ARITHMETIC GEOMETRY: BASED ON PROF. SZPIRO'S NOTES ON ARITHMETIC GEOMETRY

Contents

1. Operations with modules

1.1. **Tensor product and modules of finite type.**

We assume some familiarity with the notions of rings and modules over a ring. A ring for us will always mean a commutative ring with unit and for the most part $1 \neq 0$.

Proposition 1.1. *Let A be a ring and M, N be two A-modules. Consider the submodule R of $A^{(M\times N)}$ generated by the relations:*

$$a(x,y)-(ax,y), \quad (x+x',y)-(x,y)-(x',y),$$

$$a(x,y)-(x,ay), \quad (x,y+y')-(x,y)-(x,y'),$$

for $a \in A$, $x, x' \in M$ and $y, y' \in N$. We will 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 every A-module P and every A-bilinear map $\varphi : M \times N \longrightarrow P$, there exist a unique A-linear map $\psi : M \otimes_A N \longrightarrow P$ such that $\varphi(x,y) = \psi(x \otimes y)$.

The proof follows when we define the map ψ by the property above. In fact from the identity $\varphi(x,y) = \psi(x \otimes y)$ you can get:

Exercise 1.2. *Prove that for any module P we have*

$$\mathrm{Hom}(M \otimes N, P) = \mathrm{Hom}(M, \mathrm{Hom}(N, P)).$$

Remark 1.3. We could define $M \otimes_A N$ by saying that the pair $(M \otimes_A N, \pi)$, where $M \otimes_A N$ is an A-module and $\pi : M \times N \longrightarrow M \otimes_A N$ is a bilinear map, is universal for the property: for every A-module P and every A-bilinear map $\varphi : M \times N \longrightarrow P$, there exist a unique A-linear map $\psi : M \otimes_A N \longrightarrow P$ such that $\varphi = \psi \circ \pi$.

$$\begin{tikzcd}
M \times N \arrow[r, "\varphi"] \arrow[d, "\pi"'] & P \\
M \otimes N \arrow[ur, dashed, "\psi"] &
\end{tikzcd}$$

Example 1.4. It is possible for the tensor product to be zero, even when the modules M and N are not. For example take $A = \mathbb{Z}$, $M = \mathbb{Z}/n\mathbb{Z}$ and $N = \mathbb{Z}/m\mathbb{Z}$ with $(m, n) = 1$. The tensor product $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$ is annihilated by m and n by bilinearity and by Bezout theorem is then annihilated by 1.

Example 1.5. Let A be a ring and J an ideal of A, then $M \otimes_A A/J \cong M/JM$. In particular $J \otimes_A A/J \cong J/J^2$.

Definition 1.6. *Let A be a ring and m and ideal of A. We say that A is a* **local ring of maximal ideal** *m and denoted (A, m) if every proper ideal of A is contained in m.*

Exercise 1.7. *Suppose that $A^\times$ denotes the set of invertible elements of a ring A. Prove that the following are equivalent:*

(1) *If the sum of two elements $x+y \in A^\times$, then $x \in A^\times$ or $y \in A^\times$.*
(2) *If a sum $x_1 + \cdots + x_n \in A^\times$, then there exist i with $1 \leq i \leq n$, such that $x_i \in A^\times$.*
(3) *$(A, A \setminus A^\times)$ is a local ring.*

Example 1.8. The ring of formal power series $A = k[[X_1, \ldots, X_n]]$ is local with maximal ideal $m = (X_1, X_2, \ldots, X_n)$ generated by X_i. As expected, elements in $A^\times = A \setminus m$ are invertible.

Definition 1.9. *A module M over A is said to be of* **finite type** *if it is finitely generated as A-module. This is to say that, there is a surjective map $A^n \longrightarrow M \longrightarrow 0$ for some $n > 0$. A module M over A is said to have a* **finite presentation** *if for positive numbers m and n we have an exact sequence $A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0$.*

Proposition 1.10. ***(Nayakama's Lemma)*** *Let A be a local ring and M of finite type over A. If $M \otimes A/m = 0$ then $M = 0$.*

Proof. If $M \otimes A/m = 0$ then $M = mM$. Choose generators $x_1, \ldots, x_m$ of M as A-module. There exist $m_{i,j} \in m$ such that for $i \leq i, j \leq n$,

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

If we denote by T the matrix $(m_{i,j} - \delta_{i,j})$ and by x the column vector of the x_i we have

$$Tx = 0 \Rightarrow T^* Tx = 0 \Rightarrow \det(T)x = 0,$$

where T^* denotes the transpose of the matrix of the cofactors. Since $\det(T)$ equals $(-1)^n$ modulo m, it is invertible in A and $M = 0$. □

Corollary 1.11. *Let A be a local ring with maximal ideal m and M a module of finite type over A. A set of elements generates M over A if and only if their image on M/mM generate M/mM as vector space over A/m.*

Proof. Suppose that $x_1, \ldots, x_m$ of M generate a submodule M'. Apply Nakayama's lemma to the A-module M/M'. □

Remark 1.12. Let (A, m) be a local ring with residue field $k = A/m$. Let M be a finitely generated module over A. Nakayama's lemma says that M has a minimal generating set whose cardinality is

$$\dim_k(M/mM) = \dim_k M \otimes_R k.$$

In particular if m is finitely generated, it can be generated by $\dim_k(m/m^2)$ elements.

Exercise 1.13. *Let M, N, N' be an A-modules and suppose that $\varphi : N \longrightarrow M$ is A-linear. Show that there is a natural map $\varphi \otimes 1 : N \longrightarrow M \otimes_A N$ making the association $N \mapsto M \otimes_A N$ a covariant additive functor from the category of A-modules to itself. Also prove that this functor is right exact. That is, for any exact sequence*

$$0 \longrightarrow N' \longrightarrow N \longrightarrow N'' \longrightarrow 0,$$

of A-modules, we have an exact sequence

$$M \otimes N' \longrightarrow M \otimes N \longrightarrow M \otimes N'' \longrightarrow 0.$$

Exercise 1.14. *Give an example to show that the above functor is not necessarily left exact.*

Definition 1.15. *A module M is said to be* **flat** *if the functor $M \otimes .$ is exact.*

Exercise 1.16. *Show that free modules $M \cong A^n$ are flat. On the other hand, suppose that A is a domain, show that the quotient field $K(A)$ is an example of a flat module which is not free over A. See exercise 1.25 for a more general view.*

Exercise 1.17. *Let A be an integral domain, prove that a flat module M over A has no torsion, i.e. $am = 0$ forces $m = 0$ in M or $a = 0$ in A. Over principal ideal domains (like for example $\mathbb{Z}$), we can say more: flatness is actually equivalent to having no torsion.*

Exercise 1.18. *Let A be a ring and M a module over A. Show that the following are equivalent:*

(i) *M is flat.*
(ii) *For all ideal $I \subset A$, the map $I \otimes_A M \longrightarrow A \otimes_A M = M$ is injective.*
(iii) *For all ideal finitely generated $I \subset A$, the map $I \otimes_A M \longrightarrow A \otimes_A M = M$ is injective.*
(iv) *For every relation $\sum_i f_i x_i = 0$ in M there are $y_1, \ldots, y_m \in M$ such that $x_i = \sum_j a_{i,j} y_j$ and $\sum_i f_i a_{i,j} = 0$.*

1.2. **Localization.** The process of localization extends a ring to have more invertible elements. We do it at once in the more general case of a module.

Definition 1.19. *Let A be a ring. A set $S \subset A$ is said to be a* **multiplicatively stable system** *if it satisfies the two conditions*

(1) $1 \in S$,
(2) $x, y \in S \Rightarrow xy \in S$.

For an A-module M and a multiplicatively stable system $S \subset A$, the **localization of** *M* **at** *S, denoted $S^{-1}M$, is defined as the quotient of $M \times S$ modulo the equivalent relation $\sim$, where $(m, s) \sim (m', s')$ if there exist $t \in S$ such that $t(sm' - s'm) = 0$. The image of (m, s) in the quotient will be denoted sometimes $\frac{m}{s}$.*

Example 1.20. For A a domain, $S = A^* = A \setminus 0$ is a multiplicatively stable system and $S^{-1}A$ is the quotient field $K(A)$.

Example 1.21. Let $I \subset A$ be an ideal. The set $1 + I = \{1 + x \,|\, x \in I\}$ is a multiplicatively stable system.

Exercise 1.22. *Let S be a multiplicatively stable system of A and M an A-module. Show that there is a canonical map $\pi : M \longrightarrow S^{-1}M$, defined by $\pi(x) = \frac{x}{1}$. Show that the image $\pi(x)$ is zero if and only if there exist an element $s \in S$ with $sx = 0$ (This is sometimes referred to as x being S-torsion). Show that if A is a domain, the map π is injective whenever M is torsion-free.*

Exercise 1.23. *Prove that the map $\pi : A \longrightarrow S^{-1}A$ establishes a one to one correspondence between ideals of $S^{-1}A$ and ideals of A that do not meet S.*

Exercise 1.24. *Let p be a prime ideal of A and consider the multiplicatively stable system $S = A \setminus p$. We denote $S^{-1}M$ by M_p. Show that the ring A_p is in fact a local ring with maximal ideal $\pi(p)$.*

Exercise 1.25. *Let M be an A-module and S a multiplicatively stable system of A. Prove that the localization $S^{-1}M$ is an $S^{-1}A$-module and satisfies $S^{-1}M \cong M \otimes S^{-1}A$. Show that the natural map $\varphi : M \otimes S^{-1}A \longrightarrow S^{-1}M$, given by $\varphi(m \otimes \frac{a}{s}) = \frac{am}{s}$ is an isomorphism. Also show that the localization $S^{-1}A$ is a flat module over A. This generalizes our previous comment on the flatness of the quotient field of an integral domain.*

Exercise 1.26. *Take $M = A$ and S a multiplicatively stable system. Show that the pair $(S^{-1}A, \pi)$ has the following universal property: For any ring B and map $\varphi : A \longrightarrow B$, such that $\varphi(S)$ is invertible in B, there exist a unique map $\psi : S^{-1}A \longrightarrow B$ such that $\varphi = \psi \circ \pi$.*

Exercise 1.27. *Prove that if $M_{\mathfrak{p}} = 0$ for all primes $\mathfrak{p}$ then $M = 0$. Hint: It will be useful to define the ideal annihilator of an element* $\mathrm{Ann}(m) = \{a \in A \mid am = 0\}$.

Definition 1.28. *Let f be an element in A and M an A-module. We will called M localized at f and denote M_f, the module $S^{-1}M$ for the multiplicatively stable system $S = \{(f^n)\}_{n\geq 0}$.*

Exercise 1.29. *Prove that if M is an A-module of finite type and $\mathfrak{p}$ is a prime ideal of A such that $M_{\mathfrak{p}} = 0$, then there exist $f \in A \setminus \mathfrak{p}$ such that $M_f = 0$.*

1.3. **Module of differentials.** Let $\varphi : A \longrightarrow B$ a ring homomorphism. We define a B-module $\Omega_{B/A}$ taking the free module on the symbols $\{db \mid b \in B\}$ modulo the relations

$$d(b + b') = d(b) + d(b'), \quad d(bb') = bdb' + b'db,$$

for all $b, b' \in B$ and $d(\varphi(a)) = 0$ for $a \in A$.

Let $\delta : B \otimes_A B \longrightarrow B$ given by $\delta(b \otimes b') = bb'$ and $I = \ker(\delta)$. The module I is a $B \otimes_A B$-module and I/I^2 is a $B \otimes_A B/I$-module and hence a B-module since multiplication by $b \otimes 1$ and by $1 \otimes b$ gives the same result in I/I^2.

Proposition 1.30. *The B-module I/I^2 is isomorphic to $\Omega_{B/A}$.*

Proof. Define a map $D : \Omega_{B/A} \longrightarrow I/I^2$ by $D(db) = 1 \otimes b - b \otimes 1$. We have to check that it actually defines a map from $\Omega_{B/A}$. For example we compute

$$\begin{aligned} D(d(bb')) &= 1\otimes bb' - bb'\otimes 1 \\ &= (1\otimes b)(1\otimes b' - b'\otimes 1) + (b'\otimes 1)(1\otimes b - b\otimes 1), \end{aligned}$$

and the later is the image by D of $bdb' + b'db$. To define a map in the other direction we introduce the ring $R = B \oplus \Omega_{B/A}$, where B acts on $\Omega_{B/A}$ through module action and we are taking the squares of the elements on $\Omega_{B/A}$ to be zero. Let us define map $l : B \times B \longrightarrow R$ by $l(b, b') = (bb', bdb')$. We can check that the map is bilinear and therefore induces an A-linear map $l' : B \otimes_A B \longrightarrow R$. This map l' is actually a ring homomorphism and maps I to $\Omega_{B/A}$ factoring through a map $l'' : I/I^2 \longrightarrow \Omega_{B/A}$ that is the inverse of our previously defined $D : \Omega_{B/A} \longrightarrow I/I^2$. □

Exercise 1.31. *Prove that the pair $(\Omega_{B/A}, D)$ satisfies the following universal property: For any B-module M and any linear map $\varphi : B \longrightarrow M$ such that $\varphi(xy) = x\varphi(y) + \varphi(x)y$, then there exist a unique B-linear map $\psi : \Omega_{B/A} \longrightarrow M$ such that $\varphi = \psi \circ D$.*

Exercise 1.32. *Suppose that $\varphi : A \longrightarrow C$ is a ring homomorphism and J is an ideal of C with $B = C/J$. There is an exact sequence*

$$J/J^2 \longrightarrow \Omega_{C/A} \otimes_C B \longrightarrow \Omega_{B/A} \longrightarrow 0.$$

Example 1.33. Let $A = k$ a field and $B = k[X_1, \dots, X_n]/(f_1, \dots, f_m)$, then $\Omega_{B/A}$ is the B-module with generators $dX_1, \dots, dX_n$ subject to the conditions

$$df_i = \sum_{j=1}^{n} \frac{\partial f_i}{\partial X_j} dX_j = 0, \qquad i = 1 \dots m.$$

Exercise 1.34. *Take $B = K$ and $A = k$ two fields. Prove that the module of differentials $\Omega_{K/k} = 0$ if and only if K is a separably generated extension of k. An extension K/k is separably generated if there exist a transcendence basis $\{x_i \,|\, i \in I\}$ such that $K/k(x_i \,|\, i \in I)$ is separable.*

1.4. **Inverse limits and completion of a ring.** The process of completion of a ring extends a ring with certain topology defined algebraically to a ring that is complete in the sense that it contains all limits of Cauchy sequences. We present the algebraic description using inverse limits of modules.

Definition 1.35. *Let $(D, \leq)$ be a directed poset considered as a category. An* **inverse system** *of modules is a contravariant functor F from D to the category of modules. That is, we have modules $\{M_i\}_{i\in D}$*

and maps $\theta_{i,j} : M_i \longrightarrow M_j$ for $j \leq i$, such that $\theta_{i,k} = \theta_{j,k} \circ \theta_{i,j}$ for $k \leq j \leq i$ and $\theta_{i,i}$ is the identity map on M_i.

Definition 1.36. *The* **inverse limit** $\varprojlim_{i\in D} M_i$ *associated to an inverse system $\{(M_i, \theta_{i,j})\}_{j\leq i\in D}$ is a pair $(M, (\pi_i)_{i\in D})$ made of module M and projection maps $\pi_i \colon M \longrightarrow M_i$ satisfying $\theta_{i,j} \circ \pi_i = \pi_j$ whenever $j \leq i$, that is universal in the following sense: For any other module pair $(M', (\pi'_i)_{i\in D})$ satisfying the same property there will be a unique map of A-modules $\tau : M' \longrightarrow \varprojlim_{i\in D} M_i$ making the diagrams commute.*

Remark 1.37. We can always take the inverse limit as the module

$$\varprojlim_{i\in D} M_i = \{(x_i)_{i\in D} \in \prod_{i\in D} M_i \,|\, \theta_{i,j}(x_i) = x_j \,\forall\, j \leq i\},$$

with projections maps $\pi_i((x_i)_{i\in D}) = x_i$ for all $i \in D$.

Definition 1.38. *Let $I \subset A$ be an ideal and M an A-module. The* **completion** $\hat{M}_I = \hat{M}$ *is the inverse limit $\hat{M} = \varprojlim M/I^n M$ associate to the inverse system $\theta_{n+1} : M/I^{n+1} \longrightarrow M/I^n$ for $D = \mathbb{N}$. It coincides with the topological completion, when we dote M with the topology whose system of neighborhoods at 0 are given by the $I^n M$.*

Example 1.39. Let (A, m) be a local ring. The completion $\hat{A}$ denotes the completion with respect to the maximal ideal m.

Example 1.40. The completion of $A[x_1, \ldots, x_n]$ with respect to the ideal $I = (x_1, \ldots, x_n)$ is the local ring of power series $A[[x_1, \ldots, x_n]]$.

Example 1.41. Let A be the ring of integers and p a rational prime. The completion of $A = \mathbb{Z}$ with respect to the prime ideal (p) is the ring $\mathbb{Z}_p$ of p-adic integers.

Definition 1.42. *A* **noetherian ring** *is a ring A such that every ascending chain of ideals $I_1 \subset I_2 \subset \ldots$ is stationary, i.e. there exist an n such that $I_n = I_{n+1} = \ldots$. An equivalent condition is that every ideal is finitely generated. In general we say that a module M is noetherian if every submodule N of M is finitely generated.*

Remark 1.43. We have the Hilbert basis theorem saying that if A is noetherian, then the polynomial ring $A[x_1, \ldots, x_n]$ is also noetherian.

Exercise 1.44. *Let A be noetherian ring and M a module of finite type. Show that a submodule $N \subset M$ is also of finite type.*

Exercise 1.45. *Suppose that we have an ideal $I \subset A$ and a module M over A. Prove that there exist a canonical map $\hat{A} \otimes M \longrightarrow \hat{M}$. Suppose* *that A is a noetherian ring and M a finitely generated A-module, prove that this map is an isomorphism and we have $\hat{A} \otimes M \cong \hat{M}$.*

Exercise 1.46. *Find an example of a ring A and a module M over A such that $\hat{A} \otimes M \longrightarrow \hat{M}$ is not a bijection.*

Exercise 1.47. *Prove that the correspondence $M \longrightarrow \hat{M}$ is a covariant, additive functor from the categories of modules over A to itself. Also, when restricted to the subcategory of finitely generated A-modules over noetherian rings, this functor is exact. Deduce that, for A noetherian, the completion $\hat{A}$ is a flat A-module. (In this case we can say more, namely $\hat{A}$ is* **faithful flat***)*

Exercise 1.48. *Prove that for A noetherian, the completion $\hat{A}$ is also noetherian.*

1.5. **Direct limits.** The notion of direct limit is dual to that of inverse limit. Let $(D, \leq)$ be a directed poset. Let A be a ring. Suppose that we have an A-module M_i for each $i \in D$ and morphisms of A-modules $\theta_{i,j} : M_i \longrightarrow M_j$ for each $i \leq j$, such that $\theta_{i,i} = id_{M_i}$ and $\theta_{i,j} \circ \theta_{j,k} = \theta_{i,k}$ whenever $i \leq j \leq k$. The system of modules $\{(M_i, \theta_{i,j})\}_{i \leq j \in D}$ is called a **directed system** of modules.

Definition 1.49. *The* **direct limit** $\varinjlim_{i\in D} M_i$ *is a pair $(M, (\pi_i)_{i\in D})$ made of module M and maps $\pi_i \colon M_i \longrightarrow M$ satisfying $\pi_j \circ \theta_{i,j} = \pi_i$ whenever $i \leq j$, that is universal in the following sense: For any other module pair $(M', (\pi'_i)_{i\in D})$ satisfying the same property there will be a unique map of A-modules $\tau \colon \varinjlim_{i\in D} M_i \longrightarrow M'$ making the diagrams commute.*

Remark 1.50. The direct limit of a directed system of modules exist: take the direct sum $M = \bigoplus M_i$ and the submodule N generated by the elements of the form $m_j - \theta_{i,j}(m_i)$ for $m_i \in M_i$ and $i \leq j$. Then the module M/N has the required properties. An alternative description of the the direct limit that is very useful is as follows. Consider the set of pairs (M_i, m_i) where $m_i \in M_i$. Define an equivalence relation in this set by saying that $(M_i, m_i) \sim (M_j, m_j)$ if there exist k with $i, j \leq k$ and $\theta_{i,k}(m_i) = \theta_{j,k}(m_j)$. It can be checked that the set of classes $[M_i, m_i]$ has the structure of module and together with the maps $\pi_i(m_i) = [M_i, m_i]$; it satisfies the same universal property as does the direct limit.

Exercise 1.51. *Prove that for every A-module P, we can relate the inverse and direct limit by the identity*

$$\varprojlim_{i\in D} \mathrm{Hom}(M_i, P) = \mathrm{Hom}(\varinjlim_{i\in D} M_i, P).$$

Proposition 1.52. *Let M_i, N be A-modules. We have the property*

$$(\varinjlim M_i) \otimes N \cong \varinjlim (M_i \otimes N).$$

Proof. Let P be any A-module. We have the following:

$$\begin{aligned} \mathrm{Hom}(\varinjlim (M_i \otimes N), P) &= \varprojlim \mathrm{Hom}(M_i \otimes N), P) \\ &= \varprojlim \mathrm{Hom}(N, \mathrm{Hom}(M_i, P)) \\ &= \mathrm{Hom}(N, \varprojlim \mathrm{Hom}(M_i, P)) \\ &= \mathrm{Hom}(N, \mathrm{Hom}(\varinjlim M_i, P)) \\ &= \mathrm{Hom}((\varinjlim M_i) \otimes N, P). \end{aligned}$$

By Yoneda's lemma we obtain our result. □

Exercise 1.53. *Show that the direct limit of flat modules is flat. In particular direct limit of free modules is also flat. We have the converse result: every flat module is direct limit of finitely generated free modules.*

1.6. **Universal algebras.** In the same way we defined $M \otimes_A N$ for A-modules M and N, we can define (for $n > 1$) the n-fold tensor product $T_n(M) = M \otimes_A M \otimes_A \cdots \otimes_A M$ of a module M with itself. For $n = 0$ we put $T_0(M) = A$ and for $n = 1$ we have $T_1(M) = M$. Now, considering the direct sum of the modules $T_n(M)$ we gain some extra structure. The module $T(M) = \bigoplus T_n(M)$ can be given the structure of associative algebra (not necessarily commutative) defining

$$(x_1 \otimes \cdots \otimes x_n) \cdot (y_1 \otimes \cdots \otimes y_k) = x_1 \otimes \cdots \otimes x_n \otimes y_1 \otimes \cdots \otimes y_k.$$

The associative algebra $T(M)$ satisfies the following property: for any associative algebra B and any map $\varphi : M \longrightarrow B$ there exist a unique map $\psi : T(M) \longrightarrow B$ such that φ is the composition of ψ and the canonical isomorphism $M = T_1(M) \hookrightarrow T(M)$.

There are other graded algebras attached to M, we can construct for example the **symmetric algebra** $\mathrm{Symm}(M) = T(M)/I$, where I is the ideal generated by the relations $x \otimes y - y \otimes x$ for all $x, y \in M$. The ideal I is generated by homogeneous elements of degree two, therefore the ideal I is homogenous and

$$\mathrm{Symm}(M) = \bigoplus_n \mathrm{Symm}_n(M) = \bigoplus_n T_n(M)/(I \cap T_n(M)).$$

The symmetric algebra is a commutative algebra that satisfies the following property: For any commutative algebra B and any map $\varphi : M \longrightarrow B$ there exist a unique algebra homomorphism $\psi : \mathrm{Symm}(M) \longrightarrow B$ such that φ is the compositions of ψ with the natural inclusion $M = \mathrm{Symm}_1(M) \hookrightarrow \mathrm{Symm}(M)$.

Example 1.54. For $M = A^n$ a free module, the Symmetric Algebra $Symm(M) = A[x_1, \dots, x_n]$.

The **exterior algebra** $\bigwedge M = T(M)/J$, where J is the ideal generated by the elements of the form $x \otimes x$ for $x \in M$. Again we have a decomposition

$$\bigwedge M = \bigoplus_n \bigwedge^n M = \bigoplus_n T_n(M)/(J \cap \bigwedge^n M).$$

The symmetric Algebra satisfies the following property: for any associative algebra B and any map $\varphi : M \longrightarrow B$ with the property that the image $\varphi(M)$ consist of elements of square zero, there exist a unique $\psi : \bigwedge M \longrightarrow B$ such that φ is the composition of ψ with the injection $M = \bigwedge^1 M \hookrightarrow \bigwedge(M)$. It is possible to verify that $\bigwedge^n M = 0$ for n greater than the number of generators of M. The image of $x_1 \otimes x_2 \otimes \cdots \otimes x_n$ in the quotient $\bigwedge^n M$ is usually denoted $x_1 \wedge x_2 \wedge \cdots \wedge x_n$.

Exercise 1.55. *Show that $Symm_n$, T_n and $\bigwedge^n$ are functors from the category of modules over a ring A into itself. Verify that if $M = N \oplus P$ is a direct sum*

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

2. Schemes and projective schemes

We define in this section topological spaces associated to commutative rings, as a generalization of the classical work with maximal ideals in algebras of finite type over fields.

Definition 2.1. *Let A be a ring. The* **spectrum** *of a ring A, denoted* Spec(A)*, is the set of all prime ideals in A. Let I be any ideal of A, we denote by $V(I)$ the set of all prime ideals containing I. The set of all maximal ideals of a ring A will be denoted by* Spec-max(A)*.*

Theorem 2.2. *(Weak Hilbert's Nullstellensatz) let $k = \bar{k}$ be an algebraically closed field. The maximal ideals of $k[x_1, \dots, x_n]$ are of the form $\langle x_1 - a_1, \dots, x_n - a_n \rangle$ where all $a_i \in k$.*

The proof of the theorem uses the notion and properties of integral elements over a ring (c.f. definition 3.37).

Corollary 2.3. *Suppose that $k = \bar{k}$ be an algebraically closed field and $A = k[x_1, \dots, x_n]$.* **The Hilbert Nullstelensatz** *establishes a correspondence between points on the affine n-space $\mathbb{A}^n$ and the maximal* *ideals in A. For a map $\varphi : A \longrightarrow A'$ where A, A' are finitely generated k-algebras over an algebraically closed field k, the pre-image of a maximal ideal is a maximal ideal. This property is not true for all rings, hence the convenience of working with prime ideals instead of maximal ideals.*

Proposition 2.4. *The collection of sets $V(I)$ are the closed sets of a topology on $\mathrm{Spec}(A)$, called the Zariski topology. The Zariski topology admits a basis of open sets of the form $D(f) = \{\mathfrak{p} \in \mathrm{Spec}(A) \,|\, f \notin \mathfrak{p}\}$, for $f \in A$.*

Proof. Let $V(I_j)_{j\in J}$ be an arbitrary collection of closed sets. The intersection $\cap_{j\in J} V(I_j) = V(\sum_{j\in J} I_j)$. The union of finitely many closed sets $V(I_1), \ldots V(I_n)$ satisfies $V(I_1)\cup\cdots\cup V(I_n) = V(I_1\cap\cdots\cap I_n)$ and is therefore closed. The empty set is equal to $V(A)$ and the whole space $\mathrm{Spec}(A) = V((0))$. If I is the ideal generated by $(f_j)_{j\in J}$, then we have $U = \mathrm{Spec}(A) \setminus V(I) = \cup_{j\in J} D(f_j)$. □

Remark 2.5. If A is a domain, the ideal (0) is prime and is contained in every ideal. Therefore $\mathfrak{p} = (0)$ belongs to any not empty open set and two open sets have non-empty intersection. The point $\mathfrak{p} = (0) \in \mathrm{Spec}(A)$ is what is called a generic point of $\mathrm{Spec}(A)$. The topological space $\mathrm{Spec}(A)$ is clearly not T_2. It is not even T_1 because in general points are not closed.

