Algebraic Curves and Applications to Cryptography

Summer Term 2012

Université du Luxembourg

Sara Arias-de-Reyna, Gabor Wiese
sara.ariasdereyna@uni.lu
gabor.wiese@uni.lu

Version of 21st June 2012

Contents

Preface

These are notes of a one-term course (12 lectures of 90 min each) taught for students in the 6th term of the Bachelor programme at the University of Luxembourg in Summer Term 2012. Although the students had some familiarity with concepts from Algebra from previous lectures, almost no prerequisites were assumed.

The lecture starts with fundamentals of elementary number theory, that is, Euclid's algorithm, Gauß' theorem on unique factorisation of integers, and the Chinese remainder theorem, as well as some basic group theory. These concepts are applied to the RSA algorithm, which is treated in the second section. Finite fields are dealt with in generality in the third section, before being applied in the Diffie-Hellman key exchange and the El Gamal encryption scheme in the subsequent section. Section 5 contains a gentle introduction to plane curves, which is specialised to elliptic curves and extended in the subsequent section. The final section is concerned with elliptic curves over finite fields and gives a glimpse at their applications in cryptography.

In preparing these lectures we used several sources:

- Lecture notes by Gebhard Böckle and the second author from the Universität Duisburg-Essen.
- Silverman: *The Arithmetic of Elliptic Curves*.
- Washington: *Elliptic Curves, Number Theory and Cryptography*.
- Werner: *Elliptische Kurven in der Kryptographie*.

Luxembourg, June 2012.
Sara Arias-de-Reyna, Gabor Wiese

1 Some aspects of elementary number theory

The purpose of this first section is to survey the most basic concepts from elementary number theory. All students (should) have seen them before, but, it cannot hurt to recall them.

The way we present elementary number theory here is that its most fundamental concept is that of Euclid's algorithm.

Theorem 1.1 (Euclid, Bézout)**.** *Let $a, b \in \mathbb{Z}$ not both zero. Then* Euclid's algorithm *computes the greatest common divisor d of a, b, notation $d = \gcd(a, b)$, that is:*

- $d \geq 1$,
- $d \mid a$, $d \mid b$,
- *for any $e \geq 1$ such that $e \mid a$ and $e \mid b$, one has $e \mid d$.*

Moreover, the extended Euclid's algorithm *gives $r, s \in \mathbb{Z}$ such that*

$$d = ar + bs.$$

The proof is completely algorithmic. The algorithm is practiced in an exercise on Sheet 1.

Definition 1.2. *An integer $p \geq 2$ is called a* prime number *if its only positive divisors are 1 and p.*

Theorem 1.3 (Gauß; fundamental theorem of elementary number theory)**.** *Any $n \in \mathbb{N}$, $n \geq 2$, can be written as a finite product of prime numbers: There is $r \in \mathbb{N}$ and there are prime numbers $p_1, \ldots, p_r$ such that*

$$n = p_1 \cdot p_2 \cdots p_r.$$

Up to renumbering, the prime numbers occuring in the product are unique, that is: if $n = q_1 \cdot q_2 \cdots q_s$ is another such product, then $r = s$ and there is σ in the symmetric group on the letters $\{1, \ldots, r\}$ such that $q_i = p_{\sigma(i)}$ for all $i \in \{1, \ldots, r\}$.

We are going to prove this theorem. The proof is not as trivial as one might guess. It essentially uses the extended Euclid's algorithm. The existence part, however, is completely straight forward:

Proof of existence in Theorem 1.3. Let $n \geq 2$. By induction we prove the following statement:

> There are finitely many prime numbers $p_1, \ldots, p_r$ such that $n = p_1 \cdot p_2 \cdots p_r$.

Since $n = 2$ is obviously a prime number, the statement for $n = 2$ is true. Let us now suppose we have proved the statement for all integers up to $n - 1$. We prove it for n. First case: n is a prime number. Then the statement is obviously true. Second case: $n = ab$ with $1 < a < n$. We know that we can write a and b both as finite products of prime numbers, hence, the statement for n follows. □

Definition 1.4. *Let R be a ring. By $R^\times$ we denote the set of units of R, i.e. the elements $x \in R$ such that there is $y \in R$ with $1 = xy$.*

An element $0 \neq p \in R \setminus R^\times$ is called a prime element of R *if, whenever p divides a product ab with $a, b \in R$, then p divides one of the factors, i.e. $p \mid a$ or $p \mid b$.*

Lemma 1.5. *Let R be a ring and $p \in R$ a prime element. If p divides a product $r_1 r_2 \cdots r_s$ with $r_i \in R$, then p divides one of the factors, i.e. there is $i \in \{1, \ldots, s\}$ such that $p \mid r_i$.*

Proof. Iterated application of the definition. □

The next lemma shows that prime numbers and prime elements in $\mathbb{Z}$ are essentially the same.

Lemma 1.6. *Let $p \geq 2$ be an integer. Then*

$$p \text{ is a prime number } \Leftrightarrow \ p \text{ is a prime element in } \mathbb{Z}.$$

Proof. '$\Rightarrow$': Let $a, b \in \mathbb{Z}$ and suppose $p \mid ab$. If $p \mid a$, then we are done. So assume $p \nmid a$. Since the only positive divisors of p are 1 and p and p does not divide a, it follows that $1 = \gcd(a, p)$. Hence, there are $x, y \in \mathbb{Z}$ such that $1 = ax + py$. Multiply this equation by b and get: $b = abx + py$. As p divides ab by assumption and obviously p divides py, it follows that p divides b, as was to be shown.

'$\Leftarrow$': Suppose $p = ab$ with positive integers a, b. Then, as p is a prime element in $\mathbb{Z}$, it follows $p \mid a$ or $p \mid b$. Consequently, $a \geq p$ or $b \geq p$, thus $a = p$ or $b = p$, showing that p is a prime number. □

Proof of uniqueness in Theorem 1.3. We again prove this by induction on n. The case $n = 2$ is obvious. Let us suppose that we have proved the statement for all positive integers up to $n - 1$. Now consider n. We have, thus, prime numbers $p_1, \ldots, p_r$ and $q_1, \ldots, q_s$ such that

$$n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s.$$

By Lemmas 1.6 and 1.5 it follows that the prime number p_1 is a prime element which divides one of the q_i (for $i \in \{1, \ldots, s\}$), since it divides the product $q_1 \cdot q_2 \cdots q_s$. As q_i is a prime number, too, we must have $p_1 = q_i$. Dividing both sides by p_1, we obtain

$$n/p_1 = p_2 \cdot p_3 \cdots p_r = q_1 \cdot q_2 \cdots q_i \cdot q_{i+1} \cdots q_s.$$

As we already know the statement for n/p_1, we are done. □

Also the following famous theorem is based on the extended Euclid's algorithm.

Theorem 1.7 (Chinese Remainder Theorem)**.** *Let $n, m \in \mathbb{N}$ such that $\gcd(n, m) = 1$. Then the map*

$$\Phi : \mathbb{Z}/(nm) \to \mathbb{Z}/(n) \times \mathbb{Z}/(m), \quad a + (nm) \mapsto \big(a + (n), a + (m)\big)$$

is an isomorphism of rings.

Proof. The homomorphism property is easily checked.

Injectivity: Suppose $a \in \mathbb{Z}$ is in (n) and in (m). This means that $n \mid a$ and $m \mid a$. As $\gcd(n, m) = 1$, it follows $nm \mid a$, which means $a \in (nm)$, showing the injectivity.

Surjectivity: As $\gcd(n, m) = 1$, there are $x, y \in \mathbb{Z}$ such that $1 = nx + my$. We just have to interpret this equation in the right way. It means that $N := nx = 1 - my$ satisfies:

$$N \equiv 0 \mod (n) \text{ and } N \equiv 1 \mod (m).$$

In the same way we have that $M := my = 1 - nx$ satisfies:

$$M \equiv 0 \mod (m) \text{ and } M \equiv 1 \mod (n).$$

Let $b, c \in \mathbb{Z}$ and consider $\big(b + (n), c + (m)\big) \in \mathbb{Z}/(n) \times \mathbb{Z}/(m)$. Then $a := bM + cN$ is an element such that

$$a \equiv b \mod (n) \text{ and } a \equiv c \mod (m),$$

i.e. $\Phi(a + (nm)) = \big(b + (n), c + (m)\big)$, showing the surjectivity. □

Definition 1.8. *Let $n \geq 1$ be an integer. Let*

$$\varphi(n) = |\big(\mathbb{Z}/(n)\big)^\times|,$$

the order of the unit group of the ring $\mathbb{Z}/(n)$, that is, the number of units of $\mathbb{Z}/(n)$. One calls φ Euler's totient function (or: Euler's φ-function).

Lemma 1.9. *Let $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$ be the factorisation of n into prime powers with pairwise distinct prime numbers $p_1, \ldots, p_r$.*

Then $\varphi(n) = (p_1 - 1)p_1^{e_1 - 1} \cdot (p_2 - 1)p_2^{e_2 - 1} \cdot (p_r - 1)p_r^{e_r - 1}$.

Proof. By the Chinese Remainder Theorem 1.7 it suffices to prove $\varphi(p^e) = (p-1)p^{e-1}$ for any prime number p.

In fact, it turns out to be easier to count non-units in $\mathbb{Z}/(p^e)$ instead of counting units. The non-units in $\mathbb{Z}/(p^e)$ are precisely the classes $a + (p^e)$ such that $p \mid a$, that is, $0, p, 2p, \ldots, (p^{e-1} - 1)p$. So, there are p^{e-1} non-units. Hence, $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p - 1)$. □

Now we need to recall one elementary statement from group theory.

Theorem 1.10 (Lagrange)**.** *Let G be a finite group and $H \leq G$ a subgroup. Denote by $(G : H)$ the index of H in G and by $|G|$ (and $|H|$) the order of G (and H). Then*

$$|G| = |H| \cdot (G : H).$$

Proof. Let us denote by $\circ$ the group operation. As abbreviation write $r = (G : H)$. Then by definition there are r cosets, say, $g_1 \circ H, g_2 \circ H, \ldots, g_r H \circ$ such that

$$G = g_1 \circ H \sqcup g_2 \circ H \sqcup \cdots \sqcup g_r \circ H,$$

where the symbol $\sqcup$ means 'disjoint union'. Now note that

$$H \to g_i \circ H, \quad x \mapsto g_i \circ x$$

defines a bijection, so that the number of elements of H and $g_i \circ H$ are equal. Thus, $|G| = r|H|$. □

Corollary 1.11. *Let G be a finite group and $g \in G$ an element. The* order $\mathrm{ord}(g)$ *is the smallest positive $n \in \mathbb{Z}$ such that $e = g^n$ (that is, $\underbrace{g \circ g \circ \cdots \circ g}_{n\text{-times}}$), where e is the neutral element in G. Denote by $\langle g \rangle$ the smallest subgroup of G containing g.*

Then $\mathrm{ord}(g) = |\langle g \rangle|$ divides $|G|$ and $g^{|G|} = e$.

Proof. Let $H = \langle g \rangle$. We obviously have $|H| = \mathrm{ord}(g)$. Hence, Theorem 1.10 gives $\mathrm{ord}(g)$ divides $|G|$, say, $|G| = \mathrm{ord}(g) \cdot m$ for some $m \geq 1$. Then

$$g^{|G|} = g^{\mathrm{ord}(g) \cdot m} = \left(g^{\mathrm{ord}(g)}\right)^m = e^m = e,$$

finishing the proof. □

Corollary 1.12 ('Little Fermat')**.** *Let p be a prime number. We write $\mathbb{F}_p$ for the finite field $\mathbb{Z}/(p)$. (Never use this piece of notation if p is not a prime!). Let $m \in \mathbb{Z}$ be an integer such that $m \equiv 1 \mod (p-1)$.*

Then for any $x \in \mathbb{F}_p$ one has: $x^m = x$ (equality in $\mathbb{F}_p$).

Elements in $\mathbb{Z}/(p)$ are residue classes, so $x \in \mathbb{Z}/(p)$ is of the form $a + (p)$ for some $a \in \mathbb{Z}$. One, thus, often formulates the corollary in terms of congruences: For any $a \in \mathbb{Z}$, the congruence

$$a^m \equiv a \mod (p)$$

holds if $m \equiv 1 \mod (p-1)$.

Proof. The group of units of $\mathbb{F}_p$ has order $p-1$ as the only non-unit is (the class of) 0. Let $0 \neq x \in \mathbb{F}_p$. By Corollary 1.11, $x^{p-1} = 1$. We have $m = 1 + (p-1)r$ for some $r \in \mathbb{Z}$. Thus:

$$x^m = x^{1+(p-1)r} = x \cdot x^{(p-1)r} = x \cdot \left(x^{p-1}\right)^r = x \cdot 1^r = x.$$

For $x = 0$ we obviously also have $x^m = 0^m = 0 = x$. □

Corollary 1.13. *Let $p_1, p_2, \ldots, p_r$ be pairwise distinct prime numbers and put $n = p_1 \cdot p_2 \cdots p_r$. Let $m \equiv 1 \mod (\varphi(n))$.*

Then for any $x \in \mathbb{Z}/(n)$ one has: $x^m = x$ (equality in $\mathbb{Z}/(n)$).

Proof. Exercise on Sheet 1. □

2 RSA

In this section, we introduce one of the main cryptographic algorithms that are currently in use: the RSA-algorithm, named after Ron Rivest, Adi Shamir and Leonard Adleman. Each of you probably uses this algorithm several times a day (maybe, without knowing it).

There are three people in the set-up:

- Alice: She wants to send a message to Bob.
- Bob: He wants to get a message from Alice.
- Eve: She wants to know what Alice writes to Bob, but, of course, Alice and Bob want to avoid this.

Bob's preparation step

- Bob chooses two distinct (random) prime numbers p and q.
- Bob computes (multiplications):

$$n := p \cdot q, \quad \varphi(n) = (p-1) \cdot (q-1).$$

- Bob chooses a random $1 < e < \varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$.
- Bob uses the extended Euclid's algorithm in order to compute s such that

$$es \equiv 1 \mod (\varphi(n)).$$

  For that, Bob computes $s, t \in \mathbb{Z}$ such that $1 = se + t\varphi(n)$.
- Bob publishes n and e (for example, on his webpage, in the phone book).

  n is called the *modulus* and e the *public key*.
- Bob keeps s top secret.

  s is called the *secret key*.

Alice's message encryption

We assume here that Alice's message is an integer m such that $0 \leq m \leq n-1$. In an exercise on Sheet 2, you will show how to transform a text message into a sequence of such numbers. In fact, on Sheet 2, you show how to turn a sentence (or a text) into some positive integer M. However, the integer M might be bigger than n. In that case, what one does is to write M in its n-adic expansion, i.e.

$$M = \sum_{i=0}^{s} m_i n^i \text{ with } 0 \leq m_i \leq n-1.$$

Like this one breaks the message M up into the pieces $m_0, \ldots, m_s$ and one encrypts (and decrypts) each piece separately. But, as already said, for the sake of simplicitiy of the exposition, we suppose that the message only consists of one single piece $0 \leq m \leq n-1$.

- Alice looks up Bob's (n, e) (e.g. in the phone book).
- Alice computes $M := m^e \mod (n)$; we can take $0 \leq M \leq n-1$. The computation can be done by fast exponentiation, see exercise on Sheet 2.
- Alice sends M to Bob.

Bob's message decryption

Bob receives the message M from Alice.

- Bob computes $N := M^s \mod (n)$ with $0 \leq M \leq n-1$. That computation can again be done by fast exponentiation.

  He finds $N = m$ because:

  $$M^s = \left(m^e\right)^s = m^{es} \equiv m \mod (n)$$

  by Corollary 1.13.

Eve's problem

Eve knows the following:

- Bob's (n, e) (she can look them up in the phone book, too).
- The encrypted message M (because she was eavesdropping – secretly listening; that's why she's called Eve).

If Eve can compute the prime factors p and q of n, then she can decrypt the message very easily:

- Like Bob, she computes $\varphi(n) = (p-1)(q-1)$.
- Like Bob, she uses the extended Euclid's algorithm in order to compute s such that

  $$es \equiv 1 \mod (\varphi(n)).$$

  Now she know the secret key s, too!
- Like Bob, she decrypts the message by computing $N := M^s \mod (n)$, which is, of course, m again.

So, one has to prevent Eve from being able to factor n. This one does, in practice, by choosing p and q very big, e.g. of size around 2^{2048}, so that p and q have each more than 600 decimal digits. Then the currently best known algorithms for factoring n would be too slow to yield a result in less than a couple of millions of years.

Of course, one does not know whether there is not a much faster algorithm. This insecurity, one has to live with.

3 Finite fields

If p is a prime number, then $\mathbb{F}_p := \mathbb{Z}/(p)$ is a finite field with p elements. But, these are not the only ones. In fact, in this part of the lecture we are going to establish that for each prime power p^n there is a finite field having p^n elements, called $\mathbb{F}_{p^n}$, and up to isomorphism these are the only finite fields. It is very important to remember that $\mathbb{F}_{p^n} \neq \mathbb{Z}/(p^n)$, as soon as $n > 1$ (for instance, in $\mathbb{Z}/(p^n)$ the equality $0 = pp^{n-1}$ shows that $0 \neq p$ is a non-unit, but in fields all non-zero elements are units).

First we treat the example of the finite field with 4 elements in order to show that there are other finite fields than $\mathbb{F}_p$ with p a prime. Consider $f(X) := X^2 + X + 1 \in \mathbb{F}_2[X]$. It is an irreducible polynomial. This one can check by testing that it does not have any zeros in $\mathbb{F}_2$: $f(0) = 1 \neq 0$ and $f(1) = 1 \neq 0$ (always remember that this way of testing irreducibility is only valid for polynomials of degrees 2 and 3, since from degree 4 onwards, a polynomial f could factor as $f = gh$ with both g and h having no zero). We recall the notation $(f(X))$ for the principal ideal generated by $f(X)$, which consists of all multiples of $f(X)$.

We put $K := \mathbb{F}_2[X]/(X^2 + X + 1)$. We represent its elements as

$$\overline{0} := 0 + (f), \overline{1} := 1 + (f), \overline{X} := X + (f), \overline{1 + X} := 1 + X + (f).$$

It is very simple to write down the addition and the multiplication table explicitly (we did this in the lecture). It becomes obvious that every element of K different from $\overline{0}$ has a multiplicative inverse. As we already know from the general theory of quotient rings that K is a ring, the existence of the multiplicative inverses shows that K is a field. It has 4 elements and is denoted $\mathbb{F}_4$.

Definition 3.1. *Let R be a commutative ring. If there is a positive integer m such that*

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{m \text{ times}} = 0_R$$

in R (where for the sake of clarity we write 0_R (resp. 1_R) for the neutral element of addition (resp. multiplication) of R – we shall not do this at any other place), then the characteristic of R *is defined to be the minimum such m.*

If no such m exists, then we say that R has characteristic 0.

