the "point at infinity" becomes no longer singular. In fact, we could have started this construction with the line D' of equation $y = 1$. Then the vertical line corresponds to the point $(0, 1) \in \bar{D}'$, and it is now the horizontal that appears to be "at infinity". This will be made more formal.

Introduction: the projective plane. We recall that the usual, affine plane P satisfies the following axioms:

- any two distinct points lie on a unique line
- two lines are either parallel or intersect in exactly one point
- given a line and a point there is a unique line which contains a point and is parallel to the line

This distinction between parallel lines and intersecting lines is somewhat annoying. Furthermore, anyone who has looked at train tracks knows that parallel lines do appear to intersect "at infinity". So we add to the affine plane "points at infinity": actually we add one point for each line direction (i.e. equivalence class of parallel lines). The projective plane $\bar{P}$ so constructed satisfies the following modified axioms:

- any two distinct points lie on a unique line
- any two distinct lines intersect in a unique point

Note that every line of $\bar{P}$ is a projective line. Note also that by the first axiom two points at infinity must belong to a line: this is the "line at infinity", consisting of all the points we have added to P. But if we just look at the axioms, we see that the points at infinity play exactly the same role as the other points.

As for the projective line, the projective plane is in one-to-one correspondence with the set of lines passing through the origin $(0, 0, 0)$ in the 3-space. We can consider P as the plane of equation $z = 1$. Then any line through the origin intersects P in exactly one point, except for those contained in the plane of equation $z = 0$. But we know that the set of these lines is a projective line, which is exactly the line "at infinity" we have added to construct $\bar{P}$ from P.

Definition 4.2.1. *Let K field. The* projective n-space *over K is the set of lines through the origin, or one-dimensional linear subspace, of K^{n+1}. In other words,*

$$\mathbb{P}^n(K) = (K^{n+1} - \{0\})/_\sim$$

where $(x_0, \ldots, x_n) \sim (\lambda x_0, \ldots, \lambda x_n)$ for any $\lambda \in K^*$. The equivalence class of $(x_0, \ldots, x_n)$ is denoted by $[x_0 : \cdots : x_n]$; this notation is called homogeneous *or* projective coordinates*.*

Definition 4.2.2. *For $0 \leq i \leq n$, the* affine chart *$U_i \subset \mathbb{P}^n(K)$ is the set $\{[x_0 : \cdots : x_n] : x_i \neq 0\}$. The affine chart U_i is in one-to-one correspondence with the affine n-space via the map $[x_0 : \cdots : x_n] \mapsto (x_0/x_i, \ldots, x_{i-1}/x_i, x_{i+1}/x_i, \ldots, x_n/x_i)$. Then the set $\{[x_0 : \cdots : x_n] : x_i = 0\}$ is isomorphic to $\mathbb{P}^{n-1}(K)$ and is the* hyperplane at infinity *in U_i.*

Remark. More generally, if H is a projective hyperplane of $\mathbb{P}^n(K)$, then its complement $\mathbb{P}^n(K) \setminus H$ is an affine chart.

Exercise 34.

1. Construct $\mathbb{P}^2(\mathrm{GF}(2))$ and list all its lines.
2. Compute the number of points of $\mathbb{P}^n(\mathrm{GF}(q))$.

4.3 Projective algebraic set

Definition 4.3.1. *A polynomial $f \in K[X_0, \ldots, X_n]$ is called* homogeneous *of degree d if for all $\lambda \in K$, $P(\lambda X_0, \ldots, \lambda X_n) = \lambda^d P(X_0, \ldots, X_n)$. Equivalently, all the monomials of P have total degree d.*
An ideal $\mathcal{I} \subset K[X_0, \ldots, X_n]$ is homogeneous if it is generated by homogeneous polynomials.