Remark 2.6. The evaluation of a function $a \in A$ at a point $\mathfrak{p} \in \mathrm{Spec}(A)$ will be the image of a under the map $A \to \kappa_{\mathfrak{p}} = A_{\mathfrak{p}}/m_{\mathfrak{p}}$. In this way, elements of A have associated evaluation functions $e_a\colon \mathrm{Spec}(A) \longrightarrow \sqcup_{\mathfrak{p}}\kappa_{\mathfrak{p}}$ and nilpotent elements of the ring A are associated to non-zero functions that vanish everywhere on $\mathrm{Spec}(A)$.

Proposition 2.7. *Let A be a ring. The topological space $\mathrm{Spec}(A)$ is quasi-compact.*

Proof. Let $(U_j)_{j\in J}$ be a collection of opens sets forming a covering of $\mathrm{Spec}(A)$. We can refine the covering such that each $U_j = D(f_j)$ for an element $f_j \in A$. Now $\mathrm{Spec}(A) = \cup_{j\in J} D(f_j)$ forces the ideal I generated by the $(f_j)_{j\in J}$ to be equal to A, but then there exist a finite linear combination $a_1 f_{j_1} + \cdots + a_r f_{j_r} = 1$ and the open subsets $U_{j_1}, U_{j_2}, \ldots, U_{j_r}$ form a finite sub-cover. □

Exercise 2.8. *Let A be a ring and $S \subset A$ a multiplicatively stable set. Show that $\mathrm{Spec}(S^{-1}A) \simeq \{\mathfrak{p} \in \mathrm{Spec}(A) \,|\, \mathfrak{p} \cap S = \emptyset\}$. In particular if $\mathfrak{p} \in \mathrm{Spec}(A)$ we have $\mathrm{Spec}(A_{\mathfrak{p}}) \simeq \{\mathfrak{q} \in \mathrm{Spec}(A) \,|\, \mathfrak{q} \subset \mathfrak{p}\}$ and for $f \in A$, $\mathrm{Spec}(A_f) \simeq \{\mathfrak{p} \in \mathrm{Spec}(A) \,|\, f \notin \mathfrak{p}\} = D(f)$.*

2.1. **Sheaves of functions.** Sheaves will be an important tool to keep track of the local data. We will build on $\mathrm{Spec}(A)$ a structure sheaf of regular functions.

Definition 2.9. *Let X be a topological space. The category $Open(X)$ is the category whose objects are open sets with inclusions as maps.*

Definition 2.10. *Let X be a topological space. A contravariant functor from the category $Open(X)$ to the category of sets is called a* **pre-sheaf** *on X and denoted by $\mathcal{F}$. A pre-sheaf $\mathcal{F}$ is called a* **sheaf** *if for any open set U and for each covering $(U)_{i\in I}$ of U the following conditions are satisfied:*

1. *If two elements of $\mathcal{F}(U)$ has the same image on $\mathcal{F}(U_i)$ for each $i \in I$, then they are equal.*
2. *If we have elements $s_i \in \mathcal{F}(U_i)$ for each $i \in I$ such that for each pair (i, j). the image of s_i and s_j coincide on $\mathcal{F}(U_i \cap U_j)$, then there exist an element $s \in \mathcal{F}(U)$ whose image in $\mathcal{F}(U_i)$ is s_i for all $i \in I$.*

Example 2.11. One can consider for example the pre-sheaf of real functions on a topological space X, when we put for every open set $U \subset X$, the set $\mathcal{F}(U)$ of functions from X to $\mathbb{R}$. It is not hard to see that it is in fact a sheaf when we use restriction as maps. In the same way we can define sheaves of continuous functions $\mathcal{F}_c$, n-times derivable $\mathcal{F}_n$ and infinitely many times differentiable functions $\mathcal{F}_\infty$. It is because of these examples that if $\mathcal{F}$ is sheaf on X and $V \subset U$ is an inclusion of open sets we call the induced map $\mathcal{F}(U) \longrightarrow \mathcal{F}(V)$ **the restriction** of U to V. If U is an open set, the elements of $\mathcal{F}(U)$ are called **sections over** U and $\mathcal{F}(U)$ is also denoted by $\Gamma(U, \mathcal{F})$. If $s \in \mathcal{F}(U)$ is a section over U, the restriction to $V \subset U$ is denoted by $s|_V$.

Example 2.12. Not every pre-sheaf is a sheaf. For example, the pre-sheaf $\mathcal{F}(U)$ of bounded continuous function on a topological space X is not a sheaf because you can not glue sections. A locally bounded function is not necessarily bounded.

Example 2.13. A map of sheaves or pre-sheaves is a natural transformation of functors. Let X be a topological space. Let us consider the sheaves $\mathcal{O}$ and $\mathcal{O}^*$ of $\mathbb{C}$-valued functions and $\mathbb{C}^*$-valued functions on X respectively. The exponential map $\exp : \mathcal{O} \longrightarrow \mathcal{O}^*$ is a homomorphism of sheaves of abelian groups. Since we can take logarithms locally but not globally, the maps on sections $\mathcal{O}(U) \longrightarrow \mathcal{O}^*(U)$ are locally surjective, but not surjective. Hence, the image presheaf, defined by $U \to Im(\mathcal{O}(U) \longrightarrow \mathcal{O}^*(U))$, is not a sheaf.

Example 2.14. (Skyscraper sheaf) Fix a group S and $x \in X$. Define $\mathcal{F}(U) = S$ if $x \in U$ and $\mathcal{F}(U) = 0$ otherwise. The pre-sheaf $\mathcal{F}$ so defined is a sheaf of groups.

We would like to define a sheaf of algebraic functions on $\operatorname{Spec}(A)$.

Proposition 2.15. *Let A be a ring and M an A-module. Let $(U_{f_i})_{i\in I} = D(f_i))_{i\in I}$ be an open covering of* $\operatorname{Spec}(A)$ *by basics open sets. The following sequence is exact*

$$0 \longrightarrow M \longrightarrow \prod_{i\in I} M_{f_i} \xrightarrow{\varphi} \prod_{i,j\in I} M_{f_i f_j},$$

where the map on the right is $\varphi((x_i)) = (x_i|_{D(f_if_j)} - x_j|_{D(f_if_j)})_{i,j}$.

Proof. Suppose that the index of the cover is finite $I = \{1, 2, \dots, n\}$. The fact that $D(f_i)$ cover $\operatorname{Spec}(A)$ forces a unity partition

$$a_1 f_1 + \cdots + a_n f_n = 1,$$

In fact, the $D(f_i^k) = D(f_i)$ determine the same cover for all $k > 0$ and a different partition

$$a_{1,k} f_1^k + \cdots + a_{n,k} f_n^k = 1.$$

Exactness on the left: Suppose that $x \in M$ is zero in all M_{f_i}. There exist $k_i \in \mathbb{Z}$ such that $f_i^{k_i} x = 0$. Taking $k = \sup_i\{k_i\}$ we obtain $0 = a_{1,k} f_1^k x + \cdots + a_{n,k} f_n^k x = x$.
Exactness in the middle: Suppose that $(x_i)_{i\in I} \in \prod_{i\in I} M_{f_i}$, then for each $i \in I$ there exist $z_i \in M$ and k_i such that

$$x_i = \frac{z_i}{f_i^{k_i}}$$

Taking $k = \sup_i\{k_i\}$ and $y_i = x_i f_i^{k-k_i}$ we have for each $i \in I$:

$$x_i = \frac{x_i f_i^{k-k_i}}{f_i^k} = \frac{y_i}{f_i^k}.$$

Now assume that $(x_i) \in \ker(\varphi)$ then there are integers $k_{i,j} \in I$ such that

$$y_j f_i^k (f_i f_j)^{k_{i,j}} = y_i f_j^k (f_i f_j)^{k_{i,j}}.$$

Taking $K = \sup\{k_{i,j}\}$ we obtain

$$y_j f_i^k (f_i f_j)^K = y_i f_j^k (f_i f_j)^K.$$

multiplying by $a_{i,k+K}$ and adding over $i \in I$ we obtain

$$\begin{aligned} y_j f_j^K &= \sum_{i\in I} y_j f_j^K a_{i,k+K} f_i^{k+K} = \sum_{i \in I} y_i f_i^k a_{i,k+K} (f_i f_j)^K \\ &= f_j^{k+K} \sum_{i\in I} y_i a_{i,k+K} f_i^K = f_j^{k+K} y, \end{aligned}$$

where $y = \sum_{i\in I} y_i a_{i,k+K} f_i^K \in M$. Therefore the element (x_j), where x_j satisfies

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

is coming from M.

Now, given any cover $\{D(f_i))\}_{i\in I}$, we know by quasi-compactness that there exist a finite subcover $\{D(f_i))\}_{i\in K}$ for a finite subset $K \subset I$. Now, we have already shown that the sequence is exact for $i, j \in K$ we need to prove exactness for $i, j \in I$.

Exactness on the left: If $x \in M$ is zero in M_{f_i} for $i \in I$, it is also zero in M_{f_i} for $i \in K$ and therefore $x = 0$ was already proven.

Exactness in the middle: Suppose that $(x_i)_{i\in I} \in \ker(\varphi)$, by our proof for finite index there exist $x_K \in M$ such that $(x_K)_i = x_i$ for all $i \in K$. Let $j \in I \setminus K$ and $L = K \cup j$. Again we can find an element x_L such that $(x_L)_i = x_i$ for all $i \in L$. Since $x_K - x_L = 0$ in M_{f_i} for $i \in K$, By exactness for the finite cover determined by K, $x_K = x_L$ and x_K becomes equal to x_L in M_{f_j}. Since we can do that with any j, we finish the proof. □

Definition 2.16. *Let A be a ring, M an A-module and U an open set of* Spec(A)*. Suppose that $U = \bigcup_{i\in I} U_{f_i}$ is a cover of U by fundamental open sets. One denotes $M(U, \mathbf{f}) = \ker(\prod_{i\in I} M_{f_i} \xrightarrow{\varphi} \prod_{i,j} M_{f_i f_j})$ where φ is given by $\varphi((x_i)_{i\in I}) = (x_i - x_j)_{i,j}$.*

Proposition 2.17. *Let A be a ring, M an A-module and $U \subset V$ two open sets of* Spec(A)*. If $(U_{f_i})_{i\in I}$ and $(V_{g_j})_{j\in J}$ are covering of U and V respectively by fundamental open sets, then the localization homomorphisms $M_{g_j} \longrightarrow M_{f_i g_j}$ induces a canonical homomorphism $M(V, \mathbf{g}) \longrightarrow M(U, \mathbf{fg})$ that is an isomorphism when $V = U$.*

Proof. One can check that $U_f \cap U_g = U_{fg}$. It follows that is enough to analyze the diagram:

$$\begin{tikzcd} 0 \arrow[r] & M(V,\mathbf{g}) \arrow[r] \arrow[d, "\varphi"] & \prod_i M_{g_i} \arrow[r] \arrow[d] & \prod_{i,j} M_{g_i g_j} \arrow[d] \\ 0 \arrow[r] & M(U,\mathbf{gf}) \arrow[r] & \prod_{i,k} M_{g_i f_k} \arrow[r] & \prod_{i,j,k,l} M_{g_i g_j f_k f_l}. \end{tikzcd}$$

The map φ is injective by proposition 2.15 when $V = U$ because each $M_{g_i} \longrightarrow \prod_k M_{g_i f_k}$ is injective. It is then sufficient to prove that φ is surjective when $U = V$, which is done vertically using again 2.15. This shows that φ is an isomorphism when $U = V$. □

Proposition 2.18. *Let A be a ring, M an A-module. The functor on Open$(\operatorname{Spec}(A))$ defined by*

$$\tilde{M}(U) = M(U, \mathbf{f}) = \ker(\prod_{i \in I} M_{f_i} \overset{\varphi}{\to} \prod_{i,j} M_{f_i f_j})$$

for every covering of an open set U by fundamental open sets, is a sheaf.

Proof. To show that $\tilde{M}$ is actually a sheaf, we need to prove that for any open covering $\{U_i\}_i$ of the open set U, we have an exact sequence

$$0 \longrightarrow \tilde{M}(U) \longrightarrow \prod_i \tilde{M}(U_i) \longrightarrow \prod_{i,j} \tilde{M}(U_i \cap U_j),$$

where the last arrow represents the difference of localizations. We proceed by covering each U_i by fundamental open sets and apply proposition 2.17. □

2.2. **Sheaf of functions via inverse limits.** The extension from being a sheaf with respect to a basis to being a sheaf with respect to the whole topology can be explicitly carry out with the inverse limit construction.

Definition 2.19. *Let X be a topological space and B a base of open sets for the topology of X. Consider B is a subcategory of Open(X) Is $\mathcal{F}$ is a functor from B to a category of modules, we say that $\mathcal{F}$ is a sheaf with respect to B if $\mathcal{F}$ is a sheaf with respect to coverings of basic open sets by basic open sets.*

Exercise 2.20. *Let X be a topological space and B a base for the topology of X. Let $\mathcal{F}$ be a contravariant functor from B to the category of modules. Suppose that M is a module together with a family of maps $\rho_V : M \longrightarrow \mathcal{F}(V)$ for $V \in B$ such that $\rho_{W,V} \circ \rho_W = \rho_V$, whenever $W \subset V$ and $\rho_{W,V} : \mathcal{F}(W) \longrightarrow \mathcal{F}(V)$ represents the restriction map. Prove that there exist a unique map*

$$\varphi_U \colon M \longrightarrow \varprojlim_{W \in B_U} \mathcal{F}(W),$$

such that $\pi_W \circ \varphi_U = \rho_W$, where $\pi_W : \varprojlim_{W \in B_U} \mathcal{F}(W) \longrightarrow \mathcal{F}(W)$ for $W \subset U$ in B.

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

Proposition 2.21. *Let X be a topological space and let B be a base for the topology of X, that is closed under intersection. Let $\mathcal{F}$ be a contravariant functor from B to the category of modules that is a sheaf with respect to B. Defines a presheaf $\tilde{\mathcal{F}}$ on each open set U by*

$$\tilde{\mathcal{F}}(U) = \varprojlim_{W \in B_U} \mathcal{F}(W),$$

where B_U denotes the collection of sets of B contained in U. For each inclusion of open sets $V \hookrightarrow U$, we define the restriction map $\tilde{\mathcal{F}}(U) \longrightarrow \tilde{\mathcal{F}}(V)$, that sends a map $\alpha : B_U \longrightarrow \cup_{W \in B_U} \mathcal{F}(W)$ to the restriction $\alpha \mid_{B_V}$. Then $\tilde{\mathcal{F}}$ is a sheaf, and for each basic open set $U \in B$, $\tilde{\mathcal{F}} \mid U$ is naturally isomorphic $\mathcal{F}$.

Proof. Given an open set U and a covering $U = \cup_{i \in I} U_i$, we want to prove the sequence

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

is exact, where $\varphi((\alpha_i)_{i \in I}) = (\alpha_i \mid U_i \cap U_j - \alpha_j \mid U_i \cap U_j)_{i,j}$.
For exactness on the left: suppose that $\alpha \mid U_i = 0$ for each $i \in I$, Fix $W \in B_U$. Let $(W_{i,j})_{j \in J_i}$ be a covering of U_i by basic open sets $W_{i,j} \in B_{U_i}$. Since B is closed under intersections $W \cap W_{i,j}$ is an open covering of W by elements of B. By our definition of α we have

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

for each $i \in I$ and $j \in J_i$. Since $\mathcal{F}$ is a sheaf with respect to B, we have $\alpha(W) = 0$ and since W is arbitrary $\alpha = 0$.
For exactness in the middle: consider as before a basic open set $W \in B_U$ and a covering $(W_{i,j})_{j \in J_i}$ of U_i by basic open sets $W_{i,j} \in B_{U_i}$ giving an open covering $W \cap W_{i,j}$ of W by elements of B. Suppose that $(\alpha_i)_{i \in I}$ is a collection such that $\alpha_i \in \tilde{\mathcal{F}}(U_i)$ for all $i \in I$ and $\alpha_i \mid B_{U_i \cap U_j} = \alpha_j \mid B_{U_i \cap U_j}$ for each $i, j \in I$. The family of elements $\alpha_i(W_{i,j}) \in \mathcal{F}(W_{i,j})$ satisfy under our hypothesis the condition

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

Therefore because $\mathcal{F}$ is a sheaf for B there exist $s_W \in \mathcal{F}(W)$ such that $s_W \mid W_{i,j} = \alpha_i(W_{i,j})$ for each $i \in I$ and $j \in J_i$. Let $\alpha(W) = s_W$. We claim that

$$\alpha \in \tilde{\mathcal{F}}(U) = \varprojlim_{W \in B_U} \mathcal{F}(W).$$

For $V \subsetneq W \subseteq U$ and $V, W \in B$, we need to show $\alpha(W) \mid_V = \alpha(V)$. We know already that

$$\alpha(W) \mid_{W_{i,j}} = \alpha_i(W_{i,j})$$

and restricting to V we obtain

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

By the sheaf property of $\mathcal{F}$,

$$\alpha(W) \mid_V = \alpha(V) \mid_V = \alpha(V).$$

The element α satisfies for all $i \in I$ that $\alpha \mid_{B_{U_i}} = \alpha_i$. □

Definition 2.22. *Let A be a ring, and let M be an A-module. Let B be the basis for the Zariski topology on* Spec(A) *given by the sets $D(f)$ for $f \in A$. The assignment $D(f) \longrightarrow M_f$ defines an inverse system of A-modules. We define a presheaf $\tilde{M}$ on* Spec(A) *as follows. For U open in* Spec(A) *we define*

$$\tilde{M}(U) = \varprojlim_{D(f) \subset U} M_f.$$

There is a natural restriction map $\tilde{M}(U) \longrightarrow \tilde{M}(V)$ for every inclusion $V \subset U$.

Theorem 2.23. *Let A be a ring, and let M be an A-module. The functor $\tilde{M}$ is a sheaf. The affine scheme defined by A is the topological space* Spec(A) *together with a sheaf of rings $\tilde{A}$.*

2.3. **Schemes as locally ringed spaces.** The analytic idea of germs of functions around a point is caught in the notion of stalk at a point. To define the stalk of a point we use a the direct limit of neighborhoods around the point.

Definition 2.24. *Let X be a topological space, and let x be a point of X. The set of neighborhoods of x, denoted by $Nbd(X, x)$, is the set of open subsets U of X with $x \in U$.*

Example 2.25. If X is a topological space and if $x \in X$, then the set $(Nbd(X, x), \supseteq)$ of neighborhoods of x ordered by containment is a preordered, directed set.

Definition 2.26. *Suppose that X ia topological space. Let A be a ring, $\mathcal{F}$ be a presheaf of A-modules on X and $x \in X$ a point of X. The stalk of $\mathcal{F}$ at the point $x \in X$ is the direct limit associated to the directed system of A-modules $\mathcal{F} \mid (Nbd(X, x), \supseteq)^{op}$.*

Definition 2.27. *A* **topological ringed space** *is a topological space together with a sheaf of rings. A* **locally ringed space** *is a topologically ringed space* $(X, \mathcal{O}_X)$ *whose* **stalks** $\mathcal{O}_{X,x} = \varinjlim_{x\in U} \mathcal{O}_X(U)$ *at any point* $x \in X$ *are local rings.*

Remark 2.28. In locally ringed spaces the stalk $\mathcal{O}_{X,x}$ at any point x is local and therefore has a unique maximal ideal, denoted m_x. We can consider then the residue field $\kappa_x = \mathcal{O}_{X,x}/m_x$ and call, for any $a \in \mathcal{O}_{X,x}$, the image $a(x) = \bar{a} \in \kappa_x$, the "evaluation" of a at x.

Definition 2.29. *A morphism* $f\colon (X, \mathcal{O}_X) \longrightarrow (X', \mathcal{O}_{X'})$ *of topologically ringed spaces is a continuous map* $f\colon X \longrightarrow X'$ *(denoted here with the same letter), together with a family of ring homomorphisms* $f^\sharp_{U'}\colon \mathcal{O}_{X'}(U') \longrightarrow \mathcal{O}_X(f^{-1}(U'))$*, where* $U' \subset X'$ *is an open set and we have a commuting diagram:*

$$\begin{tikzcd}
\mathcal{O}_{X'}(U') \arrow[r, "f^\sharp_{U'}"] \arrow[d, "\rho'_{U'V'}"] & \mathcal{O}_X(f^{-1}(U')) \arrow[d, "\rho_{f^{-1}(U')f^{-1}(V')}"] \\
\mathcal{O}_{X'}(V') \arrow[r, "f^\sharp_{V'}"] & \mathcal{O}_X(f^{-1}(V'))
\end{tikzcd}$$

for every $V' \subset U'$ *and for* ρ, ρ' *representing in each case the appropriate restriction maps. Usually the sheaf* $U' \longrightarrow \mathcal{O}_X(f^{-1}(U'))$ *on* X' *is called the direct image of the sheaf* $\mathcal{O}_X$ *and denoted* $f_*\mathcal{O}_X$*. Therefore a morphism of ringed spaces is actually a pair of maps* $(f, f^\sharp)$*, where* $f : X \longrightarrow X'$ *is a continuous map and* $f^\sharp : \mathcal{O}_{X'} \longrightarrow f_*\mathcal{O}_X$ *is a morphism of sheaves of rings on* X'*.*

Remark 2.30. A morphism of topologically ringed spaces $f\colon (X, \mathcal{O}_X) \longrightarrow (X', \mathcal{O}_{X'})$ induces, by passing to the limit, a ring homomorphism $f^\sharp_x\colon \mathcal{O}_{X',f(x)} \longrightarrow \mathcal{O}_{X,x}$ on the stalks.

Definition 2.31. *A morphism of locally ringed spaces is a morphism as topologically ringed spaces with the extra property of being local on the stalk, that is, the induced map* $f^\sharp_x\colon \mathcal{O}_{X',f(x)} \longrightarrow \mathcal{O}_{X,x}$ *satisfies* $f_x(m_{f(x)}) \subset m_x$ *for all* $x \in X$*.*

Exercise 2.32. *Show that a morphism* $f\colon (X, \mathcal{O}_X) \longrightarrow (X', \mathcal{O}_{X'})$ *is local on the stalk if and only if the induced morphism on the completions* $\hat{f}_x\colon \widehat{\mathcal{O}_{X',f(x)}} \longrightarrow \widehat{\mathcal{O}_{X,x}}$ *is continuous with respect to the adic-topologies.*

Definition 2.33. *A locally ringed space* $(X, \mathcal{O}_X)$ *is* **a scheme** *if for each point* $x \in X$*, there exist a ring* A *and an open set* $U \subset X$ *such* *that* $(U, \mathcal{O}_X \mid U)$ *isomorphic to* $(\mathrm{Spec}(A), \tilde{A})$ *as locally ringed space. A morphism of schemes is a morphism as locally ringed spaces.*

Lemma 2.34. *Let* $\varphi^\sharp : A \longrightarrow B$ *a ring homomorphism. Then, the induced application* $\varphi : \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ *defined by* $\varphi(\mathfrak{q}) = \varphi^{\sharp-1}\mathfrak{q}$ *for* $\mathfrak{q} \in \mathrm{Spec}(B)$ *is a continuous map.*

Proof. For $f \in A$ we can check $\varphi^{-1}(D(f)) = D(\varphi^\sharp(f))$. Also, if $\mathfrak{a} \subset A$ is an ideal of A and $\mathfrak{a}^e$ denotes the extension of $\mathfrak{a}$ to the ring B, we can check $\varphi^{-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$. □

Proposition 2.35. *Let* X *be a scheme and* A *a ring. There exist a canonical bijection*

$$\mathrm{Hom}_{Schemes}(X, \mathrm{Spec}(A)) \longrightarrow \mathrm{Hom}_{Rings}(A, \Gamma(X, \mathcal{O}_X))$$

Proof. A morphism of schemes $\varphi : X \longrightarrow \mathrm{Spec}(A)$ comes together with a map of sheaves $\varphi^\sharp \colon \tilde{A} \longrightarrow \varphi_*\mathcal{O}_X$. Taking the action on global sections we find a map $\varphi^\sharp_A : A \longrightarrow \Gamma(X, \mathcal{O}_X)$. We want to prove that the association $\varphi \leftrightarrow \varphi^\sharp_A$ is a bijection. Consider an open affine cover $\{\mathrm{Spec}(A_i)\}_{i\in I}$ of X. There is a restriction map $\rho_i : \Gamma(X, \mathcal{O}_X) \longrightarrow A_i$ for each $i \in I$. The map $\varphi^\sharp_i = \rho_i \circ \varphi^\sharp_A : A \longrightarrow A_i$ gives an associated map of affine schemes $\varphi_i : \mathrm{Spec}(A_i) \longrightarrow \mathrm{Spec}(A)$. Now, if two maps $\varphi, \psi : X \longrightarrow \mathrm{Spec}(A)$ give the same maps of rings $\varphi^\sharp_A = \psi^\sharp_A$ we will have $\varphi_i = \psi_i : \mathrm{Spec}(A_i) \longrightarrow \mathrm{Spec}(A)$ for all $i \in I$ and using the fact that the $\mathrm{Spec}(A_i)$ cover X we obtain that $\varphi = \psi$ on X. To prove surjectivity we observe that for an affine covering $(U_i = \mathrm{Spec}(A_i))_{i\in I}$ of X, we have an exact sequence

$$0 \longrightarrow \Gamma(X, \mathcal{O}_X) \longrightarrow \prod_i A_i \longrightarrow \prod_{i,j} \Gamma(U_i \cap U_j, \mathcal{O}_X),$$

where the last arrow is the difference of restrictions. If $\alpha : A \longrightarrow \Gamma(X, \mathcal{O}_X)$ is a ring homomorphism, one obtains by composition a map $\mathrm{Spec}(A_i) \xrightarrow{\varphi_i} \mathrm{Spec}(A)$. The above exact sequence shows that $\varphi_i|U_i \cap U_j$ and $\varphi_j|U_i \cap U_j$ induce the same ring homomorphism: $A \longrightarrow \Gamma(U_i \cap U_j, \mathcal{O}_{U_i\cap U_j})$. By the injectivity we have proved $\varphi_i|U_i \cap U_j = \varphi_j|U_i \cap U_j$ and the maps $\varphi_i : \mathrm{Spec}(A_i) \longrightarrow \mathrm{Spec}(A)$ paste together to give a map $\varphi : X \longrightarrow \mathrm{Spec}(A)$. □

2.4. **The arithmetic surface.** Consider the ring $\mathbb{Z}[x]$. A prime ideal $\mathfrak{p}$ in the polynomial ring $\mathbb{Z}[x]$ must be in one of the categories:

(1) the zero ideal $\mathfrak{p} = (0)$.
(2) A principal ideal $\mathfrak{p} = (p) = p\mathbb{Z}[x]$ for p a rational prime in $\mathbb{Z}$.

