Basic Arithmetic Geometry

Lucien Szpiro

Based on notes by Florian Lengyel

Contents

Notation and conventions

All rings are assumed to be commutative with unit $1 \neq 0$ unless otherwise stated. If A is a ring and S is a set, then $A^{(S)}$ denotes the free A-module generated by the set S, consisting of all formal sums $\sum_{s \in S} a_s \cdot s$ with $a_s = 0$ for all but finitely many $s \in S$.

CHAPTER 1

The Picard Group

1. Tensor products and localization

Let A be a ring, and let M and N be A-modules. The tensor product of M and N solves the universal problem for A-bilinear maps from $M \times N$ to an A-module.If S is a set let $A^{(S)}$ denote the free A-module generated by the set S.

PROPOSITION 1.1. *Let R be the submodule of $A^{(M\times N)}$ generated by the elements of the form*

$$\begin{array}{ll}(x+x',y)-(x,y)-(x',y), & (ax,y)-(x,ay),\\ (x,y+y')-(x,y)-(x,y'), & (ax,y)-a\,(x,y),\end{array}$$

where $x,x^{'}\in M$, $y,y^{'}\in N$, and where $a\in A$. Denote by $M\otimes_A N$ the module $A^{(M\times N)}/R$ and by $x\otimes y$ the image of (x,y) in the quotient. Then, for each A-module P and each A-bilinear map $\varphi : M\times N\to P$, there exists a unique A-linear map $\psi : M\otimes_A N\to P$ such that for each $(x,y)\in M\times N$, $\varphi\left((x,y)\right)=\psi\left(x\otimes y\right)$.

The proof is straightforward. It is clear from the proposition that the A-module $M\otimes_A N$ is generated over A by the elements $x\otimes y$.

EXAMPLE 1.1. **The tensor product of non-zero modules can be zero**. If $A=\mathbb{Z}$, and if n and m are relatively prime integers, then $\mathbb{Z}/n\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}/m\mathbb{Z}$ is annihilated by m and by n by bilinearity. Therefore, since there exist integers a and b such that $am+bn=1$, the tensor product is annihilated by 1.

EXAMPLE 1.2. Let J be an ideal of A, then $M\otimes_A A/J=M/JM$; in particular, $J\otimes_A A/J=J/J^2$.

Let A be a ring. An ideal $\mathfrak{p}$ of A is **prime** if $A/\mathfrak{p}$ is an integral domain. An ideal $\mathfrak{m}$ of A is **maximal** if $A/\mathfrak{m}$ is a field. It is immediate that every maximal ideal is prime.

The following lemma yields a characterization of the set of nilpotent elements of a ring.

LEMMA 1.2. *Let A be a ring. If $x\in A$ satisfies $x^n\neq 0$ for each $n\in\mathbb{N}$, then there exists a prime ideal $\mathfrak{p}$ such that $x\notin\mathfrak{p}$.*

PROOF. Let $\mathcal{I}$ be the set of ideals of A that do not contain x^n for any n. The set $\mathcal{I}$ is nonempty since it contains the zero ideal, $\mathcal{I}$ is partially ordered by inclusion, and the union of a chain of ideals of $\mathcal{I}$ is an ideal of $\mathcal{I}$. By Zorn's lemma, $\mathcal{I}$ contains a maximal element. Such an element $\mathfrak{p}$ must be prime. For if $a, b \in A$ with $a \notin \mathfrak{p}$ and $b \notin \mathfrak{p}$, x^n is in $(\mathfrak{p} + (a)) \cap (\mathfrak{p} + (b))$ for some $n \geq 1$ by maximality, which implies that x^{2n} is in $\mathfrak{p} + (ab)$. By definition of $\mathcal{I}$, $ab \notin \mathfrak{p}$, hence $\mathfrak{p}$ is prime and $x \notin \mathfrak{p}$. □

COROLLARY 1.3. *Let A be a ring and let I be an ideal of A with $I \neq A$. Then A contains a maximal ideal $\mathfrak{M}$ containing I.*

PROOF. Apply Lemma 1.2 to the ring A/I and the element $x = 1$. □

DEFINITION 1.4. Let A be a ring and let I be an ideal of A. The **radical** of I is denoted by

$$\sqrt{I} = \{a \in A : a^n \in I \text{ for some } n > 0\}.$$

COROLLARY 1.5. *Let I be an ideal of A, then*

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p},\ \mathfrak{p} \text{ prime}} \mathfrak{p}.$$

PROOF. Apply Lemma 1.2 to the ring $A/\sqrt{I}$ and a nonzero element x. It follows that $A/\sqrt{I}$ contains a prime ideal $\mathfrak{p}$ that does not contain x. □

DEFINITION 1.6. The ring A is a **local ring** with maximal ideal $\mathfrak{m}$ if every ideal of A not equal to A is contained in $\mathfrak{m}$.

The ring $k[[X_1, \dots, X_n]]$ of formal power series with coefficients in a field k is a local ring with maximal ideal generated by the X_i.

DEFINITION 1.7. An A-module M is of **finite type** if M is finitely generated over A.

PROPOSITION 1.8 (**Nakayama's Lemma**). *Let A be a local ring with maximal ideal $\mathfrak{m}$, and let M be an A-module of finite type such that $M \otimes_A A/\mathfrak{m} = 0$. Then $M = 0$.*

PROOF. Let $x_1, \dots x_n$ generate M over A. By hypothesis, $\mathfrak{m}M = M$, hence there exist elements $m_{i,j} \in \mathfrak{m}$ such that for $1 \leq i \leq n$,

$$x_i = \sum_{j=1}^{n} m_{i,j} x_j.$$

Let Φ denote the matrix $(m_{i,j} - \delta_{i,j})$, and let x and 0 denote the column vector of the x_i and the zero column vector, so that $\Phi x = 0$. If Φ^* is the transpose of the matrix of cofactors of Φ one has

$$\Phi^* \Phi = \det(\Phi) Id.$$

Cramer's rule is valid in any ring, so that $\det(\Phi)\, x_i = 0$ for each i. But the determinant $\det(\Phi)$ is invertible in A since it equals $(-1)^n$ modulo $\mathfrak{m}$. $\square$

Corollary 1.9. *Let A be a local ring with maximal ideal $\mathfrak{m}$ and let M be an A-module of finite type. A set of n elements of M, generate M over A if and only if their images in $M \otimes_A A/\mathfrak{m}$ generate this A-module as a vector space over $A/\mathfrak{m}$.*

Exercise 1.1. Let A be a ring, let M, N, N' be A-modules, and let $\varphi : N' \to N$ be an A-linear map.

a) Show that the map $1 \times \varphi : M \times N' \to M \times N$ induces a natural A-linear map $M \otimes_A N' \to M \otimes_A N$, denoted by $1 \otimes \varphi$.

b) Show that the assignment $N \mapsto M \otimes_A N$ is thus an additive covariant functor from the category of A-modules to itself.

c) Show that the functor $M \otimes_A \cdot$ is right exact; that is, if

$$0 \to N' \to N \to N'' \to 0$$

is an exact sequence of A-modules, then

$$M \otimes_A N' \longrightarrow M \otimes_A N \longrightarrow M \otimes_A N'' \to 0$$

is exact.

d) An A-module M is said to be **flat** if the functor $M \otimes_A \cdot$ is exact; i.e., both left and right exact. Show that a free A-module is flat.

e) Let A be a local ring with nonzero maximal ideal $\mathfrak{m}$. Show that $A/\mathfrak{m}$ is not flat as an A-module.

Definition 1.10. Let A be a ring, and let S be a subset of A. S is said to be **multiplicatively stable** if $1 \in S$ and if $x, y \in S$ implies that $xy \in S$. Let S be a multiplicatively stable subset of A. The **localization** of M **at** S, denoted by $S^{-1}M$, is defined as the quotient of $M \times S$ modulo the equivalence relation $\sim$, where $(m, s) \sim (m', s')$ if and only if there exists $t \in S$ with $tms' = tsm'$.Often we will denote the image of (m, f) by $\frac{m}{f}$.

Exercise 1.2. Let A be a ring, S a multiplicatively stable subset of A, and let M be an A-module.

a) Verify that $S^{-1}M$ is an $S^{-1}A$-module and that

$$S^{-1}M = M \otimes_A S^{-1}A.$$

b) There is a canonical map $M \to S^{-1}M$ which sends x to $(x, 1)$. Show that the image of x is zero if and only if there exists $s \in S$ such that $sx = 0$.

DEFINITION 1.11. Let A be a ring and let M be an A-module. The **annihilator** of an element m in M is denoted by

$$\operatorname{Ann}(m) = \{a \in A : am = 0\}.$$

The annihilator of an element of M is an ideal of A. Let S be a multiplicatively stable subset of A and let m be in M. The exercise 1.2 b) above shows that if $\operatorname{Ann}(x) \cap S = \emptyset$ then x is not zero in $S^{-1}M$.

LEMMA 1.12. *Let M be an A-module such that $M_{\mathfrak{p}} = 0$ for every prime ideal $\mathfrak{p}$. Then $M = 0$.*

PROOF. Let $x \in M$, then $\operatorname{Ann}(x)$ equals A; otherwise there is a maximal ideal $\mathfrak{m}$ containing $\operatorname{Ann}(x)$. However, since $M_{\mathfrak{m}} = 0$, Exercise 1.2 b) implies that $A - \mathfrak{m}$ meets $\operatorname{Ann}(x)$. □

DEFINITION 1.13. Let f be an element of A and M be an A module.We will call M localised at f and note M_f ,the module $S^{-1}M$ where $S = \{(f^n\}_{n \geq 0}$.

EXERCISE 1.3. Let A be a ring, S a multiplicatively stable subset of A, and let M be an A-module.

a) Show that $S^{-1}A$ is flat as an A-module.

b) If $\mathfrak{p}$ is a prime ideal of A,then $S = A-\mathfrak{p}$ is multiplicatively stable. Let $A_{\mathfrak{p}}$ and $M_{\mathfrak{p}}$ denote the localization of A and M, respectively, at S. Show using Exercise 1.2 that if M is of finite type and $M_{\mathfrak{p}} = 0$, then there exists $f \in A, f \notin \mathfrak{p}$ such that $M_f = 0$.

c) Verify that if $\mathfrak{p}$ is a prime ideal of A then $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.

EXERCISE 1.4. Let A be a ring, let S be a multiplicatively stable subset of A not containing 0, and let $\varphi : A \to S^{-1}A$ be the canonical map. Show that the map given by $\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p})$ is a bijection from the set of prime ideals of $S^{-1}A$ to the set of prime ideals of A that have empty intersection with S.

DEFINITION 1.14. An A-module M is said to be of **finite presentation** if there exist positive integers n, m and an exact sequence

$$A^n \to A^m \to M \to 0.$$

For example, a module of finite type over a Noetherian ring is of finite presentation.

EXERCISE 1.5. Let S be an additive functor from the category of A-modules to the category of abelian groups. Show that for every A-module M, $F(M)$ has a natural structure as an A-module. Suppose moreover that A is right exact. Show then that $F(M) = M \otimes_A F(A)$ for every A-module M of finite presentation.

EXERCISE 1.6. The **module of differentials**. Let $A \to B$ be a homomorphism of rings. Let I be the kernel of the map $B \otimes_A B \to B$ that sends $x \otimes y$ to xy.

a) Show that I is a B-module generated by the elements of the form $x \otimes 1 - 1 \otimes x$.

b) Let d be the map from B to I/I^2 that sends x in B to the coset of $x \otimes 1 - 1 \otimes x$. Show that d satisfies the Leibniz formula $d(xy) = x\,dx + y\,dx$. The module I/I^2 is denoted by $\Omega^1_{B/A}$ and is called the module of differentials of B over A.

c) Show that if M is a B-module and $\varphi : B \to M$ is an A-linear map such that $\varphi(xy) = x\varphi(y) + y\varphi(x)$, then there exists a unique B-linear map $\psi : \Omega^1_{B/A} \to M$ such that $\varphi = \psi \circ d$.

d) Let $F(X)$ be a polynomial with coefficients in a ring A, and let B be the ring $A\,[X]\,/(F(X))$. Show that $\Omega^1_{B/A} \simeq B/(F^{'}(X))$, where $\overline{X}$ is the image of X in B, and where $F^{'}$ is the derivative of F.

e) More generally, let $A \to C$ be a homomorphism of rings, let J be an ideal of C, and let $B = C/J$. Show that there is an exact sequence

$$J/J^2 \xrightarrow{d\otimes\mathbf{1}} \Omega^1_{C/A} \otimes_B B \longrightarrow \Omega^1_{B/A} \longrightarrow 0.$$

2. Universal algebras

Let M be an A-module, and let n be a nonnegative integer. For $n > 0$, let $T_n(M)$ denote the n-fold tensor product of M with itself: $M \otimes_A M \otimes_A \cdots \otimes_A M$, and define $T_0(M) = A$.