Definition 4.3.2. *Let $f \in K[X_1, \ldots, X_n]$ a polynomial of total degree d. Then $f^h = X_0^d f(X_1/X_0, \ldots, X_n/X_0)$ is a degree d homogeneous polynomial in $K[X_0, \ldots, X_n]$, called the* homogenization *of f (with respect to X_0.*
Conversely, if $g \in K[X_0, \ldots, X_n]$ is homogeneous, its deshomogenization *(with respect to X_0) is $g^* = g(1, X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$.*
Homogenization and deshomogenization are partial inverses : for all f, $(f^h)^* = f$, but for all homogeneous g, $(g^*)^h$ is equal to g only up to multiplication by a power of X_0.

Definition 4.3.3. *Let $f \in K[X_0, \ldots, X_n]$ a homogeneous polynomial and $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$. We say that f vanishes at P if $f(x_0, \ldots, x_n) = 0$; this is denoted by $f(P) = 0$ and is independent of the choice of projective coordinates for P.*
Let $f, g \in K[X_0, \ldots, X_n]$ two homogeneous polynomials of same degree d and $P = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ such that g does not vanish at P. Then the value of the rational fraction $\frac{f}{g}$ at P is well-defined and is equal to $\frac{f}{g}(P) = f(x_0, \ldots, x_n)/g(x_0, \ldots, x_n)$.

Remark. In general, it does not make sense to speak of the value of a polynomial (even homogeneous) at a point $P \in \mathbb{P}^n(K)$.

Definition 4.3.4. *A subset $V \in \mathbb{P}^n(K)$ is a* projective algebraic set *if there exists a homogeneous ideal $\mathcal{I} \subset K[X_0, \ldots, X_n]$ such that*

$$V = \{P \in \mathbb{P}^n(K) : f(P) = 0 \textit{ for all homogeneous } f \in \mathcal{I}\}.$$

This is denoted by $V = \mathbb{V}(\mathcal{I})$. If $f_1, \ldots, f_s \in K[X_1, \ldots, X_n]$ are a set of homogeneous generators of $\mathcal{I}$, then V is the set of points P such that $f_1(P) = \cdots = f_s(P) = 0$.
If V is a projective algebraic set, its associated homogeneous ideal is the ideal $\mathbb{I}(V)$ generated by the set $\{f \in K[X_0, \ldots, X_n] : f \text{ homogeneous}, f(P) = 0\ \forall P \in V\}$. If $\mathbb{I}(V)$ is prime then V is called a projective variety*.*

Remark. Contrarily to the affine case, $\mathbb{I}(V)$ is generated by (and thus larger than) the set of homogeneous polynomials that vanish on V. Also, there is no notion of coordinate ring for a projective algebraic set.

Definition 4.3.5. *Let V be projective variety. The* function field *of V is defined as*

$$K(V) = \{f/g : f, g \in K[X_0, \ldots, X_n] \textit{ are homogeneous of same degree and } g \notin \mathbb{I}(V)\}/\sim$$

where $f/g \sim f'/g'$ if $fg' - f'g \in \mathbb{I}(V)$. As in the affine case, a function $\phi \in K(V)$ can be defined, have a pole or be undetermined at a point $P \in V$; in the first case its value $\phi(P)$ is well-defined.

Proposition 4.3.6. *Let K^n the affine space, that we identify with the affine chart $U_0 \subset \mathbb{P}^n(K)$. Let $V = (f_1, \dots, f_s)$ an affine algebraic set, where $f_1, \dots, f_s \in K[X_1, \dots, X_n]$. Then $\bar{V} = \mathbb{V}(f_1^h, \dots, f_s^h)$ is the smallest projective algebraic set containing $V \subset U_0 \subset \mathbb{P}^n(K)$, and is called the* projective closure *of V.*
Furthermore, if V is a variety then $\bar{V}$ is also a variety and $K(V) = K(\bar{V})$.