Example 3.2. *$\mathbb{Q}$ has characteristic 0 and for a prime number p, the finite field $\mathbb{F}_p$ has characteristic p. The characteristic of $\mathbb{F}_4$ is 2 (this is clear).*

Proposition 3.3. *Let R be an integral domain (e.g. a field). Then the characteristic is either 0 or a prime number.*

Proof. Suppose the characteristic of R is $m > 0$ and $m = ab$ with $1 < a, b < m$. Then

$$0 = \underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} = (\underbrace{1 + 1 + \cdots + 1}_{a \text{ times}}) \cdot (\underbrace{1 + 1 + \cdots + 1}_{b \text{ times}}).$$

As R is an integral domain, it follows $\underbrace{1 + 1 + \cdots + 1}_{a \text{ times}} = 0$ or $\underbrace{1 + 1 + \cdots + 1}_{b \text{ times}} = 0$ and both contradicts the minimality of m. □

We are now going to construct many more finite fields in a more conceptual way. Our approach is a generalisation of our construction of $\mathbb{F}_4$. The key is – again – the extended Euclid's algorithm, now applied in the polynomial ring.

Theorem 3.4 (Euclid, Bézout)**.** *Let K be a field and let $f(X), g(X) \in K[X]$ not both zero. Then* Euclid's algorithm *computes the greatest common divisor $d(X)$ of $f(X), g(X)$, notation $d(X) = \gcd(f(X), g(X))$, that is:*

- $d(X) \neq 0$ *is monic (i.e. highest coefficient equal to* 1*),*
- $d(X) \mid f(X)$, $d(X) \mid g(X)$,
- *for any* $e(X) \neq 0$ *such that* $e(X) \mid f(X)$ *and* $e(X) \mid g(X)$*, one has* $e(X) \mid d(X)$.

Moreover, the extended Euclid's algorithm *gives* $r(X), s(X) \in K[X]$ *such that*

$$d(X) = f(X)r(X) + g(X)s(X).$$

The proof is again completely algorithmic.

We presented the theorem about Euclid's algorithm in $\mathbb{Z}$ and $K[X]$ in a completely analogous manner. In fact, most of the theory can be developed for all rings, in which one has a Euclidean division (i.e. a division with remainder). Such rings are called *Euclidean rings*. You may or may not have seen them in your algebra classes. In this lecture we just need $\mathbb{Z}$ and the polynomial ring over a field, so we will not go into Euclidean rings in general. On Exercise Sheet 3, you will prove an analogue of Gauß' fundamental theorem of elementary number theory for $K[X]$ (the general statement, which you may have seen, is: Every Euclidean ring is a unique factorisation domain.).

We start with a simple, but extremely useful consequence:

Lemma 3.5. *Let* K *be a field and* $f(X) \in K[X]$ *be a non-zero polynomial. Then the following statements hold:*

(a) Suppose there is $\alpha \in K$ *such that* $f(\alpha) = 0$ *(such* α *is called a* zero *or a* root *of* f*). Then there is a polynomial* $g(X) \in K[X]$ *such that*

$$f(X) = (X - \alpha)g(X).$$

(b) $f(X)$ *has at most* $\deg(f)$ *many zeros.*

(c) Let $f'(X)$ *be the formal derivative of* $f(X)$*; that is, for* $f(X) = \sum_{i=0}^{n} a_i X^i$*, we let* $f'(X) = \sum_{i=1}^{n} a_i i X^{i-1}$*. If* $f(X) = g(X)h(X)^2$ *with* $g(X), h(X) \in K[X]$ *non-zero polynomials, then* $h(X)$ *divides the* $\gcd(f(X), f'(X))$.

Proof. (a) We use Euclidean division:

$$f(X) = q(X) \cdot (X - \alpha) + r(X),$$

where the rest $r(X)$ has degree strictly smaller than the degree of the divisor $(X - \alpha)$, whence the degree of $r(X)$ is 0. Thus, $r(X) = c$ is a constant polynomial. Now, we plug in α for X and obtain:

$$0 = f(\alpha) = q(\alpha) \cdot (\alpha - \alpha) + c = 0 + c = c,$$

showing that the rest $r(X)$ is zero, so that $(X - \alpha)$ divides f.

(b) follows by induction from (a).

(c) It is easily checked that the Leibniz rule holds for the formal derivative (see Exercise on Sheet 4):

$$f'(X) = g'(X)h(X)^2 + 2g(X)h'(X)h(X) = h(X)\big(g'(X)h(X) + 2g(X)h'(X)\big),$$

showing that $h(X)$ divides $f'(X)$ and thus it divides the greatest common divisor of $f(X)$ and $f'(X)$. □

We now turn to the construction of finite fields. The fundamental result is the following, which we first phrase in some generality and then specialise to finite fields in the corollary.

Proposition 3.6. *Let K be a field and $f \in K[X]$ an irreducible polynomial of degree $n > 0$.*
Then $K[X]/(f(X))$ is a field. Its elements can be represented as

$$\overline{\sum_{i=0}^{n-1} a_i X^i} := (\sum_{i=0}^{n-1} a_i X^i) + (f(X)) \text{ with } a_0, a_1, \ldots, a_{n-1} \in K.$$

Proof. We already know that $K[X]/(f(X))$ is a ring. Now we show that every non-zero element has a multiplicative inverse. Let $g + (f(X)) \in K[X]/(f(X))$ be a non-zero element. Being non-zero means that $g(X) + (f(X)) \neq 0 + (f(X))$, which is equivalent to $g(X) \notin (f(X))$, which is the same as g not being a multiple of f, i.e. $f(X)$ does not divide $g(X)$.

It follows that the greatest common divisor of $f(X)$ and $g(X)$ is equal to 1, whence there are $r(X), s(X) \in K[X]$ such that

$$1 = f(X)r(X) + g(X)s(X).$$

Taking residue classes in $K[X]/(f(X))$ we obtain

$$\overline{1} = 1 + (f(X)) = \big(g(X) + (f(X))\big)\big(s(X) + (f(X))\big) = \overline{gs},$$

exhibiting the desired inverse of $\overline{g} = g(X) + (f(X))$.

The representatives listed in the assertion are just the remainders for division by f. □

Corollary 3.7. *Let p be a prime number and $f \in \mathbb{F}_p[X]$ an irreducible polynomial of degree $n = \deg(f) > 0$.*
Then $\mathbb{F}_p[X]/(f(X))$ is a finite field having p^n elements, which can be represented as

$$\overline{\sum_{i=0}^{n-1} a_i X^i} := (\sum_{i=0}^{n-1} a_i X^i) + (f(X)) \text{ with } 0 \leq a_0, a_1, \ldots, a_{n-1} \leq p-1.$$

Proof. In view of the previous proposition, this is clear. □

Now we have a big supply of finite fields – under the assumption that there are many irreducible polynomials in $\mathbb{F}_p[X]$. It is possible to give a brute force proof that for every $n \in \mathbb{N}$, there is an irreducible monic polynomial $f(X) \in \mathbb{F}_p[X]$ of degree n. This can be done by counting the number of reducible monic polynomials of degree n and observing that this number is smaller than p^n (which is the total number of monic polynomials of degree n), so that there must at least be one irreducible monic polynomial. We will, however, go a slightly smarter way, which uses the notion of a splitting field of a polynomial.

The central role in the construction of the field with p^n elements is played by the polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$. For $n > 1$ it is not irreducible, so we cannot apply the previous corollary. Instead, we will take its splitting field. Although splitting fields may be known to you from a course in algebra, we shall construct them here again (in a quick and concise way).

Theorem 3.8. *Let K be a field and $f(X) \in K[X]$ a monic polynomial of degree n. Then there is a field L satisfying the following properties:*

(1) $K \subseteq L$.

(2) There are $\alpha_1, \ldots, \alpha_n \in L$ such that (in $L[X]$):

$$f(X) = (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n).$$

(3) If $K \subseteq L_1 \subseteq L$ and L_1 satisfies (1) and (2), then $L = L_1$ (i.e. L is the smallest field containing K, over which $f(X)$ factors into a product of linear polynomials).

The field L is called the splitting field (corps de décomposition, Zerfällungskörper) of f.

Proof. We show the following assertion by induction on n.

> For every field K and every monic polynomial $f(X) \in K[X]$ of degree at most n, there is a field L such that
>
> (I) $K \subseteq L$.
>
> (II) There are $\alpha_1, \ldots, \alpha_n \in L$ such that (in $L[X]$):
>
> $$f(X) = (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n).$$

If $n = 1$, then f is already linear and $L = K$ trivially satisfies (I) and (II).

Now assume that the assertion has been established for all polynomials of degrees up to $n - 1$. We now want to establish it for the polynomial $f \in K[X]$ of degree n. For this, we distinguish two cases:

f is reducible: In this case, we factor $f(X) = g(X)h(X)$ with $g(X), h(X) \in K[X]$ of degrees strictly less than n. From the induction hypothesis applied for $g(X) \in K[X]$ we deduce the existence of a field L_1 satisfying (I) and (II). We apply the induction hypothesis again for $h(X) \in L_1[X]$ (we can, of course, view $h(X)$ as a polynomial of $L_1[X]$ because K is a subfield of L_1) and obtain a field L satisfying (I) and (II) (for the polynomial $h(X)$). We have $L \supseteq L_1 \supseteq K$, showing (I) for $f \in K[X]$. Moreover, it is clear that $f(X)$ factors into linear factors over $L[X]$ because the roots of $g(X)$ lie in $L_1 \subseteq L$ and those of $h(X)$ lie in L.

f is irreducible: From Proposition 3.6 we know that $L_1 := K[X]/(f(X))$ is a field. It contains K (the classes of the constant polynomials) and the class $\alpha := \overline{X} = X + (f(X))$ is a zero of $f(X) \in L_1[X]$. To see this, let us write $f(X) = \sum_{i=0}^{n} a_i X^i$. Then:

$$f(\overline{X}) = \sum_{i=0}^{n} a_i \overline{X}^i = \sum_{i=0}^{n} a_i \big(X + (f(X))\big)^i = \sum_{i=0}^{n} a_i X^i + (f(X)) = f(X) + (f(X))$$
$$= 0 + (f(X)) = \overline{0}.$$

(Note the small ambiguity in the notation: $a = a + (f(x)) = \overline{a}$ for $a \in K$.) Hence, over $L_1[X]$ we have $f(X) = (X - \alpha)g(X)$ with $g(X) \in L_1[X]$ of degree $n - 1$. This allows us to apply the induction hypothesis for $g(X) \in L_1[X]$, yielding a field $L \supseteq L_1 \supseteq K$ over which $g(X)$ factors as a

product of linear polynomials. Consequently, over L the polynomial $f(X)$ factors into a product of linear polynomials, establishing the assertion for n.

We now prove the theorem. The above assertion gives us a field M satisfying (1) and (2). We now want to show that there is a field L for which (3) also holds. This is very easy. Namely, it suffices to let L be the smallest subfield of M which contains $\alpha_1, \ldots, \alpha_n$. □

We are now ready for the construction of a finite field with p^n elements.

Proposition 3.9. *Let p be a prime number and $n \in \mathbb{N}_{>0}$. Consider $f(X) = X^{p^n} - X \in \mathbb{F}_p[X]$. Then the splitting field L of $f(X)$ over $\mathbb{F}_p$ is a finite field with p^n elements.*

Proof. As L is the splitting field, there are elements $\alpha_1, \ldots, \alpha_{p^n} \in L$ such that $f(X) = \prod_{i=1}^{p^n}(X - \alpha_i)$. By Lemma 3.5 (c), the α_i are pairwise distinct because

$$\gcd(f(X), f'(X)) = \gcd(f(X), p^n X^{p^n-1} - 1) = \gcd(f(X), -1) = 1$$

(if $\alpha_i = \alpha_j$ for $i \neq j$, then take $h(X) = (X - \alpha_i)$ and $g(X) = f(X)/(h(X)^2)$). So, the set $M = \{\alpha_1, \ldots, \alpha_{p^n}\}$ has p^n elements and it consists precisely of the zeros (in L) of $f(X)$.

We now show that M is a subfield of L. Let $\alpha, \beta \in M$, hence $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$.

- $0, 1 \in M$ because they clearly satisfy $f(0) = 0 = f(1)$.
- Suppose $\alpha \neq 0$. Then $\alpha^{p^n} = \alpha$ implies $(\frac{1}{\alpha})^{p^n} = \frac{1}{\alpha}$, showing that M contains the multiplicative inverse of any non-zero element in M.
- From $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$, it follows $(\alpha\beta)^{p^n} = \alpha\beta$, showing that M contains the product of any two elements of M.
- From $\alpha^{p^n} = \alpha$, it follows $(-\alpha)^{p^n} = (-1)^{p^n}\alpha = -\alpha$ (note that for $p = 2$ this equation is also true), showing that M contains the negative of any of its elements.
- From $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$, it follows $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ (see Exercise on Sheet 4), showing that M contains the sum of any two elements of M.

Due to (3) of the definition of a splitting field, one has $L = M$ and this finishes the proof. □

We have thus shown that there is a field with p^n elements by constructing it as the splitting field of the polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$. Next, we prove that all finite fields with p^n elements are of this type. From that we shall deduce that any two finite fields with the same number of elements are isomorphic, so that we will obtain a complete classification of all finite fields.

Lemma 3.10. *Let K be a finite field and let p be its characteristic. Then p is a prime number and there is $n \in \mathbb{N}$ such that the number of elements of K is p^n.*

Proof. The characteristic of K cannot be 0 because in that case K would contain infinitely many elements, namely $\mathbb{N}$ and hence $\mathbb{Q}$. So, the characteristic of K is p. That means that the kernel of the ring homomorphism

$$\mathbb{Z} \to K, \quad z \mapsto \begin{cases} \underbrace{1+1+\cdots+1}_{z \text{ times}} & \text{if } z \geq 0, \\ \underbrace{-1-1-\cdots-1}_{|z| \text{ times}} & \text{if } z \leq 0. \end{cases}$$

is the prime ideal (p), whence by the homomorphism theorem (1er théorème d'isomorphisme) we obtain an injection $\mathbb{F}_p \hookrightarrow K$. So, $\mathbb{F}_p$ is a subfield of K and, thus, K is an $\mathbb{F}_p$-vector space of some dimension n. Hence, K has p^n elements. □

Proposition 3.11. *Let p be a prime number, $n \in \mathbb{N}_{>0}$, and K a finite field with p^n elements. Then K is a splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$.*

Proof. This is actually very easy. We check conditions (1), (2) and (3) in the definition of a splitting field:

(1) $\mathbb{F}_p \subseteq K$; this is clear due to Lemma 3.10.

(2) Let $a \in K$. If $a = 0$, then clearly $a^{p^n} = a$. If $a \neq 0$, then $a^{(p^n-1)} = 1$ because the multiplicative group $K^\times = K \setminus \{0\}$ has order $p^n - 1$. Hence, we also find $a^{p^n} = a$. Consequently, all elements of K are zeros of $f(X) = X^{p^n} - X \in \mathbb{F}_p[X]$. As we have $\deg(f)$ zeros of f in K, f factors into linear factors over K.

(3) Of course, no proper subfield of a field with p^n elements can contain all the zeros of f because their number is p^n. □

Lemma 3.12. *Let A be a finite abelian group. The* exponent $\exp(A)$ of A *is defined as the minimal positive integer e such that $a^e = 1$ for all elements $a \in A$. Then the following statements hold:*

(a) Let $a, b \in A$. Suppose that $1 = \gcd(\operatorname{ord}(a), \operatorname{ord}(b))$, then $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$.

(b) Let $a, b \in A$. Then there are $i, j \in \mathbb{N}$ such that $\operatorname{ord}(a^i b^j) = \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b))$ (lcm*: lowest common multiple;* ppcm*: plus petit commun multiple,* kgV*: kleinstes gemeinsames Vielfaches).*

(c) There is $a \in A$ such that $\operatorname{ord}(a) = \exp(A)$.

(d) A is cyclic $\Leftrightarrow \exp(A) = \#A$.

Proof. (a) Let $e \geq 1$ such that $a^e b^e = 1$. Since $1 = \gcd(\operatorname{ord}(a^e), \operatorname{ord}(b^e))$, it follows from $a^e = b^{-e}$ that $a^e = 1 = b^e$. Thus, $\operatorname{ord}(a) \mid e$ and $\operatorname{ord}(b) \mid e$, hence, $\operatorname{ord}(a)\operatorname{ord}(b) = \operatorname{lcm}(\operatorname{ord}(a), \operatorname{ord}(b)) \mid e$. Of course, $(ab)^{\operatorname{ord}(a)\operatorname{ord}(b)} = 1$.

(b) Let

$$\operatorname{ord}(a) = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} \text{ and } \operatorname{ord}(b) = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$$

be the prime factorisations (i.e. the $p_1, \ldots, p_k$ are pairwise distinct prime numbers), where we sort the primes in such a way that $m_1 \geq n_1, \ldots, m_s \geq n_s$ and $m_{s+1} < n_s, \ldots, m_k < n_k$. Let

$$a' := a^{p_{s+1}^{m_{s+1}} \cdot \ldots \cdot p_k^{m_k}} \text{ and } b' := b^{p_1^{n_1} \cdot \ldots \cdot p_s^{n_s}}.$$

It is clear that we have

$$\mathrm{ord}(a') = p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \text{ and } \mathrm{ord}(b') = p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k}.$$

Hence, (a) implies that the order of $a'b'$ is

$$p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \cdot p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k} = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b)).$$

Of course, $(ab)^{\mathrm{lcm}(\mathrm{ord}(a),\mathrm{ord}(b))} = 1$.

(c) Let e denote the lowest common multiple of the orders of all elements in A. It is an immediate consequence of (b) that there is an element $a \in A$ whose order is e. So, $e = \mathrm{ord}(a) \mid \exp(A)$. Clearly, $\exp(A)$ is less than or equal to e, showing the desired equality.

(d) is an immediate consequence of (c). □

Proposition 3.13. *Let K be a finite field. Then the group of units $K^\times = K \setminus \{0\}$ (group with respect to multiplication and neutral element 1) is a cyclic group of order $\#K - 1$.*

Proof. Let $\#K = p^n$. Let $e := \exp(K^\times)$. Due to Lemma 3.12 it suffices to show that $e = p^n - 1$. Suppose $e < p^n - 1$. Then every element $a \in K$ satisfies $a^{e+1} = a$, so that the p^n elements are all zeros of the polynomial $X^{e+1} - X$, which has degree $e + 1$. This is, of course, impossible because a polynomial of degree $e + 1$ has at most $e + 1$ zeros (since the coefficients of the polynomial are in a field). □

Definition 3.14. *Let K be a field, L a field containing K, and $\alpha \in L$. Consider the evaluation map $\mathrm{ev}_a : K[X] \xrightarrow{f(X)\mapsto f(\alpha)} L$.*

Let $g(X)$ be the unique monic generator of the principal ideal $\ker(\mathrm{ev}_a)$ (recall: $K[X]$ is a principal ideal domain). In particular, any other polynomial $f(X) \in K[X]$ with $f(\alpha) = 0$ is a multiple of $g(X)$.

One calls $g(X)$ the minimal polynomial of a over K.

Proposition 3.15. *Let p be a prime number, $n \in \mathbb{N}_{>0}$, and K and L finite fields with p^n elements. Then K and L are isomorphic, i.e. there is a field isomorphism $\Phi : K \to L$.*

Proof. By Proposition 3.13, the unit group $K^\times$ is cyclic of order $p^n - 1$. Let $\alpha \in K^\times$ be a generator, i.e. an element of $K^\times$ of order $p^n - 1$. Let $g(X) \in \mathbb{F}_p[X]$ be the minimal polynomial of α. It has degree n, for, if it had a smaller degree m, then the order of α would be a divisor of $p^m - 1$, which is impossible.