The product

$$(x_1 \otimes \cdots \otimes x_j) \cdot (y_1 \otimes \cdots \otimes y_k) = x_1 \otimes \cdots \otimes x_j \otimes y_1 \otimes \cdots \otimes y_k$$

provides the direct sum $T(M) = \bigoplus_{n \geq 0} T_n(M)$ with the structure of an associative algebra (noncommutative in general) with unit element. It is easy to verify that for every A-homomorphism $\varphi : M \to N$, where B is an associative A-algebra, there exists one and only one homomorphism of A-algebras $\psi : T(M) \to B$ such that φ is the composite of ψ and the canonical injection $M \to T_1(M) \hookrightarrow T(M)$. We call $\mathbf{T}(M)$ the **tensor algebra** of M.

We can then define other universal algebras that are also graded. The **symmetric algebra** of M is denoted by $\mathbf{Sym}(M)$ and is defined as $T(M)/I$, where I is the ideal of $T(M)$ generated by the elements $x \otimes y - y \otimes x$, where $x, y \in M$. The ideal I is generated by homogeneous elements of degree two, so the symmetric algebra $\mathrm{Sym}(M) = \bigoplus_{n\geq 0} \mathrm{Sym}_n(M)$ is graded, where $\mathrm{Sym}_n(M) = T_n(M)/\left(T_n(M) \cap I\right)$.

One easily verifies that the symmetric algebra is universal in the following sense: for each A-homomorphism $\varphi : M \to B$ of M to a commutative A-algebra, there exists one and only one A-algebra homomorphism $\psi : \mathrm{Sym}(M) \to B$ such that φ is the composite of ψ and the canonical injection $M \to \mathrm{Sym}_1(M) \hookrightarrow \mathrm{Sym}(M)$. For example, one verifies that if $M = A^r$ is a free A-module of rank r, then its symmetric algebra $\mathrm{Sym}(A^r)$ is a polynomial ring $A\left[X_1, \ldots, X_r\right]$.

The **exterior algebra** of M is denoted by ΛM and is defined as $T(M)/J$, where J is the ideal of $T(M)$ generated by the elements of the form $x \otimes x$, where $x \in M$. It is a graded A-algebra with direct sum decomposition $\Lambda M = \bigoplus_{n\geq 0} \Lambda^n M$, where $\Lambda^n(M) = T_n(M)/\left(T_n(M) \cap J\right)$. One verifies easily that $\Lambda^n(M) = 0$ for n strictly greater than the number of generators of M as an A-module. One customarily denotes by $x_1 \wedge \cdots \wedge x_n$ the image in $\Lambda^n(M)$ of the element $x_1 \otimes \cdots \otimes x_n$ in $T_n(M)$. The exterior algebra is universal in the following sense: for each A-homomorphism $\varphi : M \to B$ of M to an A-algebra, where $\varphi(M)$ consists of elements of square zero (for example, if B is a graded antisymmetric algebra and $\varphi(M)$ is homogeneous of odd degree), there exists one and only one A-algebra homomorphism $\psi : \Lambda(M) \to B$ such that φ is the composite of ψ and the canonical injection $M \to \Lambda^1(M) \hookrightarrow \Lambda(M)$.

EXERCISE 2.1. Show that T_n, Sym_n, and Λ^n are functors from the category of A-modules to itself. Verify that if $M = N \oplus P$ is a direct sum, then

$$T_n(M) = \bigoplus_{k=0}^{n} \left(T_k(N) \otimes_A T_{n-k}(P)\right)^{\binom{n}{k}}.$$

3. Schemes and projective schemes

We present here algebraic varieties in the language of schemes of A. Grothendieck. The language of schemes has the advantage of a uniform treatment of algebraic varieties and arithmetic varieties.

DEFINITION 3.1. Let A be a ring. The **spectrum** of A, denoted by $\mathrm{Spec}\, A$, is the set of prime ideals of A. Let I be an ideal of A we denoted by $V(I)$, the set of prime ideals of A that contain I.

We have seen that each ideal of A that is not equal to A is contained in a prime ideal of A.

We denote by Spec-max A the set of maximal ideals of A.

EXAMPLE 3.1. Let k be a field and let $A = k[x_1, \dots x_n]$ be an algebra of finite type over k. Choosing variables $X_1, \dots, X_n$, A can be regarded as a quotient of the ring of polynomials $k[X_1, \dots, X_n]$ by an ideal generated by a finite set of polynomials $F_1, \dots, F_m$. Given a finite set of polynomials F_j, an **algebraic variety** is the set of all n-tuples $a = (a_1, \dots, a_n)$ of elements of $\overline{k}$ (the algebraic closure of k) such that $F_j(a) = 0$ for each j. The set of common zeros of the F_j is denoted by $Z(F)$. There is a map $Z(F) \to \text{Spec-max}(A)$ that sends the element $a = (a_1, \dots, a_n)$ to the kernel of the map from $k[X_1, \dots, X_n]$ to k which evaluates a polynomial at the point a. Hilbert's Nullstellensatz asserts that this map is a bijection when $k = \overline{k}$.

PROPOSITION 3.2. *The collection of sets $V(I)$ of Definition 3.1 are the closed sets of a topology on Spec A. A base of open sets for this topology is given by the collection of the sets Spec A_f, where $f \in A$.*

DEFINITION 3.3. The topology on Spec A defined in Proposition 3.2 is called the **Zariski topology**. If f is in A, we denote by $D(f)$ the open set Spec A_f.

Let A be a ring and let $f \in A$. By Lemma 1.2, $D(f)$ is the set of prime ideals of A that do not contain f.

PROOF OF PROPOSITION 3.2. The intersection of an arbitrary collection $V(I_j)_{j\in J}$ of closed sets is equal to the closed set $V(\sum_{j\in J} I_j)$. (Recall that the sum of the collection $(I_j)_{j\in J}$ is the set of all finite sums of elements each of which is contained in some ideal I_j). The union of a finite set of closed sets $V(I_1), \dots, V(I_n)$ is equal to $V(I_1 \cap \dots \cap I_n)$. The empty set is equal to $V(A)$ and Spec (A) is equal to $V((0))$. $\square$

REMARK 3.4. It is clear that if I is the ideal generated by the elements $(f_j)_{j\in J}$, then

$$\text{Spec } A - V(I) = \bigcup_{j\in J} \text{Spec } A_{f_j}.$$

REMARK 3.5. If A is an integral domain, then two nonempty open subsets of Spec A always have nonempty intersection. This holds since the zero ideal (0) of an integral domain is prime, hence it is contained in every nonempty basic open set $D(f)$, for f in A. One cannot therefore separate two points of Spec A by disjoint open neighborhoods.

The Zariski topology is as we see stranger than what we are used to. Nevertheless, the following exercise shows that it is not always too bad.

Exercise 3.1. Let $A = \mathcal{C}([0,1], \mathbb{R})$ be the ring of continuous real-valued functions on the unit interval [0.1]. Show that the map which associates to x in $[0,1]$ the kernel of evaluation map $\mathcal{C}([0,1], \mathbb{R}) \to \mathbb{R}$ at x is a homeomorphism of $[0,1]$ with the usual topology onto Spec-max A with the topology induced by the Zariski topology on Spec A.

Proposition 3.6. *Let A be a ring, then Spec A with the Zariski topology is quasi-compact.*

Proof. Let $(U_i)_{i \in I}$ be an open covering of Spec A. By considering refinements of the given cover by basic open sets, we may suppose that each open set U_i has the form $D(f_i)$ for some f_i in A. The assertion that $(D(f_i))_{i \in I}$ covers Spec A means that the ideal J generated by the f_i is equal to the ring A; otherwise there would be a maximal ideal $\mathfrak{m}$ such that $f_i \in J \subseteq \mathfrak{m} \in D(f_i)$ for some i, which is a contradiction. Therefore, there exists a finite subset $i_1, \ldots, i_n$ of I and elements λ_{i_j} of A such that

$$\sum_{j=1}^{n} \lambda_{i_j} f_{i_j} = 1$$

(i.e., a partition of unity). Equivalently, the closed set $V((f_{i_1}, \ldots, f_{i_n}))$ is empty, therefore by Remark (3.4), the collection $D(f_{i_j})_{j=1,\ldots,n}$ is an open cover of Spec A. $\square$

Exercise 3.2. Show that there is a canonical bijection between the set of coverings of Spec A by two nonempty disjoint open sets and the set of pairs of nontrivial idempotent elements e_1, e_2 of A such that $e_1 + e_2 = 1$ and $e_1 e_2 = 0$.

Definition 3.7. A property is called **local** if it is true in an open neighborhood of any point.

Exercise 3.3. Let A be a ring. Show that for an A-module to be of finite type is a local property for the Zariski topology.

Definition 3.8. The category *Open*(X) of open subsets of a topological space X is the category whose objects are the open subsets of X, and whose arrows are the inclusion maps between open sets.

Definition 3.9. Let X be a topological space. A contravariant functor F on *Open*(X) with values in a category of sets is called F is a **presheaf** on X. The presheaf F is a **sheaf** if for each open set U of X, and for each open covering $(U_i)_{i \in I}$ of U, the following conditions are satisfied.

(i) If two elements of $F(U)$ have the same image in $F(U_i)$ for each i, then they are equal.

(ii) If $s_i \in F(U_i)$ for each $i \in I$, and if the images of s_i and s_j coincide in $F(U_i \cap U_j)$ for each pair (i, j), then there exists s in $F(U)$ whose image in each $F(U_i)$ is s_i.

Definition 3.10. A **ringed** space is a topological space X together with a sheaf of rings on X.

Exercise 3.4. The sheaf of real valued functions on a topological space X. For U open in X, let $F(U) = \mathcal{F}(U, \mathbb{R})$ be the set of real valued functions defined on U. If $i : V \hookrightarrow U$ is an inclusion of open subsets of X, let $F(i) : \mathcal{F}(U, \mathbb{R}) \to \mathcal{F}(V, \mathbb{R})$ be the restriction of a function defined on U to V. F is a presheaf. It is easy to see that F is a sheaf. One can also define the sheaf F^c of continuous functions, the sheaf F^i of i-times differentiable functions, the sheaf F^∞ of infinitely differentiable functions, and the sheaf F^ω of real analytic functions on any suitable topological space.

In view of the previous examples of sheaves, if F is a sheaf on X and if $V \hookrightarrow U$ is an inclusion of open sets, the induced map $F(U) \to F(V)$ is called the **restriction** of U to V. If U is an open subset of X, then an element of $F(U)$ is called a **section** over U. If V is an open subset of U, and if s is a section over U, then the restriction of s to V is denoted by $s|_V$.

The following proposition leads to a definition of the "sheaf of algebraic functions" on the topological space Spec A, where A is a ring.

Proposition 3.11. *Let A be a ring, M an A-module, and let $(D(f_i))_{i\in I}$ be a covering of Spec A by basic open sets. The following sequence is exact*

$$0 \to M \to \prod_i M_{f_i} \xrightarrow{\varphi} \prod_{i,j} M_{f_i f_j}$$

where $\varphi((x_i)) = ((x_i|_{D(f_i f_j)} - x_j|_{D(f_i f_j)}))_{i,j}$.

Proof. First, suppose that the index set I of the open cover $(D(f_i))_{i\in I}$ of Spec A is finite.

Since $(D(f_i))_{i\in I}$ is a covering of Spec A, there exists a collection $(\lambda_i)_{i\in I}$ of elements of A such that

$$\sum_{i\in I} \lambda_i f_i = 1.$$

For each $i \in I$ and for each positive integer n we have $D(f_i) = D(f_i^n)$, hence each positive integer n there exist $\lambda_{i,n} \in A$ such that

$$\sum_{i\in I} \lambda_{i,n} f_i^n = 1.$$

Exactness at M is immediate. Suppose the element x in M becomes 0 in M_{f_i} for each $i \in I$. Then for each $i \in I$, there is an n_i such that $f_i^{n_i} x = 0$. If $n = \sup\{n_i : i \in I\}$, then

$$x = \sum_{i \in I} \lambda_{i,n} f_i^n x = 0.$$

For exactness at $\prod_{i \in I} M_{f_i}$, suppose that $(x_i)_{i \in I}$ is in $\ker \varphi$. For each $i \in I$ there exist $z_i \in M$ and n_i such that

$$x_i = \frac{z_i}{f_i^{n_i}}.$$

Taking $n = \sup\{n_i : i \in I\}$ and $y_i = z_i f_i^{n-n_i}$ we have that

$$x_i = \frac{z_i f_i^{n-n_i}}{f_i^n} = \frac{y_i}{f_i^n}$$

for each $i \in I$.