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

(4) A principal ideal $\mathfrak{p} = (F)$ where F is a $\mathbb{Q}$-irreducible polynomial of positive degree in $\mathbb{Z}[x]$ whose coefficients have no common prime divisors.

Since $\mathbb{Z}[x]$ is a noetherian ring, any ideal (in particular a prime ideal) will always be $\mathfrak{p} = (a_1, \ldots, a_n, f_1, \ldots, f_m)$ for elements $a_i \in \mathbb{Z}$ and polynomials f_j of positive degree. The fact that $\mathbb{Z}$ is a principal ideal domain forces $n = 0$ or $n = 1$. For $n = 1$, we use that $F_p[x]$ is also a principal ideal ring to obtain $m = 0$ or $m = 1$. If $m = n = 1$ we have $\mathfrak{p} = (p, F)$ for some irreducible polynomial in $F_p[x]$. The case $n = 0$ is done by induction to obtain $m = 1$ and $\mathfrak{p} = (F)$. We have then that $\mathrm{Spec}(\mathbb{Z}[x])$ is an object of dimension two called the arithmetic surface.

Exercise 2.36. *Prove that a prime ideal $\mathfrak{p} = (f_1, f_2, \ldots, f_n) \in \mathbb{Z}[x]$ is necessarily generated by one element.*

Exercise 2.37. *Find the intersection of the zero-sets $V(2)$ and $V(f)$ for an irreducible polynomial $f \in \mathbb{Z}[x]$.*

Exercise 2.38. *What is the intersection of the zero-sets $V(f) \cap V(g)$ for polynomials $f \neq g \in \mathbb{Z}[x]$ irreducible over $\mathbb{Q}$?*

2.5. **Proj and projective schemes.** The first example of an scheme that is not affine is the projective space over a ring. Let A be a graded ring in nonnegative degree

$$A = \bigoplus_{n \geq 0} A_n$$

We are going to assume that A is generated by A_1 as an A_0-algebra. For example the algebra $A = A_0[x_1, \ldots, x_n]$. Also if A is a ring and I is an ideal $I \subset A$, the graded ring $\bigoplus_{n \geq 0} I^n$, is an algebra of this type.

Definition 2.39. *If A is a graded ring. We define the irrelevant ideal of A to be the ideal $A_+ = \bigoplus_{n \geq 1} A_n$*

Definition 2.40. *An element $f \in A_n$ is called homogeneous of degree n. An ideal $I \subset A$ is said to be homogeneous if for every element $f = \sum_n f_n \in I$, the degree n part f_n of f also satisfies $f_n \in I$.*

For example ideals I generated by homogeneous elements have the above property, giving examples of homogeneous ideals. Also for a homogeneous ideal to be prime is enough to test that if $fg \in I$ and f, g are homogeneous, then it must be the case that $f \in I$ or $g \in I$.

Definition 2.41. *If A if a graded ring, we define* $\mathrm{Proj}(A)$ *to be the set of all homogeneous prime ideals of A that do not contain A_+.*

If f is an homogeneous element of degree n. The localized ring A_f is $\mathbb{Z}$-graded ring. The element xf^h has degree $m + nh$ for $\deg(x) = m$ and $h \in \mathbb{Z}$. In particular if f has degree 1, the zero part of A_f, denoted $(A_f)_0$ consist of elements xf^{-n} where $\deg(x) = n$.

Lemma 2.42. *Let A be a graded ring, graded in nonnegative degrees and such that A_1 generates A over A_0. let $f \in A$ be homogenous element of degree one, then there is a canonical isomorphism*

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

sending X to f.

Proof. The map φ is onto because for any $a \in A$ homogeneous of degree d and any n, we have $\varphi(\frac{a}{f^d}X^{d-n}) = \frac{a}{f^d}f^{d-n} = \frac{a}{f^n}$. To prove injectivity suppose that $\sum_{k=-n}^{k=n} r_k f^k$, with $r_k \in (A_f)_0$, is in the kernel of φ. Multiplying by a suitable power of f we get an identity in the ring A of the sort $\sum_{k=0}^{l} x_k f^{j-d_k+k} = 0$, where x_k are of degree d_k. Now, the degree of the term $x_k f^{j-d_k+k}$ is $j + k$ and is the only homogeneous term with that degree for $k = 1, 2, \ldots, l$, therefore it must be zero. □

Definition 2.43. *Let f be a homogeneous element in A. We define the basic open set determined by f as*

$$D_+(f) = \{\mathfrak{p} \in \mathrm{Proj}(A) \mid f \notin \mathfrak{p}\}.$$

Let I be a homogenous ideal $I \subset A$. We define

$$V_+(I) = \{\mathfrak{p} \in \mathrm{Proj}(A) \mid I \subseteq \mathfrak{p}\}$$

Remark 2.44. The sets of the form $V_+(I) = V(I) \cap \mathrm{Proj}(A)$ are the closed sets of a topology. A basis for the topology is given by the collection of sets $D_+(f) = D(f) \cap \mathrm{Proj}(A)$.

Theorem 2.45. *Let $A = \bigoplus_{n \geq 0} A_n$ be a graded ring in nonnegative degrees and let $M = \bigoplus_{n \in \mathbb{Z}} M_n$ be a graded A-module ($A_d M_e \subseteq M_{d+e}$). The function which to a basic open set $D_+(f)$ associates $(M_f)_0$ extends to a sheaf, denoted by $\tilde{M}$, on* $\mathrm{Proj}(A)$. *The ringed space* $(\mathrm{Proj}(A), \tilde{A})$ *is a scheme which on $D_+(f)$ is isomorphic to* $\mathrm{Spec}(A_f)_0$. *Moreover for each A-module M we have*

$$\tilde{M} \mid D_+(f) \cong \widetilde{(M_f)_0}.$$

Proof. The first part of the proposition is a graded version of the extension of the sheaf discussed in 2.15 and later in 2.21, with the only difference that for f homogeneous polynomial of positive degree, we will use $D_+(f)$ instead of just $D(f)$. We can check then that $D_+(f) \cap D_+(g) = D_+(fg)$ for homogeneous polynomials f and g. For the second part of the proposition we want to prove that $(D_+(f), \tilde{A}|D_+(f)) \simeq \operatorname{Spec}(A_f)_0$ for f homogeneous of positive degree. Let us do the proof for degree one: Using lemma 2.42 we can create a map $\mathfrak{p} \mapsto \mathfrak{p}[x, x^{-1}]$ from $\operatorname{Spec}(A_f)_0 \to D_+(f)$. If we get the same result for two different prime ideals, i.e. $\mathfrak{p}[x, x^{-1}] = \mathfrak{q}[x, x^{-1}]$, the degree zero part are the same and therefore $\mathfrak{p} = \mathfrak{q}$ and the map is injective. On the other hand if $\mathfrak{p}$ is an homogeneous prime ideal, the map $\mathfrak{p}_n \xrightarrow{f^{-n}} \mathfrak{p}_0$ is a bijection, which proves surjectivity. The open set $D_+(fg) \subset D_+(f)$ is sent to $D(\frac{f}{g}) \subset \operatorname{Spec}(A_f)_0$ and therefore the map is also a homeomorphism. We need to verify now that for every graded A-module M we have an equality $(\widetilde{M_f})_0 = \tilde{M}|D_+(f)$. For that it is enough to check that $(\tilde{M}(D_+(fg)) = (\tilde{M}(D_+(f)))_{gf^{-n}}$ for every homogeneous element $g \in A$ of degree n. An element of $(\tilde{M}(D_+(fg))$ is of the form $x(fg)^{-m}$ where $x \in M_{m(n+1)}$ and such an element can be written as

$$x(fg)^{-m} = xf^{-(n+1)m}(gf^{-n})^{-m},$$

which gives the desired equality. □

Definition 2.46. *The* n**-dimensional projective space** $\mathbb{P}^n_A$ **over a ring** A *is defined to be* $\operatorname{Proj}(A[x_0, x_1, \ldots, x_n])$*. More generally if* M *is a finitely generated locally free* A*-module, we define the* **projective space associated to M***, denoted* $\mathbb{P}_A(M)$*, as* $\operatorname{Proj}(Symm_A(M))$*, where* $Symm_A(M)$ *denotes the symmetric algebra of* M*.*

Definition 2.47. *Let* $A = \bigoplus_{n \geq 0} A_n$ *be a graded ring in nonnegative degrees. The* **twisting sheaf** $\mathcal{O}(n)$ *on* $\operatorname{Proj}(A)$ *is defined by* $\mathcal{O}(n) = \widetilde{A(n)}$*, where* $A(n)_k = A(n+k)$ *(the degree* k *part of* $\mathcal{O}(n)$ *is* $A(n+k)$*).*

Definition 2.48. *A* **closed immersion** $f\colon Y \longrightarrow X$ *is a map of schemes, such that* f *is a homeomorphism of* Y *into a closed set of* X *and the induce map on sheaves* $f^\sharp\colon \mathcal{O}_X \longrightarrow f_*\mathcal{O}_Y$ *is surjective. A* **closed subscheme** $Y \subset X$ *is the image of a closed immersion* $f\colon Y \hookrightarrow X$ *and the ideal sheaf* $\mathcal{I}_Y$ *is the kernel of the map* $f^\sharp\colon \mathcal{O}_X \longrightarrow f_*\mathcal{O}_Y$*.*

Example 2.49. If $\varphi^\sharp\colon A \longrightarrow B$ is a surjective homomorphism of rings, the associated map of schemes $\varphi\colon \operatorname{Spec}(B) \longrightarrow \operatorname{Spec}(A)$ is a closed immersion and the ideal sheaf is the quasi-coherent sheaf associated to $\ker(\varphi^\sharp)$.

Definition 2.50. *Let* X *be a scheme and* Y *a subscheme determined by the sheaf of ideals* $\mathcal{I}$*. The* **blow-up of** X **along** Y *is defined as the* *projective scheme*

$$Bl_Y(X) = \mathrm{Proj}(A \oplus \mathcal{I} \oplus \mathcal{I}^2 \oplus \dots).$$

The projectivized cone of Y in X is the subscheme of the blow-up defined by:

$$C_{Y/X} = \mathrm{Proj}(A/\mathcal{I} \oplus \mathcal{I}/\mathcal{I}^2 \oplus \mathcal{I}^2/\mathcal{I}^3 \oplus \dots).$$

Exercise 2.51. *Let X be the affine plane $\mathbb{A}^2_k$ over an algebraically closed field k, and Y the point $(0,0) \in X$. Show that the blow-up $Bl_Y(X)$ is just*

$$Bl_Y(X) = Bl_{(0,0)}(\mathbb{A}^2_k) = \{(x,y) \times (r,s) \in \mathbb{A}^2_k \times \mathbb{P}^1_k \,|\, xs = ry\}.$$

For the curve $X'\colon\, y^2 = x^3 - x^2 \subset X$ and the natural map $\pi\colon Bl_Y(X) \longrightarrow X$, prove that $\pi^{-1}X'$ is non-singular. In this sense the blow-up has resolved the singularity of X'.

2.6. **Quasi-coherent sheaves of $\mathcal{O}_X$-modules.** The notion of quasi-coherence for a sheaf was introduced by Serre and represents a global version in schemes of our $\tilde{M}$ over affine schemes.

Definition 2.52. *A* **sheaf of $\mathcal{O}_X$-modules** *is a sheaf $\mathcal{F}$ on X such that for each open U, the group $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)$-module, in such a way that the module structure is compatible with the inclusion maps. An $\mathcal{O}_X$-module $\mathcal{F}$ is free if it is isomorphic to a direct sum of copies of $\mathcal{O}_X$. It is locally free if X can be covered by open sets U for which $\mathcal{F}|U$ is a free $\mathcal{O}_X|U$-module.* **A locally free sheaf of rank one** *is called an* **invertible sheaf**. *A set of sections $s_1, s_2, \dots, s_k$ is said to generate a sheaf if for all $x \in X$ there exist $1 \le i \le k$ such that $s_i(x) \neq 0$.*

Definition 2.53. *Let $(X, \mathcal{O}_X)$ be a scheme. A sheaf $\mathcal{F}$ of $\mathcal{O}_X$-modules is* **quasi-coherent** *if X can be covered by open affine sets $U_i = \mathrm{Spec}(A_i)$, such that for each i there is a A_i-module M_i with $\mathcal{F}(U_i) \cong \tilde{M}_i$.*

Theorem 2.54. *Let X be a scheme, $\mathcal{F}$ a sheaf of $\mathcal{O}_X$-modules. The following are equivalent:*

1. *For all $U \subset X$ affine open $\mathcal{F}|_U \cong \tilde{M}$ for some $\Gamma(U, \mathcal{O}_X)$-module M.*
2. *($\mathcal{F}$ is quasi-coherent): there is an open affine cover $\{U_i\}$ of X such that for all i, $\mathcal{F}|_{U_i} \cong \tilde{M}_i$ for some $\Gamma(U_i, \mathcal{O}_X)$-module M_i.*
3. *($\mathcal{F}$ is locally the cokernel of free modules): For all $x \in X$, there exist a neighborhood U of x and an exact sequence of $\mathcal{O}_X|_U$-modules*

$$\mathcal{O}_X|_U^{(I)} \longrightarrow \mathcal{O}_X|_U^{(J)} \longrightarrow \mathcal{F}|_U \longrightarrow 0.$$

(4) *For all $V \subset U$ open affine schemes, the canonical map*

$$\Gamma(U, \mathcal{F}) \otimes_{\Gamma(U,\mathcal{O}_X)} \Gamma(V, \mathcal{O}_X) \longrightarrow \Gamma(V, \mathcal{F}),$$

is an isomorphism.

Proof. (Mumford, [Mum99]) Suppose that we have (4) and let us prove (3). Let $x \in X$ and take an open neighborhood U of x and $A = \Gamma(U, \mathcal{O}_X)$. The A-module $\Gamma(U, \mathcal{F})$ admits a presentation

$$A^{(I)} \longrightarrow A^{(J)} \longrightarrow \Gamma(U, \mathcal{F}) \longrightarrow 0$$

applying the tilde operation to get the associated sheaves we obtain

$$\mathcal{O}_X^{(I)}|_U \longrightarrow \mathcal{O}_X^{(J)}|_U \longrightarrow \widetilde{\Gamma(U, \mathcal{F})} \longrightarrow 0$$

The canonical homomorphism $\alpha : \widetilde{\Gamma(U, \mathcal{F})} \longrightarrow \mathcal{F}|_U$ is an isomorphism because by (4) is given on basic open sets by the isomorphism

$$\Gamma(U_f, \widetilde{\Gamma(U, \mathcal{F})}) = \Gamma(U, \mathcal{F}) \otimes_A A_f \longrightarrow \Gamma(U_f, \mathcal{F}).$$

From (3) to (2), we cover X with affine open sets $U_i = \mathrm{Spec}(A_i)$ on which we have exact sequences:

$$\phi_i : \mathcal{O}_X|_{U_i}^{(I_i)} \longrightarrow \mathcal{O}_X|_{U_i}^{(J_i)} \longrightarrow \mathcal{F}|_{U_i} \longrightarrow 0$$

Since $\mathcal{O}_X|_{U_i}^{(I_i)} = \widetilde{A_i^{(I_i)}}$ and $\mathcal{O}_X|_{U_i}^{(J_i)} = \widetilde{A_i^{(J_i)}}$, the cokernel of the map ϕ_i is of the form $\tilde{K}$ and satisfies (2).

From (2) to (1) we take a basis $\{U_i\}$ for the topology of X such that $\mathcal{F}|_{U_i} \cong \tilde{M}_i$. Now, if U is an open affine with $\Gamma(U, \mathcal{O}_X) = A$ we can cover each of the U_i by smaller open sets of the form U_g, where $g \in A$ and $\mathcal{F}|_{U_i}$ is of the form $\tilde{M}_{ig}$. We have therefore a finite cover of U by affine sets U_{g_i} with $\mathcal{F}|_{U_i} = \tilde{N}_i$ (N_i is now a A_{g_i}-module) and for every open $V \subset U$ an exact sequence

$$0 \longrightarrow \Gamma(V, \mathcal{F}) \longrightarrow \prod_i \Gamma(V \cap U_{g_i}, \mathcal{F}) \longrightarrow \Gamma(V \cap U_{g_i} \cap U_{g_j}, \mathcal{F}).$$

We can define new sheaves by

$$\mathcal{F}'_i|_V = \mathcal{F}|_{V \cap U_{g_i}} \qquad \mathcal{F}''_{i,j}|_V = \mathcal{F}|_{V \cap U_{g_i} \cap U_{g_j}}$$

to have an exact sequence

$$0 \longrightarrow \mathcal{F} \longrightarrow \prod_i \mathcal{F}'_i \longrightarrow \prod_{i,j} \mathcal{F}''_{i,j}$$

and will be sufficient to prove that $\mathcal{F}_i'$ and $\mathcal{F}_{i,j}''$ are of the form $\tilde{M}$ for some A-module M. But if we look at N_i as a module over A, denoted by N_i^0 then for all open sets U_g

$$\begin{aligned}\Gamma(U_g, \mathcal{F}_i') &= \Gamma(U_g \cap U_{g_i}, \mathcal{F})\\ &= \Gamma((U_{g_i})_g, \mathcal{F}|U_{g_i})\\ &= (N_i)_g = \Gamma(U_g, \widetilde{N_i^0}),\end{aligned}$$

and the same argument works for $\mathcal{F}_{i,j}''$. From (1) to (4): Let $U = \operatorname{Spec}(A)$ be an affine open set and $V = \operatorname{Spec}(B)$ with $V \subset U$. Let $\mathcal{F}|_U = \tilde{M}$. We represent the A-module M like

$$A^{(I)} \longrightarrow A^{(J)} \longrightarrow M \longrightarrow 0.$$

and therefore

$$\mathcal{O}_X^{(I)}|_V \longrightarrow \mathcal{O}_X^{(J)}|_V \longrightarrow \mathcal{F}|_V \longrightarrow 0$$

We also have a sequence of B-modules

$$A^{(I)} \longrightarrow A^{(J)} \longrightarrow N \longrightarrow 0.$$

because $\mathcal{F}|_V = \tilde{N}$ for some B-module N. Tensoring the first sequence by B we get

$$A^{(I)} \otimes_A B \longrightarrow A^{(J)} \otimes_A B \longrightarrow M \otimes_A B \longrightarrow 0.$$

and N and $M \otimes_A B$ are equal because they are cokernels of the same map.

□

Example 2.55. Consider a ring A which is a local domain of dimension one. The spectrum $\operatorname{Spec}(A)$ consist of two points: x_0 the closed point and $x_1 = U$ an open point. The sheaf $\mathcal{F}$ consist of two sets: $M_0 = \Gamma(X, \mathcal{F})$ and $M_1 = \Gamma(U, \mathcal{F})$ and a A-linear restriction map $M_0 \longrightarrow M_1$. Let K be the quotient field of A. The set M_1 is a K-module and M_0 is an A-module. The sheaf $\mathcal{F}$ is quasi-coherent (condition (4)) if and only if the induced map on the quotient field $M_0 \otimes_A K \longrightarrow M_1$ is an isomorphism. In this case $\mathcal{F} = \tilde{M}_0$.

Definition 2.56. *A* **topological space** X **is noetherian** *if for all open sets $U \subset X$, the partially order set of closed subschemes of U satisfies the descending chain condition. Let X be a noetherian space, $\mathcal{F}$ a quasi-coherent sheaves of $\mathcal{O}_X$-modules. Then $\mathcal{O}_X$ is said to be* **coherent** *if for all affine $U \subset X$, the $\Gamma(U, \mathcal{F})$ is a finite $\Gamma(U, \mathcal{O}_X)$-module.*

Example 2.57. If A is a noetherian ring, the topological space $\operatorname{Spec}(A)$ is noetherian. More generally if a scheme X admits a finite covering by open affine sets $\operatorname{Spec}(A_i)$ with A_i noetherian, then X is a noetherian topological space.

Example 2.58. For a map of schemes $X \longrightarrow Y$, the sheaf of relative differentials $\Omega_{X/Y}$ is a quasi-coherent sheaf. If $f : X \longrightarrow Y$ is a morphism of finite type (see later definition 3.59) between noetherian spaces, then then $\Omega_{X/Y}$ is coherent. For example for $B = K[x_1, \dots, x_n]/(f_1, \dots, f_m)$ and $A = K$, the sheaf of relative differentials $\Omega_{\operatorname{Spec}(B)/\operatorname{Spec}(A)}$ is a coherent sheaf of on $\operatorname{Spec}(B)$.

Example 2.59. For any closed subscheme $Y \subset X$, the ideal sheaf $\mathcal{I}_Y$ is a quasi-coherent sheaf of ideals. If X is noetherian, if it is a coherent sheaf.

Exercise 2.60. *Consider the blow-up $\pi\colon Bl_Y(X) = \tilde{X} \longrightarrow X$ of a scheme X along a subscheme Y defined by the ideal sheaf $\mathcal{I}$. Define the inverse image ideal $\tilde{\mathcal{I}} = \pi^{-1}\mathcal{I}\mathcal{O}_{\tilde{X}}$. Prove that $\tilde{\mathcal{I}}$ is in fact equal to $\mathcal{O}_{\tilde{X}}(1)$. In particular $\tilde{\mathcal{I}}$ is an invertible sheaf on $\tilde{X}$.*

Proposition 2.61. *Let A be a noetherian ring. Let $X = \operatorname{Proj} A$ for a graded k-algebra which is finitely generated in degree 1. Then we have the following*

1. *Every coherent sheaf on X is isomorphic to $\tilde{M}$ for some finitely generated graded A-module M.*
2. *Two finitely generated $\mathbb{Z}$-graded A-modules M, N satisfy $\tilde{M} = \tilde{N}$ if and only if there is an isomorphism of graded modules $M_{\geq n} \cong N_{\geq n}$ for some $n \in \mathbb{Z}$.*

Proof. (1) Let $\mathcal{F}$ be a coherent sheaf on X and consider the associated graded module

$$M = \Gamma_*(\mathcal{F}) = \bigoplus_n \Gamma(X, \mathcal{F}(n)).$$

Let us define the map $\beta\colon \widetilde{\Gamma_*(\mathcal{F})} \longrightarrow \mathcal{F}$. Let $f \in A_1$. Since $\widetilde{\Gamma_*(\mathcal{F})}$ is coherent it is enough to give the map β on open sets of the form $D_+(f)$. A section of $\widetilde{\Gamma_*(\mathcal{F})}$ is of the form $\frac{m}{f^d}$ for $m \in \Gamma_*(X, \mathcal{F}(d))$ and f^{-d} can be considered as a section of $\mathcal{O}_X(-d)$, which means that we can take

$$\beta(\frac{m}{f^d}) = m \otimes f^{-d} \in \Gamma(D(f), \mathcal{F}).$$

Now, because $\mathcal{F}$ is coherent, the map β identifies the module $M_{(f)}$ with sections of $\mathcal{F}$ over $D_+(f)$. To do that we find elements $\{f_1, \dots, f_n\} \subset A_1$ such that X is covered by $D_+(f_i)$ and then for a section $t \in \Gamma(X_f, \mathcal{F})$

and for some $n > 0$, the section $f^n t \in \Gamma(X_f, \mathcal{F}\otimes\mathcal{O}(n))$ extends a global section of $\mathcal{F} \otimes \mathcal{O}(n)$ (Lemma 5.14 of [Har77]). In this way we prove that the map $\beta\colon \widetilde{\Gamma_*(\mathcal{F})} \longrightarrow \mathcal{F}$ is an isomorphism for $\mathcal{F}$ coherent.

(2) For a graded A-module M we have the exact sequence:

$$0 \longrightarrow M_{\geq n} \longrightarrow M \longrightarrow M/M_{\geq n} \longrightarrow 0.$$

Localization with respect the multiplicatively stable system $\{1, f, f^2, \dots\}$ for a homogeneous element $f \in A$ kills the finite dimensional vector space $M/M_{\geq n}$ and therefore we have $M_{\geq n(f)} \cong M_{(f)}$ and the equality of the associated sheafs $\widetilde{M_{\geq n}} = \tilde{M}$. On the other hand if we have two graded A-modules M, N satisfying all the conditions of the theorem and $\tilde{M} = \tilde{N}$, the sheaf $\widetilde{M(n)}$ is generated by global sections of N for n big enough. If we take the submodule $N' \subset N$ generated by those sections we have $\tilde{N'} \hookrightarrow \tilde{M}$, which gives an isomorphism $N_n \cong N'_n \cong M_n$ for n big enough. □

Let X be a noetherian scheme. The idea of **Proj** can be extended to quasi-coherent sheaves $\mathcal{L} = \bigoplus_{d\geq 0} \mathcal{L}_d$ of graded $\mathcal{O}_X$ algebras. We are going to assume that the degree zero part $\mathcal{L}_0 = \mathcal{O}_X$ and that the degree one part $\mathcal{L}_1$ is be a coherent sheaf of $\mathcal{O}_X$ algebras that generates the whole $\mathcal{L}$ as $\mathcal{L}_0 = \mathcal{O}_X$-algebra. The sheaf $\mathcal{L}$ being quasi-coherent allows us to glue together the different $\pi_U : \mathrm{Proj}(\mathcal{L}(U)) \longrightarrow U$ over the affine open sets $U = \mathrm{Spec}(A)$ along the intersection. The properties of quasicoherent sheaves give $\pi_U^{-1}(U \cap V) \cong \pi_V^{-1}(U \cap V)$. In this way we can construct the global $\pi\colon\ \mathrm{Proj}(\mathcal{L}) \longrightarrow X$

Definition 2.62. *Let X be a noetherian scheme and $\mathcal{E}$ a locally free coherent sheaf, construct the symmetric algebra $\mathcal{L}(\mathcal{E}) = S(\mathcal{E})$, then the algebra $\mathcal{L}(\mathcal{E})$ satisfies the previous conditions and we define $\mathbb{P}(\mathcal{E}) = \mathrm{Proj}(\mathcal{L}(\mathcal{E}))$. We call $\mathbb{P}(\mathcal{E})$ the* **relative projective space** *associated to $\mathcal{E}$.*

Definition 2.63. *Let $\mathcal{E}$ be a quasi-coherent sheaf of $\mathcal{O}_X$-modules. The symmetric algebra* $\mathrm{Symm}(\mathcal{E})$ *is also a quasi-coherent sheaf of $\mathcal{O}_X$-algebras and it satisfies our conditions for defining* Proj. *We denote by $\mathbb{P}(\mathcal{E}) = \mathbb{P}(\mathrm{Symm}(\mathcal{E}))$, the* **projective bundle** *associated to $\mathcal{E}$.*

Example 2.64. X be a noetherian scheme and $\mathcal{I}$ a coherent sheaf of ideals. There is a natural surjection of graded algebras

$$\mathrm{Symm}(\mathcal{I}) \longrightarrow \bigoplus_{d\geq 0} \mathcal{I}^d,$$

which allow us to consider the blowing up $Bl_{\mathcal{I}}(X)$ as a closed subset of $\mathbb{P}(\mathcal{I})$. On the other hand, the projectivized cone of Y in X is $\mathrm{Symm}_{\mathcal{O}_X/\mathcal{I}}(\mathcal{I}/\mathcal{I}^2)$.

2.7. **Projective modules and invertible sheaves.** The projective modules of rank one will represent a special case of line invertible sheaves when we work with affine schemes.