The evaluation map $\mathrm{ev}_a : \mathbb{F}_p[X] \xrightarrow{f(X)\mapsto f(\alpha)} K$ defines an isomorphism (via the homomorphism theorem) $\mathbb{F}_p[X]/(g(X)) \cong K$. We show that also $\mathbb{F}_p[X]/(g(X)) \cong L$.

Note that $g(X) \mid X(X^{p^n-1} - 1) = X^{p^n} - X$ (in $\mathbb{F}_p[X]$) because α is a zero of both polynomials, so that $X^{p^n} - X$ is in the principal ideal generated by $g(X)$. We know by Proposition 3.11 that L is a splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. Hence, also $g(X)$ splits in L into linear factors and, thus, there is $\beta \in L$ such that $g(\beta) = 0$. This means that the evaluation map $\mathrm{ev}_\beta : \mathbb{F}_p[X] \xrightarrow{f(X)\mapsto f(\beta)} L$ defines the desired isomorphism (via the homomorphism theorem) $\mathbb{F}_p[X]/(g(X)) \cong L$. □

Now we can state and prove the complete classification result of finite fields up to isomorphism.

Theorem 3.16. *(a) The number of elements of any finite field K is of the form p^n, where p is a prime number and the characteristic of K, and $n \in \mathbb{N}_{>0}$.*

(b) For any prime p and any $n \in \mathbb{N}_{>0}$, there is a finite field having p^n elements. Any two such are isomorphic. We use the notation $\mathbb{F}_{p^n}$.

(c) Let K be a subfield of $\mathbb{F}_{p^n}$. Then $\#K = p^e$ for some divisor e of n.

(d) For every divisor $e \mid n$, there is a unique subfield $K \subseteq \mathbb{F}_{p^n}$ having p^e elements.

Proof. (a) and (b) have been proved above.

(c) The field $\mathbb{F}_{p^n}$ is a field extension of K, hence, $\mathbb{F}_{p^n}$ is a K-vector space of some dimension d. Thus, $p^n = \#\mathbb{F}_{p^n} = (\#K)^d = p^{ed}$.

(d) Let $n = ed$. Then (geometric sum)

$$p^n - 1 = (p^e - 1)\underbrace{(p^{e(d-1)} + p^{e(d-2)} + \ldots + 1)}_{=:m}$$

and (again geometric sum)

$$X^{p^n-1} - 1 = (X^{p^e-1} - 1)(X^{(p^e-1)(m-1)} + X^{(p^e-1)(m-2)} + \ldots + 1),$$

showing $f(X) := (X^{p^e} - X) \mid (X^{p^n} - X)$.

The zeros of $f(X)$ form a subfield K of $\mathbb{F}_{p^n}$ with p^e-elements: it is the splitting field of $f(X)$ over $\mathbb{F}_p$. If $L \subseteq \mathbb{F}_{p^n}$ is a subfield with p^e elements, then all its elements are zeros of $f(X)$, whence $L \subseteq K$, hence $L = K$. □

4 Diffie-Hellman and El Gamal for finite fields

Symmetric encryption

Alice and Bob want to communicate secretly. A *message* is, as before, a positive integer $1 \leq m \leq N$ (for some fixed big N). A *key* is a positive integer $K \in \mathbb{N}$.

A *symmetric encryption function* (for the key K) is a pair of maps:

$$f_1 : \{1, 2, \ldots, N\} \times \mathbb{N} \to \{1, 2, \ldots, N\}$$

$$f_2 : \{1, 2, \ldots, N\} \times \mathbb{N} \to \{1, 2, \ldots, N\}$$

such that $f_2(f_1(m, K), K) = m$ and both $f_1(m, K)$ and $f_2(n, K)$ can be computed quickly for all $m, n \in \{1, 2, \ldots, N\}$. One also wants that m cannot (easily) be computed from $f_1(m, K)$ if K is unknown. One calls $f_1(m, K)$ the *encryption* of the message m for the key K.

Just to give an idea of a symmetric encryption system (this one is not perfect). Suppose the key is

$$K = \sum_{i=0}^{d-1} a_i 10^i \text{ with } a_i \in \{0, 1, \ldots, 9\}$$

and the message is

$$m = \sum_{i=0}^{e} m_i 10^i \text{ with } m_i \in \{0, 1, \ldots, 9\},$$

where we imagine that e is much bigger than d. Then we could take:

$$f_1(m, K) = \sum_{i=0}^{e} M_i 10^i,$$

where the M_i are computed as follows:

$$\begin{aligned} M_0 &\equiv m_0 + a_0 \mod (10), \ldots, & M_{d-1} &\equiv m_{d-1} + a_{d-1} \mod (10) \\ M_d &\equiv m_d + a_0 \mod (10), \ldots, & M_{2d-1} &\equiv m_{2d-1} + a_{d-1} \mod (10) \\ M_{2d} &\equiv m_{2d} + a_0 \mod (10), \ldots, & M_{3d-1} &\equiv m_{3d-1} + a_{d-1} \mod (10), \end{aligned}$$

and so on, until M_e. The function f_2 is defined in the same way, replacing $+$ by $-$.

Assumption: Alice and Bob have a common secret: a big integer $K \in \mathbb{N}$.

If Alice wants to send message m to Bob, all she has to do is compute $M := f_1(m, K)$ and send M to Bob. He can read the message by computing $m = f_2(M, K)$. Our assumptions imply that Eve, who knows M (and also f_1 and f_2), cannot deduce m. But, this all relies on the above assumption that Alice and Bob have this common secret key K. If they are far away (Bob is in New York and Alice in Luxembourg, they can only speak on the phone, and Eve listens to all their conversations), it is not so clear how they can get a common secret. That it is possible was demonstrated by Diffie and Hellman.

Diffie-Hellman key exchange

The players are the same as for RSA: Alice, Bob and Eve.

Task: Alice and Bob want to agree on a secret key, which both of them know, but which is unknown to Eve. They want to do this, even though Eve is listening to their conversation.

A revolutionary method was found by Diffie and Hellman. In order to illustrate the method, we first present the idea in a simpler setting, where it turns out to fail, and then present the right version.

First (wrong) attempt

(1) Alice and Bob agree on a big prime number p and an integer $1 < g < p$. Eve may know p and g.

(2) Alice chooses secretly $a \in \mathbb{N}$, computes $A := ag \mod (p)$ and sends A to Bob.

(3) Bob chooses secretly $b \in \mathbb{N}$, computes $B := bg \mod (p)$ and sends B to Alice.

(4) Alice receives B from Bob and computes $K_{\text{Alice}} := aB \equiv abg \mod (p)$.

(5) Bob receives A from Alice and computes $K_{\text{Bob}} := bA \equiv abg \mod (p)$.

Note: $K_{\text{Alice}} = K_{\text{Bob}}$.

Eve listened to their conversation. She knows: A, B, p and g. She now uses the Euclidean algorithm to compute $1 < h < p$ such that $gh \equiv 1 \mod (p)$ (i.e. an inverse to g in $\mathbb{F}_p^\times$). This allows her to compute

$$Ah \equiv agh \equiv a \mod (p) \text{ and } K := aB \mod (p),$$

so that $K = K_{\text{Alice}} = K_{\text{Bob}}$. Thus, Eve knows the common 'secret' K.

A slight modification of the above turns out to prevent Eve from obtaining the secret!

Correct realisation

The idea is to replace computations in $(\mathbb{F}_p, +)$ by computations in $(\mathbb{F}_{p^n}^\times, \cdot)$ (where we may, but need not, choose $n = 1$).

(1) Alice and Bob agree on a big finite field $\mathbb{F}$ (e.g. $\mathbb{F}_p$ or any $\mathbb{F}_{p^n}$) and a generator g of the cyclic group $\mathbb{F}^\times$. Eve may know $\mathbb{F}$ and g.

(2) Alice chooses secretly $a \in \mathbb{N}$, computes $A := g^a \in \mathbb{F}^\times$ and sends A to Bob.

(3) Bob chooses secretly $b \in \mathbb{N}$, computes $B := g^b \in \mathbb{F}^\times$ and sends B to Alice.

(4) Alice receives B from Bob and computes $K_{\text{Alice}} := B^a = (g^a)^b = g^{ab} \in \mathbb{F}^\times$.

(5) Bob receives A from Alice and computes $K_{\text{Bob}} := A^b = (g^b)^a = g^{ab} \in \mathbb{F}^\times$.

Note: $K_{\text{Alice}} = K_{\text{Bob}}$.

Eve again listened to their conversation. She again knows: A, B, p and g. But, in order to compute a from A (and p and g) she would have to solve the discrete logarithm problem in the finite field $\mathbb{F}$, which is defined as follows:

> Given a finite field $\mathbb{F}$ and a generator g of the cyclic group $\mathbb{F}^\times$ (with respect to multiplication).
>
> For $A \in \mathbb{F}^\times$, find a such that $g^a = A \in \mathbb{F}^\times$.
>
> The solution a is called a (discrete) logarithm of A (for the basis/generator g) because $g^a = A$.

Up to this day, no efficient algorithm is known to compute a discrete logarithm in a big finite field. Hence, Eve cannot compute a and, thus, cannot obtain the common secret $K_{\text{Alice}} = K_{\text{Bob}}$, although she has seen everything that Alice and Bob exchanged!

As a variant, one can replace the discrete logarithm problem in finite fields by the discrete logarithm problem in elliptic curves (later this term!), and obtain an elliptic curves Diffie-Hellman key exchange. This is used, for instance, in the authentication procedure for the communication between the German passport and a reader.

El Gamal encryption

A slight variation of the order of step in the Diffie-Hellman key exchange gives rise to a public key encryption system, which works similarly to RSA: Bob wants to receive messages (in particular, but, not only from Alice), and for that purpose he produces a public key, which can be looked up in a phone book, and a secret key. People (like Alice) who have looked up the public key can send encrypted messages to Bob which only he can decrypt using his secret key.

Bob's preparation step

- Bob chooses a big finite field $\mathbb{F}$ (e.g. $\mathbb{F}_p$ or any $\mathbb{F}_{p^n}$) and a generator g of the cyclic group $\mathbb{F}^\times$. Eve may know $\mathbb{F}$ and g.
- Bob chooses secretly $b \in \mathbb{N}$ and computes $B := g^b \in \mathbb{F}^\times$.
- Bob publishes B (and $\mathbb{F}$ and g) in the phone book.

Alice's message encryption

- Alice looks up Bob's B (and $\mathbb{F}$ and g) in the phone book.
- Alice chooses secretly $a \in \mathbb{N}$ and computes $A := g^a \in \mathbb{F}^\times$ (just like in the Diffie-Hellman key exchange).
- Alice computes $K_{\text{Alice}} := B^a = (g^a)^b = g^{ab} \in \mathbb{F}^\times$.
- Alice encrypts the message $M := f_1(m, K_{\text{Alice}})$.
- Alice sends M and A to Bob.

Bob's message decryption

- Bob receives M and A from Alice.
- Bob computes $K_{\text{Bob}} = A^b = (g^a)^b = g^{ab} \in \mathbb{F}^\times$. Note that again $K_{\text{Alice}} = K_{\text{Bob}}$.
- Bob decypts the message $m = f_2(M, K_{\text{Bob}})$.

And Eve?

Eve knows A, B (and $\mathbb{F}$ and g) and M. As in the Diffie-Hellman key exchange she is faced with computing b from B or a from A in order to get hold of $K_{\text{Alice}} = K_{\text{Bob}}$ (which we assume is necessary for the message decryption). This is the same discrete logarithm problem in the finite field $\mathbb{F}$, and, hence, currently undoable if the field is big enough.

5 Plane Curves

Let K be a field. Usually we will work with $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or a finite field, but, unless we say it explicitly, K denotes any (fixed) field. First we define the affine plane over the field K. This is the place where our plane (affine) curves will live.

Definition 5.1. *We define the* affine plane over K *as* $\mathbb{A}^2(K) := K \times K = \{(a, b) : a, b \in K\}$. *The elements of* $\mathbb{A}^2(K)$ *will be called* affine points.

Definition 5.2.

- *Let* $f \in K[x, y]$ *be a polynomial in two variables with coefficients in* K. *We define the following subset of the affine plane over* K*:*

$$C_f(K) := \{(a, b) \in \mathbb{A}^2(K) : f(a, b) = 0\}.$$

- *Consider the set of pairs* $\{(C, f) : C \subset \mathbb{A}^2(K), f \in K[x, y]$ *is nonzero*$\}$. *We will identify two pairs* (C_1, f_1) *and* (C_2, f_2) *if* $C_1 = C_2$ *and* $f_1 = \lambda f_2$ *for some* $\lambda \in K^\times$.

- *An* affine plane curve over K *is a (class of a) pair* $(C_f(K), f)$ *for some nonzero* $f \in K[x, y]$. *We will denote it by* C/K *or* C_f/K.

Remark 5.3.

- *Usually one identifies a plane curve* C_f/K *with the subset* $C_f(K)$ *of* $\mathbb{A}^2(K)$ *that it defines. However, given a subset* $C \subset \mathbb{A}^2(K)$*, there can be more than one polynomial* $f \in K[x, y]$ *such that* $C = C_f(K)$*, so we are loosing information if we forget about the polynomial* f. *In Sheet 6 we will see some examples of this.*

- *According to Definition 5.2, for any scalar* $\lambda \in K^\times$*, we identify the curves* C_f/K *and* $C_{\lambda f}/K$. *This stems from the fact that* f *and* λf *generate the same ideal in* $K[x, y]$. *In general, an affine variety can be defined as a pair* (V, I)*, where* V *is a subset of the affine space and* I *is an ideal of a ring of polynomials with coefficients in* K. *But for our purposes we can work with Definition 5.2.*

Example 5.4.

1. *Let* $a, b, c \in K$ *with either* $a \neq 0$ *or* $b \neq 0$. *Then the affine curve defined by the polynomial* $f(x, y) = ax+by+c$ *is called an* affine line. *The set* $C_f(K)$ *corresponds bijectively to the elements of* K. *Namely, if* $b \neq 0$*, we have* $C_f(K) = \{(t, \frac{-1}{b}(at + c)) : t \in K\}$*; if* $b = 0$*, then* $a \neq 0$ *by hypothesis and* $C_f(K) = \{(\frac{-c}{a}, t) : t \in K\}$.

2. *Let* $K = \mathbb{F}_4$*, and let* $f(x, y) = y^2 + y + x^3 + x$. *Let us compute the set* $C_f(K)$. *Recall (beginning of Section 3) that we can write* $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$*, and the elements of* K *are represented by* $\overline{0}, \overline{1}, \overline{X}, \overline{X + 1}$. *We can compute the following tables:*

x	$x^3 + x$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$
$\overline{X}$	$\overline{X + 1}$
$\overline{X + 1}$	$\overline{X}$

y	$y^2 + y$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$
$\overline{X}$	$\overline{1}$
$\overline{X + 1}$	$\overline{1}$

The points of $C_f(K)$ *are those where the values of* $y^2 + y$ *and* $x^3 + x$ *match, namely,* $C_f(K) = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$.

For many purposes it is convenient to complete the affine plane with some points at infinity. For instance, one desirable property that the affine plane does not have is that each pair of lines meet at exactly one point (which would allow us to drop the distinction between parallel and nonparallel affine lines). For this reason we introduce the projective plane.

Definition 5.5.
- *We define a relation* $\sim$ *on* $K \times K \times K \setminus \{(0,0,0)\}$ *by* $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$ *(*(a_1, b_1, c_1) is related to (a_2, b_2, c_2)*) if there exists some* $\lambda \in K^\times$ *such that* $(a_1, b_1, c_1) = (\lambda a_2, \lambda b_2, \lambda c_2)$*. This is an equivalence relation (i.e., reflexive, symmetric and transitive).*
- *The* projective plane over K *is defined as* $\mathbb{P}^2(K) = ((K \times K \times K) \setminus \{(0,0,0)\})/\sim$*. The elements of* $\mathbb{P}^2(K)$ *are called* points *of the projective plane.*
- *If* $(a, b, c) \in K \times K \times K \setminus \{(0,0,0)\}$*, we denote its equivalence class as* $[a : b : c] \in \mathbb{P}^2(K)$.

In which way is the projective plane an extension of the affine plane? We can define three different (natural) embeddings of $\mathbb{A}^2(K)$ into $\mathbb{P}^2(K)$ adding a 1 in different places:

$$i_1 : \mathbb{A}^2(K) \to \mathbb{P}^2(K);\ (a, b) \mapsto [1 : a : b]$$
$$i_2 : \mathbb{A}^2(K) \to \mathbb{P}^2(K);\ (a, b) \mapsto [a : 1 : b]$$
$$i_3 : \mathbb{A}^2(K) \to \mathbb{P}^2(K);\ (a, b) \mapsto [a : b : 1]$$

These maps provide us with a covering of $\mathbb{P}^2(K)$ by affine planes, as the following lemma shows:

Lemma 5.6. *The maps* i_1, i_2, i_3 *are injective, and* $i_1(\mathbb{A}^2(K)) \cup i_2(\mathbb{A}^2(K)) \cup i_3(\mathbb{A}^2(K)) = \mathbb{P}^2(K)$.

Proof.
- Let us see first that i_1 is injective (for i_2 and i_3 one proceeds analogously). Assume $i_1(a_1, b_1) = i_1(a_2, b_2)$. That is, $[1 : a_1 : b_1] = [1 : a_2 : b_2]$. By Definition 5.5, this means there exists a $\lambda \in K^\times$ such that $a_1 = \lambda a_2$, $b_1 = \lambda b_2$, $1 = \lambda \cdot 1$. Thus $\lambda = 1$ and $a_1 = a_2$, $b_1 = b_2$.
- Let $P \in \mathbb{P}^2(K)$ be a point, say $P = [a : b : c]$ for some $(a, b, c) \in K \times K \times K \setminus \{(0,0,0)\}$. One (at least) of the three elements a, b, c is nonzero. If a is nonzero, then $P = [a : b : c] = [1 : b/a : c/a] = i_1(b/a, c/a) \in i_1(\mathbb{A}^2(K))$. If a is zero but b is nonzero, then $P = [0 : b : c] = [0 : 1 : c/b] = i_2(0, c/b) \in i_2(\mathbb{A}^2(K))$. Finally, if both a and b are zero, then c must be nonzero and $P = [a, b, c] = [0 : 0 : c] = [0 : 0 : 1] = i_3(0, 0) \in i_3(\mathbb{A}^2(K))$.

□

Remark 5.7. *The subsets* $i_1(\mathbb{A}^2(K))$, $i_2(\mathbb{A}^2(K))$, $i_3(\mathbb{A}^2(K))$ *cover* $\mathbb{P}^2(K)$*, but they are not disjoint. For instance, the point* $[1 : 1 : 1]$ *lies in the three sets. But let* $H = i_1(\{(a, 0) : a \in K\})$ *and* $O = [0 : 1 : 0]$*. Then* $\mathbb{P}^2(K) = i_3(\mathbb{A}^2(K)) \cup H \cup \{O\}$*, and this union is disjoint. In the following lectures, unless we say the contrary, we view* $\mathbb{A}^2(K)$ *inside* $\mathbb{P}^2(K)$ *via* $i = i_3$.