Furthermore, there exist integers $n_{i,j}$ for $i, j \in I$ such that

$$y_j f_i^n (f_i f_j)^{n_{i,j}} = y_i f_j^n (f_i f_j)^{n_{i,j}}.$$

Taking $m = \sup\{n_{i,j} : i, j \in I\}$ we have

$$y_j f_i^n (f_i f_j)^m = y_i f_j^n (f_i f_j)^m.$$

Multiplying by $\lambda_{i,n+m}$ and adding over $i \in I$ we obtain

$$\begin{aligned} y_j f_j^m &= \sum_{i \in I} (y_j f_j^m) \lambda_{i,n+m} f_i^{n+m} = \sum_{i \in I} y_i f_j^n \lambda_{i,n+m} (f_i f_j)^m \\ &= f_j^{n+m} \sum_{i \in I} y_i \lambda_{i,n+m} f_i^m. \end{aligned}$$

Setting $y = \sum_{i \in I} y_i \lambda_{i,n+m} f_i^m$ we have that for each $j \in I$, $y_j f_j^m = y f_j^{n+m}$, hence

$$x_j = \frac{y_j}{f_j^n} = \frac{y}{1}.$$

This proves the exactness of the sequence of 3.11 for a finite open cover of Spec A.

Next, suppose that the open cover $(D(f_i))_{i \in I}$ of Spec A is not necessarily finite. By quasi-compactness of Spec A, there exists a finite subset K of I such that $(D(f_i))_{i \in K}$ is an open cover of Spec A. We have shown that the sequence of 3.11 is exact for $i, j \in K$. We show that the sequence of 3.11 is exact for $i, j \in I$.

Exactness at M follows trivially, since if $x \in M$ becomes 0 in M_{f_i} for each $i \in I$, then x becomes 0 in each M_{f_i} for $i \in K$, hence by exactness of 3.11 for the open cover determined by K, $x = 0$.

Exactness at $\prod_{i\in I} M_{f_i}$ also holds. Suppose that $(x_i)_{i\in I}$ is in $\ker\varphi$. By previous remarks, there exists an element x_K in M that becomes equal to x_i in M_{f_i} for $i \in K$. Let $j \in I$ and let $L = K \cup \{j\}$. Again by previous remarks, there exists an element x_L in M that becomes equal to x_i in M_{f_i} for $i \in L$. Since $x_K - x_L = 0$ in M_{f_i} for $i \in K$, by exactness for the finite cover determined by K, $x_K = x_L$. Consequently, x_K becomes equal to x_j in M_{f_j}. Since $j \in I$ is arbitrary, exactness at the product term $\prod_{i\in I} M_{f_i}$ follows. □

Let X be a topological space, and let $\mathcal{B}$ be a base of open sets for the topology of X. We may consider $\mathcal{B}$ as a category with $\mathrm{Obj}(\mathcal{B})$ equal to $\mathcal{B}$, and such that for $U, V \in \mathcal{B}$, $\mathrm{Hom}_{\mathcal{B}}(V, U)$ contains the inclusion $V \hookrightarrow U$ if V is contained in U, and is empty otherwise. If $\mathcal{F}$ is a contravariant functor from $\mathcal{B}$ to a category of modules, we say that $\mathcal{F}$ is a **sheaf with respect to $\mathcal{B}$** if $\mathcal{F}$ is a sheaf with respect to coverings of basic open sets by basic open sets; more precisely, whenever U is in $\mathcal{B}$ and $(U_i)_{i\in I}$ is a covering of U by elements U_i in $\mathcal{B}$, the following sequence is exact

$$0 \longrightarrow \mathcal{F}(U) \longrightarrow \prod_{i\in I} \mathcal{F}(U_i) \xrightarrow{\varphi} \prod_{i,j\in I} \mathcal{F}(U_i \cap U_j)$$

where $\varphi\left((s_i)_{i\in I}\right) = \left(s_i|_{U_i\cap U_j} - s_i|_{U_i\cap U_j}\right)_{i,j}$.

If U is open in X, we write $\mathcal{B}_U$ for the set of elements of $\mathcal{B}$ contained in U.

Definition 3.12. A **preordered set** $(D, \leq)$ is a nonempty set D together with a reflexive transitive relation on D.

Definition 3.13. Let $(D, \leq)$ be a preordered ordered set considered as a category. An **inverse system** of modules is a contravariant functor $\mathcal{F}$ from D to a category of modules.

Definition 3.14. Let X be a topological space and let $\mathcal{B}$ be a base for the topology of X, and let $\mathcal{F}$ be a contravariant functor from $\mathcal{B}$ to a category of modules. Fix U open in X. The **inverse limit** of the inverse system $\mathcal{F}$ is the module

$$\varprojlim_{W\in\mathcal{B}_U} \mathcal{F}(W) := \left\{ \alpha \in \prod_{W\in\mathcal{B}_U} \mathcal{F}(W) : V \subseteq W \subseteq U \Rightarrow \alpha(W)|_V = \alpha(V) \right\}$$

together with the canonical projections

$$\pi_V : \varprojlim_{W\in\mathcal{B}_U} \mathcal{F}(W) \longrightarrow \mathcal{F}(V)$$

for $V \in \mathcal{B}_U$.

Recall the universal property of the inverse limit.

EXERCISE 3.5. Let X be a topological space, let $\mathcal{B}$ be a base for the topology of X, and let $\mathcal{F}$ be a contravariant functor from $\mathcal{B}$ to a category of modules. Let M be a module together with a family of maps $\rho_V : M \to \mathcal{F}(V)$ for $V \in \mathcal{B}$ such that $\rho_{W,V} \circ \rho_W = \rho_V$, where $V \subseteq W$ and where $\rho_{W,V} : \mathcal{F}(W) \to \mathcal{F}(V)$ is the restriction.

Then for each U open in X, there is a unique map

$$\varphi_U : M \longrightarrow \varprojlim_{W \in \mathcal{B}_U} \mathcal{F}(W)$$

such that $\pi_U \circ \varphi_U = \rho_U$.

If $\mathcal{F}$ is a sheaf with respect to a base for a topology on X, the following proposition shows how to canonically extend $\mathcal{F}$ to a sheaf $\widetilde{\mathcal{F}}$ on X.

PROPOSITION 3.15. *Let X be a topological space, and suppose that $\mathcal{B}$ is a base for the open subsets of X that is closed under intersection. Let $\mathcal{F}$ be a contravariant functor from $\mathcal{B}$ to a category of modules that is a sheaf with respect to $\mathcal{B}$. Define a presheaf $\widetilde{\mathcal{F}}$ on each open set U of X by*

$$\widetilde{\mathcal{F}}(U) := \varprojlim_{W \in \mathcal{B}_U} \mathcal{F}(W)$$

and on each inclusion of open sets $V \hookrightarrow U$ by the restriction map $\widetilde{\mathcal{F}}(U) \to \widetilde{\mathcal{F}}(V)$, which sends a map $\alpha : \mathcal{B}_U \to \bigcup_{w \in \mathcal{B}_U} \mathcal{F}(W)$ to its restriction to $\mathcal{B}_V$ (i.e., $\alpha|_{\mathcal{B}_V}$). Then $\widetilde{\mathcal{F}}$ is a sheaf, and for each basic open set $U \in \mathcal{B}$, $\widetilde{\mathcal{F}}|U$ is naturally isomorphic to $\mathcal{F}$.

PROOF. Given U open in X and given a collection $(U_i)_{i \in I}$ of open subsets of X such that $U = \bigcup_{i \in I} U_i$ we show that the following sequence is exact

$$0 \longrightarrow \widetilde{\mathcal{F}}(U) \longrightarrow \prod_{i \in I} \widetilde{\mathcal{F}}(U_i) \xrightarrow{\varphi} \prod_{i,j \in I} \widetilde{\mathcal{F}}(U_i \cap U_j)$$

where $\varphi\left((\alpha_i)_{i \in I}\right) = \left(\alpha_i|_{\mathcal{B}_{U_i \cap U_j}} - \alpha_j|_{\mathcal{B}_{U_i \cap U_j}}\right)_{i,j}$.

For exactness at $\widetilde{\mathcal{F}}(U)$, suppose that $\alpha \in \widetilde{\mathcal{F}}(U)$ satisfies

$$\alpha|_{\mathcal{B}_{U_i}} = 0$$

for each $i \in I$. Fix W in $\mathcal{B}_U$. Let $(W_{i,j})_{j \in J_i}$ be an open covering of U_i by basic open sets $W_{i,j} \in B_{U_i}$. Since $\mathcal{B}$ is closed under intersection,

$(W \cap W_{i,j})_{i \in I, j \in J_i}$ is a covering of W by elements of $\mathcal{B}$. By definition of α,

$$\alpha(W)|_{W \cap W_{i,j}} = \alpha(W \cap W_{i,j}) = 0$$

for each $i \in I, j \in J_i$. Since $\mathcal{F}$ is a sheaf with respect to $\mathcal{B}$, $\alpha(W) = 0$. Since $W \in \mathcal{B}_U$ is arbitrary, $\alpha = 0$.

For exactness at $\prod_{i \in I} \widetilde{\mathcal{F}}(U_i)$, suppose that $(\alpha_i)_{i \in I}$ is a collection of elements with $\alpha_i \in \widetilde{\mathcal{F}}(U_i)$ such that

$$\alpha_i|_{\mathcal{B}_{U_i \cap U_j}} = \alpha_j|_{\mathcal{B}_{U_i \cap U_j}}$$

for each i, j in I.

Let $W \in \mathcal{B}_U$ and let $(W_{i,j})_{j \in J_i}$ be an open covering of U_i by basic open sets $W_{i,j} \in B_{U_i}$. Then the collection of $W_{i,j} = W \cap W_{i,j}$ is a covering of W by basic open sets $W_{i,j} \subseteq U_i$.

Consider the family of elements $\alpha_i(W_{i,j}) \in \mathcal{F}(W_{i,j})$. We have that

$$\alpha_i(W_{i,j})|_{W_{i,j} \cap W_{k,l}} = \alpha_i(W_{i,j} \cap W_{k,l}) = \alpha_k(W_{i,j} \cap W_{k,l}) = \alpha_k(W_{i,j})|_{W_{i,j} \cap W_{k,l}}$$

where the first and third equality holds by definition of the inverse limit, and where the second equality holds by hypothesis. By the sheaf property of $\mathcal{F}$ with respect to $\mathcal{B}$, there exists a section $s_W \in \mathcal{F}(W)$ such that

$$s_W|_{W_{i,j}} = \alpha_i(W_{i,j})$$

for each i in I and j in J_i. We set $\alpha(W) = s_W$.

We claim that

$$\alpha \in \widetilde{\mathcal{F}}(U) = \varprojlim_{W \in \mathcal{B}_U} \mathcal{F}(W);$$

that is, if V and W are in $\mathcal{B}$ and if $V \subseteq W \subseteq U$, then $\alpha(W)|_V = \alpha(V)$.

Let $W_{i,j}$ be an open cover of W with $W_{i,j} \subseteq U_i$ as above. By definition of α,

$$\alpha(W)|_{W_{i,j}} = \alpha_i(W_{i,j}).$$

Restricting the preceding equality further,

$$\alpha(W)|_{V \cap W_{i,j}} = \alpha_i(W_{i,j})|_{V \cap W_{i,j}} = \alpha_i(V \cap W_{i,j}) = \alpha(V)|_{V \cap W_{i,j}},$$

where the second equality holds by definition of α_i, and where the third equality holds by definition of $\alpha(V)$, since the collection $(V \cap W_{i.j})$ is a covering of V by basic open sets. By the sheaf property of $\mathcal{F}$,

$$\alpha(W)|_V = \alpha(V)|_V = \alpha(V).$$

Finally, it follows by previous remarks that for each i in I,

$$\alpha|_{B_{U_i}} = \alpha_i.$$

□

EXERCISE 3.6. Let A be a ring, and let M be an A-module. Show that for $f, g \in A$, if the basic open sets $D(f)$ and $D(g)$ are equal, then M_f is canonically isomorphic to M_g. Hence, show that the assignment $D(f) \mapsto M_f$ defines an inverse system of A-modules.

DEFINITION 3.16. Let A be a ring, and let M be an A-module. Let $\mathcal{B}$ be the base for the Zariski topology on Spec A given by the sets $D(f)$ for $f \in A$. By the preceding exercise, the assignment $D(f) \mapsto M_f$ defines an inverse system of A-modules. We define a presheaf $\widetilde{M}$ on Spec A as follows. For U open in Spec A, we define

$$\widetilde{M}(U) := \varprojlim_{D(f) \subseteq U} M_f$$

and for U, V open with $V \subseteq U$, the restriction map $\widetilde{M}(U) \to \widetilde{M}(V)$ sends $\alpha \in \widetilde{M}(U)$ to $\alpha|_{\mathcal{B}_V}$.

THEOREM 3.17. *Let A be a ring and let M be an A-module. The functor $\widetilde{M}$ defined in Proposition 3.15 is a sheaf.*

PROOF. By Exercise 3.6 and by Proposition 3.15 it follows that the assignment $D(f) \mapsto M_f$ defines a sheaf of modules with respect to the collection of basic open sets of Spec A. It follows from Proposition 3.15 that the functor $\widetilde{M}$ is a sheaf. □

DEFINITION 3.18. Let A be a ring. The **affine scheme** defined by A is by definition the topological space Spec A together with the sheaf of rings $\widetilde{A}$.

