Number Theory for Cryptography

DTU SP[2]

University of Luxembourg

Gabor Wiese
gabor.wiese@uni.lu

In these lectures (8 hours taught in November 2020), we mention some topics from (algebraic) number theory as well as some related concepts from (algebraic) geometry that can be useful in cryptography. We cannot go deeply into any of the topics and most results will be presented without any proofs.

One of the things that one encounters are 'ideal lattices'. In the examples I saw, this was nothing but (an ideal in) an order in a number field, which is one of the concepts that we present here in its mathematical context (i.e. embedded in a conceptual setting). It has been noted long ago (already in the 19th century) that number fields and function fields of curves have many properties in common. Accordingly, we shall also present some basic topics on affine plane curves and their function fields. This leads us to mention elliptic curves, however, only in an affine version (instead of the better projective one); we cannot go deeply into that topic at all.

The material presented here is classical and very well known. Large parts of these lecture notes are taken from my lecture notes for the lectures Commutative Algebra and Algebraic Number Theory (the latter written in collaboration with Sara Arias-de-Reyna) for the Master in Mathematics at the University of Luxembourg [Wie]. They were, in turn, heavily influenced by a number of sources, such as Neukirch: Algebraic Number Theory [Neu99], Lorenzini: An Invitation to Arithmetic Geometry [Lor96], Atiyah-Macdonald: Introduction to Commutative Algebra [AM69], Stevenhagen: Number Rings [Ste17].

1 Integers and functions

1.1 Number fields and field extensions

Example 1.1. *Let $d \in \mathbb{Z}$ be different from $0, 1$ and not a square. Put*

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \in \mathbb{C} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

We say that $\mathbb{Q}(\sqrt{d})$ is a quadratic field*.*

In particular, $\mathbb{Q}(\sqrt{d})$ is a field: we can add, substract, multiply and divide elements of $\mathbb{Q}(\sqrt{d})$ without leaving this set (except division by zero, of course).

Exercise: Make these four operations explicit.

Example 1.2. *Let $n \in \mathbb{Z}_{\geq 1}$ be a positive integer. Let $\zeta_n = \exp(2\pi i/n) = \cos(2\pi/n) + i\sin(2\pi/n) \in \mathbb{C}$. Note that ζ_n lies on the unit circle. It is a* primitive n-th root of unity*, meaning $\zeta_n^n = 1$ and $\zeta_n^j \neq 1$ for all $1 \leq j \leq n-1$. Put*

$$\mathbb{Q}(\zeta_n) = \{\sum_{j=0}^{n-1} a_j \zeta_n^j \in \mathbb{C} \mid a_0, \ldots, a_{n-1} \in \mathbb{Q}\}.$$

We say that $\mathbb{Q}(\zeta_n)$ is the n-th cyclotomic field. *In Cryptography, one sometimes encounters $\mathbb{Q}(\zeta_{2^m})$ and its 'ideal lattice' (ring of integers, see below).*

In particular, $\mathbb{Q}(\zeta_n)$ is a field. If it's not clear here, it will be clear below.

Both these examples are *number fields*.

Definition 1.3. *A* number field *is a field $F \subset \mathbb{C}$ which is a finite dimensional $\mathbb{Q}$-vector space. That means that there are elements $y_1, \ldots, y_n \in F$ such that every $x \in F$ can be written as*

$$x = \sum_{j=0}^{n-1} a_j y_j$$

with unique $a_0, \ldots, a_{n-1} \in \mathbb{Q}$.

Even though number fields (and ideal lattices) are one of the principal motivations for these objects in this course, we shall work more abstractly so that we are flexible and can transport results to other settings.

Definition 1.4. *Let F be a field. If $K \subseteq F$ is a subfield of F, then we say that $K \subseteq F$ is a* field extension.

A different piece of notation (used in mathematical literature) for a field extension is F/K.

The following lemma is fundamental because it allows us to use linear algebra in number theory!

Lemma 1.5. *Let $K \subseteq F$ be a field extension. Then F is a K-vector space.*

More precisely: As a field F has addition and multiplication (and also their 'inverses': substraction and division). To make F into a K-vector space, we need an addition; we just take the addition that we already have. We also need a 'scalar multiplication', i.e. we must be able to multiply an element of K with an element of F; we again take the multiplication that we already have. Then it's very easy to check that the associativity, commutativity and distributivity relations that one has in a field imply all the axioms in the definition of vector space.

Definition 1.6. *Let $K \subseteq F$ be a field extension. The* degree *of the field extension is defined as*

$$[F : K] := \dim_K(F),$$

the dimension of F as K-vector space. This can be finite or infinite.

If $[F : K]$ is finite, then we say that $K \subseteq F$ is a finite field extension.

Remark 1.7. *A number field F is hence a field (subfield of $\mathbb{C}$) such that $\mathbb{Q} \subseteq F$ is a finite field extension.*

Definition 1.8. *Let $K \subseteq F$ be a field extension. A polynomial $f \in K[X]$ is said to be the* minimal polynomial of $a \in F$ over K *if*

- *it is monic, i.e. its leading coefficient is 1,*
- *a is a root of f, i.e. $f(a) = 0$,*
- *any polynomial $g \in K[X]$ such that $g(a) = 0$ is a multiple of f (in particular, if $g \neq 0$, then $\deg(f) \leq \deg(g)$.*

Example 1.9. *Let $a \in \mathbb{Q}$. Its minimal polynomial over $\mathbb{Q}$ is $m_a(X) = X - a \in \mathbb{Q}[X]$.*

Example 1.10. *Let us consider quadratic fields.*

(a) Consider $\sqrt{2} \in \mathbb{C}$. Its minimal polynomial over $\mathbb{Q}$ is $m_{\sqrt{2}}(X) = X^2 - 2 \in \mathbb{Q}[X]$.

(b) Consider $\frac{1+\sqrt{5}}{2} \in \mathbb{C}$*. Its minimal polynomial over* $\mathbb{Q}$ *is* $X^2 - X - 1 \in \mathbb{Q}[X]$.

(c) Consider $\frac{1+\sqrt{-5}}{2} \in \mathbb{C}$*. Its minimal polynomial over* $\mathbb{Q}$ *is* $X^2 - X + \frac{3}{2} \in \mathbb{Q}[X]$.

Example 1.11. *Let* p *be a prime number and* $\zeta_p = \exp(2\pi i/p) \in \mathbb{C}$*. Its minimal polynomial over* $\mathbb{Q}$ *is* $X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$*. This is the* p-th cyclotomic polynomial.

More generally, the minimal polynomial of ζ_n *for* $n \in \mathbb{Z}_{\geq 1}$ *exists and can be written down rather explicitly. It is called the* p-th cyclotomic polynomial.

Definition 1.12. *Let* $K \subseteq F$ *be a field extension. An element* $a \in F$ *is called* algebraic over K *if it has a minimal polynomial in* $K[X]$.

The field extension $K \subseteq F$ *is called* algebraic *if every* $a \in F$ *is algebraic over* K.

Example 1.13. *In all preceding examples, we saw numbers that are algebraic over* $\mathbb{Q}$.

The famous number π*, defined as the ratio of the circumference of a circle over its diameter, is not algebraic over* $\mathbb{Q}$ *by a famous theorem of Lindemann. One says that it is a* transcendental number *(over* $\mathbb{Q}$*).*

Proposition 1.14. *Any finite field extension* $K \subseteq F$ *(in particular, any number field* F*) is algebraic, so* $a \in L$ *has a minimal polynomial* $m_a \in K[X]$.

Proof. The powers $1 = a^0, a = a^1, a^2, a^3, \ldots$ must be K-linearly dependent because the dimension is finite. The minimal polynomial is the shortest non-zero equation of the form

$$a^n + c_{n-1}a^{n-1} + \cdots + c_1 a^1 + c_0 a^0 = 0$$

with $c_i \in K$. □

1.2 Integers

Example 1.15. *The minimal polynomial of* $a \in \mathbb{Q}$ *over* $\mathbb{Q}$ *is* $m_a(X) = X - a \in \mathbb{Q}[X]$*. Note the following:*

$$a \in \mathbb{Z} \Leftrightarrow m_a(X) \in \mathbb{Z}[X].$$

So, we have

$$\mathbb{Z} = \{a \in \mathbb{Q} \mid m_a(X) \in \mathbb{Z}[X].$$

Definition 1.16. *If* S *is a ring and* $R \subseteq S$ *is a subring, then we also speak of a* ring extension *(in analogy to the terminology used for field extensions).*

In the sequel, we shall often be concerned with a number field F and consider the ring extension $\mathbb{Z} \subset F$.

Definition 1.17. *Let* $R \subseteq S$ *be a ring extension. Then* $a \in S$ *is called* integral *over* R *if there is a monic polynomial* $f \in R[X]$ *such that* $f(a) = 0$.

We first clarify which algebraic elements are integral in the case of interest to us.

Lemma 1.18. *Let* F *be a number field. Then* $a \in F$ *is* integral *over* $\mathbb{Z}$ *if and only if its minimal polynomial* m_a *has coefficients in* $\mathbb{Z}$.

More generally, let R *be an integrally closed integral domain (see below;* $\mathbb{Z}$ *is an example) with field of fractions* K*. Let* $K \subseteq F$ *be a finite field extension. Then* $a \in F$ *is integral over* R *if and only if its minimal polynomial* $m_a(X)$ *has coefficients in* R.

Proof. We only prove the first statement. The general statement requires more technology and will be skipped.

One implication is clear (and works without any assumption on R in the general case). For the other one, let $f \in \mathbb{Z}[X]$ be any monic polynomial such that $f(a) = 0$. Consider f as an element of $\mathbb{Q}[X]$. As such, it is a multiple of the minimal polynomial $m_a(X) \in \mathbb{Q}[X]$, i.e.

$$f(X) = m_a(X) \cdot h(X)$$

for some polynomial $h(X) \in \mathbb{Q}[X]$. Note that $h(X)$ is necessarily monic. Now, a theorem of Gauß tells us that if a monic polynomial with coefficients in $\mathbb{Z}$ factors into two monic polynomials, then both of them also have coefficients in $\mathbb{Z}$, proving $m_a(X) \in \mathbb{Z}[X]$. □

We reconsider the same examples as above.

Example 1.19. *Let $a \in \mathbb{Q}$. As its minimal polynomial over $\mathbb{Q}$ is $m_a(X) = X - a \in \mathbb{Q}[X]$, we have: $a \in \mathbb{Z}$ if and only if a is integral over $\mathbb{Q}$.*

Example 1.20. *Let us consider quadratic fields.*

(a) Consider $\sqrt{2} \in \mathbb{C}$. As its minimal polynomial over $\mathbb{Q}$ is $m_{\sqrt{2}}(X) = X^2 - 2 \in \mathbb{Z}[X]$, it follows that $\sqrt{2}$ is integral over $\mathbb{Z}$.

(b) Consider $\frac{1+\sqrt{5}}{2} \in \mathbb{C}$. As its minimal polynomial over $\mathbb{Q}$ is $X^2 - X - 1 \in \mathbb{Z}[X]$, it follows that $\frac{1+\sqrt{5}}{2} \in \mathbb{C}$ is integral over $\mathbb{Z}$.

(c) Consider $\frac{1+\sqrt{-5}}{2} \in \mathbb{C}$. As its minimal polynomial over $\mathbb{Q}$ is $X^2 - X + \frac{3}{2} \notin \mathbb{Z}[X]$, it follows that $\frac{1+\sqrt{-5}}{2} \in \mathbb{C}$ is not integral over $\mathbb{Z}$.

Example 1.21. *Let p be a prime number and $\zeta_p = \exp(2\pi i/p) \in \mathbb{C}$. As its minimal polynomial over $\mathbb{Q}$ is $X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$, it follows that ζ_p is integral over $\mathbb{Z}$. More generally, the same conclusion holds for all ζ_n for $n \in \mathbb{Z}_{\geq 1}$.*

1.3 Ring of integers and integral ring extensions

Definition 1.22. *For a number field F, define the* ring of integers of F *as*

$$\mathbb{Z}_F := \{a \in F \mid a \text{ is integral over } \mathbb{Z}\}.$$

We revisit again the above examples.

Example 1.23. *Ring of integers of $\mathbb{Q}$: As seen above: $\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$, i.e. $\mathbb{Z}$ is the ring of integers of $\mathbb{Q}$.*

Example 1.24. *Let $d \neq 0, 1$ be a squarefree integer. The ring of integers of $\mathbb{Q}(\sqrt{d})$ is*

(1) $\mathbb{Z}[\sqrt{d}]$, if $d \equiv 2, 3 \pmod 4$,

(2) $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, if $d \equiv 1 \pmod 4$.

Example 1.25. *Let $n \in \mathbb{Z}_{\geq 1}$ and $\zeta_n = \exp(2\pi i/n) \in \mathbb{C}$. The ring of integers of the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$ is*

$$\mathbb{Z}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n] = \{\sum_{j=0}^{n-1} a_j \zeta_n^j \in \mathbb{C} \mid a_0, \ldots, a_{n-1} \in \mathbb{Z}\}.$$

Attention: if n is not prime, then the powers ζ_n^j for $0 \leq j \leq n-1$ do not form a basis (there's linear dependence). For instance, for $n = 4$, we have $\zeta_4 = i$ and $1, i, i^2 = -1, i^3 = -i$ are not $\mathbb{Q}$-linearly independent.

Exercise: Work our a basis for $n = 2^m$.

Let us add an abstract definition, which we will mostly (but not exclusively) use with $R = \mathbb{Z}$ and $S = \mathbb{Z}_K$ with a number field K.

Definition 1.26. *Let S be a ring and $R \subseteq S$ a subring.*

(a) The set $R_S = \{a \in S \mid a$ is integral over $R\}$ *is called the* integral closure of R in S *(compare with the algebraic closure of R in S – the two notions coincide if R is a field).*

An alternative name is: normalisation of R in S.

(b) S is called an integral ring extension of R *if $R_S = S$, i.e. if every element of S is integral over R (compare with algebraic field extension – the two notions coincide if R and S are fields).*

(c) R is called integrally closed in S *if $R_S = R$.*

(d) An integral domain R is called integrally closed *(i.e. without mentioning the ring in which the closure is taken) if R is integrally closed in its fraction field.*

(e) Let $a_i \in S$ for $i \in I$ (some indexing set). We let $R[a_i \mid i \in I]$ (note the square brackets!) be the smallest subring of S containing R and all the a_i, $i \in I$.

Note that we can see $R[a]$ inside S as the image of the ring homomorphism

$$\Phi_a : R[X] \to S, \quad \sum_{i=0}^{d} c_i X^i \mapsto \sum_{i=0}^{d} c_i a^i.$$

Remark 1.27. *The* ring of integers of K *is the integral closure of $\mathbb{Z}$ in K, this explains the piece of notation $\mathbb{Z}_K$. An alternative notation that one often encounters in mathematical texts is $\mathcal{O}_K$.*

Example 1.28. *Every UFD (unique factoriation domain) is integrally closed. In particular, $\mathbb{Z}$ and polynomial rings $F[X_1, \ldots, X_n]$ are integrally closed.*

In the next statements, we will speak of *R-modules* for a ring R. An R-module is nothing else than a vector space (exactly the same definition), except that we allow the coefficients to be in a ring, where as the notion of *vector space* is restricted to coefficients in fields.

Proposition 1.29. *Let $R \subseteq S \subseteq T$ be rings.*

(a) For $a \in S$, the following statements are equivalent:

(i) a is integral over R.

(ii) $R[a] \subseteq S$ is a finitely generated R-module.

(b) Let $a_1, \ldots, a_n \in S$ be elements that are integral over R. Then $R[a_1, \ldots, a_n] \subseteq S$ is integral over R and it is finitely generated as an R-module.

(c) Let $R \subseteq S \subseteq T$ be rings. Then 'transitivity of integrality' holds:

$$R \subseteq T \text{ is integral} \;\Leftrightarrow\; S \subseteq T \text{ is integral and } R \subseteq S \text{ is integral.}$$

(d) R_S *is a subring of* S.