Definition 4.3.7. *Let $V \subset \mathbb{P}^n(K)$ and $V' \subset \mathbb{P}^m(K)$ two varieties. A* rational map *$\phi : V \to V'$ is the data of $(f_0, f_1, \dots, f_m) \in K(V)^{m+1}$ such that for any $P \in V$ where all the f_i are defined and do not all vanish, $\phi(P) = [f_0(P) : f_1(P) : \dots : f_m(P)]$ belongs to V'. Two $(m+1)$-tuples $(f_0, \dots, f_{m+1})$ and $(f'_0, \dots, f'_{m+1})$ define the same rational map if there exists $g \in K(V)^*$ such that $f'_i = gf_i$ for all i.*
A rational map $\phi = (f_0, \dots, f_m)$ is defined at a point $P \in V$ if there exists $g \in K(V)$ such that the gf_i are all defined and do not vanish at P. A rational map that is defined everywhere is called a morphism. *A morphism $\phi : V \to V'$ is an* isomorphism *if there exists a morphism $\psi : V' \to V$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity map (of V' and V respectively).*

4.4 Elliptic curves

Definition 4.4.1. *A (projective or algebraic) variety V is a* curve *if its function field $K(V)$ has transcendence degree* 1 *over K*

In the following we will mostly deal with *plane curves*, i.e. curves whose affine part is defined by an equation of the form $f(x, y) = 0$, where $f \in K[x, y]$ is an irreducible polynomial.

Definition 4.4.2 (Smooth point)**.** *Let $\mathcal{C}$ a plane curve defined over K by $f(x, y) = 0$. A point $P = (x_0, y_0) \in \mathcal{C}$ is* smooth *if the (formal) partial derivatives $\frac{\partial f}{\partial x}(x_0, y_0)$ and $\frac{\partial f}{\partial y}(x_0, y_0)$ do not vanish simultaneously. The plane curve is called* smooth *or* non-singular *if all its points are smooth.*
The tangent *to $\mathcal{C}$ at a smooth point $P = (x_0, y_0)$ is the line of equation $(x - x_0)\frac{\partial f}{\partial x}(x_0, y_0) + (y - y_0)\frac{\partial f}{\partial y}(x_0, y_0) = 0$.*

Remark. Note that for a projective plane curve to be smooth, its points "at infinity" must also be smooth, which has to be checked in an other affine chart.

Definition 4.4.3. *An* elliptic curve *E defined over K is a non-singular projective plane curve whose equation in an affine chart is of the following form, called* Weierstraß equation*:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in K.$$

More generally, any curve isomorphic to a curve admitting a non-singular Weierstraß equation is also called elliptic.

Property 4.4.4. *An elliptic curve admit a unique point "at infinity", of projective coordinates* $[0 : 1 : 0]$*. This point is smooth and will be denoted by $\mathcal{O}$.*

The general Weierstraß equation can be simplified. In characteristic other than 2, with a change of variable of the form $y' = y + a_1x/2 + a_3/2$ the equation becomes

$$y'^2 = x^3 + a'_2x^2 + a'_4x + a'_6.$$

If the characteristic is also different from 3, another change $x' = x + a'_2/3$ yields the more usual form

$$y'^2 = x^3 + Ax + B.$$

Other simplifications can be done in characteristic 2 (and 3, but we will leave this case aside).

Proposition 4.4.5. *Every elliptic curve admits an equation of the form*

$$y^2 = x^3 + a_4x + a_6 \tag{4.1}$$

if the characteristic is different from 2 *and* 3*, or*

$$y^2 + xy = x^3 + a_2x^2 + a_6 \tag{4.2}$$

or

$$y^2 + a_3y = x^3 + a_4x + a_6 \tag{4.3}$$

in characteristic 2.
The equation of the form (4.1) *is non-singular iff* $4a_4^3 + 27a_6^2 \neq 0$*, and similarly for the equations of the form* (4.2) *and* (4.3) *iff* $a_6 \neq 0$ *and* $a_3 \neq 0$ *respectively.*

Proposition 4.4.6. *Let* E *be an elliptic curve defined over* K *and* L *a line. Then* $E \cap L$ *consists of exactly three points in* $\mathbb{P}^n(\bar{K})$*, counted with multiplicity. If we restrict to* K*-rational points then the intersection consists of zero, one or three points.*

Remark. By multiplicity, we mean that a point $P \in E \cap L$ counts double if L is the tangent at P, and triple if furthermore P is an inflexion point (this happens in particular if P is $\mathcal{O}$ and L is the line at infinity). Note also that every vertical line intersects E at $\mathcal{O}$.