By abuse of language, one also refers to Spec A as the affine scheme determined by A.

DEFINITION 3.19. A preordered set $(D, \leq)$ is **directed** if for elements a, b in D, there exists an element c in D with $a \leq c$ and $b \leq c$.

DEFINITION 3.20. Let X be a topological space, and let x be a point of X. The **set of neighborhoods of** x, denoted by $\mathrm{Nbd}(X, x)$, is the set of open subsets U of X with $x \in U$.

EXAMPLE 3.2. If X is a topological space and if x is in X, then the set $(\mathrm{Nbd}(X, x), \supseteq)$ of neighborhoods of x ordered by containment is a preordered, directed set.

DEFINITION 3.21. Let $(D, \leq)$ be a preordered, directed set. A functor $F : (D, \leq) \to \mathcal{C}$ from $(D, \leq)$ to a category $\mathcal{C}$ of modules is called a **direct system** of modules.

EXAMPLE 3.3. Let X be a topological space, let A be a ring, and let $\mathcal{F}$ be a presheaf of A-modules on X. For any point x of X, the restriction $\mathcal{F}|(\mathrm{Nbd}(X,x),\supseteq)^{\mathrm{op}}$ of the presheaf $\mathcal{F}$ to the opposite category of the set of neighborhoods of x under containment is a direct system. Taking the opposite category converts $\mathcal{F}$ into a covariant functor.

DEFINITION 3.22. Let X be a topological space, let A be a ring, let $\mathcal{F}$ be a presheaf of A-modules on X, and let x be a point of X. The **direct limit** of the direct system of A-modules $\mathcal{F}|(\mathrm{Nbd}(X,x),\supseteq)^{\mathrm{op}}$ is the A-module

$$\varinjlim_{x\in U}\mathcal{F}(U) := \left(\bigoplus_{x\in U}\mathcal{F}(U)\right)/M$$

where M is the submodule of the direct sum generated by the elements $i_U(s) - i_V(s|_V)$, where U and V are open neighborhoods of x, $V\subseteq U$, s is in $\mathcal{F}(U)$, and where i_U denotes the canonical map of $\mathcal{F}(U)$ into the direct sum.

Recall the universal property of the direct limit.

EXERCISE 3.7. Let X be a topological space, let A be a ring, and let $\mathcal{F}$ and $\mathcal{G}$ be presheaves of A-modules. Show that a natural transformation τ from the direct system $\mathcal{F}|(\mathrm{Nbd}(X,x),\supseteq)^{\mathrm{op}}$ to $\mathcal{G}|(\mathrm{Nbd}(X,x),\supseteq)^{\mathrm{op}}$ induces a unique map

$$\tau_x : \varinjlim_{x\in U}\mathcal{F}(U) \to \varinjlim_{x\in U}\mathcal{G}(U).$$

If M is an A-module, we let M also denote the constant presheaf with value M. A natural transformation $\tau:\mathcal{F}\to M$ induces a unique map

$$\tau_x : \varinjlim_{x\in U}\mathcal{F}(U) \to M$$

for each x in X.

DEFINITION 3.23. Let X be a topological space, let A be a ring, let $\mathcal{O}_X$ be a sheaf of A-modules on X, and let x be a point of X. The **stalk** of $\mathcal{O}_X$ at x is the A-module

$$\mathcal{O}_{X,x} := \varinjlim_{x\in U}\mathcal{F}(U)$$

For each open set U containing x, there is a canonical map $\mathcal{O}_X(U)\to\mathcal{O}_{X,x}$ which sends a section s defined over U to the its equivalence class, denoted by s_x and called the **germ** of s at x.

REMARK 3.24. Let X be a topological space, let A be a ring, let $\mathcal{O}_X$ be a sheaf of A-modules on X, and let x be a point of X. The stalk $\mathcal{O}_{X,x}$ can be defined as the set of pairs (U, s) where U is an open neighborhood of x, and where s is in $\mathcal{O}_X(U)$, under the following equivalence relation. Two such pairs (U, s) and (V, t) are equivalent if and only if there exists an open set W with $x \in W \subseteq U \cap V$ such that $s|_W = t|_W$.

DEFINITION 3.25. A ringed space $(X, \mathcal{O}_X)$ is a **locally ringed space** if for each x in X, the stalk $\mathcal{O}_{X,x}$ is a local ring.

EXAMPLE 3.4. An affine scheme is a locally ringed space.

The direct image of a sheaf is needed to state the definition of a morphism of ringed spaces.

DEFINITION 3.26. Let $\varphi : X \to Y$ be a continuous map of topological spaces. If $\mathcal{F}$ is a sheaf on X, then $\varphi_*\mathcal{F}$ denotes the **direct image** presheaf Y, given on an open subset U of Y by $\varphi_*\mathcal{F}(U) = \mathcal{F}(\varphi^{-1}(U))$.

PROPOSITION 3.27. *The direct image presheaf defined in Definition 3.26 is a sheaf.*

DEFINITION 3.28. Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be ringed spaces. A **morphism of ringed spaces** $(\varphi, \varphi^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ is a pair consisting of a continuous map $\varphi : X \to Y$ and a morphism $\varphi^\# : \mathcal{O}_Y \to \varphi_*\mathcal{O}_X$ of sheaves.

REMARK 3.29. Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be ringed spaces, and let x be a point of X. A morphism of ringed spaces

$$(\varphi, \varphi^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

induces a map

$$\varphi_x^\# : \mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}$$

given by the following prescription. Represent the germ $s_{\varphi(x)}$ of a section at the point $\varphi(x)$ by a pair (U, s), where U is an open set in Y containing $\varphi(x)$, and where s is in $\mathcal{O}_Y(U)$. The map $\varphi_x^\#$ sends the germ $s_{\varphi(x)}$ to the germ of $\varphi_U^\#(s)$ at x.

EXERCISE 3.8. In the notation of Remark 3.29, show that the induced map $\varphi_x^\#$ is well-defined as follows.

(a) Show that $\varphi^\#$ induces a natural transformation of direct systems

$$\varphi_x : \mathcal{O}_Y|(\mathrm{Nbd}(Y, \varphi(x)), \supseteq)^{\mathrm{op}} \to \varphi_*\mathcal{O}_X|(\mathrm{Nbd}(Y, \varphi(x)), \supseteq)^{\mathrm{op}}$$

(b) Show that there is a natural transformation

$$\tau_x : \varphi_*\mathcal{O}_X|(\mathrm{Nbd}(Y, \varphi(x)), \supseteq)^{\mathrm{op}} \to \mathcal{O}_{X,x}$$

(c) Obtain the map $\varphi_x^\#$ as the map induced by $\tau_x \circ \varphi_x$ by taking direct limits.

DEFINITION 3.30. Let $(A, \mathfrak{m})$ and $(B, \mathfrak{n})$ be local rings. A **morphism of local rings** is a ring homomorphism $\varphi : A \to B$ such that $\varphi^{-1}(\mathfrak{n}) = \mathfrak{m}$.

DEFINITION 3.31. Let $(X, \mathcal{O}_X)$ and $(Y, \mathcal{O}_Y)$ be locally ringed spaces. A **morphism of locally ringed spaces** is a morphism

$$(\varphi, \varphi^\#) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

of ringed spaces such that for each point x of X, the induced map $\varphi_x^\# : \mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}$ on stalks is a morphism of local rings.

DEFINITION 3.32. A locally ringed space $(X, \mathcal{O}_X)$ is a **scheme** if for each point x in X, there is a ring A and an open set $U \subseteq X$ containing the point x such that the locally ringed space $(U, \mathcal{O}_X|U)$ and the affine scheme $(\text{Spec } A, \widetilde{A})$ are isomorphic as locally ringed spaces.

DEFINITION 3.33. A morphism $X \to Y$ of schemes is a morphism as locally ringed spaces.

PROPOSITION 3.34. *Let X be a scheme and let A be a ring. Then the canonical map*

$$Hom_{Sch}(X, Spec\ A)) \to Hom_{Ring}(A, \Gamma(X, \mathcal{O}_X)),$$

which sends the morphism of schemes

$$\left(\varphi, \varphi^\#\right) : (X, \mathcal{O}_X) \to \left(Spec\ A, \widetilde{A}\right)$$

to the ring homomorphism $\varphi^\#_{Spec\ A}$, is a bijection.

If A and B are rings, and if $\varphi : A \to B$ is a ring homomorphism, then the preimage of φ induces a map $\varphi^* : \text{Spec } B \to \text{Spec } A$ which sends a prime ideal $\mathfrak{p}$ of A to $\varphi^{-1}(\mathfrak{p})$, which is a prime ideal of A.

PROPOSITION 3.35. *Let $\varphi : A \to B$ be a ring homomorphism. The induced map $\varphi^* : Spec\ B \to Spec\ A$ is continuous.*

PROOF. This is an immediate consequence of the identity

$$(\varphi^*)^{-1}(D(f)) = D(\varphi(f)),$$

where f is an element of the ring A. □

EXAMPLE 3.5. Let $\varphi : A \to B$ be a ring homomorphism. The induced map

$$\varphi^* : \text{Spec } B \to \text{Spec } A$$

itself induces a morphism

$$\varphi^{\#} : \widetilde{A} \to (\varphi^*)_* \widetilde{B}$$

of the associated sheaves of A and B by the universal property of the inverse limit. In general, by taking inverse limits over basic open sets contained in a given open subset U of Spec A, the universal property of the inverse limit yields a map

$$\varphi^{\#}_U : \widetilde{A}(U) \to (\varphi^*)_* \widetilde{B}(U),$$

and such maps commute with restriction maps. Hence, a ring homomorphism $\varphi : A \to B$ induces a morphism $(\varphi, \varphi^{\#}) : (\text{Spec } B, \widetilde{B}) \to (\text{Spec } A, \widetilde{A})$ of affine schemes.

In particular, if f is in A, we have a natural map $A_f \to B_{\varphi(f)}$, which induces a map

$$\widetilde{A}(D(f)) \to (\varphi^*)_* \widetilde{B}(D(f)).$$

This map is (to within canonical isomorphism) the map $A_f \to B_{\varphi(f)}$ since $\widetilde{A}(D(f)) = A_f$ and $(\varphi^*)_* \widetilde{B}(D(f)) = \widetilde{B}((\varphi^*)^{-1} D(f)) = B(D(\varphi(f))) = B_{\varphi(f)}$ by Proposition 3.35. One may recover the original ring homomorphism φ by taking $f = 1$, so that $D(f) = \text{Spec } A$.

Example 3.6 (Arithmetic surface). A prime ideal $\mathfrak{p}$ in the polynomial ring $\mathbb{Z}[x]$ must be one of the following:

(i). the zero ideal (0).

(ii). A principal ideal $p\mathbb{Z}[x]$ for p prime in $\mathbb{Z}$.

(iii). A maximal ideal (p, F) for p prime in $\mathbb{Z}$ and where F is a primitive irreducible polynomial in $\mathbb{Z}[x]$ that remains irreducible after reduction modulo p.

(iv). A principal ideal (F) where F is an irreducible polynomial of positive degree in $\mathbb{Z}[x]$ of content 1.

A proof is as follows. Let $\mathfrak{p}$ be a prime ideal of the ring $\mathbb{Z}[x]$. Since $\mathbb{Z}[x]$ is an integral domain, the zero ideal (0) is prime, so we may suppose that $\mathfrak{p}$ is a nonzero ideal. The ring $\mathbb{Z}$ is noetherian, so by Hilbert's basis theorem, the ring $\mathbb{Z}[x]$ is noetherian. Hence the ideal $\mathfrak{p}$ is finitely generated, say

$$\mathfrak{p} = (a_1, \ldots, a_n, f_1, \ldots, f_n),$$

where the a_i, if present, are nonzero elements of $\mathbb{Z}$, and where the f_i, if present, are polynomials of positive degree.

Suppose that $\mathfrak{p} = (a_1, \ldots, a_n)$. Since $\mathbb{Z}$ is a principal ideal domain, calculating in the ideal with degree zero polynomials in $\mathbb{Z}[x]$ shows that $\mathfrak{p} = (n)$ for some integer n which must be prime since $\mathfrak{p}$ is prime.

Suppose that $\mathfrak{p} = (a_1, \dots, a_n, f_1, \dots, f_n)$. By the previous case, we may suppose that $\mathfrak{p} = (p, f_1, \dots, f_n)$ where p is a prime of $\mathbb{Z}$. Since $\mathbb{F}_p[x]$ is a principal ideal domain, we have $(f_1, \dots, f_n) = (F)$ for some polynomial F in $\mathbb{F}_p[x]$. Note that each polynomial f_i in $\mathfrak{p}$ can be replaced with its reduction modulo p without changing the ideal. Furthermore, all computations with the polynomial generators f_i in the ideal $\mathfrak{p}$ can be performed modulo p, in particular, the computation in $\mathbb{F}_p[x]$ expressing F as the greatest common divisor of the f_i can be performed in the ideal $\mathfrak{p}$, which implies that $\mathfrak{p} = (p, f_1, \dots, f_n) = (p, F)$, where F must remain irreducible modulo p since $\mathfrak{p}$ is prime.