Definition 2.65. *Let A be a ring. An A-module P is called* **projective** *if for every surjective A-homomorphism $M \longrightarrow M'$ of A-modules, the canonical homomorphism* $\mathrm{Hom}_A(P, M) \longrightarrow \mathrm{Hom}_A(P, M')$ *is onto.*

Example 2.66. The free A-module $M = A^I$ is a projective A-module.

Proposition 2.67. *The following statements are equivalent:*

(1) *P is projective.*
(2) *The functor* $\mathrm{Hom}_A(P, .)$ *is exact.*
(3) *P is a direct summand of a free module*

Proof. (2) is just a reformulation of (1). Assume (3), that is P is a direct summand of free A-module A^I. Then $\mathrm{Hom}_A(P, .)$ is a direct summand of $\mathrm{Hom}_A(A^I, .)$ and therefore exact. On the other hand if $(x_i)_{i\in I}$ is a generating system of P over A, we have a surjective map $A^I \twoheadrightarrow P$. By definition of projective we have a section $P \longrightarrow A^I$ that makes P a direct summand of A^I. □

Definition 2.68. *Let A be a ring and M an A-module. We will call M dual (denote $M^\vee$) the A-module $M^\vee = \mathrm{Hom}_A(M, A)$.*

For all A-modules M and N there is a canonical map $M^\vee \otimes_A N \longrightarrow \mathrm{Hom}_A(M, N)$ that maps $\varphi \otimes y$ to the homomorphism $x \mapsto \varphi(x)y$ from M to N.

Proposition 2.69. *The following statements are equivalent:*

(1) *P is projective of finite type*
(2) *The canonical map $P^\vee \otimes_A P \longrightarrow \mathrm{End}_A(P)$ is surjective.*

Proof. The direction (1) ⇒ (2) is a consequence of 2.67 (3). To prove the other direction we observe that the identity of P is in the image of $P^\vee \otimes_A P$. There exist then a natural number n together with $x_1, x_2 \ldots x_n \in P$ and linear forms

$$\varphi_1, \varphi_2, \ldots \varphi_n : P \longrightarrow A,$$

such that for all $y \in P$ we have $y = \sum_{i=1}^n \varphi_i(y)x_i$. The x_i generate P and we have a surjective homomorphism $A^n \longrightarrow P \longrightarrow 0$. The map $\varphi(y) = (\varphi_1(y), \ldots, \varphi_n(y))$ on other hand determines a section $\varphi : P \longrightarrow A^n$ and P is a direct summand of A^n. □

Exercise 2.70. *Show that with the conditions of the previous proposition, the map $P^\vee \otimes_A P \longrightarrow \operatorname{End}_A(P)$ is an isomorphism.*

Exercise 2.71. *(Trace of a map on projective modules of finite rank) Let A be a ring.*

(a) *For every A-module, there is a canonical (evaluation) morphism $M^\vee \otimes_A M \longrightarrow A$, such that $\varphi \otimes y$ is associated to $\varphi(y)$.*
(b) *If P is a free A-module of finite rank, verify that the image of $f\colon P \longrightarrow P$ by the previous maps is the trace of f. One can in this way define the trace of an endomorphism on a projective module of finite rank.*

Exercise 2.72. *(Projective modules are reflexive) Let M be an A-module. We have a canonical A-homomorphism $M \longrightarrow M^{\vee\vee}$. Verify that if M is projective of finite type, the above homomorphism is a bijection. Show that if M is projective of finite type, so is $M^\vee$.*

Exercise 2.73. *Show that every projective module is flat. In this sense, we have the inclusions*

$$\textit{Free Modules} \subseteq \textit{Projective Modules} \subseteq \textit{Flat Modules.}$$

Exercise 2.74. *If P is a projective module over a ring A and S is a multiplicatively stable system of A. Show that $S^{-1}P$ is a projective $S^{-1}A$-module.*

Exercise 2.75. *Let P be a projective module. Show that for all integer n, the modules $T_n(P), Symm_n(P)$ and $\wedge^n(P)$ are projective modules.*

Exercise 2.76. *Prove that a projective module of finite type is finitely presented.*

Theorem 2.77. *The following statements are equivalent*

(1) *P is projective of finite type*
(2) *P is locally free of finite type for the Zariski topology of* $\operatorname{Spec}(A.)$

Proof. For (2) ⇒ (1), we use proposition 2.69. Let $M = coker(P^\vee \otimes_A P \longrightarrow \operatorname{End}_A(P))$. The fact that P is locally free provide us with elements $f_1, f_2, \dots, f_n$ that form a unity partition and such that P_{f_i} are free A_{f_i}-modules of finite type for each i. Localization commutes with tensor product and with $Hom(P, .)$ since P is finitely presented. The module M satisfies then

$$M_{f_i} = coker(P_{f_i}^\vee \otimes_{A_{f_i}} P_{f_i} \to \operatorname{End}_{A_{f_i}}(P_{f_i})) = 0 \quad \forall i = 1, \dots, n.$$

By properties of localization in exercise 1.27 we get that $M = 0$ and P is projective. The other direction is a consequence of the following two lemmas: □

Lemma 2.78. *If P is a projective module of finite type, $\mathfrak{p}$ a prime ideal of A and we have an isomorphism $\psi : A_{\mathfrak{p}}^n \longrightarrow P_{\mathfrak{p}}$ there exist $f \in A \setminus p$ such that φ can be extended to a map $\varphi : A_f^n \longrightarrow P_f$.*

Proof. Let us show that if $\varphi : A^n \longrightarrow P$ is an A-morphism such that $\varphi_p = \psi$, then there exist $f \in A \setminus \mathfrak{p}$ such that $(\ker(\varphi))_f$ and $(\mathrm{Coker}(\varphi))_f$ are both zero. The module $\mathrm{Coker}(\varphi)$ is of finite type because P is. We need to proof that $\ker(\varphi)$ is of finite type in a neighborhood of $\mathfrak{p}$. Using exercise 1.27, we can choose $f \in A$ such that $(\mathrm{Coker}(\varphi))_f = 0$, then P_f is a projective A_f-module with

$$\ker(\varphi)_f \to P_f \to A_f^n \to 0.$$

The map φ_f splits and $\ker(\varphi)_f$ is a quotient of A_f^m and hence of finite type. □

Lemma 2.79. *If A is a local ring with maximal ideal m and P is a projective A-module of finite type then P is free of rank $\dim_{A/m}(P/m)$.*

Proof. Let $x_1, \dots, x_n$ be elements of P that represent a basis of P/mP over the field A/m. Let $\varphi : A^n \longrightarrow P$ the homomorphism sending the element e_i of the canonical basis of A^n to x_i. By Nakayama, we have a split exact sequence $0 \to N \to A^n \xrightarrow{\varphi} P \to 0$. When we tensor by A/m, the sequence is still exact

$$0 \to N \otimes A/m \to (A/m)^n \xrightarrow{\tilde{\varphi}} P/mP \to 0.$$

The map $\tilde{\varphi}$ is chosen to be an isomorphism $\tilde{\varphi} : (A/m)^n \longrightarrow P/mP$ of finite dimensional vector spaces and therefore $N \otimes A/m = 0$. Applying Nakayama for the finite type module N we obtain $N = 0$ and $\varphi : A^n \longrightarrow P$ is an isomorphism. □

Corollary 2.80. *Let A be a ring and P an A-module of finite type over A. The function $r(P)$: $\mathrm{Spec}(A) \longrightarrow \mathbb{N}$ that to a prime ideal $\mathfrak{p}$ associates the dimension of the 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 module of finite type. Consider a covering $(D(f_i))_{i=1}^n$ of $\mathrm{Spec}(A)$ by basic open sets. Using theorem 2.77, P is locally free of finite rank for the Zariski topology, therefore for each i there exist an integer n_i such that $A_{f_i}^{n_i}$ is isomorphic to P_{f_i}. Since localization is an exact functor, for every $\mathfrak{p} \in D(f_i)$, $A_{\mathfrak{p}}^{n_i}$ is isomorphic to $P_{\mathfrak{p}}$. Since the modules $P_{\mathfrak{p}}/\mathfrak{p}P_{\mathfrak{p}} \cong (A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}})^{n_i}$, 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 2.81. *Let A be a ring and P an A-module of finite type over A. One says that P is of rank n if the function $r(\mathfrak{p})\colon \operatorname{Spec}(A) \longrightarrow \mathbb{N}$ is constant and equal to n.*

Example 2.82. If $\operatorname{Spec}(A)$ is connected as topological space, then all projective A-modules of finite type are of constant rank. In particular lemma 2.79 shows that for a domain A with field of fractions K, every projective A-module P is of constant rank equals $\dim_K(P \otimes_A K)$.

Exercise 2.83. *Let A be a ring and P a projective module of constant rank.*

(a) *Prove that if P' is another projective A-module of constant rank so is $P \otimes_A P'$.*
(b) *Show that $T_i(P), \operatorname{Symm}_i(P), \wedge^i(P)$ and $P^\vee$ and projective module of constant rank.*
(c) *Let n be the rank of P, show that there is a canonical isomorphism*
$$P \longrightarrow \operatorname{Hom}(\wedge^{n-1}P, \wedge^n P).$$

Exercise 2.84. *Let A be a reduced ring and M of finite type. Suppose that the function $r(M)$ is locally constant. Show that M is projective. Find an example where this is not true for a non-reduced ring A.*

Exercise 2.85. *Prove that an A-module P is projective of finite type if and only if the localization $P_\mathfrak{p}$ is free of finite type over $A_\mathfrak{p}$ for all $\mathfrak{p} \in \operatorname{Spec}(A)$.*

Exercise 2.86. *Consider the ring $A = \mathbb{Z}/6\mathbb{Z}$. Show that the A-module $\mathbb{Z}/3\mathbb{Z}$ is projective of finite type but not free over $\mathbb{Z}/6\mathbb{Z}$.*

Exercise 2.87. *Let A be a ring such that $\operatorname{Spec}(A)$ is not connected. Find a A-module projective module of finite type over A that is not free.*

Exercise 2.88. *(Tangent bundle to the sphere) Let A be the ring of the real sphere $A = \mathbb{R}[X,Y,Z]/(X^2+Y^2+Z^2-1)$. Let T the A-module which is the kernel of the map $\varphi\colon A^3 \longrightarrow A$ defined on the canonical basis e_1, e_2, e_3 by $\varphi(e_1) = 2X$, $\varphi(e_2) = 2Y$ and $\varphi(e_3) = 2Z$.*

(a) *Show that T is a projective A-module of rank two.*
(b) *Show that $T = (\Omega^1_{A/\mathbb{R}})^\vee$.*
(c) *Let (x,y,z) be a point with real coordinates in the sphere of radius one. Verify that the kernel of the evaluation map $ev\colon A \longrightarrow \mathbb{R}$ that to any polynomial f assigns $f(x,y,z)$, is a maximal ideal $m(x,y,z)$ of A. Verify that $A/m(x,y,z) = \mathbb{R}$.*
(d) *Let (α,β,γ) a point with real coordinates in A^3. Show that if (α,β,γ) is in T then the point of $\mathbb{R}^3$ with coordinates $(x+$*

$\alpha(x,y,z), y+\beta(x,y,z), z+\gamma(x,y,z))$ is in the tangent plane to sphere at (x,y,z).

(e) *Deduce from a classical theorem of algebraic topology that the projective A-module T is not a free A-module.*

2.8. **Invertible modules over a ring.** The projective modules of rank one are particularly interested. For example an ideal of A that is a projective module is of rank one.

Definition 2.89. *Let A be a ring and let L be a module over A. We say that L is an* **invertible A-module** *if and only if L is* **projective of rank one**.

Proposition 2.90. *Let L be an A-module. the following propositions are equivalent.*

(1) *L is invertible*
(2) *The canonical map of evaluation $L\otimes_A L^\vee \longrightarrow A$ is an isomorphism.*

Proof. (1) $\Rightarrow$ (2) It is enough to tho the proof locally and therefore the proof reduces to the case $L = A$.
(2) $\Rightarrow$ (1) It is now enough to show that L is isomorphic to A when A is local. If (2) holds we have n elements $x_1,\dots,x_n \in A$ and n linear forms $\lambda_1,\dots,\lambda_n$ on L such that $\sum_{i=1}^n \lambda_i(x_i) = 1$. When A is local, we then have at least one $\lambda_i(x_i)$ that is invertible in A. Therefore we can find a linear map $\lambda : L \longrightarrow A$ and an element $x \in L$ such that $\lambda(x) = 1$ and when we sent the element $1 \in A$ to x we obtain a splitting $L = A\oplus M$. Taking dual we get $L^\vee = A \oplus M^\vee$ and

$$L\otimes_A L^\vee = A\oplus M \oplus M^\vee \oplus M\otimes M^\vee.$$

Suppose that $M \neq 0$. If $m \in M$ is an element whose image is x after the map $L\otimes_A L^\vee \to A$, the element $(-x, m)$ also in $L\otimes_A L^\vee$ will have then image 0, givin $m = 0$ and $x = 0$. Alternatively we could have observed that $M, M^\vee$ and $M\otimes M^\vee$ are projective modules because they are direct factors of A. The rank being additive will give $M = M^\vee = 0$. □

Corollary 2.91. *Let L be an invertible A-module, then the canonical endomorphism $A \longrightarrow \mathrm{End}_A(L)$ is an isomorphism*

Proof. For a projective module L of finite type over A we have an isomorphism $L^\vee\otimes_A L \longrightarrow \mathrm{Hom}_A(L,L)$. On the other hand by 2.90, for an invertible module L we have an isomorphism $L^\vee \otimes_A L \longrightarrow A$. □

Exercise 2.92. *Let P be a projective module of rank n, show that $\wedge^n P$ is an invertible A-module.*

Exercise 2.93. *Let A be an integral domain and L_1, L_2 invertible A-modules. Prove that any A-homomorphism $L_1 \longrightarrow L_2$ is injective.*

Exercise 2.94. *Prove that if L is an invertible A-module, then $L^\vee$ is also invertible.*

Proposition 2.95. *The tensor product gives the set of isomorphism classes of invertible A-modules, the structure of commutative group. The class of A is the neutral element and the class of the dual is the inverse. This group is called* **the Picard group** *of A and denoted* $\mathrm{Pic}(A)$.

Exercise 2.96. *(Grothendieck group) Let A be a ring and $Proj(A)$ the set of isomorphism classes of projective A-modules of finite type. One denotes by $K^0(A)$ the group $\mathbb{Z}^{(Proj(A))}/\mathcal{R}$, where $\mathcal{R}$ is the group generated by elements of the form $[P]-[P']-[P'']$ whenever we have a short exact sequence $0 \longrightarrow P' \longrightarrow P \longrightarrow P'' \longrightarrow 0$. We called $K^0(A)$ the Grothendieck group of the projective A-modules of finite type.*
(a) Let $\chi : Proj(A) \longrightarrow K^0(A)$ defined by $\chi(P) =$ class of $[P]$. Show that χ is the universal additive function, that is for any map $\lambda : Proj(A) \longrightarrow G$, where G is an additive group, with the property that $\lambda(P) = \lambda(P') + \lambda(P'')$ whenever there is an exact sequence of projective modules $0 \longrightarrow P' \longrightarrow P \longrightarrow P'' \longrightarrow 0$, then there is a unique $\varphi : K^0(A) \longrightarrow G$ such that $\lambda = \varphi \circ \chi$.
(b) Show using splitting that if we have an exact sequence $0 \longrightarrow P' \longrightarrow P \longrightarrow P'' \longrightarrow 0$ of projective modules of finite type, then

$$\bigwedge^n P \simeq \bigoplus_{i+j=n} \bigwedge^i P' \otimes \bigwedge^j P''.$$

(c) Deduce that if $\mathrm{Spec}(A)$ *is connected for the Zariski topology, the map $\bigwedge^{max} : Proj(A) \longrightarrow$* $\mathrm{Pic}(A)$ *that to every projective module P of rank n assigns $\bigwedge^n P$ is additive and we can therefore define a homomorphism* ***determinant****:*

$$\det : K^0(A) \longrightarrow \mathrm{Pic}(A).$$

(d) Verify that for connected $\mathrm{Spec}(A)$*, the function $rk : Proj(A) \longrightarrow \mathbb{Z}$ is also additive and therefore we have a rank homomorphism $rk : K^0(A) \longrightarrow \mathbb{Z}$.*

The notion of invertible sheaf on a scheme is a globalization of the idea of invertible A-module or projective module of rank one.

Definition 2.97. *An* **invertible sheaf over a scheme** *X is a quasi-coherent sheaf $\mathcal{L}$ such that there exist a covering of X by open sets*

$\{U_i\}_{i\in I}$ such that $\mathcal{L}|U_i \backsimeq \mathcal{O}_{U_i}$. We will refer to invertible sheaves also as **line bundles** *on X.*

Exercise 2.98. *Show that if $U = \operatorname{Spec}(A)$ is an open set of a scheme X and $\mathcal{L}$ is an invertible sheaf on X, then $L|_U = \tilde{P}$ for some projective A-module P.*

Exercise 2.99. *Show that isomorphism classes of invertible sheaves on X with the tensor product have the natural structure of abelian group. We called the* **Picard group of** *X, denoted $\operatorname{Pic}(X)$.*

A **positive Cartier divisor** is defined on the scheme X as a closed sub-scheme of X locally defined by one equation that is not a zero divisor in $\mathcal{O}_X$. It is the same as saying that the associated sheaf of ideals is invertible. **A Cartier divisor** is locally the difference of two positive Cartier divisors.

Definition 2.100. *Let A graded in positive degree. We denote $A(n)$, the graded A-module such that $A(n)_k = A_{n+k}$ and also by $\mathcal{O}_P(n)$ the sheaf $\widetilde{A(n)}$ associated to $A(n)$ on $P = \operatorname{Proj}(A)$.*

Proposition 2.101. *Let A be a graded ring in positive degree and denote $P = \operatorname{Proj}(A)$. If f is a homogeneous element of degree one, we have an isomorphism of sheaves $\mathcal{O}(n)|D_+(f) \simeq \mathcal{O}_P|D_+(f)$.*

Proof. We have an isomorphism $(A_f)_0 \xrightarrow{\sim} (A_f)_n$ given by multiplication by f^n. Therefore

$$\mathcal{O}(n)|D_+(f) \simeq \widetilde{((A_f)_n)_0} \simeq \widetilde{(A_f)_0} \simeq \mathcal{O}_P|D_+(f),$$

and we obtain the isomorphism of sheaves. □

Corollary 2.102. *Let $A = \oplus A_n$ a graded ring generated by A_1 over A_0. The sheaf $\mathcal{O}_P(n)$ is locally free on $P = \operatorname{Proj}(A)$. For integers n, m we have $\mathcal{O}(n) \otimes \mathcal{O}(m) \backsimeq \mathcal{O}(n+m)$. On the other hand for all integers n there is a A_0-homomorphism*

$$A_n \longrightarrow \Gamma(\operatorname{Proj}, \mathcal{O}_P(n)),$$

that is an isomorphism when $A = A_0[x_0, \dots, x_n]$ is the polynomial ring.

Proof. We have the isomorphism of graded A-modules $A(n) \otimes_A A(m) \xrightarrow{\sim} A(n+m)$ that will give an isomorphism of associated sheaves. For the second part note that we have a canonical homomorphism of A_0-modules $M_0 \longrightarrow (M_f)_0$ for every A_0-module M. We can paste together this maps to obtain a map $M_0 \longrightarrow \Gamma(Proj(A), \tilde{M})$. Now when $A = A_0[x_0, \dots, x_n]$, this map is injective on the open cover defined by the sets $D_+(x_i)$ for each $i = 1, \dots n$. On the other hand if we have homogeneous polynomials $P_0, \dots, P_m$ of degree $n + k$ such that we have an equality $X_j^k P_i = X_i^k P_j$ with $i \neq j$, the exponent of X_i in P_i is at least k and therefore X_i^k divides P_i and the map is surjective. □

Corollary 2.103. *Let A be a ring such that* $\mathrm{Spec}(A)$ *is a connected set, then the projective space $\mathbb{P}_A^n$ is also connected.*

Proof. The global sections of $\mathbb{P}_A^n$ are $\Gamma(\mathbb{P}_A^n, \mathcal{O}_{\mathbb{P}_A^n}) = A$. □

Proposition 2.104. *Let $A = \oplus A_n$ a graded ring generated by A_1 over A_0. Then $\mathcal{O}_P(1)$ is generated by the sections images of A_1.*

Proof. For every homogeneous element f of degree one and $x \in A_{k+1}$, the map $\theta\colon (A_f)_0 \otimes A_1 \longrightarrow ((A_1)_f)_0$ given by

$$\theta(xf^{-k-1} \otimes f) = xf^{-k-1}f = xf^{-k}$$

is a surjection on the open set $D(f)$. □

Proposition 2.105. *(Characterization of morphisms to the projective space) Let A be a ring, n an integer and X a scheme over A then the inverse image gives a natural bijection between the set of morphisms* $\mathrm{Hom}_{A-Schemes}(X, \mathbb{P}_A^n)$ *and the classes of vectors $(\mathcal{L}, s_0, \dots, s_n)$ where $\mathcal{L}$ is an invertible sheaf on X and s_i for $i = 0, \dots, n$ are global sections of $\mathcal{L}$ that generate $\mathcal{L}$ and $(\mathcal{L}, s)$ and $(\mathcal{L}', s')$ are equivalents, denoted $(\mathcal{L}, s) \sim (\mathcal{L}', s')$ when there exist an isomorphism $\theta : \mathcal{L} \longrightarrow \mathcal{L}'$ such that $\theta(s_i) = s_i'$ for all i.*

Proof. We will take the class of $(\varphi^*\mathcal{O}(1), \varphi^*T_0, \dots, \varphi^*T_n)$ as image of the map $\varphi : X \longrightarrow \mathrm{Proj}\, A[T_0, \dots, T_n]$. Let us consider the open set $X_i \subset X$ where $s_i \neq 0$, that is to say where s_i generates $\mathcal{L}$. The X_i cover X because the system of section $\{s_i\}_i$ generate $\mathcal{L}$. We have $\varphi_i = \varphi|X_i : X_i \longrightarrow U_i$ where we denote by $U_i \subset \mathbb{P}^n(A)$ the open set where $T_i \neq 0$. As $U_i = \mathrm{Spec}(A[\frac{T_j}{T_i}])$ one sees that φ_i is associated to the ring homomorphism $\varphi^* : A[\frac{T_j}{T_i}] \longrightarrow \Gamma(X_i, \mathcal{O}_{X_i})$ sending $[\frac{T_j}{T_i}]$ to $[\frac{s_j}{s_i}]$. Recall also that $L|_{X_i} = \mathcal{O}_{X_i} \cdot s_i$ and that $\varphi^*([\frac{T_j}{T_i}]) \cdot s_i = s_j$.
Surjectivity: Suppose that we define maps $\varphi_i : X_i \longrightarrow U_i$ associated to the maps of rings $\varphi_i^* : A[\frac{T_j}{T_i}] \longrightarrow \Gamma(X_i, \mathcal{O}_{X_i})$ defined by the property $\varphi^*([\frac{T_j}{T_i}]) \cdot s_i = s_j$. The isomorphism $A[\dots, \frac{T_k}{T_i} \dots]_{\frac{T_j}{T_i}} \simeq A[\dots, \frac{T_k}{T_j} \dots]_{\frac{T_i}{T_j}}$ given by the application that sends $\frac{T_k}{T_i} \mapsto \frac{T_k}{T_j}$ for $k \neq i, j$ and $\frac{T_j}{T_i} \mapsto \frac{T_i}{T_j}$, allows us to paste together the maps φ_i^* along

$$\varphi_i^* = \varphi_j^* : \Gamma(U_i \cap U_j, \mathcal{O}_{\mathbb{P}^n}) \longrightarrow \Gamma(X_i \cap X_j, \mathcal{O}_X)$$

and the same can be done for the $\varphi_i : X_i \longrightarrow U_i$ to obtain $\varphi : X \longrightarrow \mathbb{P}^n_A$ such that $(L, s) = (\varphi^*\mathcal{O}(1), \varphi^*T_0, \dots, \varphi^*T_n)$.
Injectivity: If $\varphi, \varphi' : X \longrightarrow \mathbb{P}^n_A$ are two morphisms of schemes over A such that $\varphi'^*\mathcal{O}(1) \simeq \varphi^*\mathcal{O}(1)$ by an isomorphism θ such that $\theta(\varphi'^*T_i) = \varphi^*T_i$ for all i. The open sets X_i and X'_i are equal because φ^*T_i and φ'^*T_i are non-zero simultaneously. We also have

$$\varphi_i^*(\frac{T_j}{T_i}) = \frac{s_j}{s_i}, \qquad \varphi_i'^*(\frac{T_j}{T_i}) = \frac{s'_j}{s'_i}.$$

In the ring $\Gamma(X_i, \mathcal{O}_X)$ we can apply the $\mathcal{O}_X$-linearity of θ to obtain

$$s_j = \theta(s'_j) = \theta(\lambda_{j,j} s'_i) = \lambda_{j,i}\theta(s'_i) = \lambda_{j,i}s_i.$$

This shows $\varphi_i^* = \varphi_i'^*$ and $\varphi_i = \varphi'_i : X_i \longrightarrow \mathbb{P}^n_A$ for all i. □

Corollary 2.106. *Let A be a ring and n an integer. Then, if B is a ring over A such that $\mathrm{Pic}(B) = 0$, the set $\mathbb{P}^n(B) = \mathrm{Hom}_A(\mathrm{Spec}(B), \mathbb{P}^n_A)$ is equal to the set of $(n+1)$-tuples $(b_0, \dots, b_n)$ of elements of B module the equivalence relation $(b) \equiv (b')$ if there exist a unit u of B such that $b_i = ub'_i$ for all i.*

Indeed if φ: $\mathrm{Spec}(B) \longrightarrow \mathbb{P}^n(A)$, the only choice for $\varphi^*\mathcal{O}(1)$ is $\tilde{B}$. The automorphism are given by elements $u \in B^\times$. One recover in this way the usual definition of the projective space.