(e) Any $t \in S$ *that is integral over* R_S *lies in* R_S. *In other words,* R_S *is integrally closed in* S *(justifying the name).*

Proposition 1.30. *Let* R *be an integral domain,* $K = \mathrm{Frac}(R)$, $K \subseteq F$ *a finite field extension and* $S := R_F$ *the integral closure of* R *in* F. *Then the following statements hold:*

(a) Every $a \in F$ *can be written as* $a = \frac{s}{r}$ *with* $s \in S$ *and* $0 \neq r \in R$.

(b) $F = \mathrm{Frac}(S)$ *and* S *is integrally closed.*

(c) If R *is integrally closed, then* $S \cap K = R$.

1.4 Trace and norm in field extensions

We now systematically do linear algebra in field extensions. Let $K \subseteq F$ be a finite field extension of degree $[F : K] = n$. Let $a \in L$. Note that multiplication by a:

$$T_a : F \to F, \quad x \mapsto ax$$

is F-linear and, thus, in particular, K-linear. Once we choose a K-basis of F, we can represent T_a by an $n \times n$-matrix with coefficients in K, also denoted T_a.

Example 1.31. *The complex numbers* $\mathbb{C}$ *have the* $\mathbb{R}$*-basis* $\{1, i\}$ *and with respect to this basis, any* $z \in \mathbb{C}$ *is represented as* $\binom{x}{y} = x + yi$. *Now, take* $a = \binom{b}{c} = b + ci \in \mathbb{C}$. *We obtain:* $T_a = \left(\begin{smallmatrix} b & -c \\ c & b \end{smallmatrix}\right)$, *as we can easily check:*

$$T_a(z) = az = (b + ci)(x + yi) = (bx - cy) + (cx + by)i \text{ and } T_a(z) = \left(\begin{smallmatrix} b & -c \\ c & b \end{smallmatrix}\right) \binom{x}{y} = \begin{pmatrix} bx - cy \\ cx + by \end{pmatrix}.$$

As an aside: You may have seen this matrix before; namely, writing $z = r(\cos(\varphi) + i \sin(\varphi))$, *it looks like* $r \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}$, *i.e. it is a rotation matrix times a homothety (stretching) factor.*

We can now do linear algebra with the matrix $T_a \in \mathrm{Mat}_n(K)$.
Recall that the *trace* of a matrix $M = (m_{i,j})_{1 \leq i,j \leq n} \in \mathrm{Mat}_n(K)$ is defined as

$$\mathrm{Tr}(M) = \sum_{i=1}^{n} m_{i,i},$$

the sum of its diagonal entries.

Definition 1.32. *Let* $K \subseteq F$ *be a field extension of degree* $[F : K] = n$. *Let* $a \in F$. *The* trace of a in $K \subseteq F$ *is defined as the trace of the matrix* $T_a \in \mathrm{Mat}_n(K)$ *and the* norm of a in $K \subseteq F$ *is defined as the determinant of the matrix* $T_a \in \mathrm{Mat}_n(K)$*:*

$$\mathrm{Tr}_{F/K}(a) := \mathrm{Tr}(T_a) \text{ and } \mathrm{Norm}_{F/K}(a) := \det(T_a).$$

Note that trace and norm do not depend on the choice of basis by a standard result from linear algebra.

Example 1.33. *Let us continue the example above. Let* $z = x + yi \in \mathbb{C}$. *Then* $\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(z) = 2x = 2\,\mathrm{Re}(z)$ *and* $\mathrm{Norm}_{\mathbb{C}/\mathbb{R}}(z) = x^2 + y^2 = |z|^2$.

Lemma 1.34. *Let* $K \subseteq F$ *be a finite field extension.*

(a) $\mathrm{Tr}_{F/K}$ *defines a group homomorphism* $(F,+)\to(K,+)$*, i.e.*

$$\mathrm{Tr}_{F/K}(a+b)=\mathrm{Tr}_{F/K}(a)+\mathrm{Tr}_{F/K}(b) \text{ for all } a,b\in F.$$

(b) $\mathrm{Norm}_{F/K}$ *defines a group homomorphism* $(F^\times,\cdot)\to(K^\times,\cdot)$*, i.e.*

$$\mathrm{Norm}_{F/K}(a\cdot b)=\mathrm{Norm}_{F/K}(a)\cdot\mathrm{Norm}_{F/K}(b) \text{ for all } a,b\in F.$$

Proof. (a) The trace of a matrix is additive and $T_{a+b}=T_a+T_b$ because

$$T_{a+b}(x)=(a+b)x=ax+bx=T_a(x)+T_b(x)$$

for all $x\in F$.

(b) The determinant of a matrix is multiplicative and $T_{a\cdot b}=T_a\circ T_b$ because

$$T_{a\cdot b}(x)=abx=T_a\big(T_b(x)\big)$$

for all $x\in F$. □

Lemma 1.35. *Let $K\subseteq F$ be a finite field extension of degree $[F:K]=n$. Let $a\in F$.*

(a) Let $f_a=X^n+b_{n-1}X^{n-1}+\cdots+b_1X+b_0\in K[X]$ be the characteristic polynomial of $T_a\in\mathrm{Mat}_n(K)$. Then $\mathrm{Tr}_{F/K}(a)=-b_{n-1}$ and $\mathrm{Norm}_{F/K}(a)=(-1)^nb_0$.

(b) Let $m_a=X^d+c_{d-1}X^{d-1}+\cdots+c_1X+c_0\in K[X]$ be the minimal polynomial of a over K. Then $\{1,a,a^2,\dots,a^{d-1}\}$ forms a K-basis of $K(a)$ and $[K(a):K]=d$. Moreover, the matrix T'_a representing the map $K(a)\xrightarrow{x\mapsto ax}K(a)$ with respect to this K-basis equals

$$T'_a=\begin{pmatrix}0&0&\cdots&0&-c_0\\1&0&\cdots&0&-c_1\\0&1&\cdots&0&-c_2\\\vdots&\vdots&\ddots&&\vdots\\0&0&\cdots&1&-c_{d-1}\end{pmatrix}.$$

(c) Then $d=[K(a):K]$ and with $e=[F:K(a)]$ one has $m_a(X)^e=f_a(X)$.

Proof. Exercise. □

We need some important pieces of terminology from field theory.

Definition 1.36. *Let $K\subseteq F$ and $K\subseteq L$ be field extensions. Denote*

$$\mathrm{Hom}_K^{\text{field}}(F,L)=\{\varphi:F\to L\mid \text{ field homomorphism s.t. } \forall\,x\in K:\varphi(x)=x\},$$

the set of field homomorphisms from F to L that are the identity on K.

Let $\overline{K}$ be an algebraic closure of K (i.e. and algebraic extension $K\subseteq\overline{K}$ such that every non-constant polynomial in $K[X]$ has a zero (and hence all zeros) in $\overline{K}$.

We say that a finite field extension $K\subseteq F$ is separable *if $[F:K]=\#\mathrm{Hom}_K^{\text{field}}(F,\overline{K})$.*

Example 1.37. *If K is a field of characteristic 0, i.e. a field that contains (a subfield isomorphic to) $\mathbb{Q}$, then any field extension $K\subseteq F$ is separable. If K is a finite field, the same conclusion holds.*

However, if K is an infinite field of characteristic $p>0$, then there are non-separable extensions. One encounters this when working with elliptic curves over finite fields.

Proposition 1.38. *Let $K \subseteq F$ be a finite separable field extension, $\overline{K}$ an algebraic closure of K containing F. Let, furthermore, $a \in F$ and f_a be the characteristic polynomial of T_a. Then the following statements hold:*

(a) $f_a(X) = \prod_{\sigma \in \mathrm{Hom}_K^{\text{field}}(F,\overline{K})}(X - \sigma(a))$,

(b) $\mathrm{Tr}_{F/K}(a) = \sum_{\sigma \in \mathrm{Hom}_K^{\text{field}}(F,\overline{K})} \sigma(a)$, *and*

(c) $\mathrm{Norm}_{F/K}(a) = \prod_{\sigma \in \mathrm{Hom}_K^{\text{field}}(F,\overline{K})} \sigma(a)$.

Corollary 1.39. *Let $K \subseteq F \subseteq L$ be finite separable field extensions. Then*

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{F/K} \circ \mathrm{Tr}_{L/F} \text{ and } \mathrm{Norm}_{L/K} = \mathrm{Norm}_{F/K} \circ \mathrm{Norm}_{L/F}.$$

We now apply norm and trace to integral elements. We again state the result in general, but one can think of $R = \mathbb{Z}$, F a number field and $S = \mathbb{Z}_K$ its ring of integers.

Lemma 1.40. *Let R be an integrally closed integral domain, K its field of fractions, $K \subseteq F$ a separable finite field extension and S the integral closure of R in F. Let $s \in S$. Then the following statements hold:*

(a) $\mathrm{Tr}_{F/K}(s) \in R$ *and* $\mathrm{Norm}_{F/K}(s) \in R$.

(b) $s \in S^\times \Leftrightarrow \mathrm{Norm}_{F/K}(s) \in R^\times$.

Proof. (a) directly follows from $S \cap K = R$.
(b) '$\Rightarrow$': Let $s, t \in S^\times$ such that $ts = 1$. Then

$$1 = \mathrm{Norm}_{F/K}(1) = \mathrm{Norm}_{F/K}(st) = \mathrm{Norm}_{F/K}(s)\mathrm{Norm}_{F/K}(t),$$

exhibiting an inverse of $\mathrm{Norm}_{F/K}(s)$ in R.
'$\Leftarrow$': Assume $\mathrm{Norm}_{F/K}(s) \in R^\times$. Then

$$1 = r\mathrm{Norm}_{F/K}(s) = r \prod_{\sigma \in \mathrm{Hom}_K(F,\overline{K})} \sigma(s) = \big(r \prod_{\mathrm{id} \neq \sigma \in \mathrm{Hom}_K(F,\overline{K})} \sigma(s)\big)s = ts,$$

exhibiting an inverse to s in S. □

1.5 Discriminant

Definition 1.41. *Let $K \subseteq F$ be a finite separable field extension of degree $n = [F : K]$. Let $\overline{K}$ be an algebraic closure of K. Further, let* $\mathrm{Hom}_K^{\text{field}}(F, \overline{K}) = \{\sigma_1, \ldots, \sigma_n\}$ *and let $\alpha_1, \ldots, \alpha_n \in F$ be a K-basis of F. Form the matrix*

$$D(\alpha_1, \ldots, \alpha_n) := (\sigma_i(\alpha_j))_{1 \leq i,j \leq n} = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix}.$$

The discriminant of $(\alpha_1, \ldots, \alpha_n)$ *is defined as*

$$\mathrm{disc}(\alpha_1, \ldots, \alpha_n) := \big(\det D(\alpha_1, \ldots, \alpha_n)\big)^2.$$

The trace pairing on $K \subseteq F$ *is the bilinear pairing*

$$F \times F \to K, \quad (x, y) \mapsto \mathrm{Tr}_{F/K}(xy).$$

Example 1.42. *(a) Let $0, 1 \neq d \in \mathbb{Z}$ be a squarefree integer and consider $K = \mathbb{Q}(\sqrt{d})$. Computations (exercise) show:*

$$\operatorname{disc}(1, \sqrt{d}) = 4d \text{ and } \operatorname{disc}(1, \frac{1+\sqrt{d}}{2}) = d.$$

(b) Let $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$ be an irreducible polynomial and consider $K = \mathbb{Q}[X]/(f)$. Let $\alpha \in \mathbb{C}$ be any root of f, so that we can identify $K = \mathbb{Q}(\alpha)$ and $1, \alpha, \alpha^2$ is a $\mathbb{Q}$-basis of K.

Computations (exercise) show $\operatorname{disc}(1, \alpha, \alpha^2) = -4a^3 - 27b^2$.

Remark 1.43. *The discriminant of a polynomial f can also be computed as the resultant of f and its formal derivative f'.*

Proposition 1.44. *Let $K \subseteq F$ be a finite separable field extension of degree $n = [F : K]$. Let $\alpha_1, \ldots, \alpha_n$ be a K-basis of F. Then the following statements hold:*

(a) Let $D := D(\alpha_1, \ldots, \alpha_n)$. Then $D^{\mathrm{tr}}D$ is the Gram matrix of the trace pairing with respect to the chosen K-basis. That is,

$$D^{\mathrm{tr}}D = \big(\operatorname{Tr}_{F/K}(\alpha_i\alpha_j)\big)_{1\leq i,j\leq n}.$$

(b) We have

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_n) = \det(D)^2 = \det(D^{\mathrm{tr}}D) = \det\big(\operatorname{Tr}_{F/K}(\alpha_i\alpha_j)\big)_{1\leq i,j\leq n}.$$

(c) Let $C = (c_{i,j})_{1\leq i,j\leq n}$ be an $n \times n$-matrix with coefficients in K with $\det C \neq 0$ and put $\beta_i := C\alpha_i$ for $i = 1, \ldots, n$. Then

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \det(C)^2 \operatorname{disc}(\alpha_1, \ldots, \alpha_n).$$

(d) If $F = K(a)$, then

$$\operatorname{disc}(1, a, \ldots, a^{n-1}) = \prod_{1\leq i<j\leq n} \big(\sigma_j(a) - \sigma_i(a)\big)^2,$$

where $\sigma_1, \ldots, \sigma_n$ are the K-field homomorphisms $F \to \overline{K}$.

Proof. (a) Let $\sigma_1, \ldots, \sigma_n$ be the K-field homomorphisms $F \to \overline{K}$. Then we have

$$\begin{aligned}
D^{\mathrm{tr}}D &= \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} \\
&= \begin{pmatrix} \sum_{k=1}^n \sigma_k(\alpha_1\alpha_1) & \sum_{k=1}^n \sigma_k(\alpha_1\alpha_2) & \cdots & \sum_{k=1}^n \sigma_k(\alpha_1\alpha_n) \\ \sum_{k=1}^n \sigma_k(\alpha_2\alpha_1) & \sum_{k=1}^n \sigma_k(\alpha_2\alpha_2) & \cdots & \sum_{k=1}^n \sigma_k(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{k=1}^n \sigma_k(\alpha_n\alpha_1) & \sum_{k=1}^n \sigma_k(\alpha_n\alpha_2) & \cdots & \sum_{k=1}^n \sigma_k(\alpha_n\alpha_n) \end{pmatrix} \\
&= \begin{pmatrix} \operatorname{Tr}_{F/K}(\alpha_1\alpha_1) & \operatorname{Tr}_{F/K}(\alpha_1\alpha_2) & \cdots & \operatorname{Tr}_{F/K}(\alpha_1\alpha_n) \\ \operatorname{Tr}_{F/K}(\alpha_2\alpha_1) & \operatorname{Tr}_{F/K}(\alpha_2\alpha_2) & \cdots & \operatorname{Tr}_{F/K}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \operatorname{Tr}_{F/K}(\alpha_n\alpha_1) & \operatorname{Tr}_{F/K}(\alpha_n\alpha_2) & \cdots & \operatorname{Tr}_{F/K}(\alpha_n\alpha_n) \end{pmatrix}.
\end{aligned}$$

So, the (i, j)-entry of the matrix $D^{\mathrm{tr}}D$ equals $\operatorname{Tr}_{F/K}(\alpha_i\alpha_j)$. Hence, $D^{\mathrm{tr}}D$ is the Gram matrix of the trace pairing with respect to the chosen K-basis.

(b) is clear.

(c) Exercise.

(d) Exercise. □

Proposition 1.45. *Assume the setting of the previous proposition. The discriminant* $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ *is non-zero and the trace pairing on* $K \subseteq F$ *is non-degenerate.*

1.6 Integral bases, orders and lattices in number fields

For going on, we need to introduce some more terminology on modules ('vector spaces over rings'). It is again the same as for vector spaces.

Definition 1.46. *Let* R *be a ring and let* M *be an* R*-module.*

Let $m_i \in M$ *with indices* $i \in I$ *(some set) be a collection of elements.*

The collection $(m_i)_{i \in I}$ *is called a* generating set of M *if for every* $m \in M$ *there is a finite subset of indices* $J \subseteq I$ *and for every* $j \in J$ *there is* $r_j \in R$ *such that* $m = \sum_{j \in J} r_j m_j$.

If M *possesses a generating set that is finite, then* M *is called* finitely generated as R-module.