Via the inclusion $i : \mathbb{A}^2(K) \hookrightarrow \mathbb{P}^2(K)$, we can view the affine curves inside the projective plane, $C_f(K) \mapsto i(C_f(K)) \subset \mathbb{P}^2(K)$. But, in the same way that we completed the affine plane adding a line and a point at infinity, we want to complete the affine curves to projective curves. Since each point of $\mathbb{P}^1(K)$ is determined by a triple of elements, it seems natural to try to define the projective curves as the vanishing set of polynomials in $K[X, Y, Z]$.

Example 5.8. *Let K be a field with at least three elements and let $f(X,Y,Z) \in K[X,Y,Z]$ be defined as $f(X,Y,Z) = X^2 + Y + Z$. Then $f(1,-2,1) = 0$ but for $\lambda \neq 0,1$, $f(\lambda,-2\lambda,\lambda) = \lambda^2 - 2\lambda + \lambda = \lambda(\lambda-1) \neq 0$. Therefore the point $[1:-2:1] \in \mathbb{P}^2(K)$ has a representative $(1,-2,1) \in K \times K \times K \setminus \{(0,0,0)\}$ with $f(1,-2,1) = 0$ and another one, $(1\lambda,-2\lambda,\lambda) \in K \times K \times K \setminus \{(0,0,0)\}$ such that $f(\lambda,-2\lambda,\lambda) \neq 0$.*

The previous example shows that not every polynomial in $K[X,Y,Z]$ is suitable for defining a curve in the projective plane.

Definition 5.9. *Let $d \geq 1$ be an integer. A nonzero polynomial $f \in K[X,Y,Z]$ is called* homogeneous of degree d *if*

$$f(X,Y,Z) = \sum_{\substack{\nu_1,\nu_2,\nu_3 \geq 0 \\ \nu_1+\nu_2+\nu_3 = d}} a_{\nu_1,\nu_2,\nu_3} X^{\nu_1} Y^{\nu_2} Z^{\nu_3}.$$

Example 5.10. *For example, $X+Y$, $X+Y+Z$, are homoegeneous polynomials of degree 1, $ZY^2 - X^3 + Z^2X - Z^3$, Y^3 are homogeneous polynomials of degree 3.*

Lemma 5.11. *Let $f \in K[X,Y,Z]$ be a homogeneous polynomial of degree d, $(a,b,c) \in K \times K \times K$. Then the following are equivalent:*

(i) $f(a,b,c) = 0$.

(ii) For all $\lambda \in K^\times$, $f(\lambda a, \lambda b, \lambda c) = 0$.

Proof. It is clear that the second condition implies the first. Now, assume that $f(a,b,c) = 0$. Since f is homogeneous, we can write it as

$$f(X,Y,Z) = \sum_{\substack{\nu_1,\nu_2,\nu_3 \geq 0 \\ \nu_1+\nu_2+\nu_3 = d}} a_{\nu_1,\nu_2,\nu_3} X^{\nu_1} Y^{\nu_2} Z^{\nu_3}$$

for some coefficients $a_{\nu_1,\nu_2,\nu_3} \in K$. Hence

$$f(\lambda a, \lambda b, \lambda c) = \sum_{\substack{\nu_1,\nu_2,\nu_3 \geq 0 \\ \nu_1+\nu_2+\nu_3 = d}} a_{\nu_1,\nu_2,\nu_3} (\lambda a)^{\nu_1} (\lambda b)^{\nu_2} (\lambda c)^{\nu_3} =$$

$$\sum_{\substack{\nu_1,\nu_2,\nu_3 \geq 0 \\ \nu_1+\nu_2+\nu_3 = d}} a_{\nu_1,\nu_2,\nu_3} \lambda^{\nu_1+\nu_2+\nu_3} a^{\nu_1} b^{\nu_2} c^{\nu_3} = \lambda^d \sum_{\substack{\nu_1,\nu_2,\nu_3 \geq 0 \\ \nu_1+\nu_2+\nu_3 = d}} a_{\nu_1,\nu_2,\nu_3} a^{\nu_1} b^{\nu_2} c^{\nu_3} = \lambda^d f(a,b,c) = 0$$

□

The previous lemma allows us to formulate the following definition.

Definition 5.12.

- *Let $d \geq 1$ be an integer, and let $f \in K[X,Y,Z]$ be a homogeneous polynomial of degree d. We define the following subset of the projective plane over K:*

$$C_f(K) := \{[a:b:c] \in \mathbb{P}^2(K) : f(a,b,c) = 0\}.$$

- *Consider the set of pairs $\{(C_f(K), f) : f \in K(X,Y,Z)$ homogeneous$\}$. We will identify two pairs $(C_{f_1}(K), f_1)$ and $(C_{f_2}(K), f_2)$ if $f_1 = \lambda f_2$ for some $\lambda \in K^\times$.*

- *A* projective plane curve over K *is a (class of a) pair* $(C_f(K), f)$ *for some homogeneous polynomial* $f \in K[X,Y,Z]$. *We will denote it by* C/K *or* C_f/K.

The next question we want to answer is: given a plane affine curve C_f/K, how does it extend to a projective curve? In other words, which is the "right" homogeneous polynomial $g \in K[X,Y,Z]$ such that the plane projective curve $(C_g(K), g)$ extends $(C_f(K), f)$? One of the things we want is that, whenever $(a,b) \in C_f(K)$, then $[a : b : 1] \in C_g(K)$. This will in particular happen if $f(a,b) = g(a,b,1)$ for all $a, b \in K^2$. Assume that g is a homogeneous polynomial of degree d satisfying $g(x,y,1) = f(x,y)$. If $[\alpha : \beta : \gamma] \in C_g(K)$ satisfies that $\gamma \neq 0$, then $g(\alpha,\beta,\gamma) = \gamma^d g(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}, 1) = \gamma^d f(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma})$. We can formally make the substitution $g(X,Y,Z) = Z^d f(\frac{X}{Z}, \frac{Y}{Z})$. For this expression to be a polynomial (i.e., without negative powers of Z) we need that d be greater than or equal to the degree of f (i.e., the maximum n such that there is a term $a_{\nu_1\nu_2} x^{\nu_1} y^{\nu_2}$ in $f(x,y)$ with $a_{\nu_1\nu_2} \neq 0$ and $\nu_1 + \nu_2 = n$). Since we do not want our projective curve to contain the whole H (which is already a line), we do not want that Z is a common factor of all the terms of g. In other words, if $f(x,y) = \sum_{\nu_1,\nu_2} a_{\nu_1\nu_2} x^{\nu_1} y^{\nu_2}$, and $n = \max\{\nu_1 + \nu_2 : a_{\nu_1\nu_2} \neq 0\}$, we want to have the equality $d = n$. This discussion motivates the following definition.

Definition 5.13. *1. Let* $f \in K[x,y]$ *be a nonzero polynomial, say* $f(x,y) = \sum_{\nu_1,\nu_2} a_{\nu_1\nu_2} x^{\nu_1} y^{\nu_2}$.

- *The integer* $\deg_{\mathrm{T}}(f) = \max\{\nu_1 + \nu_2 : a_{\nu_1\nu_2} \neq 0\}$ *is called the* total degree *of* f. *We will say that* f *is* nonconstant *if* $\deg_{\mathrm{T}}(f) \geq 1$.
- *The* homogenisation *of a nonconstant polynomial* $f(x,y) \in K[x,y]$ *is the polynomial* $f^* \in K[X,Y,Z]$ *defined as*

$$f^*(X,Y,Z) = \sum_{\nu_1,\nu_2} a_{\nu_1\nu_2} X^{\nu_1} Y^{\nu_2} Z^{\deg_{\mathrm{T}}(f) - (\nu_1+\nu_2)}$$

2. The projective curve C_{f^*}/K *will be called the* projectivisation *of the affine curve* C_f/K.

Remark 5.14. *The homogenisation* f^* *of a polynomial* f *as above is clearly a homogeneous polynomial of degree* $\deg_T(f)$. *The relationship between* $C_{f^*}(K)$ *and* $C_f(K)$ *will be made precise in the following lemma.*

Lemma 5.15. *Let* $f \in K[x,y]$ *be a nonconstant polynomial. It holds that*

$$i(C_f(K)) = C_{f^*}(K) \cap i(\mathbb{A}^2(K)).$$

Proof. $\subseteq$ Let $(a,b) \in C_f(K)$. $i(a,b) = [a : b : 1] \in i(\mathbb{A}^2(K))$. Moreover $f(a,b) = 0$, hence $f^*(a,b,1) = 0$, which implies $[a : b : 1] \in C_{f^*}(K)$.

$\supseteq$ Let $P \in C_{f^*}(K) \cap i(\mathbb{A}^2(K))$. Since $P \in i(\mathbb{A}^2(K))$, it can be written as $[a : b : 1] \in \mathbb{P}^2(K)$. Since $P \in C_{f^*}(K)$, we have $0 = f^*(a,b,1) = f(a,b)$. Hence $(a,b) \in C_f(K)$ and $i(a,b) = [a : b : 1] = P$. □

Example 5.16. • *Let* K *be a field,* $f(x,y) = \alpha x + \beta y + \gamma \in K[x,y]$ *a polynomial such that either* $\alpha = 0$ *or* $\beta = 0$ *and* C_f/K *the corresponding affine line. Then the homogenisation of*

f is $f^*(X,Y,Z) = \alpha X + \beta Y + \gamma Z$, and the projectivisation of C_f/K is the projective line *C_{f^*}/K. Note that*

$$C_{f^*}(K) = \{[a:b:c] \in \mathbb{P}^2(K) : f^*(a,b,c) = 0\} =$$
$$\{[a:b:1] \in \mathbb{P}^2(K) : f^*(a,b,1) = 0\} \cup \{[a:b:0] \in \mathbb{P}^2(K) : f^*(a,b,0) = 0\} =$$
$$i(C_f(K)) \cup \{[a:b:0] \in \mathbb{P}^2(K) : \alpha a + \beta b = 0\}$$

By hypothesis either α or β are nonzero. If $\alpha \neq 0$, then $\{[a:b:0] \in \mathbb{P}^2(K) : \alpha a + \beta b = 0\} = \{[-b\beta/\alpha : b : 0] \in \mathbb{P}^2(K) : b \in K^\times\} = \{[-\beta/\alpha : 1 : 0]\}$. If $\alpha = 0$, then $\beta \neq 0$ and $\{[a:b:0] \in \mathbb{P}^2(K) : \beta b = 0\} = \{[a:0:0] : a \in K^\times\} = \{[1:0:0]\}$. In both cases, the projectivisation of C_f/K contains one more point than C_f/K.

- *Recall that in Example 5.4-(2) we considered the curve $C_f/\mathbb{F}_4$ defined by $f(x,y) = y^2 + y + x^3 + x$. We now compute its projectivisation. First, $f^*(X,Y,Z) = ZY^2 + Z^2Y + X^3 + Z^2X$. Next, the set $C_{f^*}(\mathbb{F}_4)$ is defined as*

$$\{[a:b:c] \in \mathbb{P}^2(\mathbb{F}_4) : f^*(a,b,c) = 1\} =$$
$$\{[a:b:1] \in \mathbb{P}^2(\mathbb{F}_4) : f^*(a,b,1) = 0\} \cup \{[a:b:0] \in \mathbb{P}^2(\mathbb{F}_4) : f^*(a,b,0) = 0\} =$$
$$i(C_f(\mathbb{F}_4)) \cup \{[a:b:0] \in \mathbb{P}^2(\mathbb{F}_4) : f^*(a,b,0) = 0\}$$

The set $C_f(\mathbb{F}_4)$ was already computed in Example 5.4-(2). On the other hand, $g(a,b,0) = a^3$ is zero if and only if $a = 0$. So the only point of $C_{f^*}(\mathbb{F}_4)$ which is not in the affine part of the curve is $O = [0:1:0]$.

Definition 5.17. *A* projective line *is a projective curve C_f/K such that $f \in K[X,Y,Z]$ is a homogeneous polynomial of degree 1. If $f(X,Y,Z) = \alpha X + \beta Y + \gamma Z$ for $\alpha, \beta, \gamma \in K$ not all vanishing. We denote it by $L(\alpha,\beta,\gamma)/K$.*

Lemma 5.18. *(a) Let $P_1, P_2 \in \mathbb{P}^2(K)$ be two different points. There exists one and only one projective line L/K passing through P_1 and P_2 (that is to say, $P_1, P_2 \in L(K)$).*

(b) Let L_1/K, L_2/K be two different projective lines in $\mathbb{P}^2(K)$. Then they meet at exactly one point (that is to say, $L_1(K) \cap L_2(K) = \{P\}$ for some point $P \in \mathbb{P}^2(K)$).

Proof. (a) Let $P_1 = [a_1 : b_1 : c_1]$ and $P_2 = [a_2 : b_2 : c_2]$ be two different points. If $L/K = L(\alpha,\beta,\gamma)/K$ is a line such that $P_1, P_2 \in L(K)$, then it holds that

$$\begin{cases} a_1\alpha + b_1\beta + c_1\gamma = 0 \\ a_2\alpha + b_2\beta + c_2\gamma = 0. \end{cases}$$

In other words, (α,β,γ) must be a solution of

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{5.1}$$

The condition that P_1 and P_2 are different means precisely that the two rows (a_1, b_1, c_1) and (a_2, b_2, c_2) are linearly independent. In other words, the rank of the matrix $\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}$ is two. Therefore there is a 2×2 minor with nonzero determinant. Assume it is $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$ (all other cases are analogous).

Then the system of equations

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -c_1 \\ -c_2 \end{pmatrix} \tag{5.2}$$

has a unique solution (α, β). Hence the projective line $L(\alpha, \beta, 1)/K$ passes through P_1 and P_2. Now assume there was another line $L(\alpha', \beta', \gamma')/K$ passing through P_1 and P_2, that is to say, satisfying Equation (5.1). The uniqueness of the solution of the system (5.2) implies that, if this $L(\alpha', \beta', \gamma')/K$ is different from $L(\alpha, \beta, 1)/K$, then $\gamma' = 0$. But then (α', β') would be the unique solution of the system

$$\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

hence $(\alpha', \beta', \gamma') = (0, 0, 0)$, and this does not define a projective line.

(b) See Sheet 7.

□

Up to this point, we always fixed our field K and work with curves and polynomials over it. But assume we have an extension of fields E/K. Every polynomial $f \in K[x, y]$ is naturally a polynomial in $E[x, y]$ via the inclusion $K \subseteq E$. We can then consider the curves C_f/K and C_f/E. Obviously $C_f(K) \subseteq C_f(E)$ via the inclusion $\mathbb{A}^2(K) \subseteq \mathbb{A}^2(E)$ induced by $K \subseteq E$. Actually it holds that

$$C_f(K) = C_f(E) \cap \mathbb{A}^2(K).$$

It can of course happen that $C_f(E)$ is strictly bigger than $C_f(K)$, so that the two curves $(C_f(K), f)$ and $(C_f(E), f)$ are not the same object. It is important to have in mind over which field we are working (which is the reason why the curves are denoted by C_f/K). A useful particular case of this is to consider an algebraic closure $\overline{K}$ of K, and consider the curve $C_f/\overline{K}$ given by $(C_f(\overline{K}), f)$.

Example 5.19. *Let $K = \mathbb{F}_2$, $E = \mathbb{F}_4$.*

- *Recall that in Example 5.4-(2) we considered the curve $C_f/\mathbb{F}_4$ defined by $f(x, y) = y^2 + y + x^3 + x$. We had computed the set $C_f(\mathbb{F}_4)$, namely $C_f(\mathbb{F}_4) = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$.*

  Since $f(x, y) \in \mathbb{F}_2[x, y] \subset \mathbb{F}_4[x, y]$, we can also consider the curve $C_f/\mathbb{F}_2$. The set $C_f(\mathbb{F}_2)$ consists of the points of $C_f(\mathbb{F}_4)$ that are contained in $\mathbb{A}^2(\mathbb{F}_2) = \mathbb{F}_2 \times \mathbb{F}_2$. In this case all the points of $C_f(\mathbb{F}_4)$ belong to $\mathbb{A}^2(\mathbb{F}_2)$, hence $C_f(\mathbb{F}_2) = C_f(\mathbb{F}_4)$.

x	x^3+x
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$
$\overline{X}$	$\overline{X+1}$
$\overline{X+1}$	$\overline{X}$

y	y^2
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$
$\overline{X}$	$\overline{X+1}$
$\overline{X+1}$	$\overline{X}$

- *Consider now the curve $C_f/\mathbb{F}_2$ (resp. $C_f/\mathbb{F}_4$) defined by $f(x,y)=y^2+x^3+x$. We want to compute $C_f(\mathbb{F}_2)$ and $C_f(\mathbb{F}_4)$. As in Example 5.4-(2), let us make some tables (see below).*

  The points of $C_f(\mathbb{F}_4)$ are those where the values of y^2 and x^3+x match, namely $C_f(\mathbb{F}_4)=\{(\overline{0},\overline{0}),(\overline{1},\overline{0}),(\overline{X},\overline{X})(\overline{X+1},\overline{X+1})\}$. On the other hand, the subset of $C_f(\mathbb{F}_4)$ of points belonging to $\mathbb{A}^2(\mathbb{F}_2)$ is just $C_f(\mathbb{F}_2)=\{(\overline{0},\overline{0}),(\overline{1},\overline{0})\}$, so in this case $C_f(\mathbb{F}_2)\neq C_f(\mathbb{F}_4)$.

Assume again that we have a field extension $K\subset E$. Any homogeneous polynomial $f\in K[X,Y,Z]$ belongs also to $E[X,Y,Z]$, hence we can consider the curves C_f/K and C_f/E. Due to the equivalence relationship involved in the definition of the projective plane, the inclusion $\mathbb{P}^2(K)\subset\mathbb{P}^2(E)$ is not as straightforward as in the affine setting. In any case one has such an inclusion, and the relationship

$$C_f(K)=\mathbb{P}^2(K)\cap C_f(E).$$

The details will be discussed in Sheet 7.

Now we want to define the tangent line L/K to a curve C_f/K at a point $P\in C_f(K)$. For simplicity, we first consider the point $P=(0,0)$ and an affine curve that passes through P, let us say C_f/K with $f(0,0)=0$. We want to define the tangent line as "the line which is closest" to the curve in a small neighbourhood of P. Assume that $f(x,y)=\sum_{\nu_1,\nu_2}a_{\nu_1\nu_2}x^{\nu_1}y^{\nu_2}$. We can rewrite f as

$$f(x,y)=\sum_{i=1}^{n}\sum_{\nu_1+\nu_2=i}a_{\nu_1\nu_2}x^{\nu_1}y^{\nu_2}$$

for $n=\deg_{\mathrm{T}}(f)$, so that, for each i, $\sum_{\nu_1+\nu_2=i}a_{\nu_1\nu_2}x^{\nu_1}y^{\nu_2}$ is either a homogeneous polynomial of degree i or zero. Write $f_i=\sum_{\nu_1+\nu_2=i}a_{\nu_1\nu_2}x^{\nu_1}y^{\nu_2}$. As we look at the curve in a smaller and smaller neighbourhood of $(0,0)$, if $i>j$ and f_i, f_j are nonzero, $f_i(x,y)$ shrinks quicker than $f_j(x,y)$. Hence, for our purposes it suffices to look at the f_i with smallest i. Since f vanishes at $(0,0)$, it has no constant term, so the smallest possible value of i is $i=1$. If both $a_{0,1}$ and $a_{1,0}$ are zero, we have that f_1 is zero, and hence the smallest homogeneous f_i occurs for $i\geq 2$.