Proposition 2.107. *(Universal property of the Blow-up) Let X be a locally noetherian Scheme and $Y \subset X$ a closed subscheme defined by the sheaf of ideals $\mathcal{I}$. If $\pi : X' \longrightarrow X$ is the Blow-up of X along Y, the ideal $I\mathcal{O}_{X'}$ on X' is locally generated by a non-zero divisor. On the other hand the Blow-up is universal for that property: If $f : Z \longrightarrow X$ is another map of schemes such that $f^{-1}Y$ is a Cartier divisor, there exist a morphism $g : Z \longrightarrow X'$ such that $f = \pi \circ g$.*

Proof. The uniqueness allow us to do the proof locally on X. The ideal $\mathcal{I}\mathcal{O}_{X'}$ equals $\mathcal{O}_{X'}(1)$ when we write $X' = \mathrm{Proj}(\oplus_n I^n)$ and is therefore a Cartier divisor on X'. If $X = \mathrm{Spec}(A)$ with A noetherian, we will have n elements $a_0, \dots, a_n$ that generate I. If $I\mathcal{O}_Z$ is an invertible sheaf on Z, the morphism $Z \longrightarrow \mathrm{Spec}(A)$ factors through a map $Z \longrightarrow \mathbb{P}^n_A$ by proposition 2.105. The ring $\oplus I^n$ is quotient of $A[X_0, \dots, X_n]$ by the application $X_i \mapsto a_i$, which gives a closed immersion of X' on $\mathbb{P}^n_A$. The closed set X' is then defined by a system of homogeneous equations $F(a_0, \dots, a_n) = 0$ and the image of Z by the map $Z \longrightarrow \mathbb{P}^n_A$ satisfy these equations showing that we actually have $Z \longrightarrow X' \subset \mathbb{P}^n_A$. □

Exercise 2.108. *Let A be a ring and consider the affine n-dimensional space $\mathbb{A}^n_A = \mathrm{Spec}(A[x_1, \dots, x_n])$ over A. Consider the schemes $U_i =$*

$\operatorname{Spec}(T_i) \cong A^n_A$, *where* $T_i = A[x_1/x_i, \dots, x_n/x_i, x_i]$ *is a subring of* $T = A[x_1, x_1^{-1}, \dots, x_n, x_n^{-1}]$. *Show that we can form an scheme* Z, *gluing together the schemes* U_i *along* $(U_i)_{x_j} = (U_j)_{x_i}$. *Also show that we have a natural map* $\varphi \colon Z \longrightarrow \mathbb{A}^n_A$ *and* $Z \longrightarrow \mathbb{A}^n_A$ *is the blow-up of* $\mathbb{A}^n_A$ *along* $Y = V(x_1, \dots, x_n)$.

Exercise 2.109. *Consider a scheme* X *together with a rational map* $\varphi \colon X \dashrightarrow \mathbb{P}^n$ *determined by an invertible sheaf* $\mathcal{L}$ *and a set of global sections* $s_0, s_1, \dots, s_n \in \Gamma(X, \mathcal{L})$. *Let* $U \hookrightarrow X$ *be the open set where sections* s_i *generate* $\mathcal{L}$. *Show that we can construct a suitable sheaf of ideals* $\mathcal{I}$ *on* X *such that* $\mathcal{I}_x = \mathcal{O}_{X,x} \Leftrightarrow x \in U$ *and the map* $\varphi \colon U \longrightarrow \mathbb{P}^n$ *can be extended to a map* $\varphi' \colon X' \longrightarrow \mathbb{P}^n$, *where* $X' = Bl_Y(X)$ *is the blow-up of* X *along the subscheme* Y *determined by* $\mathcal{I}$.

3. Rings of dimension one

The dimension (or Krull dimension) of a ring is the supremum ($\in \mathbb{N} \cup \infty$) of the lengths of all chains of prime ideals, each of them strictly containing the previous one. For example $\mathbb{Z}$ has dimension one, because $(0) \subsetneq (p)$ for a prime number p, is a maximal chain of prime ideals. In this section we will deal with the fundamental examples of rings of dimension one in arithmetic geometry: The ring of integers in a number field and the ring of regular functions on an affine algebraic curve.

3.1. Noetherian rings of dimension zero.

We start laying the foundations with the study of rings of dimension zero.

Exercise 3.1. *Prove that if* A *is an integral domain of dimension one and* $f \neq 0$, *the ring* A/fA *is of dimension zero.*

Exercise 3.2. *Show that if* M *is a* A*-module simple (without proper sub-modules), there exist a maximal ideal* $m \subset A$ *such that* $M \simeq A/m$.

Proposition 3.3. *(Theorem of Jordan-Hölder) If we have two filtrations* $(0) = M_0 \subset M_1 \subset \cdots \subset M_n = M$, *and* $(0) = M'_0 \subset M'_1 \subset \cdots \subset M'_q = M$ *of the* A*-module* M, *where the successive quotients* M_i/M_{i-1} *and* M'_i/M'_{i-1} *are simple modules, then* $n = q$ *and there exist a permutation* σ *of* $\{1, 2, \dots, n\}$ *such that* $M_i/M_{i-1} = M'_{\sigma(i)}/M'_{\sigma(i-1)}$.

Proof. (Sketch of the proof) A finite filtration $(0) = M_0 \subset M_1 \subset \cdots \subset M_n = M$ is called of finite length n. We will prove by induction on n that $q \leq n$ and because the roles of q and n can be interchange we finish the first part. Let r the smallest number such that $M_1 \subset M'_r$.

One has the following filtration with at most one successive quotient being zero:

$$(0) \subset M'_0 \subset \cdots \subset M'_{r-1} \subset M'_r/M_1 \subset M'_{r+1}/M_1 \subset \cdots \subset M'_q/M_1 = M/M_1.$$

The module M/M_1 has therefore a filtration with simple successive quotients of length $q-1$, therefore comparing with

$$(0) = M_1/M_1 \subset M_2/M_1 \subset \cdots \subset M_n/M_1 \subset M/M_1,$$

we have $q \leq n-1$ or $q-1 \leq n-1$. In any case $q \leq n$.
Let m be a maximal ideal of A. Tensoring the filtration $(0) = M_0 \subset M_1 \subset \cdots \subset M_n = M$ with A_m we will get a filtration for the localization M_m. The successive quotients are annihilated if they are isomorphic to A/m' for some maximal ideal different from m. On the other hand the successive quotients isomorphic to A/m will remain the same. Applying the first part of the of the theorem to M_m we obtain the second part. □

A filtration $(0) = M_0 \subset M_1 \subset \cdots \subset M_n = M$, where successive quotients M_i/M_{i-1} are simple modules, is nothing but a maximal sequence where no extra module can be inserted.

Definition 3.4. *Let A be a ring and M and A-module. One says that M is of* **finite length n** *if we can find a filtration with simple successive quotients and length n.*

Corollary 3.5. *On the category of modules of finite length over A, the length is an additive function. A module has length zero if and only if it is zero.*

Corollary 3.6. *Let M be a module of finite length over A. Consider the finite set $m_1, m_2, \ldots, m_r$ of maximal ideals of A such that $M_{m_i} \neq 0$. Then the application:*

$$M \longrightarrow \prod_{i=1}^{r} M_{m_i}$$

is an isomorphism.

Proof. The two modules M and $\prod_{i=1}^{r} M_{m_i}$ have the same length. By corollary 3.5, it is enough to prove that the map is injective. That is, if x is not zero it will have a non-zero image in one of the localizations M_{m_i}. □

Corollary 3.7. *Let A be a ring of finite length as A-module. Then* $\operatorname{Pic}(A) = 0$.

Proof. If m is a maximal ideal of A and $\mathcal{L}$ is an invertible A-module, we have $\mathcal{L}_m \simeq A_m$ and therefore

$$\mathcal{L} \simeq \prod \mathcal{L}_m \simeq \prod A_m \simeq A$$

using the previous result. □

Remark 3.8. As a consequence of 3.5, every decreasing (or increasing) sequence of submodules of a module of finite length will be necessarily stationary.

Definition 3.9. *We say that the A-module M is* **artinian** *if every non-empty family of sub-modules of M has a minimal element for the inclusion. By Zorn's lemma, being artinian is equivalent to the fact that any descending chain $M_0 \supseteq M_1 \supseteq \dots$ stabilizes. An artinian ring A is a ring that an artinian when considered as module over itself.*

Example 3.10. For example every module of finite length will be artinian.

Example 3.11. Let A be a local ring and m its maximal ideal. Suppose that m is a module of finite type over A (for example if A is noetherian). Then for all natural number n, the ring A/m^n is artinian. We have a filtration of the sort

$$0 \subset m^{n-1}/m^n \subset \cdots \subset m/m^n \subset A/m^n,$$

where the successive quotients are vector spaces of finite dimension over the field A/m and therefore of finite length as A-modules. By the additivity of the length (3.5), the module A/m^n is of finite length.

Exercise 3.12. *An integral domain that is no field, is not artinian.*

Exercise 3.13. *Let $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ be an exact sequence of A-modules. Show that M is artinian if and only if M' and M'' are artinian. Verify that the same is true for finite length in place of artinian.*

Lemma 3.14. *Let A be a noetherian ring and M an A-module. Then, there exist an element $x \neq 0$ in M such that the annihilator $Ann(x)$ is a prime ideal of A.*

Proof. Because A is noetherian we can take an ideal $I = Ann(x)$ which is maximal for the set of ideals that are annihilators of non-zero elements of M. The ideal $I \neq A$ because the elements we are considering are non-zero. Let us see that I is prime. If $abx = 0$ and $ax \neq 0$ then $b \in Ann(ax) \supset I$ and therefore $b \in I$ because I is maximal. □

Corollary 3.15. *Every module M of finite type over a noetherian ring A admits a finite filtration $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ such that the successive quotients $M_{i+1}/M_i \simeq A/p_i$ where p_i is a prime ideal of A.*

Proof. The module M is noetherian, so we can choose a submodule M' maximal among the submodules satisfying the above property. Taking $M'' = M/M'$ as our module and applying the lemma above we get $M'' = 0$ and $M = M'$. □

Example 3.16. The ring $\mathbb{Z}$ is noetherian but not artinian. For every $a \in \mathbb{Z}$, we have the sequence: $(a) \supset (a^2) \supset \ldots$ On the other hand a k-vector V is noetherian if and only if it is artinian.

Proposition 3.17. *Let A be a ring. The following propositions are equivalent:*

(1) *A is a noetherian ring of dimension zero.*
(2) *A is of finite length.*
(3) *A is artinian.*

Proof. (Idea of the proof) Clearly (2) implies (3) (and also that A is noetherian). Using corollary 3.15 and the fact that in dimension zero all prime ideals are maximal we get finite length we get (1) implies (2). If we have on the other hand a ring A that is artinian and p a prime ideal in A, the domain A/p must be a field and p must be maximal. So, we have therefore that every artinian ring has dimension zero. The rest of the proof will be a consequence of the following lemmas. □

Definition 3.18. *The nilradical $\mathfrak{N}$ of an ring A is the set of nilpotent elements of A. It can be characterized as the intersection of all the prime ideals of A.*

Lemma 3.19. *The nilradical $\mathfrak{N}$ of an artin ring is nilpotent.*

Proof. Suppose that for a number k we have $\mathfrak{a} = \mathfrak{N}^k = \mathfrak{N}^{k+1} = \ldots$. If $\mathfrak{a} \neq 0$ there will be a minimal element $\mathfrak{c}$ for the (non empty) set Σ of ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} \neq 0$. By definition, there will be an element $x \in \mathfrak{c}$ such that $c\mathfrak{a} \neq 0$ and therefore $\mathfrak{c} = (x)$. But the ideal $x\mathfrak{a}$ is also in Σ giving $x\mathfrak{a} = (x)$. There exist then an element $y \in \mathfrak{a}$ such that $x = xy = xy^2 = xy^3 = \ldots$. But $y \in \mathfrak{a}$ is nilpotent!, therefore $x = 0$ and $\mathfrak{a} = 0$. □

Lemma 3.20. *Let A be an ring. If a product $\prod_i m_i$ of maximal ideals m_i (not necessarily distinct) gives the zero ideal, then the ring A is noetherian if and only if A is artinian.*

Proof. Consider the sequence $A \supsetneq m_1 \supset m_1m_2 \supset \cdots \supset m_1m_2\ldots m_n = 0$. The succesive quotient are vector spaces and therefore noetherian and artinian will be equivalent. Using properties of the chain conditions for exact sequences the same property holds for A. This is, A is noetherian if and only if A is artinian. □

Exercise 3.21. *Show that $\mathbb{Z}/n\mathbb{Z}$ is a finite length as module over $\mathbb{Z}$. Find its length.*

Proposition 3.22. *Let A be a noetherian ring of dimension one and f an element of A not contained in any prime ideal p with* $\dim(A/p) = 1$, *then* $\mathrm{Pic}(A/fA) = 0$.

Proof. If f is not contained in any prime ideal with $\dim(A/p) = 1$, then $\dim(A/fA) = 0$ and A/fA is still noetherian, therefore A/fA is artinian by 3.17 and has a trivial Picard group. □

Exercise 3.23. *Let A a noetherian ring and p a minimal prime of A.*

(a) *The ring A_p is artinian.*
(b) *In a filtration of A like 3.15 show that there will always be a successive quotient $M_{i+1}/M_i \simeq A/p$.*
(c) *Show that there exist an element $x \in A$ such that $Ann(x) = p$.*
(d) *Show that the set of minimal primes is finite.*

3.2. **Principal ideal rings.** A ring is said to be a principal ideal ring if all ideals are principal ideals. In a principal ideal ring, non-zero irreducible elements generate prime ideals. Also, when the ring is not a field, a principal ideal ring is a special case of a ring of dimension one.

Example 3.24. The ring of integers $\mathbb{Z}$ and the ring of polynomials $k[x]$, over a field k, are principal rings. We note the similar role played by the absolute value and the degree in these two examples. On the other hand $\mathbb{Z}[x]$ is not a principal ideal ring, for example, take the ideal $(2, x) \subset \mathbb{Z}[x]$. This also shows how a submodule of $\mathbb{Z}[x]$ needs not to be free as $\mathbb{Z}[x]$-module. A situation that does not happen over principal ideal rings.

Proposition 3.25. *(Theorem of elementary divisors) Let A be a principal ideal domain. Let M be a free A-module of rank n and M' a submodule of M. There exist a basis $e_1, \ldots, e_n$ of M and elements $a_i \in A$ with the property that a_i divides a_{i+1} in such a way that M' is free with basis consisting on the non-zero elements of the form (a_ie_i) for $i = 1, \ldots, n$.*

Proof. (Idea of the proof) For the first part we can proceed by induction in n, assuming that M' is a submodule of M and $\{e_1, e_2, \dots, e_n\}$ is a basis of M. Consider the projection maps $\pi_i \colon M \longrightarrow A$, given by $\pi(\sum_i a_i e_i) = a_i$. If $M' \neq 0$ there must be a π_i such that $\pi_i(M') \neq 0$ and therefore $\pi_i(M') = \alpha A$ for some α. The submodule $Ker(\pi_i) \cap M'$ of M' is free of rank $\leq n-1$ by induction hypothesis. Now $M' = Ker(\pi_i) \oplus vA$ for $v \in M'$ such that $\pi_i(v) = \alpha$ is therefore also free of rank $\leq n$. The First step in the induction being guaranteed by the definition of principal ideal ring, we finish with the first part.
For the second part we should consider the set of ideals

$$L(M') = \{T(M') \subset A \,|\, T \in M^\vee\}$$

and a maximal element $(\alpha) = T_0(M')$ in $L(M')$ with $\alpha = T_0(v)$. Using the maximality of (α), we can show that α divides $T(v)$ for all $T \in M^\vee$. In particular α divides the coordinates functions $\pi_i(v)$ and the vector v can be written as $v = \alpha w$. Now, from $\alpha = T_0(v) = \alpha T_0(w)$, we get $T_0(w) = 1$ and

$$M = Ker(T_0) \oplus Aw \quad \text{and} \quad M' = (M' \cap Ker(T_0)) \oplus A\alpha w.$$

To finish the proof we proceed again by induction on n. □

Definition 3.26. *Let A be an integral domain, a module M over A is said to be* **torsion-free** *if every element $x \in M$ is annihilated only by zero.*

Example 3.27. If M is torsion-free, any submodule will also be torsion-free over A. For instance, the dual $M^\vee$ of any module M is torsion-free contained in the torsion free module A^I.

Lemma 3.28. *Consider a noetherian integral domain A and M a torsion-free module of finite type over A. Then we have that the canonical morphism $M \longrightarrow M^{\vee\vee}$ is injective.*

Proof. Let K be the quotient field of A and consider the commutative diagram:

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[d, "i"'] & M^{\vee\vee} \arrow[d, "j"] \\
M \otimes K \arrow[r, "\varphi_K"] & M^{\vee\vee} \otimes K
\end{tikzcd}$$

The maps $i : M \longrightarrow M \otimes K$ and $j : M^{\vee\vee} \longrightarrow M^{\vee\vee} \otimes K$ are injective because M and $M^{\vee\vee}$ are torsion free. On the other hand $M^\vee$ and $M^{\vee\vee}$ are modules of finite type because the module M is of finite type and the ring A is noetherian ($A^n \to M \to 0 \Rightarrow 0 \to M^\vee \to \mathrm{Hom}(A^n, A)$).

The map $\varphi_K\colon M \otimes K \longrightarrow M^{\vee\vee} \otimes K$ is an isomorphism as $M^{\vee\vee} \otimes K \simeq (M \otimes K)^{\vee\vee}$. The conclusion is then that $\varphi\colon M \longrightarrow M^{\vee\vee}$ must be injective. □

Remark 3.29. Lemma 3.28 can be used as definition of torsion-free for modules over rings that are not domains.

Corollary 3.30. *Let A be a principal ideal domain. Every torsion-free A-module of finite type is free. For every A-homomorphism of free A-modules of finite rank $\varphi\colon M \longrightarrow M'$, there exist two basis of M and M' such that φ is diagonal.*

Proof. Applying 3.28 we know $M \hookrightarrow M^{\vee\vee} \hookrightarrow A^I$ for some finite index I and must therefore be free by 3.25. We note that if $\varphi\colon M \longrightarrow A$ is a non-zero linear form, we have a free direct factor of rank one in M. This is because $Im(\varphi) = Ax$ for some $x \in A$ and the surjective map $\varphi\colon M \longrightarrow Ax$ into the free module Ax must have a section $s\colon Ax \longrightarrow M$. Following by induction on the rank $M \otimes_A K$ one can get a direct proof that any torsion free M of finite type is in fact free over A. If $\varphi\colon M' \longrightarrow M$ is a map, then $Ker(\varphi)$ and $Im(\varphi)$ are both submodules of free modules and we can use 3.25 to obtain 3.30. □

Remark 3.31. Let A be a domain. The sequence of inclusions

Free Modules $\subseteq$ Projective Modules $\subseteq$ Flat Modules $\subseteq$ Torsion-free Modules

becomes an equality over principal ideal domains.

Corollary 3.32. *Let G be a finite subgroup of the non-zero elements of a field k. Then is cyclic.*

Proof. There exist an integer n and a exact sequence

$$0 \to Ker(\varphi) \to \mathbb{Z}^n \xrightarrow{\varphi} G \to 0.$$

By proposition 3.25, once can write $G = \oplus_{i=1}^n \mathbb{Z}/a\mathbb{Z}$ where $a_i \in \mathbb{Z}$ are non-zero. Consider $a = lcm(a_i)$. The number a annihilates G and the element $(1, 1, \ldots, 1)$ is of order exactly a. The equation $x^a = 1$ in k has at most a solutions, hence the order of G is less or equal to a. We deduce then that $(1, 1, \ldots, 1)$ generates the whole G. □

Corollary 3.33. *Let k be a field of characteristic p, then k is generated by one algebraic element as algebra over $\mathbb{F}_p$.*

Corollary 3.34. *Let G be a discrete subgroup of $\mathbb{R}^n$, then G is a free $\mathbb{Z}$-submodule of rank at most n. Moreover a basis for G is made of linearly independent elements over $\mathbb{R}$.*

Proof. Let r be the maximum cardinal of a set of elements of G that are linearly independent over $\mathbb{R}$ a let $\{x_1, x_2, \dots, x_r\}$ a set of elements of G linearly independent over $\mathbb{R}$. As a consequence every element $x \in G$ can be written as $x = \sum \lambda_i x_i$ for real numbers λ_i and we have $x = \sum [\lambda_i] x_i + \sum (\lambda_i - [\lambda_i]) x_i$. Let us denote by D the compact set of linear combinations

$$D = \{\sum_1^r \alpha_i x_i \,|\, 0 \leq \alpha_i \leq 1\}.$$

Because G is discrete, the intersection $G \cap D$ is a finite set of cardinality m that generates G as $\mathbb{Z}$-module. The $\mathbb{Z}$-module G is of finite type and torsion free over $\mathbb{Z}$ and therefore a free $\mathbb{Z}$-module. We are going to prove that there is a $d \in \mathbb{Z}$ such that dG is the free $\mathbb{Z}$-module generated by the x_i. As a consequence, our G will be finitely generated torsion free and a free module by 3.30 with rank at most r. Consider for $j \in \mathbb{N}$ the elements $y_j = \sum_{i=1}^r (j\lambda_i - [j\lambda_i]) x_i \in D \cap G$. Because $\#(D \cap G) = m$, by the Drichlet principle, there must be $j \neq j' \in \{1, \dots, m+1\}$ such that $y_j = y_{j'}$ and therefore $(j - j')x \in \sum \mathbb{Z} x_i$. Therefore $m!G$ is a free module generated by $\{x_1, \dots, x_r\}$, hence $rank(G) \leq r$. □

Exercise 3.35. *Let α be an irrational real number, show that for all $\epsilon > 0$ there are integers p, q such that $|\alpha - \frac{p}{q}| < \epsilon/q$.*

Definition 3.36. *Discrete subgroups of $\mathbb{R}^n$ of rank n are called* **lattices** *of $\mathbb{R}^n$. For a lattice Λ of $\mathbb{R}^n$ one calls the volume of Λ, denoted $vol(\Lambda)$, the Lebesgue measure of polytope build over a $\mathbb{Z}$ basis.*

3.3. **Integral elements.** We study in this part the finite morphisms on algebraic varieties and schemes.

Definition 3.37. *Let B be a ring and A a subring of B. One says that an element $x \in B$ is* **integral over** *A if it satisfies a monic equation with coefficients in A, i.e.*

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

where $a_i \in A$. B is says to be integral over A if every element $x \in B$ is integral over A.

Example 3.38. The field of complex numbers $\mathbb{C}$ is integral over the field of real numbers $\mathbb{R}$. The field of real numbers on the other hand is not integral over $\mathbb{Q}$.

Proposition 3.39. *Let $A \subset B$ be two rings and $x \in B$. The following propositions are equivalent:*

(i) *x is integral over A.*

(ii) *The module $A[x]$ is an A-module of finite type.*
(iii) *There exist an A-module of finite type containing $A[x]$.*

Proof. Assume that we have (i), then we can multiply the equation of integral dependency by x^i and obtain

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

Therefore $A[x]$ is finitely generated by $1, x, \ldots, x^n$ as A-module. Let us assume that we have (iii) and $\{x_1, \ldots, x_n\}$ is a system of generators of B as A-module. The module $A[x] \subset B$ and when we multiply the x_i by x we get

$$xx_i = \sum_{j=1}^{n} a_{i,j}x_j,$$

which can be written as $\sum_{j=1}^{n}(\delta_{i,j}x - a_{i,j})x_j = 0$. If we denote by d the determinant of the matrix $(\delta_{i,j}x - a_{i,j})_{i,j}$, we will get $dx_j = 0$ for all j and therefore $d = d(1) = 0$ because the x_j generate B over A. The equation $d = 0$ is an equation of integral dependency of x over A. □

Corollary 3.40. *Let B be a ring and $A \subset B$ a subring of B. The set of elements of B that are integral over A is a sub-ring of B called the* **integral closure** *of A in B.*

Proof. If $A[x]$ and $A[y]$ are modules of finite type over A, then $A[x, y]$ is of finite type over $A[x]$ and therefore over A. As a consequence for x, y integral elements, we have that the elements $x+y$ and xy in $A[x, y]$ are also integral over A. □

Example 3.41. The elements $\sqrt{2}$ and $\sqrt[3]{7}$ are integral over $\mathbb{Z}$, therefore $\sqrt{2} + \sqrt[3]{7}$ is also integral over $\mathbb{Z}$, although it is not obvious what will be the equation of integral dependency.

Definition 3.42. *Let A be an domain. We say that A is* **integrally closed** *if it is integrally closed in its quotient field.*

Exercise 3.43. *Show that a principal ideal domain is integrally closed.*

Exercise 3.44. *Show that if A is a domain and $S \subset A$ is a multiplicatively stable system in A, the ring A is integrally closed if and only if $S^{-1}A$ is also integrally closed.*

Exercise 3.45. *Prove that the localization $k[x]_f$ of the ring of polynomials in one variable over a field k is integrally closed.*

Exercise 3.46. *Let A be an integrally closed noetherian domain with field of fractions K and let L/K be a finite separable extension. Show that the integral closure B of A in L is finitely generated as A-module and therefore noetherian.*

Definition 3.47. *A scheme X is said to be* **normal** *if the local rings $\mathcal{O}_{X,x}$ are all integrally closed.*

Example 3.48. The curve defined in $\mathbb{A}^2$ by the equation $y^2 = x^2(x+1)$ is not normal as $y' = y/x$ satisfies the monic equation $y'^2 - (x+1) = 0$.

Proposition 3.49. *Let B be a domain and $A \subset B$ a subring such that B is integral over A. Then B is a field if and only if A is also a field.*

Proof. If B is a field and $x \in A$, then the inverse x^{-1} satisfies a monic equation

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

Multiplying by x^n we get:

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

Therefore the inverse x^{-1} is also in A and A is a field. Reciprocally suppose that A is a field and $x \in B$. We can find a monic equation $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ with minimal degree. For that equation $a_n \neq 0$ will be invertible in A and we will have

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

This proves that x is invertible and B is a field. □

We can establish some sort of converse for the proposition 3.49 in the case of finitely generated k-algebras. We recall that when A is a field, an equation of integral dependency over A not need to be monic.

Theorem 3.50. *If the the ring $k[y_1, \ldots, y_n]$ is a field, then y_i are integral over k.*

Proof. We are going to proceed by induction. For $n = 1$: if $k[y]$ is a field $y^{-1} = a_0 y^n + \cdots + a_n$ and $a_0 y^{n+1} + \cdots + a_n y - 1 = 0$ provides an equation of integral dependency y over k.
The induction step: Let $A = k[y_1] \subset K \subset k[y_1, \ldots, y_n] = B$, where K is the fraction field of A. By hypothesis $K[y_2, \ldots, y_n] = k[y_1, y_2, \ldots, y_n]$ is a field. Therefore $y_2, y_3, \ldots, y_n$ are integral over K. As the equations of integral dependency for $y_2, y_3, \ldots, y_n$ involve at most finitely many elements of $K \setminus A$, we can find a polynomial $f \in A$ such that $y_2, \ldots, y_n$ are integral over the localized ring A_f. If y_1 is algebraic over k we are done. Otherwise y_1 is a variable, the local ring $A[y_1]_f$ is integrally closed and $k[y_1, \ldots, y_n]$ is integral over $k[y_1]_f$. In particular K is integral over $k[y_1]_f$ which forces $K = k[y_1]_f$, which is impossible when we observe for example that an element $g \in A$ not dividing f is not invertible in $k[y_1]_f$. □

Exercise 3.51. *Deduce from 3.50, the weak Hilbert Nullstelensatz: If the field k is algebraically closed, the only maximal ideals of the ring $k[x_1, \dots, x_n]$ are those of the form $(x_1 - a_1, \dots, x_n - a_n)$ for a point $(a_1, \dots, a_n)$ in the affine space $\mathbb{A}^n_k$.*

Exercise 3.52. *Deduce the Hilbert Nullstelensatz from the (apparently) weaker version of the theorem. The Hilbert Nullstelensatz states that for an algebraically closed field $k = \bar{k}$ and I an ideal in the polynomial ring $A = k[x_1, \dots, x_n]$, we have $I(V(I)) = \sqrt{I}$, where for any set $S \subset k$ we are denoting by $I(S)$ the ideal of polynomials*

$$I(S) = \{f \in A \,|\, f(P) = 0 \text{ for all } P \in S\}$$

and the radical $\sqrt{I} = \{f \in A \,|\, f^n \in I \text{ for some } n > 0\}$.