The collection $(m_i)_{i \in I}$ *is called* R-linearly independent *or* R-free *if for all finite subsets of indices* $J \subseteq I$ *the only linear combination equal to zero:*

$$0 = \sum_{j \in J} r_j m_j$$

with $r_j \in R$ *for* $j \in J$ *is the one where* $r_j = 0$ *for all* $j \in J$.

An R*-free generating set of* M *is called an* R*-basis of* M.

An R*-module* M *that possesses an* R*-basis is called* R-free.

The number of elements in an (and any) R*-basis of* M *is called the* R-rank *of* M*, denoted* $\mathrm{rk}_R(M)$.

Remark 1.47. *If* $R = K$ *is a field, then any* R*-module is a* K*-vector space and by results form linear algebra it is automatically free and possesses a* K*-basis. Moreover, in that case, dimension and rank are the same.*

However, if R *is not a field, then there are in general non-free modules, which also don't have any basis (but they all have generating sets).*

We include the structure theorem of finitely generated modules over PIDs (principal ideal domains). The main example is $R = \mathbb{Z}$ or a polynomial ring in one variable over a field. The proof is not very difficult, but not included here.

Theorem 1.48. *Let* R *be a principal ideal domain and* M *a finitely generated* R*-module. Then the following statements hold:*

(a) Assume that M *is a free* R*-module of rank* m*. Then any submodule* N *of* M *is finitely generated and free of rank* $\leq m$.

(b) An element $m \in M$ *is called a* torsion element *if there is* $0 \neq r \in R$ *such that* $rm = 0$*. The set* $M_{\mathrm{torsion}} = \{m \in M \mid m \text{ is a torsion element } \}$ *is an* R*-submodule of* M.

(c) M *is a free* R*-module* $\Leftrightarrow M_{\mathrm{torsion}} = \{0\}$.

(d) There is an integer m such that

$$M \cong M_{\text{torsion}} \oplus \underbrace{R \oplus \ldots \oplus R}_{m \text{ times}}.$$

We need one more piece of terminology for modules.

Definition 1.49. *An R-module M is called* Noetherian *if all its submodules are finitely generated. A ring R is* Noetherian *if it is Noetherian as R-module; this is equivalent to asking that all ideals of R are finitely generated.*

Example 1.50. *Every principal ideal domain (PID) is Noetherian, so, in particular, $\mathbb{Z}$ is Noetherian. Moreover, the polynomial ring in n-variables over a Noetherian ring is Noetherian (this is called* Hilbert's Basissatz*).*

Definition 1.51. *Let $R \subseteq S$ be an integral ring extension. If S is free as an R-module, then, by definition, an R-basis of S (i.e. a free generating system) exists and is called an* integral basis of S over R.

We point out that, if S is an integral domain (as it always will be in this lecture), then an R-basis of S is also a K-basis of $F = \mathrm{Frac}(S)$ with $K = \mathrm{Frac}(R)$.

Note that, in general, there is no reason why an integral ring extension S should be free as an R-module. This is, however, the case for the rings of integers, as the following proposition shows. We first need a lemma.

Lemma 1.52. *Let R be an integrally closed integral domain, K its field of fractions, $K \subseteq F$ a separable finite field extension and S the integral closure of R in F.*

(a) For any K-basis $\alpha_1, \ldots, \alpha_n$ of F, there is an element $r \in R \setminus \{0\}$ such that $r\alpha_i \in S$ for all $i = 1, \ldots, n$.

(b) Let $\alpha_1, \ldots, \alpha_n \in S$ be a K-basis of F and let $d = \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ be the discriminant of this basis. Then $dS \subseteq R\alpha_1 + \cdots + R\alpha_n$.

Proof. (a) By Proposition 1.30 (a), we can write $\alpha_i = \frac{s_i}{r_i}$ with $r_i \in R$ and $s_i \in S$ for all $i = 1, \ldots, n$. Hence, we may take $r = r_1 \cdot \ldots \cdot r_n$.

(b) Let $s = \sum_{j=1}^n x_j \alpha_j$ be an element of S with $x_j \in K$ for $j = 1, \ldots, n$. We show $ds \in R\alpha_1 + \cdots + R\alpha_n$. Note that the elementary properties of the trace yield

$$\mathrm{Tr}_{F/K}(\alpha_i s) = \sum_{j=1}^n \mathrm{Tr}(\alpha_i \alpha_j) x_j \in R.$$

We can rewrite this in matrix form using $M = D^{\mathrm{tr}} D = \begin{pmatrix} \mathrm{Tr}_{F/K}(\alpha_1\alpha_1) & \cdots & \mathrm{Tr}_{F/K}(\alpha_1\alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{F/K}(\alpha_n\alpha_1) & \cdots & \mathrm{Tr}_{F/K}(\alpha_n\alpha_n) \end{pmatrix}$. Now:

$$M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n \mathrm{Tr}_{F/K}(\alpha_1\alpha_j) x_j \\ \vdots \\ \sum_{j=1}^n \mathrm{Tr}_{F/K}(\alpha_n\alpha_j) x_j \end{pmatrix} \in R^n.$$

Multiplying through with the adjoint matrix $M^{\#}$ yields

$$M^{\#} M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \det(M) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = d \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in R^n.$$

Thus, $dx_i \in R$ for all $i = 1, \ldots, n$ and, consequently, $ds \in R\alpha_1 + \cdots + R\alpha_n$. □

Proposition 1.53. *Let R be a principal ideal domain, K its field of fractions, $K \subseteq F$ a finite separable field extension and S the integral closure of R in F.*

(For instance, we can take $R = \mathbb{Z}$, $K = \mathbb{Q}$, F a number field and $S = \mathbb{Z}_F$ its ring of integers.)

Then every finitely generated S-submodule $0 \neq M \subseteq F$ is a free R-module of rank $[F : K]$. In particular, S possesses an integral basis over R. Moreover, S is a Noetherian ring.

Proof. As principal ideal domains are unique factorisation domains and, hence, integrally closed, we may apply Lemma 1.52 to obtain a K-basis $\alpha_1, \dots, \alpha_n \in S$ of F and we also have $dS \subseteq R\alpha_1 + \cdots + R\alpha_n =: N$ with $d = \operatorname{disc}(\alpha_1, \dots, \alpha_n)$. Note that N is a free R-module of rank $n = [F : K]$.

Let $m_1, \dots, m_k \in M$ be a generating system of $M \subseteq F$ as S-module. As the m_i are elements of F, by Proposition 1.30 (a) there is $r \in R$ such that $rm_i \in S$ for all $i = 1, \dots, k$, whence $rM \subseteq S$. Hence, $rdM \subseteq dS \subseteq N$. Consequently, Theorem 1.48 yields that rdM is a free R-module of rank at most n. Of course, the R-rank of rdM is equal to the R-rank of M. Let $0 \neq m \in M$. Then $Nm \leq Sm \leq M$, showing that n, the R-rank of N (which is equal to the R-rank of Nm) is at most the R-rank of M. Since finite direct sums of Noetherian modules are Noetherian, it follows that S is Noetherian. □

For the rest of this section we specialise to the case of number fields.

Definition 1.54. *Let F be a number field. A subring $\mathcal{O}$ of $\mathbb{Z}_F$ is called an* order of F *if $\mathcal{O}$ has an integral basis of length $[F : \mathbb{Q}]$. Equivalently, the index $(\mathbb{Z}_F : \mathcal{O})$ as abelian groups is finite.*

Corollary 1.55. *Let F be a number field and $\mathbb{Z}_F$ the ring of integers of F. Then the following statements hold:*

(a) $\mathbb{Z}_F$ is an order of F, also called the maximal order of F.

(b) Let $\mathcal{O}$ be an order of F and $0 \subsetneq I \trianglelefteq \mathcal{O}$ be an ideal. Then I is a free $\mathbb{Z}$-module of rank $[F : \mathbb{Q}]$ and the quotient $\mathcal{O}/I$ is finite (i.e. has finitely many elements; equivalently, the index $(\mathcal{O} : I)$ is finite).

Proof. (a) It is a trivial consequence of Proposition 1.53 that $\mathbb{Z}_F$ is a free $\mathbb{Z}$-module of rank $[F : \mathbb{Q}]$ because $\mathbb{Z}_F$ is a $\mathbb{Z}_F$-module generated by a single element, namely 1. In particular, $\mathbb{Z}_F$ has an integral basis and, hence, is an order of F.

(b) Since $I \subseteq \mathcal{O}$ is a subgroup and $\mathcal{O}$ is a free abelian group, I is free of rank $\operatorname{rk}(I) \leq \operatorname{rk}(\mathcal{O}) = [F : \mathbb{Q}]$. Let $0 \neq x \in I$, then $x\mathcal{O} \subseteq I$. As $\operatorname{rk}(\mathcal{O}) = \operatorname{rk}(x\mathcal{O}) \leq \operatorname{rk}(I)$, it follows that $\operatorname{rk}(I) = \operatorname{rk}(\mathcal{O}) = [F : \mathbb{Q}]$. The quotient of any two free $\mathbb{Z}$-modules of the same rank is $\mathbb{Z}$-torsion by Theorem 1.48. Hence, $\mathcal{O}/I$ is an abelian group generated by finitely many elements of finite order, hence, it is a finite group. □

Example 1.56. *Let $f \in \mathbb{Q}[X]$ be an irreducible monic polynomial and let $F = \mathbb{Q}[X]/(f)$ be the number field defined by f. Then $\mathbb{Z}[X]/(f)$ is an order in F, called the* equation order of f. *Note that is usually is NOT the maximal order, i.e. it is usually not the ring of integers. It may have some kind of 'singular points'. More on that later.*

Definition 1.57. *Let F be a number field with ring of integers $\mathbb{Z}_F$ and $0 \neq \mathfrak{a} \subset F$ be a finitely generated $\mathbb{Z}_F$-module. The* discriminant of $\mathfrak{a}$ *is defined as $\operatorname{disc}(\alpha_1, \dots, \alpha_n)$ for any $\mathbb{Z}$-basis of the free $\mathbb{Z}$-module $\mathfrak{a}$ (see Proposition 1.53). (By Proposition 1.44 (c), this definition does not depend on the choice of $\mathbb{Z}$-basis because the basis transformation matrix is invertible with integral entries and thus has determinant ± 1.)*

The discriminant of F *is defined as $\operatorname{disc}(\mathbb{Z}_F)$.*

Proposition 1.58. *Let F be a number field and $\mathbb{Z}_F$ its ring of integers. Let $0 \neq \mathfrak{a} \subseteq \mathfrak{b} \subset F$ be two finitely generated $\mathbb{Z}_F$-modules. Then the index $(\mathfrak{b} : \mathfrak{a})$ is finite and satisfies*

$$\operatorname{disc}(\mathfrak{a}) = (\mathfrak{b} : \mathfrak{a})^2 \operatorname{disc}(\mathfrak{b}).$$

1.7 Fields and rings of functions (on a plane curve)

In order to keep the technicalities low, we shall only work in an affine setting and not in a projective one.

Definition 1.59. *Let $K \subseteq F$ be a field extension. Let $n \in \mathbb{Z}_{\geq 1}$. The set of* F-points of affine n-space *is defined as $\mathbb{A}^n(F) := F^n$ (i.e. n-dimensional F-vector space).*
Let $S \subseteq K[X_1, \ldots, X_n]$ be a subset. Then

$$\mathcal{V}_S(F := \{(x_1, \ldots, x_n) \in \mathbb{A}^n(F) \mid f(x_1, \ldots, x_n) = 0 \text{ for all } f \in S\}$$

is called the set of F-points of the affine (algebraic) set belonging to S.
If the set S consists of a single non-constant polynomial, then $\mathcal{V}_S(\overline{K})$ is also called a hyperplane in $\mathbb{A}(\overline{K})$.
If $n = 2$ and $S = \{f\}$ with non-constant f, then $\mathcal{V}_S(\overline{K})$ is called a plane curve *(because it is a curve in the plane $\mathbb{A}^2(\overline{K})$. Its F-points are defined as $\mathcal{V}_S(F)$ for $K \subseteq F$ a field extension.*

Convention: When the number of variables is clear, we write $K[\underline{X}]$ for $K[X_1, \ldots, X_n]$. In the same way a tuple $(x_1, \ldots, x_n) \in \mathbb{A}^n(K)$ is also abbreviated as $\underline{x}$ if no confusion can arise.
The letter 'V' is chosen because of the word 'variety' or 'vanishing set'.

Example 1.60. *(a) $K = \mathbb{R}$, $n = 2$, $K[X, Y] \ni f(X, Y) = aX + bY + c$ non-constant. Then $V_{\{f\}}(\mathbb{R})$ is a line ($y = -\frac{a}{b}x - \frac{c}{b}$ if $b \neq 0$; if $b = 0$, then it is the line with x-coordinate $-\frac{c}{a}$ and any y-coordinate).*

(b) $K = \mathbb{R}$, $n = 2$, $K[X, Y] \ni f(X, Y) = X^2 + Y^2 - 1$. Then $V_{\{f\}}(\mathbb{R})$ is the circle in $\mathbb{R}^2$ around the origin with radius 1.

(c) $K = \mathbb{Q}$, $f(X, Y) := X^2 + Y^2 + 1$. Note $\mathcal{V}_{\{f\}}(\mathbb{R}) = \emptyset$, but $(0, i) \in \mathcal{V}_{\{f\}}(\mathbb{C})$.

(d) $K = \mathbb{F}_2$, $f(X, Y) := X^2 + Y^2 + 1 = (X + Y + 1)^2 \in \mathbb{F}_2[X]$. Because of $f(a, b) = 0 \Leftrightarrow a + b + 1 = 0$ for any $a, b \in L$, $L/\mathbb{F}_2$, we have

$$\mathcal{V}_{\{f\}}(L) = \mathcal{V}_{\{X+Y+1\}}(L),$$

which is a line.

Example 1.61. *(a) Let $K = \mathbb{Q}$ and consider $f(X, Y) = X^2 + Y^2 - 1$ and the $\mathbb{Q}$-points of the associated curve $C = S^1 = \mathcal{V}_{\{f\}}(\mathbb{Q})$. They correspond in a precise way to primitive pythagorean triples (a, b, c) for $a, b, c \in \mathbb{Z}$ and $a^2 + b^2 = c^2$. For details see an exercise.*

Note that this is a nice and first illustration of the deep relations between geometry and number theory (algebra). We will encounter several in this course.

(b) Let K be a field and consider $f(X, Y) = X^2 + Y^2$.

The only solution of the form $(x, 0)$ is $(0, 0)$ in any field K. Suppose now (x, y) is a solution with $y \neq 0$. Then $x^2 = -y^2$, or $z^2 = -1$ with $z = \frac{x}{y}$.

Hence, $\mathcal{V}_{\{f\}}(K) = \{(0, 0)\}$ if and only if $X^2 = -1$ has no solution in K.

In particular, $\mathcal{V}_{\{f\}}(\mathbb{R}) = \{(0, 0)\}$ (but: $\mathcal{V}_{\{f\}}(\mathbb{C}) = \mathcal{V}_{\{X-iY\}}(\mathbb{C}) \cup \mathcal{V}_{\{X+iY\}}(\mathbb{C})$, union of two lines) and $\mathcal{V}_{\{f\}}(\mathbb{F}_p) = \{(0, 0)\}$ if and only if $p \equiv 3 \pmod 4$.

Example 1.62. *Let K be a field and $f(X) = X^3 + aX^2 + bX + c$ be a separable polynomial (meaning that it has no multiple zeros over $\overline{K}$).*

Any plane curve of the form $\mathcal{V}_{Y^2 - f(X)}$ is called an elliptic curve.

Definition 1.63. *Let $\mathcal{X}$ be a subset of $\mathbb{A}^n(K)$.*

The coordinate ring of $\mathcal{X}$ *is the ring of functions $\mathcal{X} \to K$ that are described by polynomials. More precisely, it is the image of the ring homomorphism*

$$\varphi : K[\underline{X}] \to \mathrm{Maps}(\mathcal{X}, K), \quad f \mapsto \big((x_1, \ldots, x_n) \mapsto f(x_1, \ldots, x_n)\big)$$

(with $+$ and $\cdot$ on $\mathrm{Maps}(\mathcal{X}, K)$ defined pointwise: $(f+g)(\underline{x}) := f(\underline{x})+g(\underline{x})$ and $(f\cdot g)(\underline{x}) := f(\underline{x})\cdot g(\underline{x})$).