But assume this is not the case, that is to say, that $a_{0,1}$ and $a_{1,0}$ do not both vanish. The affine lines through the point $(0,0)$ are defined by a polynomial of the shape $\alpha x+\beta y$ for some $\alpha,\beta\in K$ with $\alpha,\beta\in K$ not both zero. Consider the difference

$$f(x,y)-(\alpha x+\beta y)=\sum_{i=1}^{n}\sum_{\nu_1+\nu_2=i}a_{\nu_1\nu_2}x^{\nu_1}y^{\nu_2}-(\alpha x+\beta y)=$$

$$(a_{0,1}-\beta)y+(a_{1,0}-\alpha)x+\sum_{i=2}^{n}\sum_{\nu_1+\nu_2=i}a_{\nu_1\nu_2}x^{\nu_1}y^{\nu_2}.$$

According to our discussion above, the line which makes this sum smallest in a neighbourhood of $(0,0)$, that is to say, the line that is "closest" to the curve C_f/K at $(0,0)$, is the line such that the sum of the terms of degree 1 in the expression above is zero (so that the smallest homogeneous polynomial is of degree $i \geq 2$). There is only one line doing this, namely, the one defined by the polynomial $a_{0,1}y + a_{1,0}x$. This will be the tangent line to C_f/K at $(0,0)$.

Definition 5.20.

- *Let A be a ring, and $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$. The* formal derivative *of f is defined as $f'(X) = \sum_{i=1}^{n} a_i i X^{i-1} \in A[X]$. We also define $f^{(n)}(X) \in A[X]$ (the n-*th formal derivative*) recursively as*

$$\begin{cases} f^{(1)}(X) := f'(X), \\ f^{(n)}(X) := (f^{(n-1)})'(X). \end{cases}$$

- *Let K be a field, $n \in \mathbb{N}$ and $f \in K[X_1 \dots X_n]$. Fix $i \in \{1, \dots, n\}$, let $I = \{1, \dots, n\} \setminus \{i\}$, and let $A = K[\{X_j : j \in I\}]$, so that $K[X_1, \dots, X_n] = A[X_i]$. The* partial derivative of f with respect to X_i*, is the formal derivative of f in $A[X_i]$. We denote it by $\frac{\partial f}{\partial X_i}(X_1, \dots, X_n)$.*

Remark 5.21. *Let $f(x,y) = \sum_{\nu_1,\nu_2} a_{\nu_1\nu_2} x^{\nu_1} y^{\nu_2} \in K[x,y]$ as in the discussion before Definition 5.20. Note that the values $a_{0,1}$ and $a_{1,0}$ that occur in the definition of the tangent line to C_f/K at the point $(0,0)$ satisfy that $\frac{\partial f}{\partial x}(0,0) = a_{1,0}$ and $\frac{\partial f}{\partial y}(0,0) = a_{0,1}$. Observe that in the discussion we assumed that either $a_{0,1}$ or $a_{1,0}$ is nonzero. This motivates the following definition.*

Definition 5.22. *Let $f \in K[x,y]$ be a nonzero polynomial, C_f/K be the affine curve defined by it, and $(a,b) \in \mathbb{A}^2(K)$ such that $f(a,b) = 0$.*

- *We will say that the point (a,b) of the curve C_f/K is* singular *if $\frac{\partial f}{\partial x}(a,b) = \frac{\partial f}{\partial y}(a,b) = 0$.*
- *We will say that the curve C_f/K is* nonsingular *or* smooth *if, for some algebraic closure $\overline{K}$ of K, for every point $(a,b) \in C_f(\overline{K})$, (a,b) is not a singular point of the curve $C_f/\overline{K}$.*

Example 5.23.

- *Consider the curve $C_f/\mathbb{C}$ defined by the polynomial $f(x,y) = y^2 - x^4 - 2x^2 - 1$. Since $\frac{\partial f}{\partial x}(x,y) = -4x^3 - 4x$ and $\frac{\partial f}{\partial y}(x,y) = 2y$, the singular points of this curve are those satisfying the system of equations:*

$$\begin{cases} 0 = & y^2 - x^4 - 2x^2 - 1 \\ 0 = & -4x^3 - 4x \\ 0 = & 2y \end{cases}$$

From the second equation we get $x = 0$ or $x = \pm\sqrt{-1}$ and from the last equation we see that $y = 0$. But also the first equation must be satisfied, so $x = 0$, $y = 0$ is not a solution of the system. We get thus two solutions, namely the points $(\sqrt{-1}, 0)$ and $(-\sqrt{-1}, 0)$. Those two points of $C_f(\mathbb{C})$ are singular; hence the curve $C_f/\mathbb{C}$ is not smooth.

- *Since the polynomial $f(x,y) = y^2 - x^4 - 2x^2 - 1$ from the previous example lies in $\mathbb{R}[x,y]$, we may also consider the affine curve $C_f/\mathbb{R}$. Note that the two singular points we computed above do not belong to $\mathbb{A}^2(\mathbb{R})$, so $C_f/\mathbb{R}$ does not have singular points. Nevertheless, it is not a smooth curve, since in Definition 5.22 we require that the curve has no singular point when we consider it over the algebraic closure of $\mathbb{R}$, that is, over $\mathbb{C}$.*

Now we translate Definition 5.22 to the projective setting.

Definition 5.24. *Let $f \in K[X,Y,Z]$ be a homogeneous polynomial of degree d for some positive integer d, C_f/K be the projective curve defined by f, and $[a:b:c] \in \mathbb{P}^2(K)$ such that $f(a,b,c) = 0$.*

- *We will say that the point $[a:b:c]$ of the curve C_f/K is* singular *if $\frac{\partial f}{\partial X}(a,b,c) = \frac{\partial f}{\partial Y}(a,b,c) = \frac{\partial f}{\partial Z}(a,b,c) = 0$.*
- *We will say that the curve C_f/K is* nonsingular *or* smooth *if, for some algebraic closure $\overline{K}$ of K, for every point $P \in C_f(\overline{K})$, P is not a singular point of the curve $C_f/\overline{K}$.*

Remark 5.25.

- *The notion of singularity of a point $P = [a:b:c]$ is well defined, in the sense that it does not depend on the representative (a,b,c) of the equivalence class $P \in \mathbb{P}^2(K)$.*
- *The notion of singularity of a point in an affine curve extends the notion of singularity of a point in a projective curve, in the sense that a point (a,b) belonging to an affine curve $C_f(K)$ is singular if and only if the point $i(a,b) \in \mathbb{P}^2(K)$ is a singular point of the projectivisation C_{f^*}/K of C_f/K. This will be discussed in Sheet 9.*
- *The projectivisation of a smooth affine curve need not be smooth as a projective curve. See Sheet 8 for an example of this.*

Definition 5.26. *Let C_f/K be a projective curve and $P = [a:b:c]$ a nonsingular point of C_f/K. The* tangent line *to C_f/K at P is the projective line*

$$L\left(\frac{\partial f}{\partial X}(a,b,c), \frac{\partial f}{\partial Y}(a,b,c), \frac{\partial f}{\partial Z}(a,b,c)\right)/K.$$

Remark 5.27.

- *The tangent line to a projective curve is well defined:*
  - *Since P is a nonsingular point of C_f/K, at least one of the three numbers $\frac{\partial f}{\partial X}(a,b,c)$, $\frac{\partial f}{\partial Y}(a,b,c)$, $\frac{\partial f}{\partial Z}(a,b,c)$ is nonzero. Hence the tangent line is indeed a projective line.*
  - *The definition does not depend on the choice of representative $(a,b,c) \in (K \times K \times K) \setminus \{(0,0,0)\}$. Indeed, if d is the degree of f, then $\frac{\partial f}{\partial X}$, $\frac{\partial f}{\partial Y}$, $\frac{\partial f}{\partial Z}$ are homogeneous polynomials of degree $d-1$ if $d > 1$ or constants if $d = 1$. In the first case, $\frac{\partial f}{\partial X}(\lambda a, \lambda b, \lambda c) = \lambda^{d-1}\frac{\partial f}{\partial X}(a,b,c)$, and $L\left(\frac{\partial f}{\partial X}(a,b,c), \frac{\partial f}{\partial Y}(a,b,c), \frac{\partial f}{\partial Z}(a,b,c)\right)/K$ is the same curve as $L\left(\frac{\partial f}{\partial X}(\lambda a, \lambda b, \lambda c), \frac{\partial f}{\partial Y}(\lambda a, \lambda b, \lambda c), \frac{\partial f}{\partial Z}(\lambda a, \lambda b, \lambda c)\right)/K$. In the second case, the numbers $\frac{\partial f}{\partial X}(a,b,c)$, $\frac{\partial f}{\partial Y}(a,b,c)$, $\frac{\partial f}{\partial Z}(a,b,c)$ are elements of K, and in particular equal to $\frac{\partial f}{\partial X}(\lambda a, \lambda b, \lambda c)$, $\frac{\partial f}{\partial Y}(\lambda a, \lambda b, \lambda c)$, $\frac{\partial f}{\partial Z}(\lambda a, \lambda b, \lambda c)$.*
- *Note that this definition generalises the notion of tangent line to an affine curve at the point $(0,0)$ that we discussed before Definition 5.20.*

We conclude this section with the definition of multiplicity of intersection between a projective line and a projective curve at a given point.

Definition 5.28. *Let K be a field and $f(t) \in K[t]$ nonzero, say $f(t) = \sum_{i=0}^{n} a_i t^i$ for a certain $n \in \mathbb{N}$. The* order of $f(t)$ at $t = 0$ *is defined as* $\operatorname{ord}_{t=0} f(t) := \min\{a_i : a_i \neq 0\}$.

Remark 5.29. *Note that the order at $t = 0$ of a polynomial $f(t) \in K[t]$ is the least integer m such that $f^{(m)}(0) \neq 0$.*

Definition 5.30. *Let L/K be a projective line, C_f/K be a projective curve and $P = [a : b : c] \in L(K)$. The* multiplicity of intersection *between L/K and C_f/K at P, $\mathrm{m}(C_f, L, P)$, is defined as the order at $t = 0$ of the polynomial $\psi(t) = f(a + ta', b + tb', c + tc')$, where $P' = [a' : b' : c']$ is any point in $L(K)$ different from P.*

If $P \in L(K)$, we define $\mathrm{m}(C_f, L, P) = 0$.

Remark 5.31. *The multiplicity of intersection between a projective line and a projective curve at a point of the line is well defined. Namely, we need to see that it does not depend on the representative $(a, b, c) \in (K \times K \times K) \setminus \{(0, 0, 0)\}$ of P, the choice of $P' \in L(K)$, and the representative $(a', b', c') \in (K \times K \times K) \setminus \{(0, 0, 0)\}$ of P'. We will see this in several steps (see Lemma 5.32, Lemma 5.35 and Lemma 5.36).*

Lemma 5.32. *Given a projective line L/K, a projective curve C_f/K and two points $P, P' \in L(K)$, the order at $t = 0$ of the polynomial $\psi(t) = f(a + ta', b + tb', c + tc')$ does not depend on the representatives (a, b, c) and $(a', b', c') \in (K \times K \times K) \setminus \{(0, 0, 0)\}$ of P and P'.*

Proof. Let d be the degree of f, and $m = \mathrm{ord}_{t=0}\, \psi(t)$; we can write $\psi(t) = u_m t^m + u_{m+1} t^{m+1} + \cdots + u_s t^s$ for some $s \geq m$. Let us choose some representatives of P and P', say $P = [\lambda a : \lambda b : \lambda c]$ and $P' = [\mu a' : \mu b' : \mu c']$ for $\lambda, \mu \in K^\times$. If we construct the polynomial $\tilde{\psi}(t) = f(\lambda a + t(\mu a'), \lambda b + t(\mu b'), \lambda c + t(\mu c'))$, we have

$$\begin{aligned}\tilde{\psi}(t) = f(\lambda a + t(\mu a'), \lambda b + t(\mu b'), \lambda c + t(\mu c')) &= \lambda^d f(a + t\frac{\mu}{\lambda}a', b + t\frac{\mu}{\lambda}b', c + t\frac{\mu}{\lambda}c') \\ &= \psi(\frac{\mu}{\lambda}t) = u_m \left(\frac{\mu}{\lambda}\right)^m t^m + u_{m+1}\left(\frac{\mu}{\lambda}\right)^{m+1} t^{m+1} + \cdots + u_s \left(\frac{\mu}{\lambda}\right)^s t^s,\end{aligned}$$

and it is clear that the order of $\tilde{\psi}(t)$ at $t = 0$ is also m. □

It remains to see that the definition is independent of the choice of a point $P' \neq P$ in $L(K)$. For this we will use the notion of formal derivative (see Definition 5.20). We will extend this definition from elements of $K[X]$ to elements of $K(X)$, where K is a field.

Definition 5.33. *Let K be a field and $f(X), g(X) \in K[X]$ polynomials with $g(X) \neq 0$. Set $h(X) := f(X)/g(X) \in K(X)$. We define the* formal derivative *of $h(X)$ as*

$$h'(X) = \frac{f'(X)g(X) - f(X)g'(X)}{g^2(X)},$$

where $f'(X)$, $g'(X)$ denote the formal derivative of $f(X)$ and $g(X)$ in $K[X]$. We define the order of h at $X = 0$ *to be* $\mathrm{ord}_{X=0}(h(X)) := \mathrm{ord}_{X=0}(f(X)) - \mathrm{ord}_{X=0}(g(X))$.

Remark 5.34.

- *The definition of the formal derivative of an element $h(X) \in K(X)$ does not depend on the representation of $h(X) = f(X)/g(X)$ as a quotient of elements of $K[X]$ (See Sheet 8).*

- *The definition of the order at $X = 0$ of an element $h(X) \in K(X)$ does not depend on the representation $h(X) = f(X)/g(X)$ as quotient of elements of $K[X]$ (See Sheet 8).*
- *Let $h(X) \in K(X)$. If $h(X) \in K[X]$, then the definition of order of $h(X)$ at $X = 0$ from Definition 5.20 and Definition 5.33 coincide; just write $h(X) = h(X)/1$ and apply the remark above.*

The next lemma collects some facts about formal derivatives.

Lemma 5.35. *1. Let $\varphi(X), \psi(X) \in K(X)$. Then $(\psi \circ \varphi)'(X) = \psi'(\varphi(X))\varphi'(X)$.*

2. Let $\varphi(X), \psi(X) \in K(X)$. Then $\operatorname{ord}_{X=0}(\varphi(X)\psi(X)) = \operatorname{ord}_{X=0}\varphi(X) + \operatorname{ord}_{X=0}\psi(X)$.

3. Let $\varphi(X), \psi(X) \in K[X]$ such that $\operatorname{ord}_{X=0}(\varphi(X)) = 1$. Then

$$\operatorname{ord}_{X=0}\varphi(X) = \operatorname{ord}_{X=0}\varphi \circ \psi(X).$$

Proof. See Sheets 8, 9. □

Lemma 5.36. *Given a projective line L/K, a projective curve C_f/K, points $P, P' \in L(K)$ and representatives $(a, b, c), (a', b', c') \in (K \times K \times K) \setminus \{(0, 0, 0)\}$ of P and P', for any point $P'' = [a'' : b'' : c'']$ in $L(K)$ different from P, we have that the orders of $\tilde{\psi}(t) = f(a + ta'', b + tb'', c + tc'')$ and $\psi(t) = f(a + ta', b + tb', c + tc')$ at $t = 0$ coincide.*

Proof. Let d be the degree of f, and $m = \operatorname{ord}_{t=0}(\psi(t))$; m is the least integer such that $\psi^{(m)}(0) \neq 0$. Let $L = L(\alpha, \beta, \gamma)$. The following system of equations

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

has two different solutions, namely $\begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$. Therefore $\det \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} = 0$. In other words, the rows (a, b, c), (a', b', c') and (a'', b'', c'') are not linearly independent. Hence there exist $\lambda, \mu \in K$ such that $\lambda(a, b, c) + \mu(a', b', c') = (a'', b'', c'')$. Note that, since $P'' \neq P$, we have $\mu \neq 0$. We can now write

$$\begin{aligned} \tilde{\psi}(t) = f(a + ta'', b + tb'', c + tc'') &= f(a + t(\lambda a + \mu a'), b + t(\lambda b + \mu b'), c + t(\lambda c + \mu c')) \\ &= f((1 + t\lambda)a + t(\mu a'), (1 + t\lambda)b + t(\mu b'), (1 + t\lambda)c + t(\mu c')) \\ &= (1 + t\lambda)^d f(a + \frac{\mu t}{1 + t\lambda}a', b + \frac{\mu t}{1 + t\lambda}b', c + \frac{\mu t}{1 + t\lambda}c') = (1 + t\lambda)^d \psi(\frac{\mu t}{1 + t\lambda}) \end{aligned}$$

Since $(1 + t\lambda)^d$ has order zero at $t = 0$, it follows from Lemma 5.35-(2) that $\operatorname{ord}_{t=0}(\tilde{\psi}(t)) = \operatorname{ord}_{t=0}(\psi(\frac{\mu t}{1+t\lambda}))$. Now from Lemma 5.35-(3) one gets that $\psi(t)$ and $\tilde{\psi}(t)$ have the same order at $t = 0$. □

Example 5.37. *Let us consider the projective curve $C_f/\mathbb{R}$, where $f(X,Y,Z) = Y^2Z^2 - X^4 - 2X^2Z^2 - Z^4$ and the point $P = [0:1:1]$*

- *First we consider the line $L/R = L(2,1,-1)/\mathbb{R}$. Note that $P \in L(\mathbb{R})$. Let us compute the multiplicity of intersection of C_f and L at P.*

  First, let us fix a point $P' \in L(K)$ different from P, say $P' = [1:-1:1]$. Consider the polynomial

  $$\psi(t) = f(0+t, 1-t, 1+t) = (1-t)^2(1+t)^2 - t^4 - 2t^2(1+t)^2 - (1+t)^4 = -3t^4 - 8t^3 - 10t^2 - 4t.$$

  We have that the order of $\psi(t)$ at $t = 0$ is 1, hence $\mathrm{m}(C_f, L, P) = 1$.

- *Note that $P \in C_f(\mathbb{R})$. Let us compute the tangent line to $C_f/\mathbb{R}$ at P. First we compute*

  $$\begin{cases} \frac{\partial f}{\partial X} = -4X^3 - 4Z^2X \\ \frac{\partial f}{\partial Y} = 2YZ^2 \\ \frac{\partial f}{\partial Z} = 2Y^2Z - 4X^2Z - 4Z^3 \end{cases}$$

  From these expressions we get that $\frac{\partial f}{\partial X}(0,1,1) = 0$, $\frac{\partial f}{\partial Y}(0,1,1) = 2$, $\frac{\partial f}{\partial Z}(0,1,1) = -2$. Therefore the tangent line to $C_f/\mathbb{R}$ at P is $L(0,2,-2)/K$, that is to say, $L(0,1,-1)/\mathbb{R}$.