Finally, suppose that $\mathfrak{p} = (f_1, \dots, f_n)$. We proceed by induction and suppose that $\mathfrak{p} = (f, g)$. Since $\mathfrak{p}$ is prime, f and g can be taken irreducible of content 1 (since $\mathfrak{p}$ is prime and $\mathbb{Z}[x]$ is a UFD, an irreducible factor of f must lie in $\mathfrak{p}$, so f can be taken to irreducible without changing $\mathfrak{p}$. Either the content of f is in $\mathfrak{p}$ or the primitive part of f is in $\mathfrak{p}$. The content of f cannot be in $\mathfrak{p}$ in the case under consideration).

Choose h in $\mathfrak{p}$ of minimal degree. By previous remarks, h must be irreducible of content 1. In $\mathbb{Q}[x]$, write $f = h \cdot q + r$ where either $r = 0$ or $\deg r < \deg h$. Clearing denominators, there is an integer a such that $a \cdot f = h \cdot q + r$ where we can assume that q and r lie in $\mathbb{Z}[x]$. By minimality of the degree of h, $r = 0$. By Gauss's Lemma, which states that the content is multiplicative, we have

$$a = \operatorname{cont}(a \cdot f) = \operatorname{cont}(h \cdot q) = \operatorname{cont}(q),$$

since h and f have content 1. It follows that $f = h \cdot u$ with u primitive. Since f is irreducible, u must be a unit. Therefore, $\mathfrak{p} = (f, g) = (h, g)$. Repeating the argument with g in place of f, we have $(h, g) = (h)$. By induction, we obtain what we want.

The inclusion map $i : \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$ induces a continuous map

$$i^* : \operatorname{Spec} \mathbb{Z}[x] \to \operatorname{Spec} \mathbb{Z}.$$

Figure 1 illustrates the arithmetic surface Spec $\mathbb{Z}[x]$, with primes of $\mathbb{Z}[x]$ fibred over corresponding primes of $\mathbb{Z}$. To illustrate Arakelov theory, a new "complex prime" is shown (for illustrative purposes only) adjoined to Spec $\mathbb{Z}[x]$ that is thought of as if it were fibred over a corresponding new "prime at infinity" adjoined to Spec $\mathbb{Z}$.

Our first example of a non-affine scheme is the projective scheme over a ring. Let R be a ring graded in nonnegative degrees:

$$R = \bigoplus_{n \geq 0} R_n.$$

For simplicity we suppose that R is generated as an R_0-algebra by R_1. The polynomial algebra $R_0[X_0, \ldots, X_k]$ is a graded ring of this type. If A is a ring and if I is an ideal of A, the graded ring $\bigoplus_{n\geq 0} I^n$ where $I^0 = A$ is also of this type.

DEFINITION 3.36. If R is a graded ring, we define the **irrelevant ideal** R_+ of R to be the direct sum $\bigoplus_{n\geq 1} R_n$.

DEFINITION 3.37. If R is a graded ring, we define the set Proj R to be the set of homogeneous prime ideals of R that do not contain R_+.

Let R be a graded ring, graded in nonnegative degrees. If f is a homogeneous element of degree n in R then the localized ring R_f is a $\mathbb{Z}$-graded ring (homogeneous elements of negative degree are possible). If x is homogeneous of degree m then xf^{-h} is of degree $m-hn$ for each $h \in \mathbb{Z}$. In particular, if f is of degree one, the degree zero part of R_f, denoted by $(R_f)_0$, consists of elements xf^{-n} where x is in R_n.

PROPOSITION 3.38. *Let R be a graded ring, graded in nonnegative degrees, let f be a homogeneous element of R of degree 1, and let X be a new variable of degree 1. There is a canonical isomorphism*

$$\varphi : (R_f)_0 [X, X^{-1}] \to R_f$$

which sends X to f.

PROOF. The map φ is surjective, since if $a/f^n \in R_f$ with a homogeneous of degree d, then $\varphi\left((a/f^d)X^{d-n}\right) = (a/f^d)f^{d-n} = a/f^n$.

For injectivity, suppose that $\sum_{k=-n}^{k=n} r_k X^k$ is in the kernel of φ, so that $\sum_{k=-n}^{k=n} r_k f^k = 0$ holds R_f. Multiplying by f^n, we may suppose (reindexing the r_k) that $\sum_{k=0}^{l} r_k f^k = 0$ for $l = 2n$. For each k, $r_k = x_k/f^{d_k}$ where d_k is the degree of x_k. Let j be the maximum degree d_k of the x_k. Multiplying by f^j, $\sum_{k=0}^{l} x_k f^{j-d_k+k} = 0$ in R_f, and taking j sufficiently large we may suppose that this identity holds in R. The degree of the term $x_k f^{j-d_k+k}$ is $j+k$, hence it is the only homogeneous summand of degree $j+k$ in the sum, and it must be zero. It follows that

$$\sum_{k=0}^{l} r_k X^k = \sum_{k=0}^{l} \frac{x_k}{f^{d_k}} \frac{f^{j-d_k+k}}{f^{j-d_k+k}} X^k = 0.$$

Dividing by X^n (and reindexing the r_k) we have that $\sum_{k=-n}^{k=n} r_k X^k = 0$ □

DEFINITION 3.39. Let f be a homogeneous element of R. We define the **basic open set determined by** f, denoted by $D_+(f)$, by

$$D_+(f) = \{\mathfrak{p} \in \text{Proj } R : f \notin \mathfrak{p}\}.$$

It is clear that $D_+f = D(f) \cap \text{Proj } R$.

DEFINITION 3.40. Let I be a graded ideal of R. The set $V_+(I)$ is the set of prime ideals of Proj R which contain I.

It is clear that $V_+(f) = V(f) \cap \text{Proj } R$. It is easy to check the following exercise.

EXERCISE 3.9. The subsets $V_+(I)$ defined in 3.40 are the closed sets of a topology on Proj R. A basis of opens for this topology is given by the collection of the sets $D_+(f)$ for f homogeneous in R.

THEOREM 3.41. *Let R be a ring graded in nonnegative degrees, and let M be a graded R-module. Then the function which to a basic open set $D_+(f)$, corresponding to a homogeneous element f of R of positive degree, associates the module $(M_f)_0$ extends to a sheaf on Proj R that we denote by $\widetilde{M}$. The ringed space $\left(\text{Proj } R, \widetilde{R}\right)$ is a scheme which on $D_+(f)$ is isomorphic to Spec $(R_f)_0$. Moreover, for each graded R-module M, there is a canonical isomorphism*

$$\widetilde{M}|_{D_+(f)} \to \widetilde{(M_f)_0}.$$

Towards the proof of Theorem 3.41, we prove the following.

LEMMA 3.42. *Let R be a ring graded in nonnegative degrees, and let f be a homogeneous element of R. The map*

$$\varphi : D_+(f) \to \text{Spec } (R_f)_0$$

which sends the graded ideal $\mathfrak{p} \in D_+(f)$ to the degree zero part of the extension of $\mathfrak{p}$ to $(R_f)_0$ is a homeomorphism, whose inverse ψ sends the prime ideal $\mathfrak{q}$ to the prime ideal of R given by

$$\left\{x : \text{For each homogeneous component } y \text{ of } x, \exists m, n \geq 1, \frac{y^m}{f^n} \in \mathfrak{q}\right\}.$$

PROOF. We show first that ψ is well defined. Let $\mathfrak{q}$ be a homogeneous prime ideal in $(R_f)_0$. We claim that $\mathfrak{p} = \psi(\mathfrak{q})$ is in $D_+(f)$. Clearly $f \notin \mathfrak{p}$, or else 1 is in $\mathfrak{q}$.

If x is in $\mathfrak{p}$ then by definition each homogeneous component of x is in $\mathfrak{p}$. If y is also in $\mathfrak{p}$ and x and y have no nonzero homogeneous components x_d and y_d of the same degree d, then $x + y$ is in $\mathfrak{p}$ by definition. Suppose that x and y are homogeneous elements of $\mathfrak{p}$ of the same degree. We may suppose that there are positive integers m and n

such that both x^m/f^n and y^m/f^n are in $\mathfrak{p}$. By the binomial theorem, we have

$$\frac{(x+y)^{2m}}{f^{2n}} = \sum_{k=0}^{m} \binom{2m}{k} \frac{y^{m-k}x^k}{f^n}\frac{x^m}{f^n} + \sum_{k=1}^{m} \binom{2m}{m+k} \frac{x^{m-k}y^k}{f^n}\frac{x^m}{f^n}$$

which is a sum of elements in $\mathfrak{q}$, hence $x+y$ is in $\mathfrak{p}$.

Ler r be a homogeneous element of R, and let x be a homogeneous element of $\mathfrak{p}$ so that for some $m, n \geq 1$, x^m/f^n is in $\mathfrak{q}$. Let a be the degree of r, and let b be the degree of f so that r^b/f^a is in $(R_f)_0$. Since $(r^b/f^a)^m$ is in $(R_f)_0$ and $(x^m/f^n)^b$ is in $\mathfrak{q}$, we have $(rx)^{bm}/f^{am+bn} \in \mathfrak{q}$. Hence rx is in $\mathfrak{p}$.

This shows that $\mathfrak{p}$ is a homogeneous ideal of R with $f \notin \mathfrak{p}$. We show that $\mathfrak{p}$ is prime. Let x, y be homogeneous elements of R with xy in $\mathfrak{p}$. Then

$$\frac{XY}{F} \in \mathfrak{q}$$

where X is a power of x, Y is a power of y, and F is a power of f. Let a be the degree of X, b the degree of Y, and c the degree of F. Then $a+b=c$ and

$$\left(\frac{XY}{F}\right)^c = \frac{X^c}{F^a}\frac{Y^c}{F^b} \in \mathfrak{q}$$

where the fractions X^c/F^a and Y^c/F^b have degree 0. Since $\mathfrak{q}$ is prime, either $X^c/F^a \in \mathfrak{q}$ or $Y^c/F^b \in \mathfrak{q}$. Hence either x or y is in $\mathfrak{p}$.

Note that for $\mathfrak{p} \in D_+(f)$, $\varphi(\mathfrak{p}) = \mathfrak{p}R_f \cap (R_f)_0$. It is easy to show that φ and ψ are mutually inverse. Since they preserve inclusions, they are continuous.

□

4. Projective modules

DEFINITION 4.1. Let A be a ring. An A-module P is called **projective** if for every surjective A-homomorphism $M \to M'$ of A-modules, the canonical homomorphism $\mathrm{Hom}_A(P, M) \to \mathrm{Hom}_A(P, M')$ is surjective.

The A-module A is projective. The direct sum of any set of projective A-modules is projective. Thus, if I is a set, the free A-module $A^{(I)}$ is a projective A-module.

PROPOSITION 4.2. *Let A be a ring, and let P be an A-module. The following statements are equivalent.*

(i) P is projective.

(ii) The functor $Hom_A(P, \cdot)$ is exact; i.e., transforms exact sequences into exact sequences.

(iii) P is a direct summand of a free A-module.

Proof. Statement (ii) is a reformulation of (i). If P is a direct summand of a free A-module $A^{(I)}$, then $\mathrm{Hom}_A(P, \cdot)$ is a "direct summand" of $\mathrm{Hom}_A\left(A^{(I)}, \cdot\right)$, which is clearly exact, so (iii) implies (ii). For the converse, let $(x_i)_{i\in I}$ be a family of generators for P over A, so that one has a surjection $\alpha : A^{(I)} \to P$. By (ii), the induced map $\mathrm{Hom}_A\left(A^{(I)}, P\right) \to \mathrm{Hom}_A(P, P)$ is surjective, hence there exists $\beta : P \to A^{(I)}$ such that $\alpha\circ\beta = 1_P$, which implies that $A^{(I)} = \beta(P) \oplus \ker \alpha$. To see this, note that $x \in A^{(I)}$ has the form $x = \beta\alpha(x) + (x - \beta\alpha(x))$ so that $\beta\alpha(x) \in \beta(P)$ and $x - \beta\alpha(x) \in \ker \alpha$. □

Note that P is a projective A-module of finite type if and only if P is a direct summand of a free A-module of finite type.

Definition 4.3. Let A be a ring and let A be an A-module. We denote by $M^\vee$, called M **dual**, the A-module $\mathrm{Hom}_A(M, A)$.

For A-modules M and N there is a canonical map

$$M^\vee \otimes_A N \to \mathrm{Hom}_A(M, N)$$

which to $\varphi \otimes v$ associates the A-linear map from M to N given by $w \mapsto \varphi(w)v$.

Proposition 4.4. *Let A be a ring and let P be an A-module. The following statements are equivalent.*

(i) P is a projective A-module of finite type.