Exercise 3.53. *Prove the Noether normalization theorem: Given a field k and any finitely generated commutative k-algebra A, there exists a nonnegative integer d and algebraically independent elements $y_1, y_2, \dots, y_d$ in A such that A is a finitely generated module over the polynomial ring $S := k[y_1, y_2, \dots, y_d]$.*

Exercise 3.54. *Let $A \subset B$ be a subring of B such that B is an A-algebra of finite type:*

(a) *Suppose that A is local and B is integral over A. Show that if a prime ideal $\mathfrak{p}$ of B is such that the intersection $\mathfrak{p} \cap A$ is maximal, then $\mathfrak{p}$ itself was a maximal ideal of B.*
(b) *Show that if B is integral over A, the morphism* $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ *is surjective with finite fibres.*
(c) *Show that the map* $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ *is a closed map.*

Exercise 3.55. *Show that if $A \subset B$ is an integral extension of rings, every chain or prime ideals in A can be lifted to a chain of prime ideals in B and therefore* $\dim(A) = \dim(B)$.

Definition 3.56. *A morphism $f : X \to Y$ of schemes is* **a finite morphism** *if there exist a covering of Y by open affine sets $V_i =$* $\mathrm{Spec}(B_i)$, *such that for each i, $f^{-1}(V_i)$ is affine, equal to* $\mathrm{Spec}(A_i)$, *where A_i is a B_i-algebra which is a finitely generated B_i-module.*

Example 3.57. If $A \subset B$ is an integral extension of rings, that associated map $\varphi \colon \mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ is a finite morphism. For example, let k be a field and consider the morphism of affine schemes $\mathrm{Spec}(k[t, x]/(x^n - t)) \longrightarrow \mathrm{Spec}(k[t])$.

Example 3.58. As an example of a morphism that is not finite, consider the inclusion $\mathbb{A}^1 \setminus \{0\} \hookrightarrow \mathbb{A}^1$ corresponding to the map of rings $k[x] \hookrightarrow$

$k[x, \frac{1}{x}]$. This is also an example of a map that is not finite but has finite fibres over each point.

Definition 3.59. *A morphism $f : X \to Y$ of schemes is* **locally of finite type** *if there exist a covering of Y by open affine subsets $V_i = \mathrm{Spec}(B_i)$, such that for each i, $f^{-1}(V_i)$ can be covered by affine sets $U_{ij} = \mathrm{Spec}(A_{ij})$, with A_{ij} finitely generated B_i-algebras. If, in addition, X is quasi-compact, $f : X \to Y$ will be called* **of finite type**.

Example 3.60. Let A be a ring. The map of affine schemes associated to a map of rings of the type $A \longrightarrow A[x_1, x_2, \dots, x_n]/I$, for certain ideal I, is a map of finite type.

Example 3.61. The map $\mathbb{P}^n_A \longrightarrow \mathrm{Spec}(A)$ is of finite type, as $\mathbb{P}^n_A$ can be covered by $n+1$ open sets $U_i \cong A[x_1, \dots x_n]$.

Remark 3.62. The Noether normalization theorem is saying that any affine scheme X of finite type over k admits a finite surjective morphism $X \longrightarrow \mathbb{A}^d_k$ to the affine space $\mathbb{A}^d_k$ for certain dimension d.

Remark 3.63. In the definitions of finite morphisms as well as morphisms of finite type, the phrase "there exist a covering" can be replaced by " for all coverings".

3.4. **Algebraic field extensions.** An integral extension of a field is called algebraic. If we have an extension $K \subset L$ of fields K and L and the dimension $[L : K]$ of L as K-vector space is finite, then L is algebraic over K. If we have finite field extensions $K \subset L \subset M$, then $[M : L][L : K] = [M : K]$. Let R be a ring, $K \subset R$ a field and x an element of R. There exist a K-homomorphism $\varphi\colon K[X] \longrightarrow R$ such that $X \mapsto x$. The element x is said to be algebraic over K if $Ker(\varphi) \neq 0$. In this case, the ideal $Ker(\varphi)$ is generated by an irreducible monic polynomial uniquely determined by x. This polynomial is called the minimal polynomial of x over K.

Proposition 3.64. *Let K be a field and P a non-constant polynomial with coefficients in K. There exist an algebraic extension K'/K of finite degree such that P can be decompose in factors of degree one in $K'(X)$.*

Proof. The proof is by induction on the degree d of $P(X)$. We can assume that P is irreducible. By proposition 3.49 $K' = K(X)/P(X)$ is a field where the image x of X is a root of $P(X) = 0$. The linear polynomial $(X - x)$ is a factor of $P(X)$ and $P'(X) = P(X)/(X - x)$ should split by hypothesis of induction in linear factors in some field $K''(X)$. □

Lemma 3.65. *Let K be a field of characteristic zero or a finite field, $F(X)$ a monic irreducible polynomial of degree n. Then the n roots of $F(X)$ in a finite extension K' of K are different.*

Proof. The polynomial $F(X)$ is the minimal polynomial of any of its roots. If the root is double, then it is also a root of $F'(X)$ of lower degree. If the characteristic of K is zero, the derivative $F' \neq 0$ has degree $n-1$ which contradicts the minimality of $F(X)$. If the derivative is identically zero, then $char(K) = p$ and $F(X) = X^{np} + a_1 X^{(n-1)p} + \cdots + a_{n-1}X^p + a_n$. Using that the Frobénius map $x \mapsto x^p$ is onto we get $F(X) = (X^n + b_1 X^{n-1} + \cdots + b_{n-1}X + b_n)^p$ is not irreducible. □

Definition 3.66. *An extension K'/K is called* **separable** *if for every monic polynomial $F(X)$ with coefficients in K, the roots of $F(X)$ are all different.*

Definition 3.67. *A field K is algebraically closed if it contains the roots of every polynomial with coefficients in K.*

Lemma 3.68. *Let K be a field and $\sigma\colon K \longrightarrow C$ a homomorphism from the field K into an algebraically closed field C. Let K' be a finite extension of K, then we can always find an extension $\sigma'\colon K' \longrightarrow C$ of σ.*

Proof. If $K' = K(X)$ the lemma is clear by giving a value $\sigma'(X) = x$ to X and extending by linearity. We then proceed by induction on the degree $[K' : K]$ of the extension. □

Proposition 3.69. *Assume that our field K is a finite field or a field of characteristic zero. Let $K \subset K' \subset C$ be a tower of field extensions where $[K' : K] = n$ is finite and C is algebraically closed. Then there are exactly n different K-homomorphisms of fields $\sigma\colon K' \longrightarrow C$.*

Proof. We proceed by induction on the degree $[K' : K]$ of the extension. The proposition holds for $K' = K(X)$ by lemma 3.65. Now if we have a tower of extensions $K \subset K' \subset K''$, where $[K' : K] = m < n$, we will have m different homomorphisms $\sigma_i\colon K' \longrightarrow C$. By the previous lemma we can extend those to homomorphism $\sigma_i'\colon K'' \longrightarrow C$ and we will have exactly $[\sigma_i(K'') : \sigma_i(K')] = [K'' : K']$ different extensions again by induction hypothesis. □

Exercise 3.70. *(Theorem of the primitive element). Show that if K is a field of characteristic zero or a finite field and K' is a finite extension, there exist a $x \in K'$ such that $K' = K(x)$. In general the result can be stated for separable extensions of fields.*

3.5. **Number fields: orders in a number field.** We will introduce in this section the language of the algebraic theory of numbers.

Definition 3.71. *A field K that is a finite extension of the rational numbers is called a number field. The integer $[K : \mathbb{Q}]$ is called the* **degree** *of K.*

Example 3.72. For example $\mathbb{Q}[i]$, with $i^2 = -1$, is a number field of degree 2 over $\mathbb{Q}$.

Definition 3.73. *Let K be a number field and $A \subset K$ an integral extension of $\mathbb{Z}$ such that the fraction field of A is exactly $K(A) = K$. Such rings A are called* **orders of the number field** *K.*

Example 3.74. We have for example the orders $\mathbb{Z}[\sqrt{5}]$ and $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ in the number field $\mathbb{Q}[\sqrt{5}]$. The element $\frac{1+\sqrt{5}}{2}$ is integral over $\mathbb{Z}$ because it satisfies the equation $x^2 - x - 1 = 0$.

Definition 3.75. *Let K be a number field. We call ring of integers of K to the integral closure $\mathcal{O}_K$ of $\mathbb{Z}$ in K.*

Exercise 3.76. *Let K be a quadratic extension (degree 2). Show that there exist $d \in Z$ such that $K = \mathbb{Q}(\sqrt{d})$. Show that the ring of integers of $K = \mathbb{Q}(\sqrt{d})$ is as follows:*

(a) *If $d \equiv 2, 3\, mod(4)$. The ring $\mathcal{O}_K$ is $\mathbb{Z} + \mathbb{Z}\sqrt{d}$.*

(b) *If $d \equiv 1\, mod(4)$. The ring $\mathcal{O}_K$ is $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{d}}{2})$.*

Remark 3.77. The ring of integers in a number field not need to be a UFD, the classical example being $2(3) = (1-\sqrt{5}i)(1+\sqrt{5}i)$ in $\mathbb{Z}[\sqrt{-5}]$. Also a rational prime p not need to remain prime when considered an element of $\mathcal{O}_K$ for some $K/\mathbb{Q}$. On the other hand, we will see that we have in $\mathcal{O}_K$ a **unique decomposition** of ideals $p\mathcal{O}_K = \prod_i \mathfrak{p}_i^{e_i}$ **as product of prime ideals**, where the numbers e_i denote the ramification indexes. A value $e_i \neq 1$ denotes ramification at the prime $\mathfrak{p}_i$.

Definition 3.78. *Let K be a number field. The $\mathbb{Q}$-homomorphisms $\sigma\colon K \longrightarrow \mathbb{C}$ of K into the complex numbers are called* **places of** *K* **at infinity***. A place at infinity is said to be* **real** *or* **complex** *depending on whether $\sigma(K) \subset \mathbb{R}$ or not. The images of an element $x \in K$ by the different places at infinity are called* **conjugates** *of x.*

Remark 3.79. If σ is a complex place, complex conjugation will give another place $\bar{\sigma}$. It is classic to denote by r_1 the number of real places (at infinity) of K and by $2r_2$ the number of complex places of K. If we denote also $[K : \mathbb{Q}] = n$ we have $n = r_1 + 2r_2$. Let ϕ a set of $r_1 + r_2$ places containing no pairs of conjugates.

Proposition 3.80. *Let K be a number field and A an order in K. Consider r_1, r_2 and ϕ as before. The map $\sigma\colon K \longrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ that to an element $x \in K$ associates $(\sigma_i(x))_{\sigma\in\phi}$ is such that $\sigma(A)$ is a lattice of $\mathbb{R}^n$. In particular an order of a number field of degree n is a free $\mathbb{Z}$-module of rank n.*

To prove the proposition first we will prove first a general finiteness lemma.

Lemma 3.81. *(First Finiteness lemma) Let $\bar{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Let n be an integer and h a real number. Then, the set $M^n_{\leq h}$ of elements of $\bar{\mathbb{Q}}$ integral over $\mathbb{Z}$ whose degree is bounded above by n and whose conjugates are all of absolute value at most h is a finite set.*

Proof. Let $x \in M^n_{\leq h}$ of degree $m \leq n$. For every $i = 1, \dots, m$ we have a $\mathbb{Q}$-homomorphism $\rho_i\colon \mathbb{Q}[x] \longrightarrow \mathbb{C}$ and $\mathbb{Q}$. Because x is integral over $\mathbb{Z}$, the image $\rho_i(x)$ is also integral over $\mathbb{Z}$ for all i and the minimal polynomial $P(X)$ of x over $\mathbb{Q}$ can be written as

$$P(X) = \prod_{i=1}^{m}(X - \rho_i(x)) = x^m + a_1 x^{m-1} + \cdots + a_m = 0,$$

where $a_i \in \mathbb{Z}$. Now by the hypothesis of $x \in M^n_{\leq h}$ we have $|\rho_i(x)| \leq h$ from where we get $|a_i| \leq \binom{m}{i} h^i$ and we have a finite list of coefficients (because a_i are in $\mathbb{Z}$) and therefore a finite list of possible solutions $x \in M^n_{\leq h}$. □

Proof of the theorem 3.80: By the finiteness lemma, the image $\sigma(A)$ is a discrete set and by corollary 3.34 is a free $\mathbb{Z}$-module of finite rank at most n and because $A \otimes_{\mathbb{Z}} \mathbb{Q} = K$, the rank is exactly n and $\sigma(A)$ is a lattice of $\mathbb{R}^n$.

Corollary 3.82. *Let A be an order in a number field K of degree n over $\mathbb{Q}$ and L be an invertible A-module. Then L is a free Z-module of rank n.*

Proof. The module L is torsion free because it is locally isomorphic to A. It is also of finite type and in fact free of rank n due to $L \otimes_{\mathbb{Z}} \mathbb{Q} = L \otimes_A (A \otimes_{\mathbb{Z}} \mathbb{Q}) = L \otimes_A K \simeq K$. □

Proposition 3.83. *An order in a number field is a noetherian ring of dimension one.*

Proof. Because A is an order of a number field K of degree n over $\mathbb{Q}$, the ring A is a free module of rank n over the noetherian ring $\mathbb{Z}$ and therefore noetherian. On the other hand if $\mathfrak{p} \neq 0$ is a prime ideal of

A, $\mathfrak{p}$ is a torsion free module of finite type over $\mathbb{Z}$. By 3.30, $\mathfrak{p}$ is free and $\mathfrak{p} \otimes_A K = K$ shows that $\mathfrak{p}$ is as well a free $\mathbb{Z}$-module of rank n. By proposition 3.25, the quotient $A/\mathfrak{p}$ is a a finite ring without zero divisors, hence a field. Our prime ideal $\mathfrak{p}$ is then maximal and the dimension of A is one. □

3.6. **Discrete valuation rings and Dedekind rings.** We study in this part integrally closed local noetherian rings of dimension one. For example, the ring of formal power series $K[[X]]$ are of this type.

Proposition 3.84. *Let A be an integral domain with field of fractions K. The following two propositions are equivalent:*

(1) *A is an integrally closed local noetherian rings of dimension one.*

(2) *There exist a surjective map $v\colon K^\times \longrightarrow \mathbb{Z}$ such that:*

  (i) *$v(xy) = v(x) + v(y)$.*

  (ii) *$v(x+y) \geq \inf(v(x), v(y))$.*

  (iii) *The ring A is exactly the set $A = \{x \in K \mid v(x) \geq 0\}$.*

Proof. (2) ⇒ (1) First let us see that A has to be a principal ideal domain and therefore integrally closed and noetherian. If $I \subset A$ is an ideal and $x \in I$ is an element of minimal valuation in I, then $v(y/x) \geq 0$ for all $y \in I$ and therefore $y = ax$ for some $a \in A$. So, we have $I = (x)$. If $v(x) = 0$ then $v(x^{-1})$ will also be zero and $x \in U = A^\times$. Also if $x \in A^\times$, the valuation $v(x) = 0$. If the sum of two elements $x + y$ is in $A^\times$ then $0 = v(x+y) \geq \min(v(x), v(y))$ forces one of them, say x, to have valuation zero and hence to be a unit. The ring A is then local with maximal ideal $m = A \setminus A^\times = \{x \in A \mid v(x) > 0\}$.

(1) ⇒ (2) We show first that the maximal ideal m of the local ring A is principal. Consider the inverse ideal m' of m defined by the property $m' = \{x \in K \mid xm \subset A\}$. We will prove the following three points:

(a) $m' \neq A$.

(b) $mm' = A$.

(c) m is principal.

(a) Let $x \in m$ and consider the localization A_x is a field containing A and therefore $A_x = K$. Let z be a non-zero element of A and write $\frac{1}{z} = \frac{y}{x^n}$ for some element $y \in A$. This last one is equivalent to $x^n = yz$ and every element $x \in m$ has a power in the ideal zA. Now, the ideal m is of finite type, so there exist a power n such that $m^n \subset zA$. Considering the minimum n with this property, there exist $y \in m^{n-1}$ and $y \notin zA$. We can verify that $\frac{y}{z}$ is in m' but not in A.

(b) Let $x \in m'$. We have that either $xm \subset m$ or $xm = A$. In the first case we have the endomorphism $x\colon m \longrightarrow m$ of a torsion free module

m of finite type. Using the determinant we obtain that x is integral over A and because A is integrally closed we get $mm' = A$.
(c) As we have $mm' = A$, there exist an integer n and elements $x_1, \dots, x_n \in m$ and $y_1, \dots, y_n \in m'$ such that $\sum_i x_i y_i = 1$. The ring A is local, so there exist an index i such that $u = x_i y_i$ is a unit of A. Putting $x = u^{-1}x_i \in m$ and $y = y_i \in m'$, every $z \in m$ can be expressed as $z = (yz)x$ with $yz \in A$. The element x then generates m and m is principal.
Suppose now that the element $0 \neq \pi \in m$ is a generator of the ideal m. Let us show that the infinite intersection $\cap_n m^n = 0$. Suppose that $x \in \cap_n m^n$, there elements $x_n \in A$ such that $\pi^n x_n = \pi^{n+1} x_{n+1}$ and using that the ring A is an integral domain we get $x_n = \pi x_{n+1}$. Therefore we have an increasing sequence of ideals in A:

$$(x_1) \subset \dots \subset (x_n) \subset (x_{n+1}) \subset \dots$$

As A is a noetherian ring, the sequence of ideals must be stationary, i.e. for $n >> 0$ we will have $x_{n+1} = ax_n = a\pi x_{n+1}$. Because the ring A is local $1 - a\pi$ is invertible and $\pi_{n+1} = 0$, from where deduce that $x = x_{n+1}\pi^n = 0$. So, we can define $\upsilon(x) = \sup\{n \mid x \in m^n\}$. We deduce that $\upsilon(xy) = \upsilon(x) + \upsilon(y)$. On the other hand the inequality $\upsilon(x+y) \geq \inf(\upsilon(x), \upsilon(y))$ is true when the function υ is defined as before for an ideal m. The function υ is extended to $K^\times$ as $\upsilon(\frac{x}{y}) = \upsilon(x) - \upsilon(y)$. Besides $\upsilon(x) \geq \upsilon(y)$ implies $x = ay$ for all $a \in A$. □

Exercise 3.85. *(Lemma of Artin-Rees) Let A be a noetherian ring and $I \subset A$ an ideal. One puts $R(I) = \bigoplus_{n \geq 0} I^n$.*

(a) *Show that $R(I)$ is a noetherian ring.*
(b) *If M is an A-module of finite type and N a submodule of M, show that $\bigoplus_{n \geq 0} I^n M \cap N$ is an $R(I)$-module of finite type.*
(c) *Deduce that there exist an integer k such that $I^n M \cap N = I^{n-k}(I^k M \cap N)$.*
(d) *(Separation of the m-adic topology) Suppose that (A, m) is a local ring, show that $\cap_{n \geq 0} m^n = 0$.*

Definition 3.86. *A ring A verifying the above two conditions is called a* **discrete valuation ring**. *A generator of the maximal ideal is called a* **uniformizing parameter** *or uniformizing element of A.*

Proposition 3.87. *Let A be noetherian ring integrally closed and of dimension one. Then every ideal of A is locally principal. Besides every ideal is generated by two elements.*

Proof. We need to show that a non-zero ideal is an invertible A-module. Let $\mathfrak{I}$ be an ideal of A and $\mathfrak{m}$ a maximal ideal of A. By the proof of proposition 3.84, we know that the ideal $\mathfrak{I}_{\mathfrak{m}}$ is principal. Now if $x \in \mathfrak{I}$ generates $\mathfrak{I}_{\mathfrak{m}}$ over $A_{\mathfrak{m}}$, the element x generates I in a neighborhood $V(f)$ of $\mathfrak{m}$ in $\mathrm{Spec}(A)$ and J is locally principal. For the second part of the proposition take the element f that generates $\mathfrak{I}$ locally and consider the noetherian ring A/fA of dimension zero. Therefore A/fA is artinian and $\mathrm{Pic}(A/fA) = 0$. This shows that $\mathfrak{I} \otimes_A A/fA \simeq A/fA$. By Nakayama there exist $y \in \mathfrak{I}$ that generates $\mathfrak{I}_{\mathfrak{m}}$ over $A_{\mathfrak{m}}$ for all $\mathfrak{m}$ containing f. One can check that $Af + Ay = \mathfrak{I}$. □

Definition 3.88. *A noetherian domain integrally closed and of dimension one is called a* **Dedekind ring**.

Example 3.89. The ring of integers $\mathcal{O}_K$ in a number field K is a Dedeking ring. The localization $(\mathcal{O}_K)_p$ at any prime ideal p will be a discrete valuation ring.

Exercise 3.90. *(Eisenstein polynomial): Let A be a discrete valuation ring, m the maximal ideal, K the fraction field of A and $k = A/m$ the residual field. We say that $F(X) = X^n + a_1X^{n-1} + \cdots + a_n$ is an Eisenstein polynomial over A if $a_i \in m$ for all $i = 1, \ldots, n$ but $a_n \notin m^2$. One puts $B = A[X]/F(X)$ and denotes by x the image of X in B.*

(a) *Show that a non-zero prime ideal of B contains m.*
(b) *Show that $B/mB = k[X]/(X^n)$. Deduce that B is a noetherian local ring of dimension one, where the maximal ideal is generated by x.*
(c) *Deduce that x is not nilpotent.*
(d) *Show that $\cap_n(Bx^n) = 0$.*
(e) *Show that B is a discrete valuation ring.*

3.7. **The cycle map.** We begin here the study of sub-schemes of codimension one in affine schemes.

Definition 3.91. *Let A be a ring. One calls* **Weil divisor** *to a linear combination with integer coefficients of quotients $A/\mathfrak{p}$ for prime ideals $\mathfrak{p}$ such that $\dim(A_{\mathfrak{p}}) = 1$. In general if n is an integer one calls* **cycles of codimension n** *and denote by $Z^n(A)$ the linear combinations $\sum_{i=1}^{s} n_i[A/\mathfrak{p}_i]$, where $n_i \in \mathbb{Z}$ and $\mathfrak{p}_i$ are prime ideals with $\dim(A_{\mathfrak{p}_i}) = n$. The* **Weil divisors are the cycles of codimension one**.

Remark 3.92. If I is an ideal of a noetherian ring A and $\dim(A_{\mathfrak{p}}) \geq n$ for all prime ideals of A/I, one can associate a cycle of codimension n given by

$$\mathrm{cycle}(A/I) = \sum_{\dim(A_{\mathfrak{p}})=n} \mathrm{length}(A_{\mathfrak{p}}/IA_{\mathfrak{p}})[A/\mathfrak{p}].$$

The sum is finite because for a noetherian ring A and a minimal prime ideal $\mathfrak{p}$, the ring $A_{\mathfrak{p}}$ is artininian and the set of minimal primes is finite. In the case that I is an invertible module (locally generated by one non-zero divisor element) $\dim(A_{\mathfrak{p}}) \geq 1$ for all prime ideals $\mathfrak{p}$ in A and one gets a Weil divisor.

Exercise 3.93. *Show that ideals that are invertible A-modules form a monoid for the tensor product.*

Definition 3.94. *Let A be a ring. One calls the* **group of Cartier divisor** *of A, denoted* **Div(A)** *to the group generated by the monoid of ideals from invertible A-modules. The monoid $Div_{+}(A))$, of ideals that are invertible A-modules, will be called the set of effective Cartier divisors.*

One can easily check that if I, J are ideals in $\operatorname{Div}(A)$, then the map $I \otimes J \longrightarrow IJ$ is an isomorphism.

Lemma 3.95. *let A be a Dedekind ring. The application cycle:* $\operatorname{Div}(A) \rightarrow Z^1(A)$ *is surjective.*

Proof. We know from the previous section that every prime ideal $\mathfrak{p}$ is locally generated by a non-zero element of A. Because A is of dimension one, if $\mathfrak{q} \neq \mathfrak{p}$ is a different prime ideal of A we have $\mathfrak{p}A_{\mathfrak{q}} = A_{\mathfrak{q}}$. From what we get $\operatorname{cycle}(A/\mathfrak{p}) = [A/\mathfrak{p}]$. □

Exercise 3.96. *Show that A is noetherian integral domain of dimension one and the cycle map* $\operatorname{Div}(A) \rightarrow Z^1(A)$ *is surjective, then the ring A is integrally closed.*

Proposition 3.97. *(Usual definition of Dedekind rings) Let A be a Dedekind ring, then the cycle map* $\operatorname{Div}(A) \rightarrow Z^1(A)$ *is an isomorphism.*

Proof. We already know that the generators of $Z^1(A)$ are in the image of $\operatorname{Div}_{+}(A) \rightarrow Z^1(A)$. We need to check is injective. If I, J are two different ideals of A, we can find a prime $\mathfrak{p}$ such that the localizations $I_{\mathfrak{p}} \neq J_{\mathfrak{p}}$. If we work in the discrete valuation ring $A_{\mathfrak{p}}$ with uniformizing parameter π, we get that $I_{\mathfrak{p}} = \pi^n A_{\mathfrak{p}}$ and $J_{\mathfrak{p}} = \pi^m A_{\mathfrak{p}}$ for two different integers m and n. But then $\operatorname{length}((A/I)_{\mathfrak{p}}) = n$ and $\operatorname{length}((A/J)_{\mathfrak{p}}) = m$ and $\operatorname{cycle}(A/I) \neq \operatorname{cycle}(A/J)$. □

3.8. **The map** $\operatorname{Div}(A) \rightarrow \operatorname{Pic}(A)$**.** For an ideal I of A that is an invertible A-module, we will associate the class of the dual $\operatorname{Hom}(I, A)$ in $\operatorname{Pic}(A)$.

Definition 3.98. *Let A be a ring. One calls* **principal divisors** *of A and denote them* **Pr(A)** *to the subgroup of* $\operatorname{Div}(A)$ *generated by ideals* *of the sort fA, where $f \in A$ is a non-zero divisor. For a domain A, this group is canonically isomorphic to $K^\times/A^\times$, where K is the fraction field of A.*

Example 3.99. If A is a Dedekind domain with field of fractions K and $f \neq 0$ is an element of K, then $(f) = \sum_{\dim(A_\mathfrak{p})=1} \upsilon_p(f)\,[A/p]$ is an element of $Z^1(A)$ that is in the image of $\mathrm{Pr}(A)$. The valuation υ_p is the valuation associated to the discrete valuation ring $A_\mathfrak{p}$.