  Let us compute the multiplicity of intersection between C_f and $L(0,1,-1)$ at P. First, fix a point $P' \in L(0,1,-1)(K)$, say $P' = [1:1:1]$. Consider the polynomial

  $$\psi(t) = f(0+t, 1+t, 1+t) = (1+t)^2(1+t)^2 - t^4 - 2t^2(1+t)^2 - (1+t)^4 = -2t^2 - 4t^3 - 3t^4.$$

  We see that the order of $\psi(t)$ at $t = 0$ is 2. This coincides with the naive notion that the tangent line cuts a curve with multiplicity greater than 1.

Lemma 5.38. *Let C_f/K be a projective curve, L/K a projective line and $P \in L(K)$ a projective point.*

(1) $\mathrm{m}(C_f, L, P) = 0$ if and only if P does not lie in C_f.

(2) Assume that $P \in C_f(K)$ and L/K is the tangent line to C_f at P. Then $\mathrm{m}(C_f, L, P) \geq 2$.

Proof. (1) Let $P = [a:b:c]$ and $P' = [a':b':c'] \in L(K)$ a point different from P. Set $\psi(t) = f(a+ta', b+tb', c+tc')$. Then $\psi(0) = f(a,b,c)$. Therefore $\psi(0) = 0$ if and only if $f(a,b,c) = 0$, that is to say, if and only if $P \in C_f(K)$.

(2) Fix a point $P' = [a':b':c'] \in L(K)$ different from P and consider the polynomial $\psi'(t) = f(a+a't, b+b't, c+c't)$. We have to prove that the minimal m with $\psi^{(m)}(0) \neq 0$ is greater than or equal to 2. Equivalently, we need to prove that $\psi(0) = 0$ and $\psi'(0) = 0$. The first equation follows from (1). For the second equation, we compute, using the chain rule (see Exercise 2 of Sheet 8), that

$$\begin{aligned} &\psi'(t) = (f(a+a't, b+b't, c+c't))' \\ &= \frac{\partial f}{\partial X}(a+a't, b+b't, c+c't)a' + \frac{\partial f}{\partial Y}(a+a't, b+b't, c+c't)b' + \frac{\partial f}{\partial Z}(a+a't, b+b't, c+c't)c' \end{aligned}$$

Hence $\psi'(0) = \frac{\partial f}{\partial X}(a,b,c)a' + \frac{\partial f}{\partial Y}(a,b,c)b' + \frac{\partial f}{\partial Z}(a,b,c)c' = 0$ because the point $P' = [a' : b' : c']$ belongs to $L(K) = L(\frac{\partial f}{\partial X}(a,b,c), \frac{\partial f}{\partial Y}(a,b,c), \frac{\partial f}{\partial Z}(a,b,c))(K)$.

□

In these lectures we will not discuss the notion of morphism between two curves. Nevertheless, sometimes it will be useful to make linear changes of variables to a curve. Many of the properties of a projective plane curve are preserved under linear changes of variables.

Lemma 5.39. *Let K be a field. For each matrix*

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in \mathrm{GL}_3(K),$$

the map

$$\begin{aligned} \varphi_A : \mathbb{P}^2(K) &\to \mathbb{P}^2(K) \\ [a : b : c] &\mapsto [a_{11}a + a_{12}b + a_{13}c : a_{21}a + a_{22}b + a_{23}c : a_{31}a + a_{32}b + a_{33}c] \end{aligned}$$

is well defined and bijective.

Let $f(X,Y,Z) \in K[X,Y,Z]$ be a homogeneous polynomial and set

$$f_A(X,Y,Z) := f(a_{11}X + a_{12}Y + a_{13}Z, a_{21}X + a_{22}Y + a_{23}Z, a_{31}X + a_{32}Y + a_{33}Z)$$

Then

$$C_f(K) = \varphi_A(C_{f_A}(K)).$$

Proof. See Sheet 10. □

Example 5.40. *Let $(a,b) \in \mathbb{A}^2(K)$, $(a,b) \neq (0,0)$. Consider the matrix*

$$A = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(K).$$

Then the map $\varphi_A : \mathbb{P}^2(K) \to \mathbb{P}^2(K)$ fixes the points of $\mathbb{P}^2(K) \setminus \mathbb{A}^2(K)$ and translates the points $(s,t) \in \mathbb{A}^2(K)$ to $(s+a, t+b) \in \mathbb{A}^2(K)$. We will say that φ_A is a translation by the point (a,b).

Lemma 5.41. *Let K be a field, and let $A \in \mathrm{GL}_3(K)$. Let $f(X,Y,Z) \in K[X,Y,Z]$ be a homogeneous polynomial and $f_A \in K[X,Y,Z]$ as in Lemma 5.39. Then, for each $P \in C_{f_A}(K)$, P is a singular point of C_{f_A}/K if and only if $\varphi_A(P)$ is a singular point of C_f/K.*

Proof. It suffices to prove that, if $\varphi_A(P) \in C_f(K)$ is singular, then $P \in C_f(K)$ is singular (the other implication is obtained applying the same reasoning to the linear change of variables $\varphi_{A^{-1}}$). For $i = 1,2,3$, let $\varphi_i(X,Y,Z) := a_{i1}X + a_{i2}Y + a_{i3}Z$. Then, using the chain rule, we obtain

$$\begin{aligned} \frac{\partial f_A}{\partial X}(r,s,t) = \frac{\partial f}{\partial X}(\varphi_1(r,s,t), \varphi_2(r,s,t), \varphi_3(r,s,t))\frac{\partial \varphi_1}{\partial X}(r,s,t) + \\ \frac{\partial f}{\partial Y}(\varphi_1(r,s,t), \varphi_2(r,s,t), \varphi_3(r,s,t))\frac{\partial \varphi_2}{\partial X}(r,s,t) + \\ \frac{\partial f}{\partial Z}(\varphi_1(r,s,t), \varphi_2(r,s,t), \varphi_3(r,s,t))\frac{\partial \varphi_3}{\partial X}(r,s,t) \end{aligned}$$

$$\frac{\partial f_A}{\partial Y}(r,s,t) = \frac{\partial f}{\partial X}(\varphi_1(r,s,t),\varphi_2(r,s,t),\varphi_3(r,s,t))\frac{\partial \varphi_1}{\partial Y}(r,s,t)+ \\ \frac{\partial f}{\partial Y}(\varphi_1(r,s,t),\varphi_2(r,s,t),\varphi_3(r,s,t))\frac{\partial \varphi_2}{\partial Y}(r,s,t)+ \\ \frac{\partial f}{\partial Z}(\varphi_1(r,s,t),\varphi_2(r,s,t),\varphi_3(r,s,t))\frac{\partial \varphi_3}{\partial Y}(r,s,t)$$

$$\frac{\partial f_A}{\partial Z}(r,s,t) = \frac{\partial f}{\partial X}(\varphi_1(r,s,t),\varphi_2(r,s,t),\varphi_3(r,s,t))\frac{\partial \varphi_1}{\partial Z}(r,s,t)+ \\ \frac{\partial f}{\partial Y}(\varphi_1(r,s,t),\varphi_2(r,s,t),\varphi_3(r,s,t))\frac{\partial \varphi_2}{\partial Z}(r,s,t)+ \\ \frac{\partial f}{\partial Z}(\varphi_1(r,s,t),\varphi_2(r,s,t),\varphi_3(r,s,t))\frac{\partial \varphi_3}{\partial Z}(r,s,t)$$

Let $P = [a : b : c] \in C_{f_A}(K)$, call $a' = \varphi_1(a,b,c)$, $b' = \varphi_2(a,b,c)$, $c' = \varphi_3(a,b,c)$. Then $\varphi_A(P) = [a' : b' : c']$.

Assume $\varphi_A(P)$ is a singular point of $C_f(K)$. Then

$$f(a',b',c') = 0, \quad \frac{\partial f}{\partial X}(a',b',c') = 0, \quad \frac{\partial f}{\partial Y}(a',b',c') = 0, \quad \frac{\partial f}{\partial Z}(a',b',c') = 0,$$

Therefore $f_A(a,b,c) = 0$, and

$$\frac{\partial f_A}{\partial X}(a,b,c) = \frac{\partial f}{\partial X}(a',b',c')\frac{\partial \varphi_1}{\partial X}(a,b,c) + \frac{\partial f}{\partial Y}(a',b',c')\frac{\partial \varphi_2}{\partial X}(a,b,c)+ \\ \frac{\partial f}{\partial Z}(a',b',c')\frac{\partial \varphi_3}{\partial X}(a,b,c) = 0$$

Analogously, it holds that $\frac{\partial f_A}{\partial Y}(a,b,c) = 0$ and $\frac{\partial f_A}{\partial Z}(a,b,c) = 0$; thus $[a : b : c]$ is a singular point of $C_{f_A}(K)$. □

6 Elliptic Curves

Definition 6.1. *Let K be a field. A* Weierstrass equation *is an equation of the form $f(X,Y,Z) = 0$, where $f(X,Y,Z) \in K[X,Y,Z]$ is a homogeneous polynomial of degree 3 of the form*

$$f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \tag{6.3}$$

for some $a_1, a_2, a_3, a_4, a_6 \in K$.

Remark 6.2.
- *A Weierstrass equation is uniquely given by a polynomial as in the right hand side of* (6.3)*, so we will identify Weierstrass equations with the polynomials that define them.*

- *Not every homogeneous polynomial of degree 3 defines a Weierstrass equation. Namely, a homogeneous polynomial of degree 3 has the shape*

$$g(X,Y,Z) = \sum_{\substack{\nu_1,\nu_2,\nu_3 \geq 0 \\ \nu_1+\nu_2+\nu_3=3}} a_{\nu_1,\nu_2,\nu_3} X^{\nu_1} Y^{\nu_2} Z^{\nu_3},$$

hence it can have up to 10 different terms, while the polynomial f in (6.3) *only has 7; the terms in X^2Y, XY^2 and Y^3 cannot occur.*

The numbering of the coefficients (a_5 missing) in the Weierstrass equation has historical reasons and is nowadays a standard convention.

Lemma 6.3. *Let $f(X,Y,Z) = 0$ be a Weierstrass equation and let $A \in \mathrm{GL}_3(K)$ be given by*

$$A = \begin{pmatrix} u^2 & 0 & r \\ u^2 s & u^3 & t \\ 0 & 0 & 1 \end{pmatrix}$$

for $u, r, s, t \in K$. Then the polynomial f_A obtained from f by the linear change of variables given by A (as in Lemma 5.39) also satisfies that $f_A(X,Y,Z) = 0$ is a Weierstrass equation.

Proof. See Sheet 10. □

Definition 6.4. *Let K be a field. An* elliptic curve over K *is a projective plane curve C_f/K such that:*

- *$f(X,Y,Z) = 0$ is a Weierstrass equation.*
- *C_f/K is smooth.*

We will usually denote elliptic curves by E/K when the polynomial f is clear from the context.

Example 6.5. *The curve $C_f/\mathbb{F}_4$ defined by $f(X,Y,Z) = Y^2Z + YZ^2 + X^3 + XZ^2$ whose affine part was considered in Example 5.19 is an elliptic curve. The curve $C_f/\mathbb{F}_4$ defined by $f(X,Y,Z) = Y^2Z + X^3 + XZ^2$ whose affine part was considered in Example 5.19 is not an elliptic curve because the point $[1:0:1] \in E(\mathbb{F}_4)$ is a singular point.*

Lemma 6.6. *Let $f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \in K[X,Y,Z]$. Then*

$$C_f(K) = (C_f(K) \cap \mathbb{A}^2(K)) \cup \{\mathcal{O}\}.$$

Proof.

$$\begin{aligned} C_f(K) = (C_f(K) \cap \mathbb{A}^2(K)) \cup \{[a:b:0] \in \mathbb{P}^2(K) : f(a,b,0) = 0\} = \\ (C_f(K) \cap \mathbb{A}^2(K)) \cup \{[a:b:0] \in \mathbb{P}^2(K) : a^3 = 0\} = \\ (C_f(K) \cap \mathbb{A}^2(K)) \cup \{[0:1:0]\}. \end{aligned}$$

□

Lemma 6.7. *Let $f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \in K[X,Y,Z]$. Then $\mathcal{O} = [0:1:0]$ is never a singular point of C_f/K.*

Proof. If $\mathcal{O} \in C_f(K)$ is a singular point of C_f/K, it must hold that

$$\begin{cases} f(0,1,0) & = 0 \\ \frac{\partial f}{\partial X}(0,1,0) & = 0 \\ \frac{\partial f}{\partial Y}(0,1,0) & = 0 \\ \frac{\partial f}{\partial Z}(0,1,0) & = 0 \end{cases}$$

But $\frac{\partial f}{\partial Z}(X,Y,Z) = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - a_4 2XZ - a_6 3Z^2$, so $\frac{\partial f}{\partial Z}(0,1,0) = 1 \neq 0$. □

As a consequence, if we want to check if a projective curve C_f/K, with f satisfying (6.3) is an elliptic curve, it suffices to check for singular points in the affine part of the curve.

Definition 6.8. *Let $a_1, a_2, a_3, a_4, a_6 \in K$ be given. We define the following quantities:*

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2 \\ b_4 &:= 2a_4 + a_1a_4 \\ b_6 &:= a_3^2 + 4a_6 \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

$$\begin{aligned} c_4 &:= b_2^2 - 24b_4 \\ c_6 &:= b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \end{aligned}$$

$$j := \frac{c_4^3}{\Delta} \text{ if } \Delta \neq 0.$$

We call Δ the discriminant *and j the j-*invariant *of the Weierstrass equation $f(X,Y,Z) = 0$ with $f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$.*

With the help of the quantities defined above, we can sometimes make linear changes of variables that simplify the Weierstrass equation.

Lemma 6.9. *Let K be a field of characteristic 0 or p for a prime $p \neq 2$. Let $f(X,Y,Z)$ be as in Equation* (6.3)*, and consider*

$$g(X,Y,Z) := Y^2Z - X^3 - \frac{1}{4}b_2X^2Z - \frac{1}{2}b_4XZ^2 - \frac{1}{4}b_6Z^3 \in K[X,Y,Z].$$

Then the linear change of variables $\varphi : \mathbb{P}^2(K) \to \mathbb{P}^2(K)$ given by $[a:b:c] \mapsto [a : b + \frac{a_1}{2}a + \frac{a_3}{2}c : c]$ satisfies that

$$C_f(K) = \varphi(C_g(K)).$$

Proof. Apply Lemma 5.39 to $A = \begin{pmatrix} 1 & 0 & 0 \\ \frac{a_1}{2} & 1 & \frac{a_3}{2} \\ 0 & 0 & 1 \end{pmatrix}$. □

Lemma 6.10. *Let K be a field of characteristic 0 or p for a prime $p \neq 2, 3$. Then Let $f(X, Y, Z)$ as in Equation* (6.3)*, and consider*

$$g(X, Y, Z) := Y^2Z - X^3 + 27c_4XZ^2 + 54c_6Z^3 \in K[X, Y, Z].$$

Then the linear change of variables $\varphi : \mathbb{P}^2(K) \to \mathbb{P}^2(K)$ given by $[a : b : c] \mapsto [36a+3b_2c : 216b : c]$ satisfies that

$$C_f(K) = \varphi(C_g(K)).$$

Proof. Apply Lemma 5.39 to $A = \begin{pmatrix} 36 & 0 & 3b_2 \\ 0 & 216 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. □

Lemma 6.11. *Let $f(X, Y, Z) = 0$ be a Weierstrass equation, and f_A the polynomial obtained from f by the linear change of variables given by a matrix*

$$A = \begin{pmatrix} u^2 & 0 & r \\ u^2s & u^3 & t \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(K).$$

Then $\Delta_f = u^{12}\Delta_{f_A}$ and, if $\Delta_f \neq 0$, then $j_f = j_{f_A}$.

Proof. One simply has to compute the expressions for Δ_f, Δ_{f_A}, j_f and j_{f_A} using 6.8 and check that the mentioned equalities hold. □

Proposition 6.12. *Let $f(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 \in K[X, Y, Z]$. Then the curve C_f/K is smooth if and only if the discriminant Δ_f of the corresponding Weierstrass equation is nonzero.*

Proof. Let $\overline{K}$ be an algebraic closure of K, and consider $C_f/\overline{K}$. We have to show that Δ is nonzero if and only if for all points $P \in C_f(\overline{K})$, P is not a singular point. By Lemma 6.7, $\mathcal{O}$ is never singular. So it suffices to show that Δ is nonzero if and only if for all points $P \in C_f(\overline{K}) \cap \mathbb{A}^2(K)$, P is not a singular point.

For simplicity, we will make the proof in the case that the characteristic of K is different from 2 (for a complete proof, look at Proposition 2.3.3 of the book *Elliptische Kurven in der Kryptographie* by A. Werner). Making a change of variables like in Lemma 6.9, we transform $f(X, Y, Z)$ into $f_A(X, Y, Z) = Y^2Z - X^3 - a_2'X^2Z - a_4'XZ^2 - a_6'Z^3$, and Lemma 6.11 shows that $\Delta_f = \Delta_{f_A}$. Moreover by Lemma 5.41 the curve C_f/K is smooth if and only if C_{f_A}/K is smooth. So we can assume without loss of generality that $f(X, Y, Z) = Y^2Z - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$.

Now a point P is a singular point of C_f/K if and only if it is an affine point, say $P = [a : b : 1]$, and satisfies the equations

$$\begin{cases} f(a, b) = 0 \\ \frac{\partial g}{\partial x}(a, b) = 0 \\ \frac{\partial g}{\partial y}(a, b) = 0. \end{cases}$$

where $g(x, y) = f(x, y, 1)$. The system of equations above boils down to

$$\begin{cases} b^2 = a^3 + a_2a^2 + a_4a + a_6 \\ 2b = 0 \\ 3a^3 + 2a_2a + a_4 = 0 = 0. \end{cases}$$

That is to say, $b = 0$ and a must be a double root of the polynomial $h(x) = x^3 + a_2x^2 + a_4x + a_6$. So C_f/K is smooth if and only if the polynomial $h(x)$ does not have double roots. But this condition is equivalent to the fact that the discriminant of $h(x)$ (that is, the resultant between $h(x)$ and $h'(x)$) is nonzero. Now a computation shows that the discriminant equals $16\Delta_f$, hence C_f/K is smooth if and only if $\Delta_f \neq 0$. □

Remark 6.13.
- *Let $f(X, Y, Z)$ as in Equation* (6.3)*. The curve C_f/K is an elliptic curve if and only if $\Delta_f \neq 0$.*
- *For all elliptic curves E/K, the j-invariant is defined.*
- *The j-invariant is preserved under linear changes of variables as in Lemma 6.3. That is why we call it j-*invariant*. It characterises the isomorphism class (over $\overline{K}$) of elliptic curves E/K.*

Proposition 6.14. *Let L/K be a projective line and E/K an elliptic curve. Then*

$$\sum_{P \in \mathbb{P}^2(K)} \mathrm{m}(E, L, P)$$

equals 0, 1 *or* 3.

Proof. Let $L = L(\alpha, \beta, \gamma)$ for some $\alpha, \beta, \gamma \in K$, and let $f(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$ for some $a_1, a_3, a_2, a_4, a_6 \in K$ be the polynomial defining E/K. We will do the proof in the special case when $\beta \neq 0$. For the case $\beta = 0$, see Sheet 11.

We may assume, without loss of generality, that $L = L(\alpha, 1, \gamma)$ for some $\alpha, \gamma \in K$. Moreover, the only point $P = [a : b : c]$ of $E(K)$ with $c = 0$ is $\mathcal{O} = [0 : 1 : 0]$ (see Lemma 6.6) which does not belong to $L(K)$. So we only need to compute $\mathrm{m}(E, L, P)$ for points of the form $P = [a : b : 1]$.