(ii) The canonical map

$$P^\vee \otimes_A P \to End_A\ (P)$$

is surjective.

Proof. The implication (i) implies (ii) is evident for free modules of finite type. By Proposition 4.2 it is also true for projective modules. For (ii) implies (i), observe that the identity map 1_P on P is in the image of $P^\vee \otimes_A P$. Hence, for some positive integer n, there exist linear maps $\varphi_1, \dots, \varphi_n : P \to A$, and elements $x_1, \dots, x_n$ of P such that $y = \sum_{i=1}^n \varphi_i(y)x_i$ for each y in P. Therefore, the x_i generate P, and so one has a surjection $\alpha : A^n \to P \to 0$ which associates the standard basis element e_i of A^n with x_i. The map $\beta : A^n \to P$ defined by $\beta(y) = \sum_{i=1}^n \varphi_i(y)e_i$ satisfies $\alpha \circ \beta = 1_P$, hence (i) holds by Proposition 4.2. □

Exercise 4.1. Under the conditions of Proposition 4.4 show that $P^\vee \otimes_A P \to \mathrm{End}_A\,(P)$ is an isomorphism (verify this first for P free of finite type).

Exercise 4.2. Let A be a ring.

a) For each A-module M, verify that there is a canonical A-linear map (the evaluation map) $M^\vee \otimes_A M \to A$ which sends $\varphi \otimes y$ to $\varphi(y)$.

b) If P is an free A-module of finite type, verify, using Exercises 4.1 and 4.2 a), that the image of $f \in \mathrm{End}_A(P)$ by the composite map

$$\mathrm{End}_A(P) \to P^\vee \otimes_A P \to A$$

is the trace of f. One thus defines the **trace of an endomorphism** of a **projective** module of finite type.

Exercise 4.3. Let A be a ring. For each A-module M there is a canonical A-linear map

$$M \to M^{\vee\vee}.$$

a) Verify that if M is projective of finite type, then the preceding homomorphism is bijective.

b) Show that if M is projective of finite type then so is $M^\vee$.

Exercise 4.4. Let A be a ring.

a) Verify that a projective A-module is flat. b) Let S be a multiplicatively stable subset of A. Show that if P is a projective A-module, then $S^{-1}P$ is a projective $S^{-1}A$-module.

c) If P is a projective A-module, show that for each integer n, the A-modules $T_n(P), \mathrm{Sym}_n(P)$, and $\Lambda^n(P)$ are projective.

Proposition 4.5. *Let A be a ring and let M be an A-module. If M is projective of finite type, then M is finitely presented.*

Proof. Suppose that M is projective of finite type, and let $\alpha : A^n \to M$ be an epimorphism. Since M is projective, there is a map $\beta : M \to A^n$ such that $\alpha \circ \beta = 1_M$. It follows that $A^n = \ker\alpha \oplus M$, hence $\ker\alpha$ is of finite type, since it is a quotient of A^n. Therefore, there is an exact sequence

$$A^m \longrightarrow A^n \xrightarrow{\alpha} M \longrightarrow 0.$$

□

Exercise 4.5. Let M be an A-module, suppose that $(D(f_i))_{i=1}^n$ is an open cover of Spec A, and suppose that M_{f_i} is a free A_{f_i}-module of finite rank for each i. Show that M is finitely presented.

DEFINITION 4.6. Let A be a ring and let M be an A-module. We say that M is **punctually free of finite type** if for each prime ideal $\mathfrak{p} \in \operatorname{Spec} A$, the localized module $M_{\mathfrak{p}}$ is a free $A_{\mathfrak{p}}$-module of finite type.

THEOREM 4.7. *Let A be a ring and let P be an A-module. The following statements are equivalent.*
i) P is projective of finite type.
ii) P is locally free of finite type for the Zariski topology on Spec(A).
iii) P is punctually free of finite type.

PROOF. Lemma 4.8 below shows that (iii) implies (ii), while Lemma 4.9 below shows that (i) implies (iii).

To show that (ii) implies (i) we use Proposition 4.4. Let

$$M = \operatorname{coker}\left(P^{\vee} \otimes_A P \to \operatorname{End}_A\ (P)\right).$$

Since P is locally free for the Zariski topology, there exist elements $f_1, \ldots, f_n \in A$ which form a partition of unity, such that P_{f_i} is a free A_{f_i}-module of finite type for each i.

To show that for each i, $M_{f_i} = 0$, we use the following two facts. First, localization commutes with the tensor product; i.e., there is a canonical isomorphism $S^{-1}\left(P \otimes_A Q\right) \to S^{-1}P \otimes_{S^{-1}A} S^{-1}Q$.

In addition, if P is finitely presented, then there is a canonical isomorphism

$$S^{-1}\operatorname{Hom}_A(P, Q) \to \operatorname{Hom}_{S^{-1}A}\left(S^{-1}P, S^{-1}Q\right).$$

By Exercise 4.5, M is finitely presented, hence

$$M_{f_i} = \operatorname{coker}\ \left(P_f^{\vee} \otimes_{A_f} P_f \to \operatorname{End}_{A_f}(P_f)\right)$$

Since for each i, P_{f_i} is a free A_{f_i}-module of finite type, the map

$$P_f^{\vee} \otimes_{A_f} P_f \to \operatorname{End}_{A_f}(P_f)$$

is surjective, hence $M_{f_i} = 0$ for each i. By Lemma 1.12, $M = 0$. □

LEMMA 4.8. *Let P be an A-module of finite type. Let $\mathfrak{p}$ be a prime ideal of A and suppose that $\psi : A_{\mathfrak{p}}^n \to P_{\mathfrak{p}}$ is an isomorphism. Then there exists $f \in A - \mathfrak{p}$ and an isomorphism $\varphi : A_f^n \to P_f$ that extends ψ.*

PROOF. Let e_i be the standard basis element of $A_{\mathfrak{p}}^n$ for $1 \leq i \leq n$. There exist elements y_i in P and $g_i \in A - \mathfrak{p}$ such that

$$\psi(e_i) = \frac{y_i}{g_i}.$$

Let $f = \prod g_i$. If $\varphi = f\psi$, then $\varphi/f : A_f^n \to P_f$ extends ψ, although it need not be an isomorphism. Since P is of finite type, so is coker ψ. Moreover, coker $(\varphi/f)_{\mathfrak{p}} =$ coker $\psi = 0$, so by Exercise 1.3 b) there exists g in $A - \mathfrak{p}$ with coker $(\varphi/f)_g = 0$.

P_{fg} is a projective A_{fg}-module of finite type by Exercise 4.4 b). Consequently, the map $(\varphi/f)_g : A^n_{fg} \to P_{fg}$ splits, making the kernel ker $(\varphi/f)_g$ a quotient of A^n_{fg}, hence an A_{fg}-module of finite type. Since ker $((\varphi/f)_g)_{\mathfrak{p}} =$ ker $\psi = 0$, again by Exercise 1.3 b), there exists h in $A - \mathfrak{p}$ such that ker $(\varphi/f)_{gh} = 0$. It follows that $(\varphi/f)_{gh} : A^n_{fgh} \to P_{fgh}$ extends ψ. □

LEMMA 4.9. *Let A be a local ring with maximal ideal $\mathfrak{m}$ and let P be a projective A-module of finite type. Then P is a free A-module of rank equal to dim$_{A/\mathfrak{m}}(P/\mathfrak{m}P)$.*

PROOF. Let $x_1, \cdots, x_n$ be elements of P that yield a basis of $P/\mathfrak{m}P$ over the field $A/\mathfrak{m}$. Let $\varphi : A^n \to P$ be an A-homomorphism that sends the standard basis element e_i of A^n to x_i. By Proposition 1.8 φ is surjective. Define the A-module N by the exact sequence

$$0 \to N \to A^n \xrightarrow{\varphi} P \to 0.$$

Tensoring by $A/\mathfrak{m}$, it follows that

$$0 \to N \otimes_A A/\mathfrak{m} \to (A/\mathfrak{m})^n \xrightarrow{\overline{\varphi}} (P/\mathfrak{m}P) \to 0$$

is also exact. By definition, $\overline{\varphi}$ is a vector space isomorphism, hence its kernel $N \otimes_A A/\mathfrak{m} = N/\mathfrak{m}N$ is zero; i.e., $N = \mathfrak{m}N$. The module N is of finite type since P is projective, hence φ splits ($A^n = N \oplus P$). By Proposition 1.8, $N = 0$. It follows that P is free of rank $n = \dim_{A/\mathfrak{m}}(P/\mathfrak{m}P)$. □

COROLLARY 4.10. *Let A be a ring and let P be a projective A-module of finite type. The rank function $r(P)$: Spec $A \to \mathbb{N}$ which to a prime ideal $\mathfrak{p}$ of A associates the dimension of the vector space $P_{\mathfrak{p}}/\mathfrak{p}P_{\mathfrak{p}}$ over the field $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$, is locally constant.*

PROOF. Suppose that P is a projective A-module of finite type. Let $(D(f_i))_{i=1}^n$ be a finite open covering of Spec A by basic open sets. By Theorem 4.7, P is locally free of finite rank for the Zariski topology on Spec A, hence for each i, there exists an integer $n_i \geq 1$ such that $A^{n_i}_{f_i}$ is isomorphic to P_{f_i} as an A_{f_i}-module. Since localization is an exact functor, for each prime ideal $\mathfrak{p}$ in $D(f_i)$, $A^{n_i}_{\mathfrak{p}}$ is isomorphic to $P_{\mathfrak{p}}$ as an $A_{\mathfrak{p}}$-module. Since the module $P_{\mathfrak{p}}/\mathfrak{p}P_{\mathfrak{p}} = A^{n_i}_{\mathfrak{p}}/\mathfrak{p}A^{n_i}_{\mathfrak{p}} = (A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})^{n_i}$, we have that

$$\dim_{A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}} P_{\mathfrak{p}}/\mathfrak{p}P_{\mathfrak{p}} = n_i$$

for each prime ideal $\mathfrak{p}$ in $D(f_i)$. □

Definition 4.11. Let A be a ring and let P be a projective A-module of finite type. We say that P **is of rank** n, if the rank function $r(P) : \mathrm{Spec}\ A \to \mathbb{N}$ defined above is constant and equal to n.

5. Invertible modules

Definition 5.1. Let A be a ring. L is an invertible A-module if and only if L is a projective module of rank one.

Proposition 5.2. *Let A be a ring. The following statements are equivalent.*

(1) L is an invertible A-module.

(2) $L \otimes_A L^\vee \to A$ is an isomorphism.

Corollary 5.3. *If L is invertible, then*

$$A \to End_A(L)$$

is an isomorphism.

Exercise 5.1. Let k be a field, let $A = k[x, y]$ be the polynomial ring in two variables over k, and let $I = (x, y)$.

1) Show that $\mathrm{End}_A(I) = A$. (Hint: if K is the field of fractions of A, check that $\mathrm{End}_k(I \otimes_A K) = K$).

2) Prove that I is not an invertible A-module.

Exercise 5.2. a) Let P be a projective module of rank n. Show that $\wedge^n P$ is invertible.

b) Show that $\mathrm{Hom}_A(\wedge^{n-1}P, \wedge^n P) = P^\vee$.

Remark 5.4. If L is an invertible A-module, $L^\vee$ is also invertible (note that $L^\vee \otimes_A L^{\vee\vee} \to A$ is an isomorphism).

The following exercise is used repeatedly.

Exercise 5.3. If A is a domain, if L_1 and L_2 are invertible A-modules, and if $\varphi : L_1 \to L_2$ is an A-linear map, show that if $\varphi \neq 0$ then it is injective.

Definition 5.5. Let A be a ring. The Picard group of A, denoted by $\mathrm{Pic}(A)$, is the set of isomorphism classes of invertible A-modules.

Proposition 5.6. *The tensor product $\otimes_A$ makes $Pic(A)$ into an abelian group in which the class of the ring A is the neutral element, and the inverse of the class of an invertible A-module is the class of its dual.*

Proof. Canonical isomorphisms involving the tensor product $\otimes_A$ imply that $\mathrm{Pic}(A)$ is a commutative semigroup with neutral element A.

If L is an invertible A-module, the isomorphism $L \otimes_A L^\vee \to A$ implies that the inverse of the class of an invertible module is the class of its dual. $\square$

EXERCISE 5.4. Given an exact sequence

$$0 \to P' \to P \to P'' \to 0$$

of projective A-modules of finite type, show that

$$\wedge^{\max} P = \wedge^{\max} P' \otimes_A \wedge^{\max} P''.$$

That is, show that

$$\wedge^{\max} : \{\text{Projective modules of constant rank}\} \to \operatorname{Pic}(A)$$

is an additive function.