Proposition 3.100. *For an integral domain A, we have the exact sequence:*

$$0 \longrightarrow \mathrm{Pr}(A) \longrightarrow \mathrm{Div}(A) \longrightarrow \mathrm{Pic}(A) \longrightarrow 0.$$

Proof. If $f \neq 0$, the ideal fA is a free A-module of rank one and therefore the image in $\mathrm{Pic}(A)$ will be trivial. Every element of $\mathrm{Div}(A)$ is the difference of two elements in $\mathrm{Div}_+(A)$. To prove exactness in the middle will be enough to show that if I and J are two ideals in $\mathrm{Div}(A)$ with $\mathrm{Hom}(I, A) = \mathrm{Hom}(J, A)$ then there exist $a, b \in A$ such that $aI = bJ$. We have $I \otimes_A K \simeq K \simeq J \otimes_A K$, where K is the function field of K. We deduce that $\mathrm{Hom}(I, J) = \{f \in K \mid fI \hookrightarrow J\}$ and that is enough to prove our statement. What is left to do is to prove the surjectivity of the map $\mathrm{Div}(A) \to \mathrm{Pic}(A)$ which will be based on the lemma: □

Lemma 3.101. *Let A be an integral domain and L an invertible A-module. Suppose that $s \in L$ is non-zero element of L and consider the map $\varphi_s \colon A \longrightarrow L$ sending $1 \mapsto s$. The map φ_s is injective and the dual map $L^{-1} \longrightarrow A$ identifies L^{-1} with an ideal $\mathfrak{a}_s \subset A$ such that $\mathfrak{a}_s = \mathrm{Ann}(L/A_s)$, where A_s is the image of φ_s.*

Proof. The injectivity of $\varphi_s \colon A \to L$ is based on exercise 2.93. The dual map is not zero, because $\varphi_s^{\vee\vee} = \varphi_s$ and therefore identifies L^{-1} with an ideal $\mathfrak{a}_s$. For the last part we proceed locally and assume $L \simeq A$, then φ_s is identified with the multiplication $\lambda \colon A \to A$ by a non-zero element $\lambda \in A$. The dual map will also be multiplication by λ and the result will be clear. □

Remark 3.102. When A is a Dedekind ring, the group $Z^1(A)/\mathrm{Pr}(A) \simeq \mathrm{Pic}(A)$ is classically known as **the group of divisor classes** and is denoted **Cl(A)**. This group measures to what extend the ring A fails to be a unique factorization domain.

Example 3.103. The ring of integers $A = \mathbb{Z}[\sqrt{-5}]$ in $K = \mathbb{Q}(\sqrt{-5})$ is an example of non-trivial class group $Cl(A)$, or what is equivalent, it has $\mathrm{Pic}(\mathbb{Z}[\sqrt{-5}]) \neq 0$. First we note that the ring A is integrally closed.

The norm of an element $x \in \mathbb{Z}[\sqrt{-5}]$ is $N(x) = a^2 + 5b^2$ and for any two elements $x, y \in A$, we have $N(xy) = N(x)N(y)$. If $\mathrm{Pic}(A) = 0$, then the ring A will be necessarily a principal ideal ring and therefore every irreducible element will generate a prime ideal. Let us show that $1+\sqrt{5}i$ is irreducible. We have $N(1+\sqrt{5}i) = N(1-\sqrt{5}i) = 6$, $N(2) = 4$ and $N(3) = 9$. If x divides $1 + \sqrt{5}i$ and is not a unit or $\pm(1 + \sqrt{5}i)$, then $N(x) = 2$ or $N(x) = 3$. On the other the equations $a^2 + 5b^2 = 2$ and $a^2 + 5b^2 = 2$ has no solutions, because squares are equal only to 1 or 4 modulo 5. If the ideal generated by $1+\sqrt{5}i$ were to be prime, then $6 \in (1 + \sqrt{5}i)$ and therefore either 2 or 3 will be in the ideal as well. This last one will force either $\frac{4}{6} \in \mathbb{Z}$ or $\frac{9}{6} \in \mathbb{Z}$. The ideal $(2, 1+\sqrt{5}i)$ is an example of an ideal in A that is not principal.

The following proposition establishes how the ideals $\mathfrak{a}_s$ depends on the element s.

Proposition 3.104. *Let A be an integral domain and s, t two non-zero elements in the invertible A-module L. In this sense we have the maps $\varphi_s\colon A \to L$ and $\varphi_t\colon A \to L$ and the ideals $\mathfrak{a}_s$ and $\mathfrak{a}_t$. There exist elements $a, b \in A$ such that $as = bt$ and $a\mathfrak{a}_s = b\mathfrak{a}_t$.*

Order in number fields, as we explained before, are examples of noetherian domains of dimension one. In case that the integral domain A is noetherian and of dimension one, the lemma 3.101 has a a more attractive statement

Proposition 3.105. *Let A be an integral domain, noetherian and of dimension one. Suppose that L is an invertible A-module. For every non-zero element $s \in L$, we have $L/A_s \simeq A/\mathfrak{a}_s$.*

Proof. The A-modules L/A_s and $A/\mathfrak{a}_s$ are Artinian. To prove $L/A_s \simeq A/\mathfrak{a}_s$ it will be enough to prove the isomorphism locally. But then, if L is a free A-module of rank one, the map φ_s is just multiplication by $\lambda \in A$. The image of φ_s is the principal ideal $A_s = \lambda A$ and so is the ideal $\mathfrak{a}_s = \mathrm{Ann}(A/\lambda A) \subset A$. □

3.9. **Rational points on a projective scheme over a Dedekind ring.** We establish here, the part of the valuative criterion of properness that will be useful for us: A rational point of a projective scheme over a field K can be extended in a unique way to a point over the Dedekind ring whose field of fractions is K.

Definition 3.106. *Let A be a ring and B an A-algebra and X an scheme over A. We denote by $X(B)$ the rational points of X over B, i.e. the set* $\mathrm{Hom}(\mathrm{Spec}(B), X)$.

Proposition 3.107. *Let A be a ring, K a field, B a Dedekind ring such that B is an A-algebra and K is the field of fractions of B. Then if X is a closed subscheme of $\mathbb{P}^n_A$ one has a canonical bijection between the rational points of X over B and the rational points of X over K:*

$$X(B) \leftrightarrow X(K).$$

Proof. The inclusion $B \hookrightarrow K$ gives rise to a morphism $\mathrm{Spec}(K) \longrightarrow \mathrm{Spec}(B)$ and, by composition, to a map $X(B) \longrightarrow X(K)$. Let us prove that this last map is onto: a point of $X(K)$ is also a point in $\mathbb{P}^n_A(K)$ and then given by a surjective $K-$homomorphism $K^{n+1} \longrightarrow K \longrightarrow 0$. Eliminating the denominators we can consider that the previous homomorphism comes from a B-morphism $B^{n+1} \longrightarrow B$ whose image is a non-zero ideal of B. Because B is a Dedekind ring, every ideal is an invertible B-module. By 2.105, we have an element of $\mathrm{Hom}_{A\text{-sch}}(\mathrm{Spec}(B), \mathbb{P}^n_A)$ that factors though X, when restricted to $\mathrm{Spec}(K)$. The scheme X is a closed set of $\mathbb{P}^n_A$ and therefore defined by a set of homogeneous equations $\{F_i\}$ with coefficients in A. If $b_0, \ldots, b_n$ are elements of B such that $F_i(b_0, \ldots, b_n) = 0$ in K, they also satisfy $F_i(b_0, \ldots, b_n) = 0$ in B. So, we have a morphism from $\mathrm{Spec}(B) \longrightarrow X$ that has by image precisely the point $X(K) = \mathrm{Hom}(\mathrm{Spec}(K), X)$ we started with.
To prove the injectivity of the map, it is enough to do it locally when $B = V$ is a discrete valuation ring. Let $(x_0, \ldots, x_n)$ and $(y_0, \ldots, y_n)$ in V^{n+1}, such that there are $0 \leq k, l \leq n$ such that x_k and y_l are invertible in V. Suppose that the corresponding elements are the same in $\mathrm{Hom}(\mathrm{Spec}(K), X)$, then there exist $\lambda \neq 0$ in K such that for all $0 \leq i \leq n$ $x_i = \lambda y_i$. Because V is a discrete valuation ring either $\lambda \in V$ or $\lambda^{-1} \in V$. Suppose that $\lambda \in V$, then $x_k = \lambda y_k$ is invertible in V and therefore λ is also invertible in V and the two elements $(x_0, \ldots, x_n)$ and $(y_0, \ldots, y_n)$ represent by 2.106 the same element in $\mathrm{Hom}(\mathrm{Spec}(V), X)$. □

Remark 3.108. Let A be a ring and $X \xrightarrow{f} \mathrm{Spec}(A)$ a projective A-scheme then, by definition, an element of $\mathrm{Hom}_A(\mathrm{Spec}(A), X)$ is a section of f. In this way, if A is a Dedekind ring with fraction field K one has a bijection between

$$X(K) \leftrightarrow \{ \text{ sections of } f \colon X \longrightarrow \mathrm{Spec}(A)\}.$$

Definition 3.109. *If A is a Dedekind ring with field of fractions K and if X is a projective scheme over A, one denotes by s_P, the section of $X \longrightarrow \mathrm{Spec}(A)$ correspondent to the rational point $P \in X(K)$.*

We have a pairing $X(K) \times \mathrm{Pic}(X) \longrightarrow \mathrm{Pic}(A)$ such that $(P, \mathcal{L}) \mapsto s_P^* \mathcal{L}$.

Definition 3.110. *Let X, Y be schemes. We say that a morphism $f : X \to Y$ is* **separated** *if the diagonal morphism $\Delta : X \to X \times_Y X$ is a close immersion.*

Example 3.111. The diagonal morphism associated to the morphism of affine schemes $f\colon \operatorname{Spec}(S) \longrightarrow \operatorname{Spec}(R)$ is the morphism on spectra corresponding to the ring map $S \otimes_R S \longrightarrow S$, given by $a \otimes b \mapsto ab$. This map is clearly surjective, so $S \cong (S \otimes_R S)/J$ for some ideal $J \subset S \otimes_R S$ and f is separated.

Suppose that X, X' are two schemes and $f, g\colon X' \longrightarrow X$ are morphisms of schemes. We say that the maps f and g take the same value at $x' \in X'$, written $f(x') \equiv g(x')$, if $f(x') = g(x')$ and the two maps $f^{\#}_{x'}, g^{\#}_{x'}\colon k(f(x')) \longrightarrow k(x')$ are identical. The notion of being separated for a map $f : X \to Y$ is equivalent to the set

$$\{x' \in X \times_Y X \mid p_1(x') \equiv p_2(x')\}$$

being closed, where $p_i\colon X \times_Y X \longrightarrow X$ for $i = 1, 2$ represent the projections. In fact, If $f : X \to Y$ is separated, for any scheme $X' \longrightarrow Y$ over Y and maps $f, g\colon X' \longrightarrow X$, the set

$$\{x' \in X' \mid f(x') \equiv g(x')\}$$

is a closed subscheme of X'. Suppose, for example, that we take two copies U_1 and U_2 of $\mathbb{A}^1$ and create a scheme X identifying U_1 and U_2 along the open sets $x_1 \neq 0$ and $x_2 \neq 0$. We have isomorphisms $\iota_i\colon \mathbb{A}^1 \xrightarrow{\sim} U_i \subset X$ for $i = 1, 2$, but $\{y \in \mathbb{A}^1 \mid \iota_1(x) = \iota_2(x)\} = \mathbb{A}^1 \setminus \{0\}$ is not closed in $\mathbb{A}^1$ and X is therefore not separated.

Theorem 3.112. *(Valuative Criterion of Separatedness) Let $f : X \to Y$ a morphism of schemes, and assume that X is noetherian. Then f is separated if and only if the following condition holds. For any valuation ring R with quotient field K, let $T = \operatorname{Spec} R$, $U = \operatorname{Spec} K$, and $i : U \to T$ be the morphism induced by the inclusion $R \subset K$. Given a morphism of T to Y and a morphism from U to X making the obvious diagram commute, there is at most one morphism from T to X making the whole diagram commutative.*

Definition 3.113. *Let X, Y be schemes. A morphism $f : X \to Y$ is* **proper** *if it is separated, of finite type and universally closed. Here we say that a morphism is universally closed if for any morphism $Y' \to Y$ the extension $f' : X' = X \times Y' \to Y'$ is closed.*

Example 3.114. As a consequence of the fundamental theorem of elimination theory the structure map $\mathbb{P}^n_A \longrightarrow A$ is closed. As closed immersions $X \hookrightarrow \mathbb{P}^n_A$ are proper, we can see that for any ring A, a projective scheme $X \longrightarrow \operatorname{Spec}(A)$ over A is proper.

The general valuative criterion for properness can be expressed as follows:

Theorem 3.115. *(Valuative Criterion of Properness) Let $f\colon X \to Y$ a morphism of schemes of finite type, and assume that X is noetherian. Then f is proper if and only if the following condition holds. For any valuation ring R with quotient field K, let $T = \operatorname{Spec} R$, $U = \operatorname{Spec} K$, and $i : U \to T$ be the morphism induced by the inclusion $R \subset K$. Given a morphism of T to Y and a morphism from U to X making the obvious diagram commute, there is a unique morphism from T to X making the whole diagram commutative.*

4. The compactified Picard group of an order of a number field

We introduce here the invention of Arakelov: to put hermitian metrics at places over infinity.

4.1. **Vector spaces of dimension one over $\mathbb{C}$.** A vector space V over the complex numbers $\mathbb{C}$ is equipped with a hermitian scalar product if one has a bi-additive application $(.,.)\colon V \times V \longrightarrow \mathbb{C}$ such that $(\lambda x, y) = \lambda(x, y)$ and $(x, y) = \overline{(y, x)}$, for all $\lambda \in \mathbb{C}$ and $x, y \in V$. We say that the scalar product is positive nondegenerated if $(x, x) = \|x\|^2 \geq 0$ for all x and $\|x\| = 0$ implies $x = 0$.

Example 4.1. Let V be a vector space of dimension one over $\mathbb{C}$. To provide V with a hermitian scalar product is equivalent to give the length $\|x\|$ of a non-zero vector x. Indeed if $y, z \in V$ with $y = \lambda x$ and $z = \mu x$ then $(y, z) = \lambda\overline{\mu}\|x\|^2$.

Proposition 4.2. *The set of positive nondegenerated hermitian scalar products on a vector space V of dimension one over $\mathbb{C}$ form a homogeneous principals space over $\mathbb{R}_+^\times$.*

Proof. Indeed if we have two products $(.,.)$ and $(.,.)_1$ with the above mentioned characteristic on V and $x \in V$ is a non-zero vector, one has $\|x\| = \lambda\|x\|_1$ for some $\lambda \in \mathbb{R}_+^\times$. □

Remark 4.3. If V_1 and V_2 are two vector spaces of dimension one over $\mathbb{C}$ and equipped with nondegenerated positive hermitian scalar products $(.,.)_1$ and $(.,.)_2$, the tensor product $V_1 \otimes_{\mathbb{C}} V_2$ is canonically equipped with a nondegenerated positive hermitian scalar product such that $\|x_1 \otimes x_2\| = \|x_1\|\|x_2\|$ where $0 \neq x_i \in V_i$ for $i = 1, 2$. In the same way the dual $V^\vee$ is equipped with the norm $\|\varphi\|^\vee = \frac{|\varphi(x)|}{\|x\|}$, for every $x \neq 0$ in V. The induced scalar product is positive and nondegenerated on $V^\vee$.

Exercise 4.4. *Let V be a vector space of dimension one over $\mathbb{C}$ equipped with a nondegenerate positive hermitian scalar product. Show that the trace map $V \otimes_{\mathbb{C}} V^{\vee}$ induces on $\mathbb{C}$ the tautological hermitian scalar product with $\|1\| = 1$.*

Remark 4.5. A little bit of Vocabulary: Let V be a vector space of dimension one over $\mathbb{C}$. We will use indistinctly:

(i) V is equipped with a nondegenerate positive hermitian scalar product.
(ii) V is equipped with a hermitian metric.

Definition 4.6. *Let V be a vector space of dimension one over $\mathbb{C}$ equipped with a hermitian metric $\|.\|$. The canonical volume element over V is such that the unit disk $\{z \in V \mid \|z\| \leq 1\}$ is of volume π.*

The choice of a canonical element of volume on V is the same as to pick a non-zero element of $\wedge^2_{\mathbb{R}} V$, which a vector space of dimension one over $\mathbb{R}$. A positive defined scalar product on a vector space of dimension one over $\mathbb{R}$ will be determined by the length of a non-zero vector. The canonical element of volume will be such that $\{x \mid \|x\| \leq 1\} = 2$. For example if V is a vector space of dimension one over $\mathbb{C}$ defined as $V = V_0 \otimes_{\mathbb{R}} \mathbb{C}$, where V_0 is a vector space of dimension one over $\mathbb{R}$, a nondegenerate positive hermitian scalar product on V induces on V_0 such structure.

4.2. Metrized invertible modules on an order of a number field.

Let K be a number field of degree $[K : \mathbb{Q}] = n$ and with r_1 real places and $2r_2$ pairs of complex conjugate places at infinity. One fixes once and for all a set Φ of r_1 real places and r_2 complex places such that no pair of conjugate places is in Φ. Let A be an order of K.

Definition 4.7. A metrized invertible module *on A is an invertible module L over A equipped for every place $\sigma \in \Phi$ of a nondegenerate positive hermitian scalar product $(.,.)_\sigma$ on $(L \otimes_A \sigma(A)) \otimes_{\sigma(A)} \mathbb{C}$. If $\|.\|_\sigma$ is the norm associated to $(.,.)_\sigma$, we denote the metrized invertible A-module L by $\bar{L} = (L, \|.\|_\sigma) = (L, \|.\|_\sigma)_{\sigma \in \Phi}$.*

Definition 4.8. *An isometry between two metrized invertible A-modules $(L_1, \|.\|_{1,\sigma})$ and $(L_2, \|.\|_{2,\sigma})$ is an A-isomorphism $\varphi \colon L_1 \xrightarrow{\sim} L_2$ such that $\|\varphi(x)\|_{2,\sigma} = \|x\|_{1,\sigma})$, for all $x \in L_1$ and $\sigma \in \Phi$.*

Lemma 4.9. *Let $(L, \|.\|_{1,\sigma})$ and $(L, \|.\|_{2,\sigma})$ be two metrized invertible A-modules structures on the same invertible module L. Then $\bar{L}_1 \simeq \bar{L}_2$ if and only if there exist a unit $u \in A^\times$ such that $\|x\|_{1,\sigma} = |\sigma(u)|\|x\|_{2,\sigma}$ for all $x \in L$ and all $\sigma \in \Phi$.*

Proof. We know that $\mathrm{Hom}_A(L,L) = A$ and $Isom_A(L) = A^\times$. On the other hand for all $x \in L$ and $\sigma \in \Phi$ we get $\|ux\|_{2,\sigma} = |\sigma(u)|\|x\|_{1,\sigma}$. □

Proposition 4.10. *The tensor product induces on the classes of isometry of invertible A-modules an intern binary law of composition that makes the set of isometry classes into a commutative group called the* **The compactified Picard group of A**. *It will be denoted by* $\mathrm{Pic}_c(A)$.

Proof. The result is a consequence of the remark 4.3 and the exercise 4.4. The dual element $(L^\vee, \|.\|_\sigma^\vee)$ will be the inverse of the element $(L, \|.\|_\sigma)$ and the neutral element will be the trivial module A with the metric $\|1\|_\sigma = 1$ for all $\sigma \in \Phi$. □

Example 4.11. Let $\{x_\sigma\}_{\sigma\in\Phi}$ positive real numbers, one denotes by $(A,(x_\sigma))$, the element in $\mathrm{Pic}_c(A)$ where the trivial module A is equipped with the metric $\|1\|_\sigma = x_\sigma$. In this way $(A,(1)_\sigma)$ is the neutral element of $\mathrm{Pic}_c(A)$.

Exercise 4.12. *Prove that the map* $(\mathbb{R}_+^\times)^\Phi \longrightarrow \mathrm{Pic}_c(A)$ *where* $(x_\sigma) \mapsto (A,(x_\sigma))$ *is a group homomorphism.*

Exercise 4.13. *Prove that the forgetful map* $\mathrm{Pic}_c(A) \longrightarrow \mathrm{Pic}(A)$ *that maps* $(A,(x_\sigma)) \mapsto A$ *is a surjective group homomorphism.*

Proposition 4.14. *(***First fundamental exact sequence***) One has the exact sequence:*

$$0 \to \mu(A) \to A^\times \xrightarrow{\sigma} (\mathbb{R}_+^\times)^\Phi \to \mathrm{Pic}_c(A) \longrightarrow \mathrm{Pic}(A) \to 0,$$

where $\mu(A)$ *is the set of roots of unity in* A *and* $\sigma\colon A^\times \longrightarrow (\mathbb{R}_+^\times)^\Phi$ *is the map that assigns to any unit* $u \in A^\times$ *the value* $(|\sigma(u)|)_\sigma$ *in* $(\mathbb{R}_+^\times)^\Phi$.

The kernel of the surjective application $\mathrm{Pic}_c(A) \longrightarrow \mathrm{Pic}(A)$ is the set of structures at infinity, that is the image of the map $(\mathbb{R}_+^\times)^\Phi \longrightarrow \mathrm{Pic}_c(A)$ given by $(x_\sigma) \mapsto (A,(x_\sigma))$. Using 4.9 we have that $(A,(x_\sigma))$ is isometric to $(A,(1))$ if and only if there exist a unit $u \in A^\times$ with $|\sigma(u)| = x_\sigma$. To finish the proof we need to prove the following lemma:

Lemma 4.15. *Let A be an order in a number field K, for an element x of A the following are equivalent:*

(i) *x is a root of unity.*
(ii) *For every field homomorphism $\sigma\colon K \longrightarrow \mathbb{C}$, $\sigma(x)$ is of absolute value 1.*

Moreover the set of roots of unity is a finite set.

Proof. (i) ⇒ (ii) is clear because $x^k = 1$ implies $|\sigma(x)|^k = 1$ and the absolute value $|\sigma(x)| = 1$ for all places $\sigma\colon K \longrightarrow \mathbb{C}$.

(ii) ⇒ (i) By the first finiteness lemma 3.81, the set $\{x^n\}_{n\in\mathbb{N}}$ will be in the finite set $M_{\leq 1}^{\deg(K:\mathbb{Q})}$ and will be therefore finite which forces x to be a root of unity. As a consequence we get more, all roots of unity in A are inside the finite set $M_{\leq 1}^{\deg(K:\mathbb{Q})}$ and form a finite set. □

4.3. **The norm of an ideal.** We start to highlight some finite rings build from orders.

Proposition 4.16. *Let A be an order in a number field K and $\mathfrak{a}$ a non-zero ideal of A, then $A/\mathfrak{a}$ is finite. Moreover if $(\mathfrak{p}_i)_{i=1,2,\ldots,r}$ are the prime ideals of A containing $\mathfrak{a}$, one has*

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

and $\log(\#(A_{\mathfrak{p}_i}/\mathfrak{a}A_{\mathfrak{p}_i})) = \mathrm{length}(\#(A_{\mathfrak{p}_i}/\mathfrak{a}A_{\mathfrak{p}_i}))\log(\#(A/\mathfrak{p}_i))$.

Proof. For the first part we can prove more: if $x \in \mathfrak{a}$ is a non-zero element, then A/xA is finite. If $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ is an equation of integral dependency of x over $\mathbb{Z}$, one has $a_n \neq 0$. Then A/xA is a module of finite type over $\mathbb{Z}/a_n\mathbb{Z}$ and therefore finite. The rest of proposition is a consequence of $A/\mathfrak{a}$ being artinian and therefore of finite length, so we can use corollary 3.6. Note that over a local artinian ring the only simple module is the residual field. □

Definition 4.17. *Let A be an order in a number field K and $\mathfrak{a}$ a non-zero ideal of A. We call* **norm** *of $\mathfrak{a}$ and denoted by $N(\mathfrak{a})$ the cardinal of $A/\mathfrak{a}$.*

Example 4.18. For example $N(\mathbb{Z}n) = |n|$ for any $n \in \mathbb{Z}$.

Proposition 4.19. *(Multiplicative property of the Norm) Suppose that A is an order in a number field K. La application norm:* $\mathrm{Div}_+(A) \longrightarrow \mathbb{N}$ *is multiplicative.*

Suppose that A is an order in a number field K. We want to prove for ideals $I, J \in \mathrm{Div}_+(A)$ that $\#(A/IJ) = \#(A/I)\#(A/J)$. To that end we prove the following general lemma:

Lemma 4.20. *Let B be a ring, J an ideal of B and $x \in B$ an element that is not a zero divisor. We have an exact sequence of B-modules:*

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

Proof. The kernel of the canonical map $B/xJ \longrightarrow B/xB$ is the module xB/xJ. Let us find the kernel of the surjective morphism $\varphi\colon B \longrightarrow xB/xJ$ defined such that $\varphi(1) = [x]$. If $\lambda \in B$ and $z \in J$ are such that $\lambda x = xz$ then $\lambda = z \in J$ because x is not a zero divisor in B. Therefore the kernel of φ is J and $B/J \simeq xB/xJ$. □

End of the proof of 4.19: Applying lemma 4.20 to the ring $A_{\mathfrak{p}}$, where I and J are generated by one element one obtains

$$\operatorname{length}(A_{\mathfrak{p}}/IJA_{\mathfrak{p}}) = \operatorname{length}(A_{\mathfrak{p}}/IA_{\mathfrak{p}}) + \operatorname{length}(A_{\mathfrak{p}}/JA_{\mathfrak{p}}).$$

The proposition is a result then of the second part of 4.16.

Corollary 4.21. *The norm map can be extended to a group homomorphism $N\colon \operatorname{Div}(A) \longrightarrow \mathbb{Z}$.*

We will like a group of homomorphism with domain $\operatorname{Pic}(A)$ instead of $\operatorname{Div}(A)$. To that end we need to study the norm of principal divisors. In fact we will be able to construct a group homomorphism $N\colon \operatorname{Pic}_c(A) \longrightarrow \mathbb{R}$, with values in $\mathbb{R}$ extending the notion of norm to compactified divisors. Firs we establish the fact that the norm allows a first classification of the ideals in an order.

Lemma 4.22. *(***second finiteness lemma***) Let A be an order of a number field and r be an integer. Then the set of ideals $\mathfrak{a}$ and of norm at most r is a finite set.*

Proof. Every element of a finite group is annihilated by the order of the group. If $\mathfrak{a}$ is an ideal in A with norm $N(\mathfrak{a}) \leq r$, then $r!$ annihilates the finite group $A/\mathfrak{a}$ and therefor $r! \in \mathfrak{a}$. The set of ideals in A with norm at most r are then in one to one correspondence with a subset of the finite set $A/(r!)A$ and is therefore finite. □

4.4. **The norm of an element in a number field.** Let x be a element of the number field K, let d be the degree of the extension $[\mathbb{Q}[x] : \mathbb{Q}]$. Then $(-1)^d$ multiplied by the determinant of the multiplication by x in the $\mathbb{Q}$-vector space $\mathbb{Q}[x]$ is the constant coefficient of the minimal polynomial of x. In this case the characteristic polynomial of the matrix representation of $m_x = \times x$ is the same as the minimal polynomial of x.

Proposition 4.23. *Let K be a number field and x an element of K. Then the determinant of m_x, the multiplication by x in K, is a rational number that satisfies:*

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

Proof. The proof is clear for $K = \mathbb{Q}[x]$. On the other hand if K is an extension of $\mathbb{Q}[x]$ of degree m, one will have $m[\mathbb{Q}[x] : \mathbb{Q}] = [K : \mathbb{Q}]$ and the matrix of m_x as a map on K will consist of m blocks equals to the matrix of m_x restricted $\mathbb{Q}[x]$. We have then

$$\det(m_x) = \prod_{\sigma\colon \mathbb{Q}[x] \to \mathbb{C}} \sigma(x)^m,$$

and because there are exactly m $\mathbb{Q}$-homomorphisms of $K \to \mathbb{C}$ extending each $\sigma\colon \mathbb{Q}[x] \to \mathbb{C}$, the proof is finish in this case too. □

Definition 4.24. *Let K be a number field and x an element of K, one calls* **norm of** *x, denoted by $N(x)$, the rational number $\prod_{\sigma\colon K\to\mathbb{C}} \sigma(x)$.*

Remark 4.25. If $x \in \mathcal{O}_K$, all conjugates of x are also in $\mathcal{O}_K$ and the norm $N(x) \in \mathbb{Z}$.