Theorem 4.4.7. *Let* E *be an elliptic curve in* $\mathbb{P}^n(\bar{K})$*. Then there exists a unique abelian group law on the set of points of* E *such that*

- *the neutral element is* $\mathcal{O}$*;*
- *for any line* L*, the sum of the three points of* $L \cap E$ *is* $\mathcal{O}$*.*

If furthermore E *is defined over a field* $K \subset \bar{K}$*, then the set of* K*-rational points* $E(K)$ *forms a subgroup.*

Proof. Let $P = (x_1, y_1)$ a point of E. The vertical line of equation $x = x_1$ also intersects E in $P' = (x_1, -y_1 + a_1x + a_3)$ and in $\mathcal{O}$. The two axioms imply that P' is necessary the opposite of P, denoted by $-P$. Now let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ two points of E such that $P_2 \neq -P1$. According to Proposition 4.4.6, the line passing through P_1 and P_2 (or the tangent at P_1 if $P_1 = P_2$) intersects E in a third point $P_3 = (x_3, y_3)$, which is K-rational if P_1 and P_2 are also K-rational. The second axiom implies that $P_1 + P_2 + P_3 = \mathcal{O}$, so the sum $P_1 + P_2$ is necessary equal to the point $-P3 = (x_3, -y_3 + a_1x_3 + a_3)$. Thus the operation law $+$ on E (and on $E(K)$ is well-defined and is clearly commutative, the existence of a neutral element and of opposites is clear, and it only remains to show that this law is associative. This can be computationally checked once the addition formulas will be given. □

Formulas for the addition law:

We have seen that if $P = (x_0, y_0)$ then $-P = (x_0, -y_0 + a_1x + a_3)$. One also has, obviously, that $P + \mathcal{O} = P$ and $P + (-P) = \mathcal{O}$. So let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ two points of $E(K) \setminus \mathcal{O}$ such that $P_2 \neq -P1$. There are two cases :

- If $P_2 \neq P_1$, i.e. $x_2 \neq x_1$: the line L through P_1 and P_2 has equation $y = \lambda x + \mu$ where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\mu = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}$. Replacing y by $\lambda x + \mu$ in the equation of E, we obtain a degree 3 polynomial equation $x^3 + (a_2 - \lambda^2 - a_1 \lambda)x^2 + \cdots = 0$, of which x_1 and x_2 are already roots. If $P_3 = (x_3, y_3)$ is the third intersection point of E and L then x_3 is the third root of this polynomial so that $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda + a_2$, and $y_3 = \lambda x_3 + \mu$. The point $P_1 + P_2$ is then $-P_3 = (x_3, -y_3 + a_1 x_3 + a_3)$. To sum up, if $x_1 \neq x_2$ then $P' = P_1 + P_2$ has coordinates

$$x' = \lambda^2 + a_1\lambda + a_2 - x_1 - x_2, \quad y' = -\lambda x' - \mu + a_1 x' + a_3, \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \mu = \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1}.$$

- If $P_1 = P_2$ only the equation of L changes since it is now the tangent at P_1; its equation is $y = \lambda x + \mu$ where $\lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}$ and $\mu = y_1 - \lambda x_1$. Thus the point $P' = 2P$ has coordinates

$$x' = \lambda^2 + a_1\lambda + a_2 - 2x_1, \quad y' = -\lambda x' - \mu + a_1 x' + a_3, \quad \lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}, \quad \mu = y_1 - \lambda x_1.$$

Obviously these expressions are much simpler when using the reduced equations of Proposition 4.4.5

Theorem 4.4.8. *Let $q = p^n$ be a prime power and E an elliptic curve defined over $GF(q)$. Then $E(GF(q))$ is a finite group, and one has the* Hasse bound

$$-2\sqrt{q} \leq |E(GF(q)| - q + 1 \leq 2\sqrt{q}.$$

As a group,

$$E(GF(q)) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

where n_1 and n_2 are two integers such that $n_1 | n_2$ and $n_1 | q - 1$ (note that it is possible to have $n_1 = 1$).