6. Invertible sheaves on a scheme

DEFINITION 6.1. Let $(X, \mathcal{O}_X)$ be a ringed space. A sheaf $\mathcal{F}$ of modules on X is an $\mathcal{O}_X$**-module** if for each open subset U of X, $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$-module, and the module action is compatible with the restriction maps of $\mathcal{F}$ and $\mathcal{O}_X$. An $\mathcal{O}_X$-module $\mathcal{F}$ is **locally free** if there is an open cover $(U_i)_{i \in I}$ of X such that for each $i \in I$, $\mathcal{F}|_{U_i}$ is a free $\mathcal{O}_X|_{U_i}$-module.

DEFINITION 6.2. Let $(X, \mathcal{O}_X)$ be a scheme. An **invertible sheaf on** X is a locally free $\mathcal{O}_X$-module $\mathcal{L}$ of rank 1.

DEFINITION 6.3. Let X be a topological space and let $\mathcal{F}$ and $\mathcal{G}$ be sheaves on X. We let $\operatorname{Hom}(\mathcal{F}, \mathcal{G})$ denote the collection of all natural transformations from $\mathcal{F}$ to $\mathcal{G}$. The assignment

$$\operatorname{Hom}(\mathcal{F}, \mathcal{G})(U) = \operatorname{Hom}(\mathcal{F}|_U, \mathcal{G}|_U)$$

defines a sheaf on X called the **sheaf Hom**.

DEFINITION 6.4. Let $(X, \mathcal{O}_X)$ be a ringed space, and let $\mathcal{F}$ be an $\mathcal{O}_X$-module. The **dual sheaf** $\mathcal{F}^\vee$ is the sheaf $\operatorname{Hom}(\mathcal{F}, \mathcal{O}_X)$.

EXERCISE 6.1. Let $(X, \mathcal{O}_X)$ be a ringed space. The following properties of the sheaf hom and the dual sheaf hold for a locally free $\mathcal{O}_X$-module $\mathcal{F}$ of finite rank.

1) $(\mathcal{F}^\vee)^\vee = \mathcal{F}$

2) If $\mathcal{G}$ is an $\mathcal{O}_X$-module (not necessarily locally free of finite rank), then $\operatorname{Hom}(\mathcal{F}, \mathcal{G}) = \mathcal{F}^\vee \otimes_{\mathcal{O}_X} \mathcal{G}$.

EXERCISE 6.2. Let $(X, \mathcal{O}_X)$ be a ringed space. Prove that the set of isomorphism classes of invertible sheaves on X is a group under the tensor product $\otimes_{\mathcal{O}_X}$ of sheaves.

Definition 6.5. Let $(X, \mathcal{O}_X)$ be a ringed space. The set of isomorphism classes of invertible sheaves on X is called the **Picard group** of X, denoted by $\operatorname{Pic}(X)$.

Exercise 6.3. Let X be a scheme. If $\operatorname{Spec} A \hookrightarrow X$ is an affine open subset of X, and if $\mathcal{L}$ is an invertible sheaf on X, prove that

$$\mathcal{L}|_{\operatorname{Spec} A} = \widetilde{M},$$

where M is an invertible A-module.

Definition 6.6. Let $(X, \mathcal{O}_X)$ be a scheme, and let $\mathcal{F}$ be an $\mathcal{O}_X$-module. $\mathcal{F}$ is a **quasi-coherent sheaf on** X if there is an open covering $(U_i)_{i\in I}$ of X by affine open subsets $U_i = \operatorname{Spec} A_i$ such that for each $i \in I$ there is an A_i-module M_i such that $\mathcal{F}|_{U_i} = \widetilde{M_i}$. If each A_i-module M_i is of finite presentation (for example, if A_i is noetherian and M_i is of finite type), we say that $\mathcal{F}$ is a **coherent sheaf on** X.

An invertible sheaf on a scheme is coherent.

Let $(X, \mathcal{O}_X)$ be a ringed space, and $\mathcal{I}$ be an $\mathcal{O}_X$-module. If for each open subset U of X, $\mathcal{I}(U)$ is an ideal of the ring $\mathcal{O}_X(U)$, then we call $\mathcal{I}$ a **sheaf of ideals** on X. A coherent sheaf $\mathcal{I}$ of ideals of the structure sheaf $\mathcal{O}_X$ of a scheme X can be used to define a closed subscheme Y of X, given by $Y = \operatorname{Supp}(\mathcal{O}_X/\mathcal{I}) = \{\mathfrak{p} \in X : (\mathcal{O}_X/\mathcal{I})_{\mathfrak{p}} \neq 0\}$. The construction of this subscheme is the "sheaf analogue" of the support of an A-module M, which is the set of prime ideals $\mathfrak{p} \in \operatorname{Spec} A$ such that $M_{\mathfrak{p}} \neq 0$.

Definition 6.7. A **Cartier divisor** on a scheme X is a closed subscheme defined an invertible sheaf of ideals $\mathcal{I}$ on X. Equivalently, $\mathcal{I}$ is locally defined by a single element that is not a divisor of zero.

CHAPTER 2

Rings of dimension one

1. Noetherian rings of dimension zero

2. Principal ideal rings

3. Integral elements

Definition 3.1. Let B be a ring and let A be a subring of B. One says that the element x of B is **integral over** A if it satisfies an equation called an equation of integral dependence of the form

$$x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

where the a_i are in A. One says that B is **integral** over A if each element of B satisfies an equation of integral dependence with coefficients in A.

For example, the field $\mathbb{C}$ of complex numbers is integral over the field $\mathbb{R}$ of real numbers. Neither $\mathbb{C}$ nor $\mathbb{R}$ is integral over the field $\mathbb{Q}$ of rational numbers.

Proposition 3.2. *Let B be a ring and let A be a subring of B. Let x be an element of B. The following assertions are equivalent.*

(i) X is integral over A.

(ii) The ring $A[x]$ is an A-module of finite type.

(iii) There exists a subring of B, containing $A[x]$, and which is an A-module of finite type.

Corollary 3.3. *Let B be a ring and let A be a subring. Then the set of elements of B which are integral over A is a subring of B, called the* **integral closure** *of A in B.*

Proof. In effect, if $A[x]$ and $A[y]$ are A-modules of finite type, then $A[x, y]$ is an $A[x]$-module of finite type. Since $A[x]$ is an A-module of finite type, $A[x, y]$ is an A-module of finite type. It follows that $x - y$ and xy are integral over A. $\square$

Example 3.1. The real numbers $\sqrt{2}$ and $\sqrt[3]{7}$ are integral over $\mathbb{Z}$. It is tedious to find an equation of integral dependence for $\sqrt{2} + \sqrt[3]{7}$.

The following particular case is of constant interest.

DEFINITION 3.4. An integral domain A is **integrally closed** if it is integrally closed in its field of fractions.

EXERCISE 3.1. a) Show that a principal ideal domain is integrally closed.

b) Let A be an integral domain, and let S be a multiplicatively stable subset of A. Show that if A is integrally closed then so is $S^{-1}A$.

PROPOSITION 3.5. *Let B be an integral domain and let A be a subring of B such that B is integral over A. Then B is a field if and only if A is field.*

PROOF. If B is a field and if x is a nonzero element of A, then x^{-1} satisfies the equation

$$x^{-n} + a_1 x^{-n+1} + \cdots + a_{n-1} x^{-1} = 0.$$

Multiplying by x^n one sees that

$$x(-a_1 - a_2 x - a_3 x^2 - \cdots - a_{n-1} x^{n-2} - a_n x^{n-1}) = 1.$$

Conversely, if A is a field and if B is integral over A, every element x of B satisfies an equation $x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$. Given such an equation of minimal degree, one sees that $a_n \neq 0$. Therefore, a_n is invertible and $x a_n^{-1}(-x^{n-1} - a_1 x^{n-2} - \cdots - a_{n-1}) = 1$. □

EXERCISE 3.2. Let A be a ring and let B be integral over A. Show that the map Spec $B \to$ Spec A is surjective.

EXERCISE 3.3. Let B be an A-algebra of finite type, and suppose that A is contained in B.

a) Suppose that A is local and that B is integral over A. Show that if $\mathfrak{q}$ is a prime ideal of B such that $\mathfrak{q} \cap A$ is a maximal ideal of A, then $\mathfrak{q}$ is a maximal ideal of B.

b) Show that if B is integral over A, the morphism Spec $B \to$ Spec A is surjective with finite fibres.

4. Algebraic extensions of fields

5. Number fields, order of a number field, rings of algebraic integers

6. Discrete valuation rings, Dedekind rings

7. The cycle map

8. The map $Div(A) \to Pic(A)$

9. Rational points on a projective scheme over a Dedekind ring

CHAPTER 3

The compactified Picard group of an order of a number field

We introduce an invention of Arakelov: the assignment of a hermitian metric at each place at infinity of a number field to an invertible sheaf.

1. Complex vector spaces of dimension one

A **hermitian scalar product** on a vector space V over the field $\mathbb{C}$ of complex numbers has is a bilinear map $(\ ,\ ) : V \times V \to \mathbb{C}$ such that $(\lambda x, y) = \lambda(x, y)$ and $(x, y) = \overline{(y, x)}$ for each λ in $\mathbb{C}$ and for each x and y in V. Such a scalar product is called **positive** if $(x, x) = \|x\|^2 \geq 0$ for each x and if $\|x\| = 0$ implies $x = 0$. Positive hermitian scalar products are automatically nondegenerate.

Example 1.1. Let V be a vector space of dimension one over $\mathbb{C}$. Specifying a positive hermitian scalar product on V is the same as specifying the length $\|x\| \neq 0$ of a nonzero element x of V. In effect, if y and z are in V, one has $y = \lambda x, z = \mu x$ and therefore $(y, z) = \lambda\overline{\mu}\|x\|^2$.

Proposition 1.1. *The set of positive hermitian scalar products on a vector space V of dimension one over $\mathbb{C}$ is a principal homogeneous space over $\mathbb{R}_+^\times$.*

Proof. In effect, if $(\ ,\ )$ and $(\ ,\ )_1$ are hermitian scalar products on V and if $x \neq 0, x \in V$, one has $\|x\| = \|x\|_1$ for some real number λ. If the hermitian scalar products are positive then $\lambda \in \mathbb{R}_+^\times$. □

Remark 1.2. If V_1 and V_2 are two one dimensional complex vector spaces endowed with positive non-degenerate hermitian scalar products $(\ ,\ )_1$ and $(\ ,\ )_2$ respectively, the **tensor product** $V_1 \otimes_{\mathbb{C}} V_2$ is canonically endowed with the positive hermitian scalar product such that $\|x_1 \otimes x_2\| = \|x_1\|\|x_2\|$ where $x_i \neq 0$ and $x_i \in V_i$ for $i = 1, 2$. The **dual** $V^\vee$ vector space is endowed with the norm

$$\|x\| = \frac{|\varphi(x)|}{\|x\|}$$

for each nonzero x in V. By example 1.1 this norm is a positive hermitian scalar product.

EXERCISE 1.1. Let V be a one dimensional vector space over $\mathbb{C}$ endowed with a positive hermitian scalar product. Show that the trace map $V \otimes_{\mathbb{C}} V^{\vee} \to \mathbb{C}$ induces by 1.2 a hermitian scalar product.

DEFINITION 1.3. Let V be a one dimensional complex vector space. A bf hermitian metric on V is a positive hermitian scalar product on V.

DEFINITION 1.4. Let V be a one dimensional complex vector space endowed with a positive hermitian metric. The **canonical volume element** on V assigns the volume π to the unit disk in V:

$$\mathrm{Vol}\{z \in V : \|x\| \leq 1\} = \pi.$$

If W be a one dimensional real vector space endowed with a positive hermitian metric, then the **canonical volume element** on W assigns the length 2 to the unit interval in W:

$$\mathrm{Vol}\{z \in W : \|x\| \leq 1\} = 2.$$

We note that giving a volume element of V is the same as choosing a nonzero element of $\Lambda^2_{\mathbb{R}} V$.

2. Metrized invertible modules of an order of a number field

Let K be a number field. A **place** of K is a field embedding $\sigma : K \to \mathbb{C}$. Let $n = [K : \mathbb{Q}]$, so that $n = r_1 + 2r_2$, where r_1 the number of real places, and $2r_2$ the number of complex places. We let ϕ be a set of places at infinity containing r_1 real places and r_2 complex places, none of which is a conjugate of any other complex place.

DEFINITION 2.1. Let A be an order of the number field K. An invertible A-module $L \in \mathrm{Pic}(A)$ (i.e., L is a projective A-module of rank 1) endowed for each place σ in ϕ with a positive hermitian scalar product $(\ ,\ )_\sigma$ defined on the complex vector space $(L \otimes_A K) \otimes_\sigma \mathbb{C}$ is called a **metrized invertible A-module**. If $\|.\|_\sigma$ is the norm associated with $(\ ,\ )_\sigma$, then $(L, \|.\|_\sigma)$ denotes this metrized invertible A-module.