A point $P = [a : b : 1]$ lies in $L(K) \cap E(K)$ if and only if

$$\begin{cases} \alpha a + b + \gamma = 0 \\ f(a, b, 1) = 0 \end{cases}$$

Assume P satisfies these equations. Substituting $b = -\alpha a - \gamma$ in the second equation gives that $f(a, -\alpha a - \gamma, 1) = 0$.

Consider the polynomial $g(x) = f(x, -\alpha x - \gamma, 1)$. $g(x)$ is a polynomial of degree 3 in $K[x]$ with leading coefficient -1, such that a point $P \in \mathbb{P}^2(K)$ belongs to $E(K) \cap L(K)$ if and only if $P = [a : -\alpha a - \gamma : 1]$ with $g(a) = 0$.

Now we compute $\mathrm{m}(E, L, P)$ for $P = [a : -\alpha a - \gamma : 1]$. Note that the point $P' = [1 : -\alpha : 0]$ lies in $L(K)$ but not in $E(K)$, so it is different from P and we can use it as auxiliary point. Let $\psi(t) = f(a+t, (-\alpha a-\gamma)-\alpha t, 1)$. Note that $\psi(t) = g(a+t)$. Therefore $\mathrm{ord}_{t=0}\,\psi(t) = \mathrm{ord}_{x=a}\,g(x)$.

Note that the polynomial $g(x)$ does not depend on the choice of the point $P = [a : -\alpha a - \gamma : 1]$, so the formula

$$\mathrm{m}(E, L, [a : -\alpha a - \gamma : 1]) = \mathrm{ord}_{x=a}\, g(x)$$

is valid for all $P \in E(K) \cap L(K)$.

If $L(K) \cap E(K) = \emptyset$, then $\sum_{P \in \mathbb{P}^2(K)} m(E, L, P) = 0$, and we are done. So we may assume that $L(K) \cap E(K)$ has at least one point. Fix one such point $P = [a_0 : b_0 : 1] \in L(K) \cap E(K)$. We distinguish several cases:

- $\mathrm{ord}_{x=a_0} g(x) = 3$. In this case $g(x) = -(x - a_0)^3$ has a unique zero $x = a_0$ of multiplicity three, and
$$\sum_{P \in \mathbb{P}^2(K)} \mathrm{m}(E, L, P) = \mathrm{m}(E, L, [a_0 : -\alpha a_0 - \gamma : 1]) = 3.$$
- $\mathrm{ord}_{x=a_0} g(x) = 2$. In this case $g(x) = (x - a_0)^2 \tilde{g}(x)$, and $\tilde{g}(x)$ has degree 1, hence one root $\tilde{a}_0 \in K$ of multiplicity one. Therefore
$$\sum_{P \in \mathbb{P}^2(K)} \mathrm{m}(E, L, P) = \mathrm{m}(E, L, [a_0 : -\alpha a_0 - \gamma : 1]) + \mathrm{m}(E, L, [\tilde{a}_0 : -\alpha \tilde{a}_0 - \gamma : 1]) = 2 + 1 = 3.$$
- $\mathrm{ord}_{x=a_0} g(x) = 1$. In this case $g(x) = (x - a_0)^2 \tilde{g}(x)$, and $\tilde{g}(x)$ has degree 2, hence it has either two roots $\tilde{a}_1, \tilde{a}_2 \in K$ of multiplicity one, one root $\tilde{a}_0 \in K$ of multiplicity two, or no roots in K. In the first case
$$\sum_{P \in \mathbb{P}^2(K)} \mathrm{m}(E, L, P) = \mathrm{m}(E, L, [a_0 : -\alpha a_0 - \gamma : 1]) + \mathrm{m}(E, L, [\tilde{a}_1 : -\alpha \tilde{a}_1 - \gamma : 1]) + \mathrm{m}(E, L, [\tilde{a}_2 : -\alpha \tilde{a}_2 - \gamma : 1]) = 1 + 1 + 1 = 3,$$
in the second case
$$\sum_{P \in \mathbb{P}^2(K)} \mathrm{m}(E, L, P) = \mathrm{m}(E, L, [a_0 : -\alpha a_0 - \gamma : 1]) + \mathrm{m}(E, L, [\tilde{a}_0 : -\alpha \tilde{a}_0 - \gamma : 1]) = 1 + 2 = 3,$$
and in the third case
$$\sum_{P \in \mathbb{P}^2(K)} \mathrm{m}(E, L, P) = \mathrm{m}(E, L, [a_0 : -\alpha a_0 - \gamma : 1]) = 1.$$

In all cases our claim holds. □

Remark 6.15. *Let E/K be an elliptic curve and L/K a projective line.*

- *If there are two different points $P_1, P_2 \in E(K) \cap L(K)$, then either there exists a (unique) point $P_3 \in E(K) \cap L(K)$ different from P_1 and P_2 and the multiplicity of intersection of E and L at P_1, P_2 and P_3 is 1, or there is no other point in $E(K) \cap L(K)$ and one of the points P_1 or P_2 has multiplicity 2 and the other has multiplicity 1.*

- *If there is a point $P \in E(K) \cap L(K)$ with $\mathrm{m}(E, C, P) \geq 2$, then either there exists a (unique) point $Q \in E(K) \cap L(K)$ and $\mathrm{m}(E, L, P) = 2$, $\mathrm{m}(E, L, Q) = 1$, or $E(K) \cap L(K) = \{P\}$ and $\mathrm{m}(E, L, P) = 3$.*

We can sumarize all these cases by saying that, if L and E intersect at two points of $\mathbb{P}^2(K)$ (counting multiplicities), then they intersect at another point (counting multiplicities).

In other words, given E/K, L/K and two points (counting multiplicities) in $E(K) \cap L(K)$, they determine a third point (counting multiplicities) in $E(K) \cap L(K)$.

Now we have all the tools we need to define a group law on $E(K)$.

Definition 6.16. *Let E/K be an elliptic curve. We define a map*

$$\begin{aligned} \oplus : E(K) \times E(K) &\to E(K) \\ (P, Q) &\mapsto P \oplus Q \end{aligned}$$

with the following two steps recipe:

- ***Step 1:** If $P \neq Q$, consider the unique projective line L_1/K passing through P and Q. If $P = Q$, set L_1/K to be the tangent line to E at P. L_1/K has a third point of intersection with E (counting multiplicities); call it $P * Q$.*
- ***Step 2:** If $P * Q \neq \mathcal{O}$, consider the unique projective line L_2/K passing through $P * Q$ and $\mathcal{O}$. If $P * Q = \mathcal{O}$, set L_2/K to be the tangent line to E at $\mathcal{O}$. L_2/K has a third point of intersection with E (counting multiplicites). We define $P \oplus Q$ to be this point.*

Example 6.17. *Let E/K be the elliptic curve defined by the polynomial $f(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$.*

Recall that

$$\begin{cases} \frac{\partial f}{\partial X} = a_1YZ - 3X^2 - 2a_2XZ - a_4Z^2 \\ \frac{\partial f}{\partial Y} = 2YZ + a_1XZ + a_3Z^2 \\ \frac{\partial f}{\partial Z} = Y^2 + a_1XY + 2a_3Z - a_2X^2 - 2a_4XZ - 3a_6Z^2 \end{cases}$$

- *Let $P \neq \mathcal{O}$. What is $P \oplus \mathcal{O}$?*
  - ***Step 1:** Since the point P lies in the affine part of E/K, we can write it as $P = [a : b : 1]$. The line L_1 passing through P and $\mathcal{O}$ is $L(1, 0, -a)$. One can easily check that the line L_1 intersects the affine part of $E(K)$ into two points (counting multiplicities); in other words, if we call $P * \mathcal{O}$ the third point of intersection of L_1 and E, then $P * \mathcal{O} \neq \mathcal{O}$.*
  - ***Step 2:** The line L_2 is the unique projective line passing through $P * \mathcal{O}$ and $\mathcal{O}$. But L_1/K is a projective line passing through these two points: hence $L_2 = L_1$. The third point of intersection of L_2 and E is thus P. Therefore $P \oplus \mathcal{O} = P$.*
- *What is $\mathcal{O} \oplus \mathcal{O}$?*
  - ***Step 1:** Take $P = Q = \mathcal{O}$. The line L_1/K is the tangent line to E/K at $\mathcal{O}$, that is to say, $L(0, 0, 1)$. Now $E(K) \cap L(K) = \{\mathcal{O}\}$, so $P * Q = \mathcal{O}$.*

– ***Step 2:*** *The line L_2/K is again the tangent line to E/K at $\mathcal{O}$, that is, $L(0,0,1)$, so that again the third point of intersection is $\mathcal{O}$. Therefore $\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$.*

Proposition 6.18. *The set $E(K)$ is a commutative group with the operation $\oplus$ and neutral element $\mathcal{O}$.*

Proof. Observe first that the operation $\oplus$ is commutative, since the line L_1 does not depend on the order in which we give the points P and Q defining it. Example 6.17 shows that there is a neutral element for $(E(K), \oplus)$, namely $\mathcal{O} \in E(K)$. We need to show the existence of inverse elements and the associativity of the operation.

- Inverse element: We need to show that, for all $P \in E(K)$, there exists a unique $Q \in E(K)$ with $P \oplus Q = \mathcal{O}$. Let us see first the existence (the uniqueness follows then in a standard way as soon as we prove associativity). If $P = \mathcal{O}$, then in Example 6.17 we saw that $Q = \mathcal{O}$ satisfies our condition. So we may assume that $P \neq \mathcal{O}$. Consider the unique projective line L/K passing through P and $\mathcal{O}$, and let Q be the third point of intersection of $E(K)$ with $L(K)$. Now we compute $P \oplus Q$. First, the line L_1 coincides with L, so $P * Q = \mathcal{O}$. Therefore the line L_2/K is the tangent line to E through $\mathcal{O}$, that is to say, $L(0,0,1)$. But then $L_2(K) \cap E(K) = \{\mathcal{O}\}$, hence $P \oplus Q = \mathcal{O}$.

- Associativity: We need to show that, for all $P_1, P_2, P_3 \in E(K)$, $(P_1 \oplus P_2) \oplus P_3 = P_1 \oplus (P_2 \oplus P_3)$. One can give a geometric (although very long and tedious) proof of this fact, by computing both sides of the equation for arbitrary $P_1, P_2, P_3 \in E(K)$. At all steps of the proof, when constructing the lines L_1 and L_2, one must distinguish whether the two points determining it are equal or different, yielding a long list of cases. We will not do this here. Nevertheless, we want to point out that there is a less tedious but more conceptual proof of this fact, if one relates $\oplus$ to the group structure of the Picard group of E. This proof goes beyond the scope of these notes, but the interested reader can look it up in Chapter III of the book *The arithmetic of elliptic curves* by J. H. Silverman. Yet another proof can be done using explicit formulas for the addition of points: see Proposition 6.20.

□

Remark 6.19. *Given an elliptic curve E/K and points $P, P_1, P_2 \in E(K)$, we will denote $P_1 \oplus P_2$ by $P_1 + P_2$, the inverse of P by $-P$, and the sum $P \oplus \cdots \oplus P$ of P with itself k times by $[k]P$.*

Assume we have $P_1 = [x_1 : y_1 : 1]$ and $P_2 = [x_2 : y_2 : 1] \in E(K)$. If $P_3 = [x_3 : y_3 : 1]$ satisfies that $P_1 + P_2 = P_3$, can we express x_3 and y_3 in terms of x_1, x_2, y_1, y_2?

Proposition 6.20. *Let E/K be an elliptic curve defined by $f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$. Then the following hold:*

- *Let $P = [x_1 : y_1 : 1] \in E(K)$. Then $-P = [x_1, -y_1 - a_1x_1 - a_3 : 1]$.*

- *Let $P_1 = [x_1 : y_1 : 1]$ and $P_2 = [x_2 : y_2 : 1]$. Then*

  – *If $x_1 = x_2$ and $y_1 = -y_2 - a_1x_2 - a_3$, then $P_1 + P_2 = \mathcal{O}$.*

– *Otherwise, let $P_3 = P_1 + P_2$, say $P_3 = [x_3 : y_3 : 1]$. Then*

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = -(\lambda_1 + a_1)x_3 - \nu - a_3, \end{cases}$$

where $\lambda, \nu \in K$ are defined as follows:

* *If $x_1 \neq x_2$,*

$$\begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1} \\ \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1} \end{cases}$$

* *If $x_1 = x_2$,*

$$\begin{cases} \lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \\ \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \end{cases}$$

Proof. The reader can find a proof of this proposition in Chapter 2, section 3 the book *Elliptische Kurven in der Kryptographie* by Annette Werner, or in Chapter III of the book *Arithmetic of Elliptic Curves* by J. H. Silverman. □

Remark 6.21. *In particular, the previous proposition proves that x_3 and y_3 can be obtained as a quotient of two polynomials in $K[x_1, x_2, y_1, y_2, a_1, a_2, a_3, a_4, a_6]$.*

7 Elliptic Curves over finite fields

Let p be a prime number, q a power of p and $\mathbb{F}_q$ the finite field with q elements. In this section we will consider elliptic curves E defined over $\mathbb{F}_q$. We are interested in the group $(E(\mathbb{F}_q), +)$. One first remark is that, since $E(\mathbb{F}_q) \subset \mathbb{P}^2(\mathbb{F}_q)$ and this set is finite, the group $(E(\mathbb{F}_q), +)$ is a finite group. One interesting question is to determine its order. The inclusion $E(\mathbb{F}_q) \subset \mathbb{P}^2(\mathbb{F}_q)$ already gives us that $|E(\mathbb{F}_q)| \leq |\mathbb{P}^2(\mathbb{F}_q)| = (q^3 - 1)/(q - 1) = q^2 + q + 1$. But one can do better than this.

Proposition 7.1. *Let $E/\mathbb{F}_q$ be an elliptic curve. Then $|E(\mathbb{F}_q)| \leq 2q + 1$.*

Proof. Let $f(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$ be the polynomial defining E. We know that

$$E(K) = (E(K) \cap \mathbb{A}^2(K)) \cup \{\mathcal{O}\},$$

that is to say, the only point at infinity is $\mathcal{O} \in E(\mathbb{F}_q)$. Therefore it suffices to see that the set of solutions $(x, y) \in \mathbb{A}^2(\mathbb{F}_q)$ of the equation $y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ has cardinality smaller than or equal to $2q$. Now for each $x_0 \in \mathbb{F}_q$, there exist at most two roots of the polynomial $y^2 + (a_1x_0 + a_3)y - x_0^3 - a_2x_0^2 - a_4x_0 - a_6$ in $\mathbb{F}_q$. Therefore the number of solutions of the equation above is smaller than or equal to $2q$. □

Let $E/\mathbb{F}_q$ be an elliptic curve, and fix $x_0 \in \mathbb{F}_q$. Then we have three possibilities: either the polynomial $g(y) = y^2 + (a_1x_0 + a_3)y - x_0^3 - a_2x_0^2 - a_4x_0 - a_6 \in \mathbb{F}_q[y]$ has two roots in $\mathbb{F}_q$, or it has one root, or it has none, depending on whether the discriminant of $g(y)$ is a square, is zero, or is not a

square. If we choose an element randomly in $\mathbb{F}_q$, then we will get a square with the same probability as a nonsquare. This argument suggests that, more or less, one half of the values of x_0 will give two solutions of $g(y) = 0$ and half of the values of x_0 will give none. Therefore the number of points of $E(\mathbb{F}_q) \cap \mathbb{A}^2(K)$ should be close to q. Actually one can prove the following.

Proposition 7.2 (Hasse)**.** *Let $E/\mathbb{F}_q$ be an elliptic curve. Then*

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

Proof. The proof of this fact goes beyond the scope of these notes. The reader can consult it in Chapter V of the book *The arithmetic of elliptic curves* by J. H. Silverman. □

Let $E/\mathbb{F}_q$ be an elliptic curve, and consider the finite commutative group $(E(\mathbb{F}_q), +)$. Let $P \in E(\mathbb{F}_q)$ be a point. Let $\langle P \rangle \subset E(\mathbb{F}_q)$ be the subgroup generated by P, that is to say,

$$\langle P \rangle = \{[k]P : k \in \mathbb{Z}\}.$$

Note that $\langle P \rangle$ is a cyclic group of order equal to the order of P in $E(\mathbb{F}_q)$, that is, $\min\{k \in \mathbb{N} : [k]P = \mathcal{O}\}$.

We can apply the cryptographic algorithms from Section 4 (that is to say, Diffie-Helman key exchange and El Gamal encryption) replacing the multiplicative group of a finite field by the group $\langle P \rangle$. But not all elliptic curves $E/\mathbb{F}_q$ and not all points $P \in E(\mathbb{F}_q)$ will give us secure algorithms. For this method to work in practice, we need that the corresponding *discrete logarithm problem* is hard to solve:

> **Discrete logarithm problem for elliptic curves:** Given $E/\mathbb{F}_q$ an elliptic curve, $P \in E(\mathbb{F}_q)$ and $Q \in \langle P \rangle$, compute $k \in \mathbb{Z}$ so that $[k]P = Q$.

Remark 7.3.

- *Of course, one first requirement is that $n = \langle P \rangle$ is big, so that in practice we cannot just compute all $[k]P$ for $k \in \{0, \ldots, n\}$. But this is not the only aspect one has to be careful about. There are families of elliptic curves (for example,* supersingular elliptic curves, *which are those that satisfy $|E(\mathbb{F}_q)| = q + 1$), for which the discrete logarithm problem can be solved in a reasonable amount of time. The interested reader can consult Chapter 4 of the book* Elliptische Kurven in der Kryptographie *by Annette Werner, or Chapter 5 of* Elliptic curves, number theory and cryptography *by L. Washington.*

- *The main advantage of replacing the multiplicative group of a finite field $(\mathbb{F}_{\ell^s})^\times$ by a cyclic subgroup $\langle P \rangle \subset E(\mathbb{F}_q)$ is that one can obtain the "same level of security" using keys that are much smaller. In this way the data to be transmitted or stored will have smaller size.*

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 1

21/02/2012

One of you will present one of the two exercises in the lecture on 28/02/2012.

1. (a) Compute $d := \gcd(282, 228)$ using Euclid's algorithm. From the computation, find $a, b \in \mathbb{Z}$ such that $d = 282 \cdot a + 228 \cdot b$.

   (b) Let $n = 282$ and let $e = 91$. Find $s \in \mathbb{N}$ such that $1 \leq s \leq 282$ and $es \equiv 1 \mod (n)$.

2. Let $p_1, p_2, \ldots, p_r$ be distinct prime numbers and put $n = p_1 \cdot p_2 \cdots p_r$. Let $m \equiv 1 \bmod (\varphi(n))$, where $\varphi(n)$ is Euler's totient function, that is, the number of units of the ring $\mathbb{Z}/(n)$.

   Prove that for any $x \in \mathbb{Z}/(n)$ one has: $x^m = x$ (equality in $\mathbb{Z}/(n)$).