The kernel of φ is called the vanishing ideal of $\mathcal{X}$*:*

$$\mathcal{I}_{\mathcal{X}} := \ker(\varphi) = \{f \in K[\underline{X}] \mid f(\underline{x}) = 0 \text{ for all } \underline{x} \in \mathcal{X}\}.$$

By the isomorphism theorem, we have $K[\mathcal{X}] = K[X]/\mathcal{I}_{\mathcal{X}}$.

Proposition 1.64. *Let K be a field and $f \in K[X, Y]$ a nonconstant irreducible polynomial. Let $C = \mathcal{V}_f(K)$ be the associated plane curve. Assume that $\mathcal{V}_f(K)$ is infinite (which is automatic if $K = \overline{K}$ is algebraically closed).*

Then the vanishing ideal $\mathcal{I}_C$ is (f) and the coordinate ring $K[C]$ is isomorphic to $K[X, Y]/(f)$.

Example 1.65.

- *Line $f(X, Y) := X - Y + 2 \in \mathbb{R}[X, Y]$, $\mathcal{L} := \mathcal{V}_f(\mathbb{R})$:*

  We have $\mathcal{I}_{\mathcal{L}} = (X - Y + 2)$, i.e. that the vanishing ideal of L is the principal ideal generated by f. This is a consequence of Proposition 1.64.

  We compute the structure of the coordinate ring in this case. Consider the ring homomorphism:

  $$\varphi : \mathbb{R}[X, Y] \to \mathbb{R}[T], \quad g(X, Y) \mapsto g(T, T + 2).$$

  Note that this homomorphism is chosen such that $X - Y + 2$ gets mapped to $T - (T + 2) + 2 = 0$ and so lies in the kernel. We now prove that the kernel is equal to $\mathcal{I}_{\mathcal{L}}$ (and hence to $(X - Y + 2)$). Let $g \in \ker(\varphi)$. This means $g(T, T + 2)$ is the zero polynomial. If we now take a point $(x, y) \in \mathcal{L}$, then it satisfies $y = x + 2$, whence $g(x, y) = g(x, x + 2) = 0$ because it is equal to $g(T, T + 2)$ evaluated at $T = x$. This means $g \in \mathcal{I}_{\mathcal{L}}$, as claimed.

  From the isomorphism theorem, we now obtain that the coordinate ring is just the polynomial ring in one variable:

  $$\mathbb{R}[\mathcal{L}] = \mathbb{R}[X, Y]/\mathcal{I}_{\mathcal{L}} = \mathbb{R}[X, Y]/(X - Y + 2) \cong \mathbb{R}[T].$$

  In other words, the coordinate functions satisfy the equality $\mathfrak{x}_2 = \mathfrak{x}_1 + 2$.

- *Parabola $f(X, Y) := X^2 - Y + 2 \in \mathbb{R}[X, Y]$, $\mathcal{P} := \mathcal{V}_f(\mathbb{R})$:*

  Again by Proposition 1.64 we have $\mathcal{I}_{\mathcal{P}} = (X^2 - Y + 2)$.

  With arguments similar to those used before, we conclude that the coordinate ring is

  $$\mathbb{R}[\mathcal{P}] = \mathbb{R}[X, Y]/\mathcal{I}_{\mathcal{P}} = \mathbb{R}[X, Y]/(X^2 - Y + 2) \cong \mathbb{R}[T],$$

  where the last isomorphism is given by sending the class of $g(X, Y)$ to $g(T, T^2 + 2)$. So, it is again isomorphic to the polynomial ring in one variable.

- *Hyperbola $f(X, Y) := XY - 1 \in \mathbb{R}[X, Y]$, $\mathcal{H} := \mathcal{V}_f(\mathbb{R})$:*

  We again have $\mathcal{I}_{\mathcal{H}} = (XY - 1)$ by Proposition 1.64. This time we obtain

  $$\mathbb{R}[\mathcal{H}] = \mathbb{R}[X, Y]/(XY - 1) \cong \mathbb{R}[X, \frac{1}{X}]$$
  $$= \{\sum_{i=e}^{f} a_i X^i \mid e, f \in \mathbb{Z}, a_i \in \mathbb{R}\} \subset \mathbb{R}(X) := \mathrm{Frac}(\mathbb{R}[X]).$$

Note that this ring is not isomorphic to the polynomial ring in one variable. For, suppose to the contrary that there is a ring isomorphism $\varphi : \mathbb{R}[X, \frac{1}{X}] \to \mathbb{R}[T]$. As X is a unit, so is $\varphi(X)$. Thus, $\varphi(X) \in \mathbb{R}[T]^\times = \mathbb{R}^\times$ is a constant polynomial. Consequently, the image of φ lands in $\mathbb{R}$, contradicting the surjectivity.

Definition 1.66. *Let $\mathcal{X} \subseteq \mathbb{A}^n(K)$ be a subset. We say that $\mathcal{X}$ is* reducible *if there are two affine subsets $\mathcal{X}_1 = \mathcal{V}_{S_1}, \mathcal{X}_2 = \mathcal{V}_{S_2}(K) \subseteq \mathbb{A}^n(K)$ such that*

$$\mathcal{X} \subseteq \mathcal{X}_1 \cup \mathcal{X}_2$$

and

$$\mathcal{X} \not\subseteq \mathcal{X}_1 \text{ and } \mathcal{X} \not\subseteq \mathcal{X}_2.$$

An affine set $\mathcal{X} \subseteq \mathbb{A}^n(K)$ is called an affine variety *if $\mathcal{X}$ is irreducible (i.e. not reducible).*

Example 1.67.

- *Let $f(X, Y) = XY \in \mathbb{R}[X, Y]$. Then $\mathcal{V}_f(\mathbb{R})$ is the union of the x-axis and the y-axis, so clearly $\mathcal{V}_f(\mathbb{R})$ is reducible. More precisely,*

$$\mathcal{V}_f(\mathbb{R}) = \mathcal{V}_X(\mathbb{R}) \cup \mathcal{V}_Y(\mathbb{R}).$$

- *The line $X - Y + 2$ is irreducible. Attention: it is reducible for the usual real topology (take two closed 'half lines' overlapping).*
- *The hyperbola $\mathcal{H}$ is also irreducible. This is a consequence of the next proposition, since the coordinate ring $\mathbb{R}[\mathcal{H}]$ is an integral domain.*

We can now formulate a topological statement on an affine algebraic set as a purely algebraic statement on the coordinate ring! This kind of phenomenon will be encountered all the time in the sequel of the lecture.

Proposition 1.68. *Let $\emptyset \neq \mathcal{X} \subseteq \mathbb{A}^n(K)$ be an affine set. Then the following statements are equivalent:*

(i) $\mathcal{X}$ is irreducible (i.e. $\mathcal{X}$ is a variety).

(ii) The coordinate ring $K[\mathcal{X}]$ is an integral domain.

Definition 1.69. *Let $\mathcal{X} \subseteq \mathbb{A}^n(K)$ be an affine variety (so that its coordinate ring $K[\mathcal{X}]$ is an integral domain).*
Then the function field of $\mathcal{X}$ *is the field of fractions of $K[\mathcal{X}]$. It is denoted $K(\mathcal{X})$.*

The elements in the function field are thus fractions $\frac{f}{g}$ with $f, g \in K[\mathcal{X}]$.
IMPORTANT: We cannot view these fractions inside $\mathrm{Maps}(\mathcal{X}, K)$ because the denominator $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$ may be zero for some $(x_1, \ldots, x_n) \in \mathcal{X}$. So, an element $\frac{f}{g}$ of the function field only gives us a map

$$\mathcal{X} \setminus \mathcal{V}_g(K) \to K, \quad (x_1, \ldots, x_n) \mapsto \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}.$$

It is not everywhere defined. If one introduces a suitable topology, one can see that it is defined on an open set.
We will go more into that when we discuss local vs. global below.

1.8 Morphisms between curves

Definition 1.70. *Let $C_1 = \mathcal{V}_f(K)$ and $C_2 = \mathcal{V}_g(K)$ be affine plane curves. A map $\varphi : C_1 \to C_2$ is a* morphism of curves *if it is given by polynomials in the following sense: there are $\varphi_1, \varphi_2 \in K[C_1]$ such that for all $(x, y) \in C_1$ we have*

$$\varphi(x, y) = (\varphi_1(x, y), \varphi_2(x, y)) \in C_2.$$

We speak of an isomorphism if there is also a morphism $\psi : C_2 \to C_1$ such that $\psi \circ \varphi = \mathrm{id}$ and $\varphi \circ \psi = \mathrm{id}$.

Example 1.71. *Let $f(X, Y) = X^2 + Y^2 - 1$ and $g(X, Y) = X + Y - 1$ be polynomials (say in $\mathbb{R}[X, Y]$). The associated curves $\mathcal{V}_f(\mathbb{R})$ and $\mathcal{V}_g(\mathbb{R})$ are the unit circle and the line through $(0, 1)$ and $(1, 0)$ (of slope -1). Then*

$$\varphi : \mathcal{V}_f(\mathbb{R}) \to \mathcal{V}_g(\mathbb{R}), \quad (x, y) \mapsto (x^2, y^2)$$

is a morphism of curves.

Proposition 1.72. *Let $\varphi : C_1 \to C_2$ be a morphism of curves given by $\varphi_1, \varphi_2 \in K[C_1]$.*
Then the map

$$\varphi^* : K[C_2] \to K[C_1], \quad g \mapsto \varphi^*(g) := g \circ f$$

is a K-algebra homomorphism.
Explicitly, we have $\varphi^*(g)(x, y) = g(\varphi(x, y)) = g(\varphi_1(x, y), \varphi_2(x, y))$.

We also have a converse.

Proposition 1.73. *Let C_1, C_2 be affine plane curves. Let $\psi : K[C_2] \to K[C_1]$ be a K-algebra homomorphism. Put $\varphi_1 := \psi(X + \mathcal{I}_{C_2}) \in K[C_1]$ and $\varphi_2 := \psi(Y + \mathcal{I}_{C_2}) \in K[C_1]$.*
Then the map

$$\varphi : C_1 \to C_2, \quad (x, y) \mapsto (\varphi_1(x, y), \varphi_2(x, y))$$

is well-defined and $\varphi^* = \psi$.

Proof. We must check that $(\varphi_1(x, y), \varphi_2(x, y))$ lies in C_2 whenever (x, y) lie in C_1. For that purpose, let $g \in \mathcal{I}_{C_2}$ be any polynomial in the vanishing ideal of C_2. Note that

$$g(X + \mathcal{I}_{C_2}, Y + \mathcal{I}_{C_2}) = g(X, Y) + \mathcal{I}_{C_2} = 0 + \mathcal{I}_{C_2}.$$

Consequently, we have

$$0 = \psi\big(g(X + \mathcal{I}_{C_2}, Y + \mathcal{I}_{C_2})\big) = g\big(\psi(X + \mathcal{I}_{C_2}), \psi(Y + \mathcal{I}_{C_2})\big) = g\big(\varphi_1, \varphi_2\big) \in K[C_1].$$

Hence,

$$g\big(\varphi_1(x, y), \varphi_2(x, y)\big) = 0 \ \forall (x, y) \in C_1.$$

This implies $(\varphi_1(x, y), \varphi_2(x, y))$ lies in C_2.
It suffices to check the equality $\varphi^* = \psi$ on generators: $X + \mathcal{I}_{C_2}, Y + \mathcal{I}_{C_2} \in K[C_2]$.

$$\varphi^*(X + \mathcal{I}_{C_2})(x, y) = \varphi_1(x, y) = \psi(X + \mathcal{I}_{C_2})$$

and similarly for the other one. □

Now we do the same thing again, but not with the coordinate rings, but their quotient fields, i.e. function fields. In order for the latter to be defined, we will impose that the curves are irreducible.

Definition 1.74. *Let $C_1 = \mathcal{V}_f(K)$ and $C_2 = \mathcal{V}_g(K)$ be irreducible affine plane curves.*
A rational map φ of curves *from C_1 to C_2 is given by rational functions $\varphi_1, \varphi_2 \in K(C_1)$ such that for all $(x, y) \in C_1$ where both φ_1 and φ_2 are defined, we have*

$$\varphi(x, y) = (\varphi_1(x, y), \varphi_2(x, y)) \in C_2.$$

We use the piece of notation $\varphi : C_1 \dashrightarrow C_2$.

Proposition 1.75. *Let $\varphi : C_1 \dashrightarrow C_2$ be a rational map of irreducible affine plane curves given by $\varphi_1, \varphi_2 \in K(C_1)$.*
Then the map

$$\varphi^* : K(C_2) \to K(C_1), \quad g \mapsto \varphi^*(g) = g \circ f$$

is a K-field homomorphism, i.e. a (necessarily injective) field homomorphism that is the identity on K. In other words, we have field extensions

$$K \subset \varphi^*\big(K(C_2)\big) \subseteq K(C_1).$$

The extension $\varphi^*\big(K(C_2)\big) \subseteq K(C_1)$ is finite.
Explicitly, we have $\varphi^*(g)(x, y) = g(\varphi(x, y)) = g(\varphi_1(x, y), \varphi_2(x, y))$.

Also as before, we also have a converse with a similar proof.

Proposition 1.76. *Let C_1, C_2 be irreducible affine plane curves. Let $\psi : K(C_2) \to K(C_1)$ be a K-field homomorphism. Put $\varphi_1 := \psi(X + \mathcal{I}_{C_2}) \in K(C_1)$ and $\varphi_2 := \psi(Y + \mathcal{I}_{C_2}) \in K(C_1)$.*
Then the map

$$\varphi : C_1 \to C_2, \quad (x, y) \mapsto (\varphi_1(x, y), \varphi_2(x, y))$$

is well-defined and $\varphi^* = \psi$.

Example 1.77. *Let F be a field and let E_1 and E_2 be two elliptic curves over F. In line with the approach in these lectures, we see the elliptic curves as affine plane curves, but we equip them with 'a point at infinity' $\mathcal{O}$. Then they have the structure of an abelian group with $\mathcal{O}$ as neutral element.*
An isogenies *between E_1 and E_2 is a morphism of curves*

$$\varphi : E_1 \to E_2$$

such that $\varphi(\mathcal{O}) = \mathcal{O}$. It is known that if φ is not the zero map, then it is surjective with finite kernel and in that case we obtain the injection of function fields

$$\varphi^* : \overline{F}(E_2) \to \overline{F}(E_1).$$

The degree of this field extension is called the degree of the isogeny. *Moreover, the isogeny is called* separable *if the function field extension has this property.*
The most important isogenies are those given by multiplication by an integer $m \in \mathbb{Z}$.

$$[m] : E \to E, \quad P \mapsto mP$$

for any elliptic curve. Its degree is m^2.

2 Local versus global

2.1 Local rings and localisation

Definition 2.1. *Let R be a ring. An ideal $\mathfrak{m} \subsetneq R$ is called* maximal *if there is no ideal $J \subsetneq R$ such that $\mathfrak{m} \subsetneq J \subsetneq R$.*
An ideal $\mathfrak{p} \subsetneq R$ is called prime *if whenever $rs \in \mathfrak{p}$ with $r, s \in R$ one has $r \in \mathfrak{p}$ or $s \in \mathfrak{p}$.*

Lemma 2.2. *Let R be a ring and $I \subsetneq R$ be an ideal.*

(a) I is a prime ideal $\Leftrightarrow$ R/I is an integral domain.

(b) I is a maximal ideal $\Leftrightarrow$ R/I is a field.

(c) If I is maximal, then it is also prime.

Example 2.3. *The prime ideals of $\mathbb{Z}$ (or any other PID) are exactly the ideal (0) and all ideals generated by prime numbers/elements. The maximal ideals are the same, with the exception of (0).*

Lemma 2.4. *Let L/K be a field extension and $\mathcal{X} \subseteq \mathbb{A}^n(L)$ be a subset.*

(a) Every L-point $(a_1, \ldots, a_n) \in \mathcal{X}$ gives rise to the K-algebra homomorphism

$$\mathrm{ev}_{(a_1,\ldots,a_n)} : K[\mathcal{X}] = K[X_1, \ldots, X_n]/\mathcal{I}_{\mathcal{X}} \to L, \quad g(X_1, \ldots, X_n) + \mathcal{I}_{\mathcal{X}} \mapsto g(a_1, \ldots, a_n).$$

(b) If $L = K$, then the kernel of $\mathrm{ev}_{(a_1,\ldots,a_n)}$ is the maximal ideal equal to $(X_1 - a_1, \ldots, X_n - a_n) + \mathcal{I}_{\mathcal{X}}$.