The notation $(L \otimes_A K) \otimes_\sigma \mathbb{C}$ means that K acts on $\mathbb{C}$ by the restriction of scalars to K defined be the field embedding $\sigma : K \to \mathbb{C}$, so that if $l \in L, k \in K$, and $z \in \mathbb{C}$, then

$$l \otimes k \otimes z = l \otimes 1 \otimes \sigma(k) \cdot z.$$

Let A be an order of a number field K, let L be a projective rank one A-module, let ϕ be as above and let $\sigma \in \phi$ be a nonreal place of K. We will suppose that the hermitian metric $\|.\|_\sigma$ defined on the one-dimensional complex vector space $V = (L \otimes_A K) \otimes_\sigma \mathbb{C}$ at the place σ satisfies

$$\|v\|_{\overline{\sigma}} = \|v\|_\sigma.$$

for each $v \in V$ to make our choice of metrics is independent of our choice of nonconjugate nonreal places of K.

EXAMPLE 2.1. $(A, (x_\sigma)_{\sigma\in\phi})$, where $x_\sigma \in \mathbb{R}^+$. We will use the notation

$$\|1\|_\sigma = x_\sigma,$$

which defines a hermitian metric on A for $\sigma \in \phi$ by the rule

$$\|a\|_\sigma = x_\sigma \cdot |\sigma(a)|$$

for $a \in A$, where $|.|$ is the usual absolute value on $\mathbb{C}$.

EXAMPLE 2.2. The order A together with the metrics defined at each place $\sigma \in \phi$ by $\|1\|_\sigma = 1$ in the notation of the preceding example. The metrized invertible module $(A, 1)$ is called the **trivial** metrized invertible A-module.

One has a notion of isomorphism between metrized invertible modules.

DEFINITION 2.2. An **isometry** between two metrized invertible modules $(L_1, \| \|_{1,\sigma})$ and $(L_2, \| \|_{2,\sigma})$ of an order A of a number field is an A-isomorphism $\varphi : L_1 \to L_2$ such that $\|\varphi(x)\|_{2,\sigma} = \|x\|_{1,\sigma}$ for each x in L_1.

EXAMPLE 2.3. Let u be a unit of A. The metrized invertible modules $(A, 1)$ and $(A, (|\sigma(u)|)_\sigma)$ are isometric. An isometry from $(A, 1)$ to $(A, (|\sigma(u)|)_\sigma)$ is given by $1 \mapsto u^{-1}$, since

$$\|u^{-1} \cdot x\|_{2,\sigma} = |\sigma(u)| \cdot |\sigma(u^{-1} \cdot x)| = |\sigma(x)| = \|x\|_{1,\sigma}.$$

LEMMA 2.3. *Two metrized invertible A-modules $(L, \| \|_{1,\sigma})$ and $(L, \| \|_{2,\sigma})$ having the same underlying invertible A-module L are isometric if and only if there exists a unit u of A such that $|\sigma(u)|\|x\|_{2.\sigma} = \|x\|_{1,\sigma}$ for each x in L and each σ in ϕ.*

PROOF. In essence, $\mathrm{Hom}_A(L, L) = A$ and therefore $\mathrm{Aut}_A(L, L) = A^\times$, hence self-isometries of the A-module L are given by multiplication by a unit of the order A, since L is projective of rank 1. Hence if u is a unit of A such that $|\sigma(u)|\|x\|_{2,\sigma} = \|x\|_{1,\sigma}$ for each x in L and each σ in ϕ, then the map $\varphi(x) = u \cdot x$ is an isometry of L. $\square$

3. The compactified Picard Group

PROPOSITION 3.1. *The tensor product induces on the set of isometry classes of metric invertible A-modules the structure of a commutative group. This group is called the* **compactified Picard group** *of A and is denoted by $Pic_c(A)$.*

PROOF. $\square$

EXAMPLE 3.1. For each infinite place $\sigma \in \phi$, let x_σ be a positive real number. The pair $(A, (x_\sigma)_{\sigma\in\phi})$ represents an element of $\mathrm{Pic}_c(A)$ with underlying module A endowed with the hermitian metric $\| \ \|_\sigma$ at such that $\|1\|_\sigma = x_\sigma$ for each $\sigma \in \phi$. Similarly, $(A, (1))$ represents the identity element of $\mathrm{Pic}_c(A)$.

EXERCISE 3.1. Show that the map

$$\left(\mathbb{R}_+^\times\right)^\phi \to \mathrm{Pic}_c(A)$$

which to $(x_\sigma)_{\sigma\in\phi}$ associates the element $(A, (x_\sigma)_{\sigma\in\phi})$ is a group homomorphism.

EXERCISE 3.2. Show that the map

$$\mathrm{Pic}_c(A) \to \mathrm{Pic}(A).$$

which "forgets places at infinity" is a group homomorphism.

PROPOSITION 3.2 (First fundamental exact sequence). *There exists an exact sequence*

$$0 \to \mu(A) \to A^\times \xrightarrow{\sigma} \left(\mathbb{R}_+^\times\right)^\phi \to Pic_c(A) \to Pic(A) \to 0$$

where $\mu(A)$ is the group of roots of unity of A, and where

$$\sigma : A^\times \to \left(\mathbb{R}_+^\times\right)^\phi$$

is the map which to $u \in A^\times$ associates the element $(|\sigma(u)|)_{\sigma\in\phi}$ of $\left(\mathbb{R}_+^\times\right)^\phi$.

PROOF. By example 1.1 the map $\mathrm{Pic}_c(A) \to \mathrm{Pic}(A)$ is surjective. Its kernel is the set of "hermitian structures at places at infinity of A". By 1.1 and 3.1, this kernel is the image of $\left(\mathbb{R}_+^\times\right)^\phi$. By an application of lemma 2.3 one sees that the metrized invertible A-module $(A, (x_\sigma)_{\sigma\in\phi})$ is isometric to $(A, (1))$ if and only if there exists a unit u of A such that $x_\sigma = |\sigma(u)|$ for each $\sigma \in \phi$. It remains to prove the following lemma. $\square$

LEMMA 3.3. *Let K be a number field and let A an order of K. For each element x of A the following assertions are equivalent:*
(i) x is a root of unity

(ii) for each homomorphism of fields $\sigma : K \to \mathbb{C}$, $\sigma(x)$ has absolute value 1.

Moreover, the set $\mu(A)$ of roots of unity of A is a finite group.

Proof. □

4. The norm of an ideal

Proposition 4.1. *Let A be an order of a number field and let $\mathfrak{a}$ be a nonzero ideal of A such that $A/\mathfrak{A}$ is finite. If $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ are prime ideals of A containing $\mathfrak{a}$, then*

$$\#(A/\mathfrak{a}) = \prod_{i=1}^{r} \#\left(A_{\mathfrak{p}_i}/\mathfrak{a}A_{\mathfrak{p}_i}\right)$$

and

$$\log\left(\#(A_{\mathfrak{p}_i}/\mathfrak{a}A_{\mathfrak{p}_i})\right) = \mathit{length}\,(A_{\mathfrak{p}_i}/\mathfrak{a}A_{\mathfrak{p}_i})\log(\#(A/\mathfrak{p}_i)).$$

Definition 4.2. Let A be an order of a number field and let $\mathfrak{a}$ be a nonzero ideal of A. The **norm** of $\mathfrak{a}$, denoted by $N(\mathfrak{a})$, is the cardinality of $A/\mathfrak{a}$.

Example 4.1. If n is a nonzero integer, $N(n\mathbb{Z}) = |n|$.

Proposition 4.3. *The map $Div_+(A) \to \mathbb{N}$ is multiplicative.*

If I and J are two ideals in $\mathrm{Div}_+(A)$ we show

$$\#(A/IJ) = \#(A/I) \cdot \#(A/J).$$

Lemma 4.4. *Let B be a ring, and let x be an element of B that is not a zero divisor. If J is an ideal of B, then there is an exact sequence of B-modules*

$$0 \to B/J \to B/xJ \to B/xB \to 0.$$

Proof. The desired sequence can be obtained by combining two simpler exact sequences. First, the kernel of the canonical surjection

$$B/xJ \to B/xB \to 0$$

is xB/xJ. Next, the ideal J is the kernel of the surjection

$$B \to xB/xJ \to 0$$

defined by $1 \mapsto [x]$. This follows from the fact that multiplication by x is injective: whenever the elements y, z of B satisfy $xy = xz$, then $y = z$ since x is not a divisor of zero. Hence B/J is isomorphic to xB/xJ, which is the kernel of the map $B/xJ \to B/xB$. □

Applying lemma 4.4 to a localized ring $A_\mathfrak{p}$, where I and J are generated by one element, one obtains

$$\#(A_\mathfrak{p}/IJA_\mathfrak{p}) = \#(A_\mathfrak{p}/IA_\mathfrak{p})\#(A_\mathfrak{p}/IA_\mathfrak{p}).$$

COROLLARY 4.5. *The norm map extends to a group homomorphism $Div(A) \to \mathbb{N}$.*

LEMMA 4.6 (Second finiteness lemma). *Let A be an order of a number field and let r be a positive integer. Then the set of ideals of A of norm bounded by r is finite.*

PROOF. Each element of a finite group is annihilated by the order of the group. If $\mathfrak{a}$ is an ideal of A such that $N(\mathfrak{a}) \leq r$, then by Cayley's theorem that $A/\mathfrak{a}$ embeds in the symmetric group S_r on r elements, $r!$ annihilates $A/\mathfrak{a}$, hence $r! \in \mathfrak{a}$. Therefore, each ideal $\mathfrak{a}$ of A of norm at most r contains the ideal $r!A$, hence by ideal correspondence, $\mathfrak{a}$ corresponds to exactly one of the finitely many ideals of the ring $A/r!A$. □

5. The norm of an element, the product formula

Let x be an element of a number field K, and let d be the degree of $\mathbb{Q}[x]$ over $\mathbb{Q}$. Let

$$m_x : \mathbb{Q}[x] \to \mathbb{Q}[x]$$

denote multiplication by x on $\mathbb{Q}[x]$, considered as a vector space over $\mathbb{Q}$. Then $(-1)^d$ multiplied by the determinant of m_x is the constant coefficient of the minimal polynomial of x. In effect, the characteristic polynomial is equal to the minimal polynomial in this case.

PROPOSITION 5.1. *Let K be a number field and let x be an element of K. The the determinant of m_x, the multiplication by x on K, is a rational number which satisfies*

$$\det m_x = \prod_{\sigma : K \to \mathbb{C}} \sigma(x)$$

where the product is taken over all $\mathbb{Q}$-embeddings of K in $\mathbb{C}$.

PROOF. Suppose that the element x has degree d over $\mathbb{Q}$. If the number field K is $\mathbb{Q}[x]$, then $(1, x, \ldots, x^{d-1})$ is a basis for K over $\mathbb{Q}$.

With respect to this basis, m_x has the matrix

$$\begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & -a_2 \\ & & \ddots & 0 & \vdots \\ & & & 1 & -a_{d-1} \end{pmatrix}$$

where the minimal polynomial relation satisfied by x over $\mathbb{Q}$ is

$$x^d + a_{d-1}x^{d-1} + \cdots + a_0 = 0.$$

The determinant of multiplication by x is

$$\det m_x = (-1)^d \det \begin{pmatrix} a_0 & & & & \\ a_1 & 0 & & & \\ a_2 & 1 & \ddots & & \\ \vdots & & \ddots & 0 & \\ a_{d-1} & & & 1 & 0 \end{pmatrix} = (-1)^d a_0,$$

where the last equality follows from Laplace's determinant expansion by expanding the first column of the displayed matrix, noting that each minor corresponding to a_j for $1 \leq j \leq d-1$ is zero since it is the determinant of a matrix whose last column is zero.

If K is a vector space of dimension n over $\mathbb{Q}[x]$, then

$$n[\mathbb{Q}[x] : \mathbb{Q}] = [K : \mathbb{Q}].$$

Recalling that a basis for K over $\mathbb{Q}$ is given by all products $\alpha_i x^j$, where $(\alpha_1, \ldots \alpha_n)$ is a basis for K over $\mathbb{Q}[x]$ and where $0 \leq j \leq d-1$, it follows that the matrix of m_x can be written with n blocks equal to the matrix of m_x restricted to $\mathbb{Q}[x]$. Therefore,

$$\det m_x = \prod_{\sigma:\mathbb{Q}[x]\to\mathbb{C}} \sigma(x)^n$$

and since there are precisely n distinct embeddings of K in $\mathbb{C}$ over $\mathbb{Q}$ that extend a given embedding $\sigma : \mathbb{Q}[x] \to \mathbb{C}$ over $\mathbb{Q}$, the formula of 5.1 holds. $\square$

Definition 5.2. Let K be a number field and let x be an element of K. The **norm** x is the rational number

$$N(x) = \prod_{\sigma:K\to\mathbb{C}} \sigma(x)$$

6. The local definition of the degree of $Pic_c(A)$

7. Volume, global definition of degree

8. Sections of a compactified invertible module, the Riemann-Roch theorem

CHAPTER 4

The classical theorems of algebraic number theory

CHAPTER 5

Height of rational points of a scheme over a number field