If you want to read more on elementary number theory, the RSA algorithm and other topics, and want to play with them on a computer, we recommend:

> William Stein: Elementary Number Theory: Primes, Congruences, and Secrets, Springer-Verlag.
>
> Free online version: `http://modular.math.washington.edu/ent/ent.pdf`

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 2

28/02/2012

1. Finish Sheet 1.
2. In this exercise you see how to transform a sentence (for simplicity, just consisting of capital letters and some punctuation marks) into an integer. For this we use the following table:

Letter	0	1	…	9	A	B	…	Z	.	,	:	;	!	?	Space
Integer	0	1	…	9	10	11	…	35	36	37	38	39	40	41	42

   The sentence 'YOU ARE.' is turned into a number as follows:
   Y=34, O=24, U=30, Space=42, A=10, R=27, E=14, .=36

$$34 + 24 \cdot 43 + 30 \cdot 43^2 + 42 \cdot 43^3 + 10 \cdot 43^4 + 27 \cdot 43^5 + 14 \cdot 43^6 + 36 \cdot 43^7 = 9877975894339.$$

   (a) Describe a procedure how to turn a positive integer back into a sentence.
   Hint: Use division with remainder.

   (b) Which sentence is represented by the number 1769468?
   Hint: This can be done on a pocket calculator. Of course, it is easier on a computer.

3. In this exercise you see how 'fast exponentiation' works.

   Let the natural number n be given in binary notation $n = (a_r, a_{r-1}, \ldots, a_1, a_0)_2$ with digits $a_i \in \{0, 1\}$ for $i = 0, \ldots, r$. That means:

$$n = \sum_{i=0}^{r} a_i 2^i.$$

   Examples: $3 = (1, 1)_2 = 1 \cdot 2^1 + 1 \cdot 2^0$, $10 = (1, 0, 1, 0)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$.

   Let $x \in \mathbb{Z}$ (or in any other ring). We want to compute x^n by performing as few multiplications as possible. Note:

$$x^n = x^{(\sum_{i=0}^{r} a_i 2^i)} = (x^{(2^0)})^{a_0} \cdot (x^{(2^1)})^{a_1} \cdot (x^{(2^2)})^{a_2} \cdot \ldots \cdot (x^{(2^r)})^{a_r}.$$

   Let us compute x^{10}: In the standard way: $x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x$ one makes 9 multiplications. We can do with fewer, namely 4:

$$e_1 := x \cdot x = x^2, \;\; e_2 := e_1 \cdot e_1 = x^4, \;\; e_3 := e_2 \cdot e_2 = x^8, \;\; e_1 \cdot e_3 = x^{10}$$

   (a) Imitate the computation of x^{10} in order to compute x^{20}. How many multiplications do you need?

   (b) Let $n = (a_r, a_{r-1}, \ldots, a_1, a_0)_2$. Show that one never needs more than $2r$ multiplications.

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 3

06/03/2012

1. In this exercise, you construct explicitly a field with 9 elements.

   (a) Find $a, b \in \mathbb{F}_3$ such that $X^2 + aX + b$ is an irreducible polynomial in $\mathbb{F}_3[X]$.

   (b) With the values of a, b from (a), let $K := \mathbb{F}_3[X]/(X^2 + aX + b)$. List the elements of K.

   (c) Compute an inverse for each nonzero element of K.
   (This shows that K is a field, since we know that K is a ring.)

2. Let K be a field. In this exercise, you prove an analogue of Gauß' fundamental theorem of elementary number theory for $K[X]$. You should deduce it from the extended Euclid's algorithm (Bézout's theorem) and you can follow the proof of Gauß' theorem presented in the lecture.

   (a) Let $f \in K[X]$ be a polynomial of degree $n := \deg(f) > 0$. Show that there are finitely many irreducible polynomials $p_1(X), \ldots, p_r(X) \in K[X]$ such that

   $$f(X) = p_1(X) \cdot p_2(X) \cdot \ldots \cdot p_r(X).$$

   (b) Let $p(X) \in K[X]$ be a polynomial of degree $n := \deg(f) > 0$. Show that the following statements are equivalent:

      (i) $p(X)$ is an irreducible polynomial.

      (ii) $p(X)$ is a prime element in the ring $K[X]$.
      (Recall that, by definition, $p(X)$ is a prime element in $K[X]$ if and only if, whenever $p(X)$ divides a product $g(X)h(X)$ with $g(X), h(X) \in K[X]$, then $p(X)$ divides $g(X)$ or $p(X)$ divides $h(X)$.)

   (c) Let $f(X) \in K[X]$ be a monic polynomial of degree $n := \deg(f) > 0$. Show that $f(X)$ can be written as a finite product of monic irreducible polynomials: There is $r \in \mathbb{N}$ and there are irreducible monic polynomials $p_1(X), \ldots, p_r(X)$ such that

   $$f(X) = p_1(X) \cdot p_2(X) \cdot \ldots \cdot p_r(X).$$

   Up to renumbering, the irreducible monic polynomials occuring in the product are unique, that is: if $f(X) = q_1(X) \cdot q_2(X) \cdot \ldots \cdot q_s(X)$ is another such product, then $r = s$ and there is σ in the symmetric group on the letters $\{1, \ldots, r\}$ such that $q_i(X) = p_{\sigma(i)}(X)$ for all $i \in \{1, \ldots, r\}$.

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 4

13/03/2012

1. This exercise checks the Leibniz rule for the formal derivative of a polynomial. Let K be a field. The formal derivative of $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ is defined as $f'(X) = \sum_{i=1}^{n} a_i i X^{i-1}$.

   Let now $f(X), g(X) \in K[X]$ and set $h(X) = f(X)g(X)$. Show:

   $$h'(X) = f'(X)g(X) + f(X)g'(X).$$

2. Let K be a finite field with p^n elements.

   (a) Prove $(\alpha + \beta)^p = \alpha^p + \beta^p$ for all $\alpha, \beta \in K$.

   (b) Conclude from (a): $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$ for all $d \in \mathbb{N}$.

   (c) Prove that the map

   $$F : K \to K, \quad x \mapsto x^p$$

   defines a field isomorphism, the so-called *Frobenius isomorphism*.

   (d) Compute the order of F.

   (e) Let $1 \leq d \leq n$ and let $F^d = \underbrace{F \circ F \circ \cdots \circ F}_{d \text{ times}}$. Show that the set $K^{\langle F^d \rangle} := \{x \in K \mid F^d(x) = x\}$ is a subfield of K and compute the number of elements of $K^{\langle F^d \rangle}$.

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 5

20/03/2012

1. (a) Show that the polynomial $f(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$ is irreducible.

   (b) Consider $K = \mathbb{F}_2[X]/(f(X))$. We know that this is a field with 16 elements, hence, $K^\times$ is a cyclic group of order 15.

   Find a generator of $K^\times$.

2. *Shamir's no key protocol.* Shamir found a clever method how Alice can send a message to Bob, which cannot be read by anyone but Bob. The method has the special feature that Alice and Bob do not need any common key (neither known beforehand nor agreed via the Diffie-Hellman key exchange or anything similar).

   In terms of everyday things, the method works like this. Alice puts her message into a box and locks the box with a lock of hers (only she has the key and she does not give the key to anyone else). No one but Alice can open the box. She sends the locked box to Bob. Bob locks the box once more with a lock of his own (only he has the key and he does not give the key to anyone else). He sends the doubly locked box back to Alice. She removes her lock and sends the box, which is now only locked by Bob, back to Bob, who opens it with his own key and gets the message.

   Let p be a big prime number and let the message be $1 \leq m \leq p-1$ (one should also assume $m \in \mathbb{F}_p^\times$ has order $p-1$ for security reasons, but, for this exercise this can be neglected). Alice wants to send m to Bob.

   (a) Describe a version of Shamir's no key protocol in $\mathbb{F}_p^\times$.

   (b) Assume Eve can solve discrete logarithm problems in $\mathbb{F}_p$ (for any basis) and that Eve knows all the conversation between Alice and Bob. Show that Eve can then compute m.

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 6

27/03/2012

1. First exercise. In this exercise you will see that different polynomials can have the same set of zeroes in $\mathbb{A}^2(K)$.

   (a) Let $K = \mathbb{R}$, and consider the polynomials $f, g \in K[x, y]$ defined as $f(x, y) = x^2 + 4$, $g(x, y) = (x + y)^2 + 1$. Show that $C_f(K) = C_g(K)$.

   (b) Let K be a field, and $f, g \in K[x, y]$ nonzero polynomials. Show that $C_{f^2g}(K) = C_{fg}(K)$.

   (c) Let p be a prime number, $q = p^f$ and consider $K = \mathbb{F}_q$. Show that the polynomials $f, g \in K[x, y]$ defined as $f(x, y) = x - y$, $g(x, y) = x^q - y$ satisfy $C_f(K) = C_g(K)$.

   (d) Let $K = \mathbb{F}_4$. Find polynomials $f, g \in K[x, y]$, of degree less than 4, such that $C_f(K) = C_g(K)$.

   If K is algebraically closed and $f \in K[x, y]$ is a nonzero irreducible polynomial, then f is uniquely determined (up to a scalar) by $C_f(K)$. You can check that these conditions were not satisfied in the previous examples. In our lecture we will be concerned with elliptic curves over finite fields, so we have to be careful!

2. Second exercise. Let K be a field. Recall that we have written $\mathbb{P}^2(K)$ as a disjoint union

$$\mathbb{P}^2(K) = i(\mathbb{A}^2(K)) \cup H \cup \{O\}.$$

   Prove that for all $P \in H \cup \{O\}$ (i.e., the "extra" points that we added at infinity) there exist two affine lines whose projectivisations meet in P. This shows that there is no proper subspace of $\mathbb{P}^2(K)$ containing $\mathbb{A}^2(K)$ where all affine lines have a point of intersection.

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 7

10/04/2012

1. First exercise. Let L_1/K, L_2/K be two different projective lines in $\mathbb{P}^2(K)$. Prove that they meet at exactly one point (that is to say, $L_1(K) \cap L_2(K) = \{P\}$ for some point $P \in \mathbb{P}^2(K)$).
2. Second exercise. Let $K \subset E$ be an extension of fields.
   (a) Prove that the map
   $$\begin{aligned} j : \mathbb{P}^2(K) &\to \mathbb{P}^2(E) \\ [a : b : c] &\mapsto [a : b : c] \end{aligned}$$
   is well-defined and injective.
   (b) Let $f \in K[X, Y, Z]$ be a homogeneous polynomial of degree d for some positive integer d. Consider the curves C_f/K and C_f/E. Prove that
   $$C_f(K) = \mathbb{P}^2(K) \cap C_f(E).$$

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 8

17/04/2012

1. Let $f(x,y) = x^3 + yx^2 - y$, and let $f^*(X,Y,Z) = X^3 + YX^2 - YZ^2$ be its homogenisation. Show that the affine curve $C_f/\mathbb{C}$ is smooth while the projective curve $C_{f^*}/\mathbb{C}$ is not smooth.
2. Let K be a field. In this exercise we prove the chain rule for formal derivatives in $K(X)$.
   (a) Show that the definition of the formal derivative of an element $\varphi(X) \in K(X)$ does not depend on the representation of $\varphi(X) = f(X)/g(X)$ as a quotient of elements of $K[X]$.
   (b) Let $g(X) \in K[X]$. Prove that $(g^n)'(X) = ng^{n-1}(X)g'(X)$ for all $n \geq 1$. (Hint: Use induction and the Leibnitz rule from Sheet 4).
   (c) Let $f(X), g(X) \in K[X]$. Show that $(f \circ g)'(X) = f'(g(X))g'(X)$.
   (d) Let $\varphi(X), \psi(X) \in K(X)$. Show that $(\varphi(X) \cdot \psi(X))' = \varphi'(X)\psi(X) + \varphi(X)\psi'(X)$ (Hint: Apply the Leibnitz rule in $K[X]$).
   (e) Let $\varphi(X) = (f(X)/g(X))^n$. Show that $\varphi'(X) = n(f(X)/g(X))^{n-1} \cdot (f(X)/g(X))'$ (Hint: Analogous to (2b)).
   (f) Let $f(X) \in K[X]$, $\varphi(X) \in K(X)$. Show that $(f \circ \varphi)'(X) = f'(\varphi(X))\varphi'(X)$ (Hint: Analogous to (2c)).
   (g) Let $\varphi(X), \psi(X) \in K(X)$. Show that $(\psi \circ \varphi)'(X) = \psi'(\varphi(X))\varphi'(X)$.

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 9

24/04/2012

1. Let K be a field. In this exercise we collect some facts we used in the Lecture about the order of an element of $K(X)$ at $X = 0$.

   (a) Let $f(X), g(X) \in K[X]$. Show that $\mathrm{ord}_{X=0}(f(X)g(X)) = \mathrm{ord}_{X=0} f(X) + \mathrm{ord}_{X=0} g(X)$.

   (b) The definition of the order at $X = 0$ of an element $\varphi(X) \in K(X)$ (Definition 5.33) does not depend on the representation $\varphi(X) = f(X)/g(X)$ as quotient of elements of $K[X]$.

   (c) Let $\varphi(X), \psi(X) \in K[X]$ such that $\mathrm{ord}_{X=0}(\psi(X)) = 1$. Show that

   $$\mathrm{ord}_{X=0} \varphi(X) = \mathrm{ord}_{X=0} \varphi \circ \psi(X).$$

   (Hint: First show by induction on m that for all $m \geq 0$ we have the equality $(\varphi \circ \psi)^{(m)}(X) = \varphi^{(m)}(\psi(X)) \cdot (\psi'(X))^m$. Conclude that $\varphi^{(m)}(0) = 0$ if and only if $(\varphi \circ \psi)^{(m)}(0) = 0$).

2. Let K be a field. In this exercise we prove the chain rule for formal derivatives in three variables.

   (a) Let $\nu_1, \nu_2, \nu_3 \geq 1$ integers, $g_1(T), g_2(T), g_3(T) \in K(T)$ and $h(T) = g_1(T)^{\nu_1} g_2(T)^{\nu_2} g_3(T)^{\nu_3}$. Prove that

   $$\begin{aligned} h'(T) = {} & \nu_1 g_1(T)^{\nu_1 - 1} g_1'(T) g_2(T)^{\nu_2} g_3(T)^{\nu_3} \\ & + \nu_2 g_1(T)^{\nu_1} g_2(T)^{\nu_2 - 1} g_2'(T) g_3(T)^{\nu_3} + \nu_3 g_1(T)^{\nu_1} g_2(T)^{\nu_2} g_3(T)^{\nu_3 - 1} g_3'(T) \end{aligned}$$

   (b) Let $f \in K[X, Y, Z]$ and $g_1(T), g_2(T), g_3(T) \in K(T)$, $h(T) = f(g_1(T), g_2(T), g_3(T))$. Then

   $$\begin{aligned} h'(T) = {} & \frac{\partial f}{\partial X}(g_1(T), g_2(T), g_3(T)) g_1'(T) \\ & + \frac{\partial f}{\partial Y}(g_1(T), g_2(T), g_3(T)) g_2'(T) + \frac{\partial f}{\partial Z}(g_1(T), g_2(T), g_3(T)) g_3'(T). \end{aligned}$$

3. Let K be a field, $f \in K[x, y]$ a nonzero polynomial, $f^*(X, Y, Z) \in K[X, Y, Z]$ its homogenisation. Let $(a, b) \in \mathbb{A}^2(K)$. Prove that (a, b) is a singular point of the affine curve C_f/K if and only if the point $i(a, b) = [a : b : 1] \in \mathbb{P}^2(K)$ is a singular point of the projective curve C_{f^*}/K.

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 10

08/05/2012

1. Let K be a field. For each matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in \mathrm{GL}_3(K),$$

prove that the map

$$\begin{aligned} \varphi_A : \mathbb{P}^2(K) &\to \mathbb{P}^2(K) \\ [a:b:c] &\mapsto [a_{11}a + a_{12}b + a_{13}c : a_{21}a + a_{22}b + a_{23}c : a_{31}a + a_{32}b + a_{33}c] \end{aligned}$$

is well defined and bijective.

Let $f(X,Y,Z) \in K[X,Y,Z]$ be a homogeneous polynomial and set

$$f_A(X,Y,Z) := f(a_{11}X + a_{12}Y + a_{13}Z, a_{21}X + a_{22}Y + a_{23}Z, a_{31}X + a_{32}Y + a_{33}Z)$$

Prove that

$$C_f(K) = \varphi_A(C_{f_A}(K)).$$

2. Let K be a field, $f(X,Y,Z) \in K[X,Y,Z]$ a homogeneous polynomial of degree 3 of the form

$$f(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

for some $a_1, a_2, a_3, a_4, a_6 \in K$.

Let $A \in \mathrm{GL}_3(K)$ be of the following shape

$$A = \begin{pmatrix} u^2 & 0 & r \\ u^2s & u^3 & t \\ 0 & 0 & 1 \end{pmatrix}.$$

Prove that the polynomial f_A obtained from f by the linear change of variables given by A (as above) has the shape

$$f_A(X,Y,Z) = u^6(Y^2Z + a_1'XYZ + a_3'YZ^2 - X^3 - a_2'X^2Z - a_4'XZ^2 - a_6'Z^3)$$

for some $a_1', a_2', a_3', a_4', a_6' \in K$.

Exercises in Algebraic Curves and Cryptography

Summer Term 2012

Université du Luxembourg
Prof. Dr. Gabor Wiese
Dr. Sara Arias-de-Reyna

Sheet 11

15/05/2012

1. Let $L/K = L(\alpha, 0, \gamma)/K$ be a projective line and E/K an elliptic curve. Then

$$\sum_{P \in \mathbb{P}^2(K)} \mathrm{m}(E, L, P)$$

equals 0, 1 or 3.

Hints:

- Consider first the case $\alpha = 0$, that is to say, the line $L(0, 0, 1)$, compute $L(K) \cap E(K)$ and, for each $P \in L(K) \cap E(K)$, compute $\mathrm{m}(E, L, P)$.
- Next consider the case $\alpha \neq 0$. You can write L/K as $L(1, 0, \gamma)/K$ for some $\gamma \in K$. Note that $\mathcal{O} = [0 : 1 : 0] \in L(K) \cap E(K)$, and compute $\mathrm{m}(E, L, \mathcal{O})$ directly. Any other point $P \in L(K) \cap E(K)$ can be written as $P = [-\gamma : b : 1]$ for some $b \in K$, and you can use the point $\mathcal{O}$ as auxiliary point to express $\mathrm{m}(E, L, P)$ as the order at $t = 0$ of a polynomial $\psi(t)$. Now consider $g(y) = f(-\gamma, y, 1) \in K[y]$ and relate $g(b + t)$ to $\psi(t)$.

2. Let $E/\mathbb{F}_2$ be the elliptic curve defined by the polynomial $f(X, Y, Z) = Y^2Z + YZ^2 + X^3 + XZ^2$. In Example 5.19 we computed that

$$E(\mathbb{F}_2) \cap \mathbb{A}^2(\mathbb{F}_2) = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}.$$

- Write all the points of $E(\mathbb{F}_2)$. Hint: Use Lemma 6.5.
- Compute the summation table of $(E(\mathbb{F}_2), +)$. (That is to say, for all $P, Q \in E(\mathbb{F}_2)$, compute $P + Q$. Recall that since the sum is commutative, it suffices to compute 15 sums).

  Hint: A group with 5 elements is always a cyclic group, and each element which is not the neutral element is a generator. Pick one generator P and compute $P + P$, $P + P + P$, $P + P + P + P$. All other sums can be easily written down (without any need of further computations).