Proof. (a) is clear.
(b) The ideal $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n)$ is clearly maximal because the quotient by it is K. As $(X_1 - a_1, X_2 - a_2, \ldots, X_n - a_n) \subseteq \ker(\mathrm{ev}_{(a_1,\ldots,a_n)})$ it follows that the two are equal (as $\mathrm{ev}_{(a_1,\ldots,a_n)}$ is not the zero-map – look at constants). □

We now determine the maximal ideals of the coordinate ring of any affine algebraic set over an algebraically closed field.

Corollary 2.5. *Let K be an algebraically closed field and $\mathfrak{a} \lhd K[X_1, \ldots, X_n]$ a proper ideal.*

(a) The maximal ideals $\mathfrak{m} \lhd K[X_1, \ldots, X_n]$ are precisely $(X_1 - a_1, \ldots, X_n - a_n)$ for $(a_1, \ldots, a_n) \in K^n$.

(b) The maximal ideals $\mathfrak{m} \lhd K[X_1, \ldots, X_n]$ which contain $\mathfrak{a}$ are precisely $(X_1 - a_1, \ldots, X_n - a_n)$ for $(a_1, \ldots, a_n) \in \mathcal{V}_{\mathfrak{a}}(K)$.

(c) The maximal ideals of $K[X_1, \ldots, X_n]/\mathfrak{a}$ are $(X_1 - a_1 + \mathfrak{a}, \ldots, X_n - a_n + \mathfrak{a})$ for $(a_1, \ldots, a_n) \in \mathcal{V}_{\mathfrak{a}}(K)$.

Definition 2.6. *A ring R is called* local *if it has a single maximal ideal.*

Example 2.7. *(a) Every field K is a local ring, its unique maximal ideal being the zero ideal.*

(b) Let p be a prime number. The ring $\mathbb{Z}/(p^n)$ is a local ring with unique maximal ideal generated by p.

Reason: (p) is a maximal ideal, the quotient being $\mathbb{F}_p$, a field. If $\mathfrak{a} \subsetneq \mathbb{Z}/(p^n)$ is a proper ideal and $x \in \mathfrak{a}$, then $x = py + (p^n)$, as otherwise x would be a unit. This shows that $x \in (p)$, whence $\mathfrak{a} \subseteq (p)$.

(c) $\{\frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z}, \gcd(a, b) = 1, 2 \nmid b\}$ is a local ring (see Example 2.12, where one also finds a geometric example).

Example 2.8. *Let $\mathcal{X} \subseteq \mathbb{A}^n(F)$ be an algebraic variety and $F(\mathcal{X}) = \mathrm{Frac}(F[\mathcal{X}])$ be its function field. Recall that its elements are fractions of functions given by polynomials, and since the denominator may vanish at some points, a rational function is not everywhere defined, in general.*
Let $P \in \mathcal{X}$ be a point. Consider the subring

$$F[\mathcal{X}]_P = \{f \in F(\mathcal{X}) \mid f \text{ is defined at } P\} \subset F(\mathcal{X}).$$

It is a local ring. Its maximal ideal is

$$\{f \in F(\mathcal{X}) \mid f \text{ is defined at } P \text{ and } f(P) = 0\} \subset F(\mathcal{X}).$$

We will encounter this ring later again as the localisation of the coordinate ring $F[\mathcal{X}]$ at P, from which we already borrowed the piece of notation.

We will now introduce/recall the process of localisation of rings and modules, which makes modules/rings local.

Proposition 2.9. *Let R be a ring, $T \subset R$ a multiplicatively closed subset (i.e. for $t_1, t_2 \in T$ we have $t_1 t_2 \in T$) containing 1.*

(a) An equivalence relation on $T \times R$ is defined by

$$(t_1, r_1) \sim (t_2, r_2) \;\Leftrightarrow\; \exists s \in T : \; s(r_1 t_2 - r_2 t_1) = 0.$$

The equivalence class of (t_1, r_1) is denoted by $\frac{r_1}{t_1}$.

(b) The set of equivalence classes $T^{-1}R$ is a ring with respect to

$$+ : T^{-1}R \times T^{-1}R \to T^{-1}R, \;\; \frac{r_1}{t_1} + \frac{r_2}{t_2} = \frac{r_1 t_2 + r_2 t_1}{t_1 t_2}$$

and

$$\cdot : T^{-1}R \times T^{-1}R \to T^{-1}R, \;\; \frac{r_1}{t_1} \cdot \frac{r_2}{t_2} = \frac{r_1 r_2}{t_1 t_2}.$$

Neutral elements are $0 := \frac{0}{1}$ and $1 := \frac{1}{1}$.

(c) The map $\mu : R \to T^{-1}R$, $r \mapsto \frac{r}{1}$, is a ring homomorphism with kernel $\{r \in R \mid \exists t \in T : rt = 0\}$. In particular, if R is an integral domain, then this ring homomorphism is injective.

Proof. Easy checking. □

Note that for an integral domain R, the equivalence relation takes the easier form

$$(t_1, r_1) \sim (t_2, r_2) \;\Leftrightarrow\; r_1 t_2 - r_2 t_1 = 0,$$

provided $0 \notin T$ (if $0 \in T$, then $T^{-1}R$ is always the zero ring, as any element is equivalent to $\frac{0}{1}$).
If R is an integral domain and $1 \in T' \subset T$ is a multiplicatively closed subset, then $T'^{-1}R$ is the subring of $T^{-1}R$ the elements of which can be written as fractions $\frac{r}{t'}$ with denominator $t' \in T'$.

Example 2.10. *Let R be an integral domain. Then $T = R \setminus \{0\}$ is a multiplicatively closed subset. Then $\mathrm{Frac}(R) := T^{-1}R$ is the field of fractions of R.*
Subexamples:

(a) For $R = \mathbb{Z}$, we have $\mathrm{Frac}\,\mathbb{Z} = \mathbb{Q}$.

(b) Let K be a field and $R := K[X_1, \dots, X_n]$. Then $\operatorname{Frac} K[X_1, \dots, X_n] =: K(X_1, \dots, X_n)$ *is the* field of rational functions over K (in n variables). *To be explicit, the elements of $K(X_1, \dots, X_n)$ are equivalence classes written as $\frac{f(X_1,\dots,X_n)}{g(X_1,\dots,X_n)}$ with $f, g \in K[X_1, \dots, X_n]$, $g(X_1, \dots, X_n)$ not the zero-polynomial. The equivalence relation is, of course, the one from the definition; as $K[X_1, \dots, X_n]$ is a UFD, we may represent the class $\frac{f(X_1,\dots,X_n)}{g(X_1,\dots,X_n)}$ as a 'lowest fraction', by dividing numerator and denominator by their greatest common divisor.*

Definition 2.11. *Let R be a ring and $\mathfrak{p} \lhd R$ be a prime ideal. Then $T := R \setminus \mathfrak{p}$ is multiplicatively closed and $1 \in T$ and $0 \notin T$.*

Then $R_\mathfrak{p} := T^{-1}R$ is called the localisation of R at $\mathfrak{p}$.

Example 2.12. *(a) Let R be an integral domain. Then (0) is a prime ideal and $\operatorname{Frac}(R) = R_{(0)}$ (hence the examples above can also be seen as localisations).*

In that case, we also have $T = R \setminus \mathfrak{p} \subseteq R \setminus \{0\}$ and so the localisation $R_\mathfrak{p}$ at any prime ideal $\mathfrak{p}$ is the subring of $R_{(0)} = \operatorname{Frac}(R)$ consisting of fractions $\frac{r}{t}$ that can be written with denominator $t \in T$, i.e. $t \notin \mathfrak{p}$.

(b) Let $R = \mathbb{Z}$ and p a prime number, so that (p) is a prime ideal. Then the localisation of $\mathbb{Z}$ at (p) is $\mathbb{Z}_{(p)}$ and its elements are $\{\frac{r}{t} \in \mathbb{Q} \mid p \nmid t, \gcd(r, t) = 1\}$. Here we used that $\mathbb{Z}$ is an integral domain and so $\mathbb{Z}_{(p)} \subset \operatorname{Frac}(\mathbb{Z}) = \mathbb{Q}$.

(c) Let K be a field and consider $\mathbb{A}^n(K)$. Let $\underline{a} = (a_1, \dots, a_n) \in \mathbb{A}^n(K)$.

Let $\mathfrak{p}$ be the kernel of the ring homomorphism

$$K[X_1, \dots, X_n] \to K, \quad f \mapsto f(a_1, \dots, a_n).$$

Explicitly, $\mathfrak{p} = \{f \in K[X_1, \dots, X_n] \mid f(\underline{a}) = 0\}$. As this homomorphism is clearly surjective (take constant polynomials as preimages), we have that $K[X_1, \dots, X_n]/\mathfrak{p}$ is isomorphic to K, showing that $\mathfrak{p}$ is a maximal (and, hence, a prime) ideal.

The localisation $K[X_1, \dots, X_n]_\mathfrak{p}$ is the subring of $K(X_1, \dots, X_n)$ consisting of elements that can be written as $\frac{f(X_1,\dots,X_n)}{g(X_1,\dots,X_n)}$ with $g(a_1, \dots, a_n) \neq 0$.

This is the same as the set of rational functions $K(X_1, \dots, X_n)$ that are defined in a Zariski-open neighbourhood of a. Namely, let $\frac{f}{g} \in K[X_1, \dots, X_n]_\mathfrak{p}$ so that $g(\underline{a}) \neq 0$. Then the function $\underline{x} \mapsto \frac{f(\underline{x})}{g(\underline{x})}$ is well-defined (i.e. we do not divide by 0) on the Zariski-open set $\mathbb{A}^n(K) \setminus \mathcal{V}_{(g)}(K)$, which contains $\underline{a}$. On the other hand, if for $\frac{f}{g} \in K(X_1, \dots, X_n)$ the function $\underline{x} \mapsto \frac{f(\underline{x})}{g(\underline{x})}$ is well-defined in some Zariski-open neighbourhood of $\underline{a}$, then, in particular, it is well-defined at $\underline{a}$, implying $\frac{f}{g} \in K[X_1, \dots, X_n]_\mathfrak{p}$.

In conclusion, $K[X_1, \dots, X_n]_\mathfrak{p}$ is the ring of rational functions that are well-defined in a Zariski-open neighbourhood of $\underline{a}$.

Corollary 2.13. *Let R be a ring and $\mathfrak{p} \lhd R$ be a prime ideal. Then the localisation $R_\mathfrak{p}$ of R at $\mathfrak{p}$ is a local ring (in fact, its maximal ideal is $T^{-1}\mathfrak{p}$, in the notation of Proposition 2.14).*

Proposition 2.14. *Let R be a ring, $T \subset R$ a multiplicatively closed subset containing 1. Let M be an R-module.*

(a) An equivalence relation on $T \times M$ is defined by

$$(t_1, m_1) \sim (t_2, m_2) \;\Leftrightarrow\; \exists s \in T : \; s(t_1 m_2 - t_2 m_1) = 0.$$

(b) The set of equivalence classes $T^{-1}M$ is an $T^{-1}R$-module with respect to

$$+ : T^{-1}M \times T^{-1}M \to T^{-1}M, \quad \frac{m_1}{t_1} + \frac{m_2}{t_2} = \frac{t_2 m_1 + t_1 m_2}{t_1 t_2}$$

and scalar-multiplication

$$\cdot : T^{-1}R \times T^{-1}M \to T^{-1}M, \quad \frac{r}{t_1} \cdot \frac{m}{t_2} = \frac{rm}{t_1 t_2}.$$

The neutral element is $0 := \frac{0}{1}$.

(c) The map $\mu : M \to T^{-1}M$, $m \mapsto \frac{m}{1}$, is an R-homomorphism with kernel $\{m \in M \mid \exists t \in t : tm = 0\}$.

Remark 2.15. *A concept related to localisation is completion. For example, completing $\mathbb{Q}$ with respect to the 'usual' absolute value, one obtains the real numbers $\mathbb{R}$. Completing with respect to the p-adic absolute value for a prime number p, one obtains the p-adic numbers. Completing a ring of functions at a point, one gets a power series ring, allowing one to consider the Taylor expansion, for example. We won't have the time to look into this at all during these lectures.*

2.2 Singular and non-singular points on a curve

Let $f(X,Y) \in K[X,Y]$ and $a, b \in K$ such that $f(a,b) = 0$. Recall the Taylor expansion of f:

$$\frac{\partial f}{\partial X}|_{(a,b)}(X-a) + \frac{\partial f}{\partial Y}|_{(a,b)}(Y-b) + \text{ terms of higher degree in } (X-a) \text{ and } (Y-b).$$

Definition 2.16. *Let K be a field, $f \in K[X,Y]$ a non-constant irreducible polynomial and $C = \mathcal{V}_{(f)}(K)$ the associated plane curve.*

Let $(a,b) \in C$ be a point. The tangent equation to C at (a,b) *is defined as*

$$T_{C,(a,b)}(X,Y) = \frac{\partial f}{\partial X}|_{(a,b)}(X-a) + \frac{\partial f}{\partial Y}|_{(a,b)}(Y-b) \in K[X,Y].$$

If $T_{C,(a,b)}(X,Y)$ is the zero polynomial, then we call (a,b) a singular point of C.

If (a,b) is non-singular (also called: smooth*), then $\mathcal{V}_{T_{C,(a,b)}}(K)$ is a line (instead of $\mathbb{A}^2(K)$), called the* tangent line to C at (a,b).

A curve all of whose points are non-singular is called non-singular (or smooth).

Example 2.17. *(a) Let $f(X,Y) = Y^2 - X^3 \in K[X,Y]$ with K a field (say, of characteristic 0).*

We have $\frac{\partial f}{\partial X} = -3X^2$ and $\frac{\partial f}{\partial X} = 2Y$. Hence, $(0,0)$ is a singularity and it is the only one. (Draw a sketch.)

This kind of singularity is called a cusp *(Spitze/pointe) for obvious reasons. The tangents to the two branches coincide at the cusp.*

(b) Let $f(X,Y) = Y^2 - X^3 - X^2 \in K[X,Y]$ with K a field (say, of characteristic 0).

We have $\frac{\partial f}{\partial X} = -3X^2 - 2X$ and $\frac{\partial f}{\partial X} = 2Y$. Hence, $(0,0)$ is a singularity and it is the only one. (Draw a sketch.)

This kind of singularity is called an ordinary double point*. The tangents to the two branches are distinct at the ordinary double point.*

We now prove the following theorem, which relates a geometric property (a point on a curve is nonsingular) and an algebraic property (the localisation of the coordinate ring is regular).

Theorem 2.18. *Let K be an algebraically closed field, $f \in K[X,Y]$ a non-constant irreducible polynomial, $C = \mathcal{V}_{(f)}(K)$ the associated plane curve and $K[C] = K[X,Y]/(f(X,Y))$ the coordinate ring. Let $(a,b) \in C$ be a point and $\mathfrak{m} = (X-a+(f), Y-b+(f)) \lhd K[C]$ be the corresponding maximal ideal (see Lemma 2.4).*

Then the following two statements are equivalent:

(i) The point (a,b) is non-singular.

(ii) $K[C]_{\mathfrak{m}}$ is a local ring such that its maximal ideal is principal.

Proof. After a linear variable transformation we may assume $(a,b) = (0,0)$. Then

$$f(X,Y) = \alpha X + \beta Y + \text{ higher terms.}$$

It is a fact (that is not hard to prove using the so-called Nakayama Lemma) that the maximal ideal $\mathfrak{m}K[C]_{\mathfrak{m}}$ of the localised ring $K[C]_{\mathfrak{m}}$ is principal if and only if the $K = K[C]/\mathfrak{m}$-vector space $\mathfrak{m}/\mathfrak{m}^2$ is of dimension 1. Note that $\mathfrak{m}^2$ is generated by $X^2+(f), Y^2+(f), XY+(f)$, so that the K-vector space $\mathfrak{m}/\mathfrak{m}^2$ is generated by $X+(f)$ and $Y+(f)$. Hence, the minimal number of generators is at most 2, but could be 1.

'(i) $\Rightarrow$ (ii)': We assume that $(0,0)$ is not a singular point. Then $\alpha \neq 0$ or $\beta \neq 0$. After possibly exchanging X and Y we may, without loss of generality, assume $\alpha \neq 0$. It follows:

$$X+(f) = \frac{1}{\alpha}\big(-\beta Y - \text{ higher terms} + (f)\big) \equiv -\frac{\beta}{\alpha}Y + (f) \pmod{\mathfrak{m}^2}.$$

So, $Y+(f)$ generates $\mathfrak{m}/\mathfrak{m}^2$ as K-vector space, whence the dimension of this space is 1.

'(ii) $\Rightarrow$ (i)': We now assume that $(0,0)$ is a singular point. Then $\alpha = \beta = 0$. So, $X+(f)$ and $Y+(f)$ are K-linearly independent in $\mathfrak{m}/\mathfrak{m}^2$, whence the K-dimension of $\mathfrak{m}/\mathfrak{m}^2$ is bigger than 1. □

2.3 Local properties, smooth curves and Dedekind rings

Definition 2.19. *As for rings, if $\mathfrak{p} \subset R$ is a prime (or maximal) ideal and M an R-module, then we write $M_{\mathfrak{p}}$ for $T^{-1}M$ with $T = R \setminus \mathfrak{p}$, and call it the* localisation of M at $\mathfrak{p}$.

A property P that a module M may or may not have is called a local property *if*

$$M \text{ has property } P \Leftrightarrow \forall\, \mathfrak{p} \subset R \text{ prime: } M_{\mathfrak{p}} \text{ has property } P.$$

Lemma 2.20. *Let R be a ring and M an R-module. Then being the zero module is a local property. More precisely, the following statements are equivalent:*

(i) M is the zero module.

(ii) For all prime ideals $\mathfrak{p} \lhd R$, the localisation $M_{\mathfrak{p}}$ is the zero module.

(iii) For all maximal ideals $\mathfrak{m} \lhd R$, the localisation $M_{\mathfrak{m}}$ is the zero module.

Proposition 2.21. *Let R be a ring and $\varphi : M \to N$ an R-homomorphism. For a prime ideal $\mathfrak{p} \lhd R$, denote by $\varphi_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ the localisation at $\mathfrak{p}$. Then being injective/surjective/bijective is a local property. More precisely, the following statements are equivalent:*

(i) φ is injective (surjective).

(ii) For all prime ideals $\mathfrak{p} \lhd R$, the localisation $\varphi_{\mathfrak{p}}$ is injective (surjective).

(iii) For all maximal ideals $\mathfrak{m} \lhd R$, the localisation $\varphi_{\mathfrak{m}}$ is injective (surjective).

Proposition 2.22. *Let R be an integral domain. Then being integrally closed is a local property. More precisely, the following statements are equivalent:*

(i) R is integrally closed.

(ii) $R_{\mathfrak{p}}$ is integrally closed for all prime ideals $\mathfrak{p} \lhd R$.

(iii) $R_{\mathfrak{m}}$ is integrally closed for all maximal ideals $\mathfrak{m} \lhd R$.

Recall that by definition, a curve is non-singular (smooth) if it is non-singular at all its points. So, already 'in spirit' smoothness is a local property. But we can make even phrase this in terms as above.

Proposition 2.23. *Let K be an algebraically closed field and $C = \mathcal{V}_f(K)$ be an affine plane curve. Then the following statements are equivalent:*

(i) C is smooth.

(ii) For all maximal ideals $\mathfrak{m}$ in the coordinate ring $K[C]$, the maximal ideal of the localisation $K[C]_{\mathfrak{m}}$ is principal.

Proof. This is a combination of Theorem 2.18 with the description of the maximal ideals of $K[C]$ from Corollary 2.5. □

Definition 2.24. *A ring R is said to be of* Krull dimension 1 *if there is a maximal ideal $\mathfrak{m}$ which strictly contains another prime ideal $\mathfrak{p} \subsetneq \mathfrak{m}$, but there are no three prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$.*

Example 2.25. *(a) The Krull dimension of $\mathbb{Z}$ and of any other principal ideal domain (such as $K[X]$ with a field K) is 1 because the prime ideals are exactly the zero ideal and all maximal ideals, so that every maximal ideal strictly contains exactly one other prime ideal, namely the zero ideal.*

(b) The main property is the following. If $R \subseteq S$ is an integral ring extension and R is of Krull dimension 1, then so is S.

(c) The main property implies that the ring of integers $\mathbb{Z}_F$ of a number field F and all orders in it are of Krull dimension 1.

(d) An important lemma in the theory of plane curves states that the coordinate ring of a plane curve is an integral extension of a polynomial ring in one variable. Hence, the coordinate ring of a plane curve is of Krull dimension 1.

Proposition 2.26. *Let R be a local Noetherian ring with maximal ideal $\mathfrak{m}$ of Krull dimension 1. Then the following statements are equivalent:*

(i) R is an integrally closed integral domain.

(ii) R is regular, i.e. $\mathfrak{m}$ is a principal ideal (equivalently, $\mathfrak{m}/\mathfrak{m}^2$ can be generated by one element as $R/\mathfrak{m}$-vector space).

(iii) R is a principal ideal domain.

A ring satisfying these conditions is also called regular.

In this case, one has the following very simple description.

Proposition 2.27. *Let R be a regular local ring as in the previous proposition.*

(a) There is $x \in R$ such that all non-zero ideals are of the form (x^n) for some $n \in \mathbb{N}$.

(b) Every non-zero $r \in R$ can be uniquely written as ux^n with $u \in R^\times$ and $n \in \mathbb{N}$.

Definition 2.28. *A Noetherian integrally closed integral domain of Krull dimension* 1 *is called a* Dedekind ring.

We can now conclude from our previous work the following local characterisation of Dedekind rings.

Proposition 2.29. *Let R be a Noetherian integral domain of Krull dimension* 1*. Then the following assertions are equivalent:*

(i) R is a Dedekind ring.

(ii) R is integrally closed.

(iii) $R_\mathfrak{m}$ is integrally closed for all maximal ideals $\mathfrak{m} \lhd R$.

(iv) $R_\mathfrak{m}$ is regular, i.e. $\mathfrak{m}R$ is a principal ideal, for all maximal ideals $\mathfrak{m} \lhd R$.

(v) $R_\mathfrak{m}$ is a principal ideal domain for all maximal ideals $\mathfrak{m} \lhd R$.

We now state and prove our main theorem about coordinate rings of plane curves. It again relates a geometric statement (smoothness of a curve) and an algebraic statement (coordinate ring is Dedekind).

Theorem 2.30. *Let K be an algebraically closed field, $f \in K[X,Y]$ a non-constant irreducible polynomial, $C = \mathcal{V}_{(f)}(K)$ the associated plane curve and $K[C] = K[X,Y]/(f(X,Y))$ the coordinate ring. Then the following two statements are equivalent:*

(i) The curve C is smooth.

(ii) $K[C]$ is a Dedekind ring.

Proof of Theorem 2.30. This is just a combination of Proposition 2.23 and Proposition 2.29. □

Example 2.31. *Let K be a field. Let $g(X) \in K[X]$ be a polynomial and consider the affine plane curve E defined by $f(X,Y) = Y^2 - f(X) \in K[X,Y]$. We compute the singular points of this curve.*
Let (x_0, y_0) be a point on that curve. Then the tangent line to E at (x_0, y_0) is given by the equation

$$T_{E,(x_0,y_0)}(X,Y) = \frac{\partial f}{\partial X}|_{(x_0,y_0)}(X - x_0) + \frac{\partial f}{\partial Y}|_{(x_0,y_0)}(Y - y_0) = g'(x_0)(X - x_0) + 2y_0(Y - y_0).$$

It is the zero equation if and only if $y_0 = 0$ and $g'(x_0) = 0$. Note that $y_0 = 0$ implies $g(x_0) = 0$.
We conclude: the point (x_0, y_0) is a singular point if and only if $y_0 = 0$ and $(X - x_0)^2$ divides $g(X)$.
This means: E is smooth if and only if the polynomial $g(X)$ does not have any multiple root. By properties of the discriminant of $g(X)$, this is the case if and only if the discriminant of $g(X)$ is non-zero.
Recall that the discriminant of $g(X) = X^3 + aX + b \in K[X]$ equals $-4a^3 - 27b^2$. This explains the condition one finds in the definition of elliptic curves.

2.4 Ideals in Dedekind rings

Definition 2.32. *Let R be an integral domain and $K = \mathrm{Frac}(R)$.*

(a) An R-submodule $I \leq K$ is called a fractional ideal of R *(or:* fractional R-ideal*) if*

- $I \neq (0)$ *and*
- *there is $x \in K^\times$ such that $xI \subseteq R$.*

Note that x can always be chosen in $R \setminus \{0\}$. Note also that xI is an ideal of R (in the usual sense).

(b) A fractional R-ideal I is called an integral ideal *if $I \subseteq R$.*

Note that for a subset $(0) \neq I \subset K$, one trivially has:

$$I \trianglelefteq R \text{ is an ideal of } R \text{ in the usual sense} \Leftrightarrow I \text{ is an integral fractional } R\text{-ideal.}$$

(c) A fractional R-ideal I is called principal *if there is $x \in K^\times$ such that $I = Rx$.*

(d) Let I, J be fractional R-ideals. The ideal quotient *of I by J is defined as*

$$I : J = (I : J) = \{x \in K \mid xJ \subseteq I\}.$$

(e) The inverse ideal *of the fractional R-ideal I is defined as*

$$I^{-1} := (R : I) = \{x \in K \mid xI \subseteq R\}.$$

(f) The multiplier ring *of the fractional R-ideal I is defined as*

$$r(I) := (I : I) = \{x \in K \mid xI \subseteq I\}.$$

Example 2.33. *The fractional ideals of $\mathbb{Z}$ are all of the form $I = \frac{a}{b}\mathbb{Z}$ with $a, b \in \mathbb{Z} \setminus \{0\}$. Hence, all fractional $\mathbb{Z}$-ideals are principal.*

It is clear that $\frac{a}{b}\mathbb{Z}$ is a fractional ideal. Conversely, let I be a fractional ideal such that bI is an ideal of $\mathbb{Z}$, whence $bI = (a) = a\mathbb{Z}$, so that $I = \frac{a}{b}\mathbb{Z}$.

Let $I = \frac{a}{b}\mathbb{Z}$ and $J = \frac{c}{d}\mathbb{Z}$, then

$$(I : J) = \{x \in \mathbb{Q} \mid x\frac{c}{d}\mathbb{Z} \subseteq \frac{a}{b}\mathbb{Z}\} = \{x \in \mathbb{Q} \mid x \in \frac{ad}{bc}\mathbb{Z}\} = \frac{ad}{bc}\mathbb{Z}.$$

In particular, $I^{-1} = \frac{b}{a}\mathbb{Z}$ and $II^{-1} = \mathbb{Z}$ (because, clearly $\subseteq$ and $1 \in II^{-1}$).

The next three lemmas are simple exercises.

Lemma 2.34. *Let R be an integral domain and $K = \mathrm{Frac}(R)$. Let $I, J \subset K$ be fractional R-ideals. Then the following sets are fractional R-ideals: $I + J = \{x + y \mid x \in I, y \in J\}$, $IJ = \{\sum_{i=1}^{n} x_i y_j \mid n \in \mathbb{N}, x_1, \ldots, x_n \in I, y_1, \ldots, y_n \in J\}$, $I^n = \underbrace{I \cdot I \cdot \ldots \cdot I}_{n \text{ times}}$, $I \cap J$, $(I : J)$.*

Lemma 2.35. *Let R be an integral domain and $H, I, J \subset K$ fractional R-ideals. Then the following properties hold:*

(a) $IJ \subseteq I \cap J$ (assume here that I and J are integral ideals),

(b) $H + (I + J) = (H + I) + J = H + I + J$,

(c) $H(IJ) = (HI)J$,

(d) $H(I+J) = HI + HJ$.

Lemma 2.36. *Let R be an integral domain and $I, J \trianglelefteq R$ be ideals (in the usual sense). If $I + J = R$, then we call I and J* coprime ideals*.*
Suppose now that I and J are coprime. Then the following statements hold:

(a) I^n *and* J^m *are coprime for all* $n, m \in \mathbb{N}$.

(b) $I \cap J = IJ$.

(c) $R/(IJ) \cong R/I \times R/J$ *(Chinese Remainder Theorem).*

(d) If $IJ = H^n$ *for some* $n \in \mathbb{N}$*, then* $I = (I+H)^n$, $J = (J+H)^n$ *and* $(I+H)(J+H) = H$.
In words: If an ideal is an n-th power, then so is each of its coprime factors.

Proposition 2.37. *Let R be a Noetherian integral domain, $K = \mathrm{Frac}(R)$ and $(0) \neq I \subset K$ a subset. Then the following two statements are equivalent:*

(i) I is a fractional R-ideal.

(ii) I is a finitely generated R-submodule of K (this is the definition in Neukirch's book).

Proof. '(i)⇒(ii)': By definition, there is $r \in R \setminus \{0\}$ such that $rI \subseteq R$, hence, rI is an ideal of R in the usual sense. As R is Noetherian, rI is finitely generated, say by $a_1, \ldots, a_n$. Then I is finitely generated as R-submodule of K by $\frac{a_1}{r}, \ldots, \frac{a_n}{r}$.
'(ii)⇒(i)': Suppose I is generated as R-submodule of K by $\frac{a_1}{r_1}, \ldots, \frac{a_n}{r_n}$. Then $r = r_1 \cdot \ldots \cdot r_n$ is such that $rI \subseteq R$. □

This proposition also shows us how we must think about fractional R-ideals, namely, just as R-linear combinations of a given set of fractions $\frac{a_1}{r_1}, \ldots, \frac{a_n}{r_n}$ (where we may choose a common denominator).

Definition 2.38. *Let R be an integral domain and $K = \mathrm{Frac}(R)$. A fractional R-ideal I is called an* invertible R-ideal *if there is a fractional R-ideal J such that $IJ = R$.*

Note that the term 'invertible R-ideal' applies only to fractional R-ideals (which may, of course, be integral).

Lemma 2.39. *Let R be an integral domain, $K = \mathrm{Frac}(R)$ and I a fractional R-ideal. Then the following statements hold:*

(a) $II^{-1} \subseteq R$.

(b) I is invertible $\Leftrightarrow II^{-1} = R$.

(c) Let J be an invertible R-ideal. Then $(I : J) = IJ^{-1}$.

(d) If $0 \neq i \in I$ *such that* $i^{-1} \in I^{-1}$*, then* $I = (i)$.

Corollary 2.40. *Let R be an integral domain. The set $\mathcal{I}(R)$ of invertible fractional R-ideals forms an abelian group with respect to multiplication of ideals, with R being the neutral element, and the inverse of $I \in \mathcal{I}(R)$ being I^{-1}.*
The set $\mathcal{P}(R) := \{xR \mid x \in K^\times\}$ of principal fractional R-ideals forms a subgroup of $\mathcal{I}(R)$.

Proof. This just summarises what we have seen. That $\mathcal{P}(R)$ is a subgroup is clear. □

Definition 2.41. *Let R be an integral domain. One calls $\mathcal{I}(R)$ the* group of invertible R-ideals *and $\mathcal{P}(R)$ the* subgroup of principal invertible R-ideals.

The quotient group $\mathrm{Pic}(R) := \mathcal{I}(R)/\mathcal{P}(R)$ is called the Picard group of R.

If K is a number field and $\mathbb{Z}_K$ its ring of integers, one also writes $\mathrm{CL}(K) := \mathrm{Pic}(\mathbb{Z}_K)$, and calls it the ideal class group of K.

Corollary 2.42. *Let R be an integral domain and $K = \mathrm{Frac}(R)$. Then we have the exact sequence of abelian groups*

$$1 \to R^\times \to K^\times \xrightarrow{f} \mathcal{I}(R) \xrightarrow{\mathrm{proj}} \mathrm{Pic}(R) \to 1,$$

where $f(x)$ is the principal fractional R-ideal xR.

Proof. The exactness is trivially checked. Note, in particular, that $xR = R$ (the neutral element in the group) if and only if $x \in R^\times$. □

Corollary 2.43. *Let R be a principal ideal domain. Then $\mathrm{Pic}(R) = \{R\}$ (the group with one element).*

Proof. This is the case by definition: that every ideal is principal implies that every fractional ideal is principal, i.e. $\mathcal{I}(R) = \mathcal{P}(R)$, whence their quotient is the group with one element. □

Example 2.44. *The groups $\mathrm{CL}(\mathbb{Q}) = \mathrm{Pic}(\mathbb{Z})$ and $\mathrm{Pic}(K[X])$ (for K a field) are trivial.*

The next statement says that being an invertible ideal is a local property.

Theorem 2.45. *Let R be a Noetherian integral domain and I a fractional R-ideal. Then the following statements are equivalent:*

(i) I is invertible.

(ii) $I_\mathfrak{m}$ is a principal fractional $R_\mathfrak{m}$-ideal for all maximal ideals $\mathfrak{m} \lhd R$.

Corollary 2.46. *Let R be a Dedekind ring. Then any fractional R-ideal is invertible.*

Proof. By Proposition 2.29 we know that $R_\mathfrak{m}$ is a principal ideal domain for all maximal ideals $\mathfrak{m} \lhd R$. Hence, given any fractional R-ideal I, we have that $I_\mathfrak{m}$ is principal for all $\mathfrak{m}$, which by Theorem 2.45 implies that I is invertible. □

Remark 2.47. *Corollary 2.46 applies in particular to rings of integers $\mathbb{Z}_F$ of number fields F, as well as to coordinate rings of smooth curves.*

However, it fails for orders $\mathcal{O} \subsetneq \mathbb{Z}_F$ (for example, in general, it fails for equation orders). It also fails for coordinate rings of curves that have singular points.

The meaning of the next theorem is that any non-zero invertible ideal $I \lhd R$ is uniquely determined by all its localisations $I_\mathfrak{p}$ (at the non-zero prime ideals of R).

Theorem 2.48. *Let R be a Noetherian integral domain of Krull dimension 1. Then the map*

$$\Phi : \mathcal{I}(R) \to \bigoplus_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} \mathcal{P}(R_\mathfrak{p}), \quad I \mapsto (\ldots, I_\mathfrak{p}, \ldots),$$

is an isomorphism of abelian groups.

Lemma 2.49. *Let R be a regular local ring of Krull dimension 1 and let $\mathfrak{p}$ be its maximal ideal. Recall from Proposition 2.27 that then there is $x \in R$ such that all fractional ideals of R are of the form $(x)^n = \mathfrak{p}^n$ for some $n \in \mathbb{Z}$. Moreover, the map*

$$\mathbb{Z} \to \mathcal{I}(R), \quad n \mapsto \mathfrak{p}^n$$

is an isomorphism of abelian groups.

Definition 2.50. *Let R be a Dedekind ring and I be an invertible R-ideal. For a maximal ideal $\mathfrak{p} \lhd R$, by Lemma 2.49, there is a unique integer $n \geq 0$ such that $I_\mathfrak{p} = (\mathfrak{p}R_\mathfrak{p})^n$. We write $\mathrm{ord}_\mathfrak{p}(I) := n$.*

Now we can prove unique ideal factorisation.

Theorem 2.51. *Let R be a Dedekind ring. The map*

$$\Phi : \mathcal{I}(R) \to \bigoplus_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} \mathbb{Z}, \quad I \mapsto (\ldots, \mathrm{ord}_\mathfrak{p}(I), \ldots)$$

is an isomorphism of abelian groups. Every $I \in \mathcal{I}(R)$ can be uniquely written as

$$I = \prod_{0 \neq \mathfrak{p} \lhd R \text{ prime ideal}} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(I)}$$

(note that the product is finite).

Remark 2.52. *Theorem 2.51 is a generalisation of unique factorisation in a principal ideal domain.*

3 Geometry of numbers

This part was partly written by Sara Arias-de-Reyna.

3.1 Introduction

Recall (cf. Corollary 2.42) that, for any integral domain S, we have the following exact sequence

$$1 \longrightarrow S^\times \longrightarrow F^\times \xrightarrow{f} \mathcal{I}(S) \xrightarrow{\mathrm{proj}} \mathrm{Pic}(S) \longrightarrow 1$$

where:

- F is the field of fractions of S.
- $\mathcal{I}(S)$ is the group of invertible ideals of S.
- $\mathrm{Pic}(S)$ is the Picard group of S, that is to say, the quotient of $\mathcal{I}(S)$ modulo the group $\mathcal{P}(S)$ of principal fractionals ideals of S.
- $f : F^\times \to \mathcal{I}(S)$ maps an element $x \in F$ to the principal fractional ideal xS.
- $\mathrm{proj} : \mathcal{I}(S) \to \mathcal{I}(S)/\mathcal{P}(S) = \mathrm{Pic}(S)$ is the projection.

We want to study this exact sequence in the particular case where $S = \mathbb{Z}_F$ is the ring of integers of a number field F. Since $\mathbb{Z}_F$ is a Dedekind domain, all fractional ideals are invertible (see Corollary 2.46).

Hence $\mathcal{I}(\mathbb{Z}_F)$ is the set of all fractional ideals. Recall also that we denote $\mathrm{Pic}(\mathbb{Z}_F) = \mathrm{CL}(F)$ and call it the *class group* of F. The exact sequence boils down to:

$$1 \longrightarrow \mathbb{Z}_F^\times \longrightarrow F^\times \xrightarrow{f} \mathcal{I}(\mathbb{Z}_F) \xrightarrow{\text{proj}} \mathrm{CL}(F) \longrightarrow 1 \tag{3.1}$$

The group $\mathrm{CL}(F)$ measures the failure of $\mathbb{Z}_F$ to be a principal ideal domain. More precisely, if $\mathrm{CL}(F)$ has just one element, then the map $f : F^\times \to \mathcal{I}(S)$ is surjective, so that each fractional ideal can be expressed as xS for some $x \in F^\times$. In other words, every fractional ideal is principal. On the other hand, the greater $\mathrm{CL}(F)$ is, the further is f from being surjective, meaning there will be "many" fractional ideals which are not principal.

One of the fundamental results that we will prove is that $\mathrm{CL}(F)$ is finite (hence, although $\mathbb{Z}_F$ is not a principal ideal domain, it is also "not too far" from it). Another important result will be that $\mathbb{Z}_F^\times$ is finitely generated.

The tool that we will use to study the exact sequence (3.1) is called Geometry of Numbers. This consists of viewing rings of integers as special subsets of $\mathbb{S}^n$ (namely lattices), and using some analytic tools (computing volumes) to obtain results concerning $\mathbb{Z}_F$.

3.2 Lattices

Definition 3.1. *A* lattice *in $\mathbb{R}^n$ is a $\mathbb{Z}$-module generated by n linearly independent vectors. A* basis *of a lattice $H \subset \mathbb{R}^n$ is a basis of H as a $\mathbb{Z}$-module.*

Note that a basis of a lattice H consists of n linearly independent vectors of $\mathbb{R}^n$, so in particular is a basis of $\mathbb{R}^n$ as $\mathbb{R}$-vector space.

Definition 3.2. *A* half-open parallelotope *(resp.* closed parallelotope*) is a subset of $\mathbb{R}^n$ of the form*

$$P := \{v \in \mathbb{R}^n : v = \sum_{i=1}^m a_i v_i \text{ with } 0 \le a_i < 1 \text{ for all } i\},$$

$$\left(\text{resp. } P := \{v \in \mathbb{R}^n : v = \sum_{i=1}^m a_i v_i \text{ with } 0 \le a_i \le 1 \text{ for all } i\}\right)$$

where $v_1, \ldots, v_m \in \mathbb{R}^n$ are linearly independent. We say that P is the half-open parallelotope determined by $v_1, \ldots, v_m$ *(resp.* closed parallelotope determined by $v_1, \ldots, v_m$*)*

Let $H \subset \mathbb{R}^n$ be a lattice, and $\mathcal{U} = \{u_1, \ldots, u_n\}$ a basis of H. We will say that the (half-open) parallelotope P determined by $\mathcal{U}$ is a fundamental domain for H.

We will denote by μ the Lebesgue measure on $\mathbb{R}^n$. We will not recall here its definition, but just one very important property: it is invariant under translation; that is, for all measurable sets A and all vectors $v \in \mathbb{R}^n$, the set $A + v := \{w + v : w \in A\}$ is measurable and we have

$$\mu(A) = \mu(A + v).$$

Moreover the measure is normalized so that the measure of the standard cube $\{\sum_{i=1}^n \lambda_i e_i : 0 \le \lambda_i \le 1\}$ is equal to 1.

Remark 3.3. *(a) Fundamental domains of a lattice are not unique.*

(b) Let P be the parallelotope defined by n linearly independent vectors $v_1, \ldots, v_n \in \mathbb{R}^n$, where each $v_i = \sum_{j=1}^n a_{ij} e_j$. Then $\mu(P) = |\det((a_{ij})_{1 \le i,j \le n})|$.

(c) Let $H \subset \mathbb{R}^n$ be a lattice, P, P' fundamental domains for H. Then $\mu(P) = \mu(P')$.

Definition 3.4. *Let $H \subset \mathbb{R}^n$ be a lattice. We define the* volume *of H as*

$$v(H) := \mu(P),$$

for some fundamental domain P of H.

Definition 3.5. *A subgroup $H \subset \mathbb{R}^n$ is called* discrete *if, for any compact subset $K \subset \mathbb{R}^n$, $H \cap K$ is a finite set.*

Remark 3.6. *Let $H \subset \mathbb{R}^n$ be a discrete subgroup of $\mathbb{R}^n$. The H is a lattice if and only if H is generated by n linearly independent vectors.*

Now we will state the fundamental result of this section. The idea is the following: given a lattice H, if a measurable set $S \subset \mathbb{R}^n$ is big enough (with respecto to μ), no matter what it looks like, it must contain two elements which are "equivalent modulo H", that is to say, two different elements $v_1, v_2 \in S$ with $v_1 - v_2 \in H$.

Theorem 3.7 (Minkowski)**.** *Let $H \subset \mathbb{R}^n$ be a lattice and $S \subset \mathbb{R}^n$ be a measurable subset of $\mathbb{R}^n$ satisfying $\mu(S) > v(H)$. Then there exist $v_1, v_2 \in S$ different elements with $v_1 - v_2 \in H$.*

We will use a particular case of this theorem, when S has some special properties.

Definition 3.8. *Let $S \subset \mathbb{R}^n$.*

- *S is* centrally symmetric *if, for all $v \in S$, $-v \in S$.*
- *S is* convex *if, for all $v_1, v_2 \in S$, for all $\lambda \in [0,1]$, $\lambda v_1 + (1-\lambda)v_2 \in S$.*

Corollary 3.9. *Let $H \subset \mathbb{R}^n$ be a lattice and $S \subset \mathbb{R}^n$ be a centrally symmetric, convex, measurable set such that $\mu(S) > 2^n v(H)$. Then $S \cap (H \setminus \{0\}) \neq \emptyset$.*

3.3 Number rings as lattices and finiteness of the class group

In this section we want to study number fields of degree n by embedding them into $\mathbb{R}^n$, in such a way that the ring of integers corresponds to a lattice.

Let $F \subset \overline{\mathbb{Q}} \subset \mathbb{C}$ be a number field of degree $[F : \mathbb{Q}] = n$, where $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid z \text{ is algebraic over } \mathbb{Q}\}$ is the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Let us enumerate the n field homomorphisms in $\mathrm{Hom}_{\mathbb{Q}}^{\text{field}}(F, \mathbb{C})$ in the following way:

- Let $\sigma_1, \ldots, \sigma_{r_1}$ be all field homomorphisms $F \to \mathbb{C}$ with image contained in $\mathbb{R}$.
- Let us enumerate the r_2 pairs $\{\sigma, \alpha \circ \sigma\}$ and, for each pair, choose one of the two homomorphisms. The chosen homomorphism of the i-th pair ($1 \leq i \leq r_2$) will be σ_{r_1+i}, the other one will be $\sigma_{r_1+r_2+i}$.

Note that $n = [F : \mathbb{Q}] = r_1 + 2r_2$.

Now we can define a ring homomorphism

$$\begin{aligned} \Phi_1 : F &\to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ x &\mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)) \end{aligned}$$

Definition 3.10. *Define the injective group homomorphism*

$$\Phi : F \to \mathbb{R}^{r_1} \times \mathbb{R}^{2r_2}$$
$$x \mapsto (\sigma_1(x), \dots, \sigma_{r_1}(x), \mathrm{Re}(\sigma_{r_1+1}(x)), \mathrm{Im}(\sigma_{r_1+1}(x)) \dots, \mathrm{Re}(\sigma_{r_1+r_2}(x)), \mathrm{Im}(\sigma_{r_1+r_2}(x))).$$

Proposition 3.11. *Let $M \subset F$ be a free $\mathbb{Z}$-module of rank n, say with basis $\{x_1, \dots, x_n\}$. Then*

(a) $\Phi(M)$ is a lattice in $\mathbb{R}^n$.

(b) Let $D = (\sigma_i(x_j))_{1 \le i,j \le n}$. Then $v(\Phi(M)) = 2^{-r_2} |\det D| = 2^{-r_2} \sqrt{|\operatorname{disc}(x_1, \dots, x_n)|}$.

Definition 3.12. *(a) Let $\mathfrak{a} \subset \mathbb{Z}_F$ be a nonzero integral ideal. We define the* norm *of $\mathfrak{a}$ as $N(\mathfrak{a}) = [\mathbb{Z}_F : \mathfrak{a}]$.*

(b) Let $I \subset F$ be a fractional ideal. We define the norm *of I as $N(I) = N(xI)/|N_{F/\mathbb{Q}}(x)|$, where $x \in \mathbb{Z}_F$ is some element different from zero such that xI is an integral ideal.*

Corollary 3.13. *Let $F/\mathbb{Q}$ be a number field of degre $n = r_1 + 2r_2$ and $\mathfrak{a}$ an integral ideal of $\mathbb{Z}_F$. Then we have that $\Phi(\mathbb{Z}_F)$, $\Phi(\mathfrak{a})$ are lattices of $\mathbb{R}^n$ and*

$$v(\Phi(\mathbb{Z}_F)) = 2^{-r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_F)|}, \quad v(\Phi(\mathfrak{a})) = 2^{-r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_F)|} N(\mathfrak{a}).$$

Proof. We know that both $\mathbb{Z}_F$ and $\mathfrak{a}$ are free $\mathbb{Z}$-module of rank n. The formula for the volume of $\Phi(\mathbb{Z}_F)$ follows directly from the definition of $\mathrm{disc}(\mathbb{Z}_F)$; the formula for the volume of $\Phi(\mathfrak{a})$ follows from Proposition 1.58. □

Proposition 3.14. *Let $\mathfrak{a} \subset \mathbb{Z}_F$ be a nonzero integral ideal. There exists $a \in \mathfrak{a}$ different from zero such that*

$$|N_{F/\mathbb{Q}}(a)| \le \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_F)|} N(\mathfrak{a}).$$

We do not give the proof, but state that the key ingredient in it are Corollaries 3.9 and 3.13.

Theorem 3.15 (Dirichlet)**.** *Let F be a number field. The class group $\mathrm{CL}(F) = \mathcal{I}(\mathbb{Z}_F)/\mathcal{P}(\mathbb{Z}_F)$ is finite.*

Before proceeding to the proof, let us establish a technical lemma.

Lemma 3.16. *Let $C \in \mathrm{CL}(F)$ be a class of ideals. Then there exists a nonzero integral ideal $\mathfrak{a}$ of $\mathbb{Z}_F$ which belongs to C and satisfies*

$$N(\mathfrak{a}) \le \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_F)|}.$$

Proof. Let I be a fractional ideal in C. Then $I^{-1} = \{a \in \mathbb{Z}_F : aI \subset \mathbb{Z}_F\}$ is also a fractional ideal. Therefore there exists a nonzero $x \in F$ such that $\mathfrak{b} = xI^{-1}$ is a nonzero integral ideal. We can apply Proposition 3.14 to the ideal $\mathfrak{b}$; there exists $b \in \mathfrak{b}$ nonzero such that

$$|N_{F/\mathbb{Q}}(b)| \le \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_F)|} N(\mathfrak{b}) = \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_F)|} |N_{F/\mathbb{Q}}(x)| N(I)^{-1}.$$

The ideal $\mathfrak{a} = \frac{b}{x} I$ belongs to the class C, is contained in $\mathbb{Z}_F$ and furthermore

$$N(\mathfrak{a}) = \frac{|N_{F/\mathbb{Q}}(b)|}{|N_{F/\mathbb{Q}}(x)|} N(I) \le \left(\frac{2}{\pi}\right)^{r_2} \sqrt{|\mathrm{disc}(\mathbb{Z}_F)|}.$$

□

Proof of Theorem 3.15. Since every class $C \in \mathrm{CL}(F)$ contains a nonzero integral ideal of norm smaller than $\left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(\mathbb{Z}_F)|}$ (because of Lemma 3.16), it suffices to prove that, for any $M \in \mathbb{N}$, there are only finitely many integral ideals of norm smaller than M. First of all, note that it suffices to see that there are only finitely many prime integral ideals of norm smaller than M; indeed if $\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$ is a factorisation of $\mathfrak{a}$ into a product of prime ideals, then $N(\mathfrak{a}) = \prod_{i=1}^{r} N(\mathfrak{p}_i)^{e_i}$, so if $N(\mathfrak{a})$ is smaller than M, the only prime ideals that can occur in the factorisation of $\mathfrak{a}$ are those with norm smaller than M, and the exponents e_i that can occur must also be smaller than M.

Assume now that $\mathfrak{p}$ is a prime integral ideal of norm smaller than M, say m. Then $\overline{1} \in \mathbb{Z}_F/\mathfrak{p}$ satisfies that $m \cdot \overline{1} = 0 \in \mathbb{Z}_F/\mathfrak{p}$, thus $m \in \mathfrak{p}$. But we know that that there are only a finite number of maximal ideals of $\mathbb{Z}_K$ containing a given ideal I. In particular, for $I = (m)$, we get that there are only finitely many prime ideals $\mathfrak{p}$ of $\mathbb{Z}_F$ of norm m. □

Remark 3.17. *(a) Let F be a number field. Then $\mathrm{CL}(F)$ is generated by the classes of the prime ideals $\mathfrak{p} \in \mathcal{I}(\mathbb{Z}_F)$ such that $N(\mathfrak{p}) \leq \left(\frac{2}{\pi}\right)^{r_2}\sqrt{|\mathrm{disc}(\mathbb{Z}_F)|}$. This allows one to compute explicitly the class group of a given number field, provided one knows how to compute the prime ideals of given norm.*

(b) There are better bounds. For instance, one can show that $\mathrm{CL}(F)$ is generated by the classes of the prime ideals $\mathfrak{p} \in \mathcal{I}(\mathbb{Z}_F)$ such that $N(\mathfrak{p}) \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}\sqrt{|\mathrm{disc}(\mathbb{Z}_F)|}$.

3.4 Dirichlet's Unit Theorem

The aim of this section is to prove the following result:

Theorem 3.18 (Dirichlet)**.** *Let F be a number field of degree $n = r_1 + 2r_2$ as above. Then there is a group isomorphism*

$$\Psi : \mathbb{Z}_F^\times \simeq \mu_F \times \mathbb{Z}^{r_1+r_2-1},$$

between the (multiplicative) group of units of $\mathbb{Z}_F$ and the direct product of the finite (multiplicative) subgroup μ_F of $\mathbb{Z}_F^\times$, consisting of all roots of unity contained in F, and the (additive) group $\mathbb{Z}^{r_1+r_2-1}$.

Remark 3.19. *More precisely, there exist $\xi_1, \ldots, \xi_{r_1+r_2-1} \in \mathbb{Z}_F^\times$ such that every element $u \in \mathbb{Z}_F^\times$ can be written in a unique way as*

$$u = \mu \cdot \xi_1^{n_1} \cdot \cdots \cdot \xi_{r_1+r_2-1}^{n_{r_1+r_2-1}}$$

for some root of unity $\mu \in F$ and some tuple $(n_1, \ldots, n_{r_1+r_2-1}) \in \mathbb{Z}^{r_1+r_2-1}$.

Such elements are called a fundamental system of units.

Definition 3.20. *Let F be a number field of degree $n = r_1 + 2r_2$. We define the* logarithmic embedding *as the group morphism*

$$\begin{aligned} \Phi_{\log} : F^\times &\to \mathbb{R}^{r_1+r_2} \\ a &\mapsto (\log|\sigma_1(a)|, \ldots, \log|\sigma_{r_1+r_2}(a)|). \end{aligned}$$

Proposition 3.21. *The kernel of $\Phi_{\log}|_{\mathbb{Z}_F^\times}$ is a finite group, consisting of the roots of unity contained in $\mathbb{Z}_F$.*

One uses Corollary 3.9 to prove the following proposition, which is the final step in the proof of Dirichlet's Unit Theorem.

Proposition 3.22. *We have that $\Phi_{\log}(\mathbb{Z}_F^\times)$ is a discrete subgroup of rank equal to $r_1 + r_2 - 1$.*

4 Analytic aspects

A complete treatment of these topics (with the exception of the effective versions of Chebotarev below) can be found in [Neu99, Ch. 7].

Proposition 4.1. *(a) The* Riemann zeta-function *is defined as*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ for } s \in \mathbb{C} \text{ s.t. } \Re(s) > 1$$

and satisfies the Euler product

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}.$$

It has a simple pole at $s = 1$.

(b) Let $m \in \mathbb{Z}_{\geq 1}$ and $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character (i.e. a group homomorphism). The Dirichlet L-function *is defined as*

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \text{ for } s \in \mathbb{C} \text{ s.t. } \Re(s) > 1$$

and satisfies the Euler product

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-\chi(p)p^{-s}}.$$

(c) Let F be a number field. The Dedekind zeta-function of F *is defined as*

$$\zeta_F(s) = \sum_{0 \neq \mathfrak{a} \subseteq \mathbb{Z}_F \text{ ideal}} \frac{1}{\mathrm{Norm}(\mathfrak{a})^s} \text{ for } s \in \mathbb{C} \text{ s.t. } \Re(s) > 1$$

and satisfies the Euler product

$$\zeta(s) = \prod_{\mathfrak{p} \text{ prime ideal of} \mathbb{Z}_F} \frac{1}{1-\mathrm{Norm}(\mathfrak{p})^{-s}}.$$

It has a simple pole at $s = 1$.

Taking the logarithm of the Euler product and remembering that the series $\sum_{n \geq 1} \frac{1}{n^t}$ converges for any $t > 1$, one obtains the following corollary.

Corollary 4.2. *(a)* $\log \zeta(s) = \sum_{p \text{ prime}} \frac{1}{p^s} + g(s) = \log(\frac{1}{s-1}) + h(s)$ *in a neighbourhood of $s = 1$, where $h(s), g(s)$ are holomorphic at $s = 1$.*

(b) $\log \zeta_F(s) = \sum_{\mathfrak{p} \text{ prime ideal}} \frac{1}{\mathrm{Norm}(p)^s} + g(s) = \log(\frac{1}{s-1}) + h(s)$ *in a neighbourhood of $s = 1$, where $h(s), g(s)$ are holomorphic at $s = 1$.*

From an essentially formal computation, one obtains the following proposition.

Proposition 4.3. *Let $m \in \mathbb{Z}_{\geq 1}$ and $F = \mathbb{Q}(\exp(2\pi i/m)$ be the m-th cyclotomic field. Its Galois group is $G = \mathrm{Gal}(F/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$. Let $\hat{G} = \{\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times\}$ be the group of Dirichlet characters (i.e. the character group of G). Then*

$$\zeta_K(s) = H(s) \cdot \prod_{\chi \in \hat{G}} L(\chi, s)$$

where $H(s) = \prod_{\mathfrak{p} | m \text{ prime ideal}} \frac{1}{1-\mathrm{Norm}(\mathfrak{p})^{-s}}$.

A very important result is the following one.

Corollary 4.4. *Let $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ be a non-trivial Dirichlet character. Then $L(\chi, 1) \neq 0$.*

Proof. Since $L(\chi, s) = \zeta(s) \cdot \prod_{p|m}(1 - p^{-s})$ for the trivial character χ and since both $\zeta(s)$ and $\zeta_K(s)$ both have a simple pole at $s = 1$, the corollary follows from Proposition 4.3. □

Definition 4.5. *Let F be a number field. Let S be a set of prime ideals of F.*

(a) The Dirichlet density of S *is defined as the limit*

$$d(S) = \lim_{s \searrow 1} \frac{\sum_{\mathfrak{p} \in S \text{ prime ideal}} \frac{1}{\mathrm{Norm}(p)^s}}{\sum_{\mathfrak{p} \text{ prime ideal}} \frac{1}{\mathrm{Norm}(p)^s}}$$

if it exists.

(b) The natural density of S *is defined as the limit*

$$\delta(S) = \lim_{x \to \infty} \frac{\#\{\mathfrak{p} \in S \text{ prime ideal} \mid \mathrm{Norm}(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \text{ prime ideal} \mid \mathrm{Norm}(\mathfrak{p}) \leq x\}}$$

if it exists.

If a set S of prime ideals has a natural density, then it has a Dirichlet density and the two are the same. The reverse direction is not always true.

As an illustration, we now prove Dirichlet's prime number theorem.

Theorem 4.6 (Dirichlet)**.** *Let $m \in \mathbb{Z}_{\geq 1}$ and $a \in (\mathbb{Z}/m\mathbb{Z})^\times$. Then the set of primes*

$$\{p \text{ prime } \mid p \equiv a \mod m\}$$

has Dirichlet density $\frac{1}{\#(\mathbb{Z}/m\mathbb{Z})^\times}$.

Proof. Let χ be a Dirichlet character of $(\mathbb{Z}/m\mathbb{Z})^\times$. Then by taking the logarithm of the Euler product of $L(\chi, s)$, we obtain

$$\log L(\chi, s) = \sum_{p \text{ prime}} \frac{\chi(p)}{p^s} + g(s) = \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(a) \sum_{p \equiv a \mod m} \frac{1}{p^s} + g(s)$$

where $g(s)$ is a function that is holomorphic at $s = 1$ (in it we collect all fractions that have at least a square in the denominator). Let $b \in (\mathbb{Z}/m\mathbb{Z})^\times$. We multiply this by $\chi(b^{-1})$ and sum over all Dirichlet characters χ to obtain

$$\begin{aligned} &\log(\zeta(s)) + \sum_{1 \neq \chi \in \hat{G}} \chi(b^{-1}) \log L(\chi, s) \\ =&\sum_{\chi \in \hat{G}} \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(b^{-1}a) \sum_{p \equiv a \mod m} \frac{1}{p^s} + h(s) \\ =&\#(\mathbb{Z}/m\mathbb{Z})^\times \cdot \sum_{p \equiv b \mod m} \frac{1}{p^s} + h(s) \end{aligned}$$

where $h(s)$ is holomorphic at $s = 1$. We used

$$\sum_{\chi \in \hat{G}} \chi(b^{-1}a) = \begin{cases} \#(\mathbb{Z}/m\mathbb{Z})^\times & \text{if } a = b \\ 0 & \text{otherwise.} \end{cases}$$

The result is now immediate by Corollary 4.2. □

In order to formulate Chebotarev's density theorem, we first have to clarify what we mean by a Frobenius conjugacy class.

Lemma 4.7. *Let $F \subseteq L$ be a Galois extension of number fields. Any prime ideal $\mathfrak{p} \subset \mathbb{Z}_F$ factors in L*

$$\mathfrak{p}\mathbb{Z}_L = \mathfrak{P}_1^e \cdots \mathfrak{P}_r^e$$

for pairwise distinct prime ideals $\mathfrak{P}_i \subset \mathbb{Z}_L$ and a positive exponent e.

One says that $\mathfrak{p}$ is unramified in L *if $e = 1$. In that case, for every $\mathfrak{P}_i$, there is an element $\Phi_{\mathfrak{P}_i} \in \mathrm{Gal}(L/F)$ such that on the residue field $\mathbb{Z}_L/\mathfrak{P}_i$ it acts as $x \mapsto x^q$ with $q = \mathrm{Norm}(\mathfrak{p})$. It is called the* Frobenius of $\mathfrak{P}_i$. *All these $\Phi_{\mathfrak{P}_i}$ are conjugate in $\mathrm{Gal}(L/F)$ and they form the* Frobenius conjugacy class $\mathcal{C}_\mathfrak{p}$ of $\mathfrak{p}$.

Theorem 4.8 (Chebotarev's density theorem)**.** *Let $F \subseteq L$ be a Galois extension of number fields with Galois group $G = \mathrm{Gal}(L/F)$. Let $C \subseteq G$ be a subset that is stable under conjugation. Let $P(C)$ be the set of prime ideals $\mathfrak{p}$ of F such that the Frobenius conjugacy class $\mathcal{C}_\mathfrak{p}$ lies in C.*

Then $P(C)$ has Dirichlet density equal to $\frac{\#C}{\#G}$.

This is a generalisation of Dirichlet's theorem (take $F = \mathbb{Q}$ and $L = \mathbb{Q}(\exp(2\pi i/m))$). The interesting thing is that one reduces the proof of Chebotarev's density theorem by rather elementary means to the abelian case, which works essentially as above (however one needs it over a general number field F and not just $\mathbb{Q}$, so one needs some more generalisations).

If one assumes the Generalised Riemann Hypothesis (i.e. the Riemann Hypothesis for the Dedekind zeta-function of the relevant number field), one obtains a stronger version of Chebotarev's density theorem with error bounds.

Define

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

It satisfies $\mathrm{Li}(x) \sim \frac{x}{\log(x)}$ for $x \to \infty$.

We also set

$$\pi_C(x) = \#\{\mathfrak{p} \text{ prime ideal} \mid \mathrm{Norm}(\mathfrak{p}) \leq x,\ \mathcal{C}_\mathfrak{p} \subseteq C\}.$$

Theorem 4.9 (Effective Chebotarev)**.** *([Ser97, Th. 4, Rem.(1)])*
Assume GRH. The for all $x \geq 2$, we have

$$\left|\pi_C(x) - \frac{\#C}{\#G}\mathrm{Li}(x)\right| \leq 2\frac{\#C}{\#G}\sqrt{x}\big(\log \mathrm{disc}(F) + [F:\mathbb{Q}]\log(x)\big).$$

It is also possible to give an upper bound, under GRH, for the norm of the first prime ideal $\mathfrak{p}$ such that the corresponding Frobenius conjugacy class $\mathcal{C}_\mathfrak{p}$ lies in C.

Theorem 4.10. *([Ser97, Th. 5])*
Suppose $C \neq \emptyset$. Then $\pi_C(x) \geq 1$ for all $x \geq \max(2, 70(\log \mathrm{disc}(F))^2)$.

A concrete example of an application of Chebotarev's density theorem is the following one.

Proposition 4.11. *Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial and let ℓ be a prime such that ℓ does not divide the discriminant of the equation order $\mathbb{Z}[X]/(f(X))$ and such that $\overline{f}(X) \in \mathbb{F}_\ell[X]$ factors as a product $\overline{f}(X) = \prod_{i=1}^r \overline{f_i}(X) \in \mathbb{F}_\ell[X]$ with pairwise distinct irreducible polynomials $\overline{f_i}(X) \in \mathbb{F}_\ell[X]$. Let $d_i = \deg(\overline{f_i}(X))$.*

Then the set of primes p such that $f(X) \mod p \in \mathbb{F}_p[X]$ factors into r factors of degrees $d_1, \ldots, d_r$ has a positive Dirichlet density. Moreover, there is an explicit bound for the smallest such prime p.

References

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[Lor96] Dino Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996.

[Neu99] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[Ser97] Jean-Pierre Serre. Répartition asymptotique des valeurs propres de l'opérateur de Hecke T_p. *J. Amer. Math. Soc.*, 10(1):75–102, 1997.

[Ste17] Peter Stevenhagen. Number rings. `http://websites.math.leidenuniv.nl/algebra/ant.pdf`, 2017.

[Wie] Gabor Wiese. Lecture notes on commutative algebra. `https://orbilu.uni.lu/handle/10993/34936`.