Remark 4.26. Is clear that $N\colon K^\times \longrightarrow \mathbb{Q}^x$ is a **group homomorphism**. Let A be an order in the number field K. The norm of an invertible element $u \in A^\times$ is an invertible element of $\mathbb{Z}$ and therefore ± 1. If we compose the norm with the absolute value, one gets a group homomorphism $|N|\colon K^\times/A^\times \longrightarrow \mathbb{Q}_+^\times$. As we know $K^\times/A^\times = \mathrm{Pr}(A)$, we can compare the two notions on norms on $\mathrm{Pr}(A)$.

Proposition 4.27. *(product formula) Let K be a number field, A an order in K and x an element in A. Then the norm of the ideal xA generated by x in A is the same as the absolute value of the norm of the element x.*

We need to establish the following identity:

$$N(xA) =\mid N(x) \mid=\mid \prod_{\sigma\colon K\to\mathbb{C}} \sigma(x) \mid$$

Since the element x is in A, the determinant of the multiplication by x in K is the same as the determinant of the multiplication by x in A. We will use the following lemma:

Lemma 4.28. *Let $\varphi\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ be an injective homomorphism of free $\mathbb{Z}$-modules then*

$$\#(Coker(\varphi)) = \#(Coker(\det(\varphi))) = \#(\mathbb{Z}/\det(\varphi)\mathbb{Z}).$$

Proof. By the theorem on elementary divisors 3.25, we can diagonalize φ. If $a_1, a_2, \ldots, a_n$ are the elements of the diagonal, we know by hypothesis of injectivity that $a_i \neq 0$ for all i and the determinant is given by the product $\prod_i a_i$. □

End of the proof of the product formula identity 4.27: We have

$$\begin{aligned}\prod_{\sigma\colon K\to\mathbb{C}} |\sigma(x)| = |\det(m_x)| &= \#(Coker(m_x))\\ &= \#(\mathbb{Z}/\det(m_x)\mathbb{Z})\\ &= \#(A/xA)\\ &= N(xA).\end{aligned}$$

Exercise 4.29. *Let A a noetherian ring of dimension one and let $\varphi\colon A^n \longrightarrow A^n$ an A-homomorphism:*

(a) *Show that both $Ker(\varphi)$ and $Coker(\varphi)$ are annihilated by $\det(\varphi)$.*

(b) *Show that if $A/\det(\varphi)A$ is of dimension zero, the function $M \longrightarrow \chi(M,\varphi) = \mathrm{length}(Coker(\varphi\otimes M)) - \mathrm{length}(Ker(\varphi\otimes M))$ is additive with values in $\mathbb{N}$, for A-modules M of finite type. Compute $\chi(M)$ in terms of $\chi(A)$ when A is an integral domain.*

(c) *Show that $\chi(A^n,\varphi) = \chi(A,\det(\varphi))$. (This is delicate, it deserves the name of theorem of* **Riemann-Roch for noetherian rings of dimension one***).*

(d) *Let A be a noetherian ring of dimension one and with characteristic equals a prime p. Let the map φ be represented by an $n\times n$ matrix with coefficients in A. Let us consider the map $\varphi^{(p)}$ with the coefficients of φ raised to the p-th power. Show that under the same hypothesis as (b), there exist a polynomial $p_\chi(M,\varphi)$ such that $\chi(M,\varphi^{(p)}) = p_\chi(M,\varphi)$ for every A-module of finite type.*

Definition 4.30. *Let $\mathcal{O}_K$ be the ring of integers of a number field K. One calls* **a finite place of** *K to a valuation v on K (associated by proposition 3.84 to a prime ideal $\mathfrak{p}_v$ of $\mathcal{O}_K$). By abuse of notation, we denote $N(v) = N(\mathfrak{p}_v)$. We can see that the function $f \mapsto N(v)^{-v(f)}$ is an ultrametric norm on K that we will denote $|f|_v$.*

Corollary 4.31. *(classic product formula) For an element $f \in K^\times$, we have*

$$\prod_{v \text{ place of } K} |f|_v = 1.$$

The product in the formula is made out of places at infinity $v = \sigma\colon K \longrightarrow \mathbb{C}$ and finite places v associated to prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$. Suppose that $a \in K^*$ and $\mathcal{O}_v$ is the valuation ring associated to the valuation v. We have $\#(\mathcal{O}_v/a\mathcal{O}_v) = N(v)^{v(a)}$ and proceed to use the product formula 4.27 together with proposition 4.16.

Exercise 4.32. *(product formula on the projective line) Let $A = k[T]$ be the ring of polynomials in one variable over the algebraically closed field k. Let P be a point on the affine line $\mathbb{A}^1(k)$ with coordinate t and let $m_P = (T-t)$ be the ideal of A generated by $T-t$.*

(a) *Let f be an element of A. Show that the valuation v_t associated to m_P is such that $v_t(f)$ is the order of P as zero of f.*

(b) *Let f be an element of A of degree n. Show that f has a pole of order n at infinity (i.e. $F(T) = \frac{1}{u^n} g(u)$ for $u = \frac{1}{T}$ and $g \in k[u]$ with $g(u) \neq 0$.*

(c) *Let f be an element of A. Show that $\upsilon_\infty = -$(order of the pole of f at infinity) is a valuation υ_∞ on $k(T)$.*

(d) *Show that for all $f \in A$ we have $\sum_{t \in k \cup \infty} \upsilon_t(f) = 0$.*

Exercise 4.33. *Let K be a* **function field of one variable over** *k, i.e. K is a finite extension of a rational functions field $k(T)$. We say that the ring A is an order of K, if A is a $k[T]$-module of finite type contained in K with fraction field exactly K.*

(a) *Prove that $A \simeq k[T]^n$ where $n = [K : k(t)]$.*

(b) *Let $\mathfrak{a}$ be a non-zero ideal of A, one puts* $\deg(\mathfrak{a}) = \dim_k(A/\mathfrak{a})$. *Show that* $\deg \colon \operatorname{Div}_+(A) \longrightarrow \mathbb{N}$ *is an additive homomorphism.*

(c) *Suppose that k is a finite field. Prove that the set of ideals $\mathfrak{a} \subset A$ such that* $\deg(\mathfrak{a}) \leq r$, *for a fixed r is a finite set.*

4.5. **The local definition of degree.** Assume that A is an order in the number field K. We give a notion of degree on compactified divisors on A.

Definition 4.34. *On calls* **the group of compactified divisors of** *A, denoted $Z^1_c(A)$ to the group $Z^1(A) \times \mathbb{R}^\Phi$. One denotes by*

$$\sum_{\mathfrak{p} \in \operatorname{Spec}(A)} n_\mathfrak{p}[A/\mathfrak{p}] + \sum_{\sigma \in \Phi} \lambda_\sigma[\sigma]$$

a generic element of $Z^1_c(A)$.

In the same way, we define the **group of compactified Cartier divisors on** A, denoted $\operatorname{Div}_c(A)$. We have an injection $\operatorname{Div}(A) \hookrightarrow \operatorname{Div}_c(A)$. We also have a group homomorphism $\operatorname{Div}_c(A) \longrightarrow Z^1_c(A)$ extending the cycle map $\operatorname{Div}(A) \longrightarrow Z^1(A)$ and adding the component at infinity.

Definition 4.35. *One calls* **degree on the compactified one cycle** *$\sum n_\mathfrak{p}[a/\mathfrak{p}] + \sum \lambda_\sigma[\sigma]$ to the real number*

$$\sum n_\mathfrak{p} \log(N(\mathfrak{p})) + \sum \epsilon_\sigma \lambda_\sigma,$$

where $\epsilon_\sigma = 1$ for real places and $\epsilon_\sigma = 2$ for complex places. By composition we define **the degree of a compactified divisor**.

Proposition 4.36. *The degree map :* $\operatorname{Div}_c(A) \longrightarrow \mathbb{R}$ *is a group homomorphism, denoted by* deg. *If $\mathfrak{a}$ is an element of* $\operatorname{Div}_+(A)$ *on A (considered as a compactified divisor without components at infinity) then:*

$$\deg(\mathfrak{a}) = \log(N(\mathfrak{a})).$$

Example 4.37. Let $x \in A$ then we define the compactified divisor $(x) = xA - \sum_{\sigma\in\Phi} \epsilon_\sigma \log|\sigma(x)|$. We extend this map to a map $K^\times \longrightarrow \mathrm{Div}_c(A)$ and will denote by (f) the **compactificed principal divisor** associated to $f \neq 0$. We denote by $\mathrm{Pr}_c(A)$ the subgroup of $\mathrm{Div}_c(A)$ consisting of compactified principal divisors.

Proposition 4.38. *(***The homomorphism** $\mathrm{Div}_c(A) \longrightarrow \mathrm{Pic}_c(A)$*)* *There exist a natural homomorphism* $\mathrm{Div}_c(A) \longrightarrow \mathrm{Pic}_c(A)$ *such that the following diagram commutes*

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & \\
 & \mathrm{Pr}_c(A) \arrow[d] & \mathrm{Pr}(A) \arrow[d] & \\
\mathbb{R}^\Phi \arrow[r] \arrow[d] & \mathrm{Div}_c(A) \arrow[r] \arrow[d] & \mathrm{Div}(A) \arrow[r] \arrow[d] & 0 \\
(\mathbb{R}_+^\times)^\Phi \arrow[r] & \mathrm{Pic}_c(A) \arrow[r] \arrow[d] & \mathrm{Pic}(A) \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 &
\end{tikzcd}$$

Let $\mathfrak{a} + \sum_\sigma x_\sigma[\sigma]$ an element of $\mathrm{Div}_c(A)$ such that $\mathfrak{a}$ is invertible ideal of A. One can associate the following element of $\mathrm{Pic}_c(A)$:

(a) The invertible module $\mathfrak{a}^{-1} = \mathrm{Hom}(\mathfrak{a}, A)$.

(b) By dualizing the inclusion $\mathfrak{a} \hookrightarrow A$, one obtains a homomorphism $A \to \mathfrak{a}^{-1}$ and one puts $|Im(1)|_\sigma^{\epsilon_\sigma} = e^{-x_\sigma}$.

In this way if $L \in \mathrm{Pic}_c(A)$ and $0 \neq s \in L$. L is coming from the element $\mathfrak{a}_s - \sum \log|s|_\sigma[\sigma] \in \mathrm{Div}_c(A)$.

Example 4.39. If x is an element of A and (x) the associated compactified divisor. Then the element of $\mathrm{Pic}_c(A)$ corresponding to (x) is the neutral element $(A, (1)_\sigma)$.

Proposition 4.40. *The degree map* $\mathrm{Div}_c(A) \longrightarrow \mathbb{R}$*, is zero on the group of principal compactified divisors* $\mathrm{Pr}_c(A)$*. It defines a map, that we still call degree,* $\deg\colon \mathrm{Pic}_c(A) \longrightarrow \mathbb{R}$*. If L is in* $\mathrm{Pic}_c(A)$ *and $0 \neq s \in L$ one has*

$$\deg(L) = \log \frac{\#(L/A_s)}{\prod_{\sigma\in\Phi} |s|_\sigma^{\epsilon_\sigma}}.$$

Proof. The degree of an element $x \in A$ is $\deg(x) = \log(N(xA)) - \epsilon_\sigma \log|\sigma(x)\| = \log(N(xA)) - \log|N(x)|$ which is zero by the product formula 4.27. For the second part of the proposition 4.40, consider the ideal $\mathfrak{a}_s$ introduced in lemma 3.101. We have $L/A_s \simeq A/\mathfrak{a}_s$, and after 4.38, the element $L \in \mathrm{Pic}_c(A)$ comes from the element $\mathfrak{a}_s - \sum \log |s|_\sigma [\sigma] \in \mathrm{Div}_c(A)$. Computing the degree:

$$\deg(L) = \deg(\mathfrak{a}_s - \sum_{\sigma \in \Phi} \epsilon_\sigma \log |s|_\sigma),$$

we get our formula in 4.40. □

Exercise 4.41. *Prove that the kernel of the map $K^\times \longrightarrow \mathrm{Div}_c(A)$ defined in 4.37 is exactly $\mu(A)$.*

Example 4.42. Let $t = e^r$ be a positive real number and $L \in \mathrm{Pic}_c(A)$, one denotes by L_r the element of $\mathrm{Pic}_c(A)$ obtained by multiplying the norms on L by t. As a corollary of 4.40, the degree of L_r is $\deg(L) - nr$.

Example 4.43. Let $(x_\sigma) \in \mathbb{R}_+^\Phi$ and let $(A, (x_\sigma))$ be the element of $\mathrm{Pic}_c(A)$ defined in 4.11, proposition 4.40 implies that $\deg(A, (x_\sigma)) = -\sum_\sigma \epsilon_\sigma \log(x_\sigma)$.

4.6. **Volume, global definition of degree.** If L is in $\mathrm{Pic}_c(A)$, the $\mathbb{R}$-vector space $\oplus_{\sigma \in \Phi} L \otimes_A K_\sigma$, where K_σ equals $\mathbb{R}$ or $\mathbb{C}$ depending if σ is a real or a complex place at infinity, is equipped with a canonical volume element build out of the canonical volume elements in each $L \otimes K_\sigma$.

Proposition 4.44. *Let L be an invertible module over an order A of a number field K of degree n. The diagonal map $L \longrightarrow \oplus_{\sigma \in \Phi} L \otimes_A K_\sigma$ identifies L with a lattice in a vector space of dimension n over $\mathbb{R}$.*

Proof. we know that L is a free $\mathbb{Z}$-module of rank n. We need to show that the image under the map is discrete in $\oplus_{\sigma \in \Phi} L \otimes_A K_\sigma$. Choose an element $s \in L$ with $s \neq 0$, one has an injective map $\varphi_s \colon A \longrightarrow L$ sending $1 \mapsto s$. We have that $\varphi_s \otimes K_\sigma$ is an isomorphism for all σ. One has a commutative diagram

$$\begin{tikzcd} A \arrow[r, "\varphi_s"] \arrow[d] & L \arrow[d] \\ \oplus K_\sigma \arrow[r, "\sim"] & \oplus L \otimes K_\sigma . \end{tikzcd} ,$$

Let $r = \#(L/As)$ and let B be a compact set in $\oplus_\sigma L \otimes K_\sigma$. If $x \in L \cap B$ then rx is in $A \cap rB$. Like A is discrete in $\oplus K_\sigma$, the set $A \cap rB$ is a finite set and so is $L \cap B$. □

Corollary 4.45. *The canonical map $L \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow \oplus_\sigma L \otimes K_\sigma$ is an isomorphism.*

An element $L \in \operatorname{Pic}_c(A)$ has a non-zero volume defined as a lattice of $\mathbb{R}^n$. This is nothing but the volume of $\oplus L \otimes K_\sigma / L$ measured by the volume element describe in the introduction of this subsection. We denoted by **Vol(L)**.

Proposition 4.46. *For any $L \in \operatorname{Pic}_c(A)$ we have:*

$$\log \frac{vol(A)}{vol(L)} = \deg(L).$$

Proof. Choose a non-zero element $s \in L$. One has the exact sequence

$$0 \to A \xrightarrow{1 \mapsto s} L \to L/As \to 0.$$

The map $A \otimes K_\sigma \longrightarrow L \otimes K_\sigma$ does not necessarily preserves the volume, the image of the unit disk becomes the elements $z \in L \otimes K_\sigma$ such that $|z|_\sigma \leq |s|_\sigma$, where the measure has been taken to be $\pi |s|_\sigma^2$ for complex places and $2|s|_\sigma$ for real places. The volume is then multiplied by $\prod_{\sigma \in \Phi} |s|_\sigma^{\epsilon_\sigma}$ in the map $\oplus A \otimes K_\sigma \longrightarrow \oplus L \times K_\sigma$. Using the exact sequence above we get

$$vol(L) \#(L/As) = vol(A) \prod_{\sigma \in \Phi} |s|_\sigma^{\epsilon_\sigma},$$

and the formula follows from our definition of degree in $\operatorname{Pic}_c(A)$. □

The expression in 4.46 represents a **global definition of degree** in $\operatorname{Pic}_c(A)$ in contrast to the **local definition of degree** in 4.40. The additivity of the degree is less obvious from the global definition, a situation that we will encounter again in the Riemann-Roch theorem for curves. We will see later a more Riemann-Roch interpretation of the formula.

4.7. **Sections of a compactified invertible module, theorem of Riemann-Roch.** We put together here the fundamental problems of the geometry of numbers due to Minkowski.

Definition 4.47. *Let L be an element of* $\operatorname{Pic}_c(A)$*, one calls* **global section of L** *to an element s of the associated invertible A-module L with the extra property that $|s|_\sigma \leq 1$ for all places σ at infinity. The set of global sections of $L \in \operatorname{Pic}_c(A)$ is denoted by $H^0(L)$. One notice that $H^0(L) = B \cap L$, where B denotes the unit ball of $\oplus L \otimes K_\sigma$.*

Remark 4.48. A compactified invertible module L is discrete in $\oplus L \otimes K_\sigma$ and $H^0(L)$ is therefore a finite set.

Example 4.49. $H^0(A) = \mu(A) \cup \{0\}$. For all $L \in \operatorname{Pic}_c(A)$, the set $\mu(A)$ acts on $H^0(L)$ and the action is free on $H^0(L) \setminus \{0\}$.

Definition 4.50. *The Euler characteristic $\chi_s(L)$ of an element $L \in \operatorname{Pic}_c(A)$ is defined as*

$$\chi_s(L) = \log \frac{2^{r_1}\pi^{r_2}}{vol(L)}.$$

We will show that $\chi_s(L)$ is an approximation to $\log(\#H^0(L))$, which justifies the name of the following remark

Remark 4.51. (**Theorem of Riemann-Roch**) One has the formula:

$$\chi_s(L) = \deg(L) + \chi_s(A).$$

Our remark here is equivalent to the global definition of degree 4.46. We use the subindex s in χ_s to indicate that we are working with the volume of the unit ball for the sup norm: $2^{r_1}\pi^{r_2}$. One could have taken $\chi(L) = -\log vol(L)$ or like we are going to do later $\chi'(L) = \log \dfrac{2^{r_1}\pi^{r_2}}{2^n vol(L)}$. The name of Riemann-Roch comes from the case of non-singular projective curves C over fields k. If L is a line bundle on C, there is a notion of degree and a notion of global sections $H^0(C, L)$. One has also an $H^1(C, L)$ and the χ is defined by $\chi(L) = \dim_k(H^0(C, L)) - \dim_k(H^1(C, L))$ to obtain

$$\chi(L) = \deg(L) + \chi(\mathcal{O}_C).$$

The term $\dim_k(H^1(C, L))$ is the error term due to Roch and is zero for big degree $\deg(L) >> 0$ and $\chi(L)$ can be taken as an approximation of $\dim_k(H^0(L))$.

5. Different, discriminant and conductor

The discriminant of a number field K gives information about the primes $p \in \mathbb{Q}$ that ramify in K. The different will provide information about what particular primes $\mathfrak{p} \subset \mathcal{O}_K$ appear in the ramification locus of the extension.

Definition 5.1. *Let K'/K be a finite extension of number fields. The trace map $Tr = Tr_{K'/K} \colon K' \longrightarrow K$ is the K-linear map defined for each element $a \in K'$ as the trace of the linear map $m_a \colon K' \longrightarrow K'$ given by the multiplication $m_a(x) = ax$.*

Exercise 5.2. *Prove that every linear map $\lambda \colon K' \longrightarrow K$ can be expressed as $\lambda(y) = Tr(x_\lambda y)$ for some x_λ.*

Definition 5.3. *Let K'/K be a finite extension of number fields. The dual lattice of $\mathcal{O}_{K'}$ or* **codiferent** *is the submodule of K' defined by*

$$\mathcal{O}_{K'}^\vee = \{\alpha \in K' \,|\, Tr_{K'/K}(\alpha\mathcal{O}_{K'}) \subset \mathcal{O}_K\}.$$

Suppose that K'/K is simply a separable extension of fields, the ring A is a Dedekind domain with field of fractions K and A' is the integral closure of A in K'. If $\alpha_1, \dots, \alpha_n \in A'$ is a basis of K'/K and $d = \det(Tr(\alpha_i\alpha_j))$, we can write $\alpha \in A'$ as $\alpha = x_1\alpha_1 + \cdots + x_n\alpha_n$, for some $x_1, \dots, x_n \in A$. Then, for every $\lambda \neq 0$ in A, the λx_i will satisfy, for $j = 1$ to n, the system of linear equations

$$\lambda x_1 Tr(\alpha_1\alpha_j) + \cdots + \lambda x_n Tr(\alpha_n\alpha_j) = Tr(\lambda\alpha_j\alpha).$$

As a consequence, if $\alpha \in \{x \in K' \mid Tr(xA') \subset A\}$, so is $d\lambda\alpha$. In particular the dual lattice is a fractional ideal of A'. The fractional ideal

$$(A'/A)^\vee = \{\alpha \in K' \mid Tr(\alpha A') \subset A\}$$

will be called the relative co-different or dual modulo of the extension A'/A.

Definition 5.4. *The* **different ideal** $\mathcal{D}_{K'/K}$ *of* K' *over* K *is the inverse of the dual lattice*

$$\mathcal{D}_{K'/K} = (\mathcal{O}_{K'}^\vee)^{-1} = \{x \in K' \mid x\mathcal{O}_{K'}^\vee \subset \mathcal{O}_K\}.$$

We will denote $\mathcal{D}_{K/\mathbb{Q}}$ *simply by* $\mathcal{D}_K$. *We can extend the notion of different to a separable extension* K'/K, *and a Dedekind domain* A *with integral closure* A' *in* K'. *Based on our previous discussion we define the different ideal as*

$$\mathcal{D}_{A'/A} = \{x \in K' \mid x(A'/A)^\vee \subset A\}.$$

Example 5.5. Since $\mathbb{Z}[i]^\vee = \frac{1}{2}\mathbb{Z}[i]$, the different $\mathcal{D}_{\mathbb{Q}(i)} = 2\mathbb{Z}[i]$.

Exercise 5.6. *Suppose that we have a number field* $K = \mathbb{Q}(\alpha)$ *with* $\mathcal{O}_K = \mathbb{Z}[\alpha]$, *prove that the different is the principal ideal* $(f'(\alpha))$, *where* $f \in \mathbb{Z}[t]$ *is the minimal polynomial of* α. *Hint: If we denote by* $\alpha_1, \dots, \alpha_n$ *the conjugates of* α, *we have the Euler identity:*

$$\sum_i \frac{\alpha_i^k f(T)}{f'(T)(T-\alpha_i)} = T^k.$$

If we put $f(T) = (T-\alpha)(c_0(\alpha) + c_1(\alpha)T + \dots c_{n-1}(\alpha))$, *the above identity says that the dual basis of* $\{1, \alpha, \dots, \alpha^{n-1}\}$, *with respect to the trace product, is* $\{\frac{c_0(\alpha)}{f'(\alpha)}, \dots, \frac{c_{n-1}(\alpha)}{f'(\alpha)}\}$. *The proof will be finished then when we find a recursive formula for the* $c_i(\alpha)$ *and exhibit the equality of the two* $\mathbb{Z}$*-span*

$$\mathbb{Z} + \alpha\mathbb{Z} + \cdots + \alpha^{n-1}\mathbb{Z} = c_0(\alpha)\mathbb{Z} + c_1(\alpha)\mathbb{Z} + \cdots + c_{n-1}(\alpha)\mathbb{Z}.$$

Definition 5.7. *Let K be a number field. Let A be an order in K and $a = \{a_1, \dots, a_n\}$ an integral basis of A over $\mathbb{Z}$. The* **discriminant** *$d_A(a)$ of A in K with respect to the base (a) is the determinant $d_A(a) = \det(Tr_K(a_i a_j))$.*

Remark 5.8. If we choose a different integral base (a') of A over $\mathbb{Z}$, we will have $a' = Ma$ for some invertible matrix M with rational integer coefficients and

$$d_A(a') = \det(M)^2 d_A(a) = d_A(a).$$

As a consequence we have the right to call d_A the discriminant of A independent of the basis. In the special case of the integrally closed order $A = \mathcal{O}_K$, the discriminant $d_{\mathcal{O}_K}$ will be denote simply d_K.

Remark 5.9. An alternative definition for the **discriminant** d_K of K is the square of the determinant $\det^2((\sigma_i(a_j))_{i,j})$, for a complete set of embeddings $\{\sigma_1, \dots, \sigma_n\}$ of K into $\mathbb{C}$ and a basis $a = \{a_1, \dots, a_n\}$ of $\mathcal{O}_K$ over $\mathbb{Z}$. The equivalency is a consequence of the formula

$$Tr(a_i a_j) = \sum_k \sigma_k(a_i a_j) = \sum_k \sigma_k(a_i)\sigma_k(a_i).$$

Exercise 5.10. *Show that the discriminant d_K of $K = \mathbb{Q}(\sqrt{d})$ is:*

(a) $d_K = 4d$ *if* $d \equiv 2, 3\, mod(4)$.
(b) $d_K = d$ *if* $d \equiv 1\, mod(4)$.

Proposition 5.11. *For any number field K we have $N(\mathcal{D}_K) = |d_K|$*

Proof. The norm $N(\mathcal{D}_K) = \#(\mathcal{O}_K/\mathcal{D}_K) = \#(\mathcal{O}_K^\vee/\mathcal{O}_K)$. We can choose a basis $\{a_1, \dots, a_n\}$ of $\mathcal{O}_K$ over $\mathbb{Z}$, together with a dual basis $\{a_i^\vee, \dots, a_n^\vee\}$ of $\mathcal{O}_K^\vee$ over $\mathbb{Z}$. By properties of dual basis, the elements a_j of the basis of $\mathcal{O}_K$ can be expressed as $a_j = \sum_i a_{i,j} a_i^\vee$, where $a_{i,j}$ is precisely $a_{i,j} = Tr(a_i a_j)$. The index $\#(\mathcal{O}_K^\vee/\mathcal{O}_K)$ is therefore the absolute value of the determinant of the matrix $(a_{ij}) = Tr(a_i a_j)$, in other words $|d_K|$. □

Theorem 5.12. *(Dedekind) The prime factors in $\mathcal{D}_K$ are the prime factors that ramify over $\mathbb{Q}$.*

Proof. For a prime $\mathfrak{p}/p$ we have $\mathcal{D}_K = \mathcal{D}_{\mathcal{O}_\mathfrak{p}/\mathcal{O}_p}$, where $\mathcal{O}_p$ and $\mathcal{O}_\mathfrak{p}$ denote the completions of the local ring respectively at p and $\mathfrak{p}$. We can therefore assume that $\mathcal{O}_K$ is a complete discrete valuation ring. In this situation however, we have $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and we can use exercise 5.6 to determine that if $\mathfrak{p}^s$ is the maximal power of $\mathfrak{p}$ dividing $\mathcal{D}_K$, then $s = \nu_\mathfrak{p}(f'(\alpha))$, where $f(T)$ is the minimal polynomial of α. If K is unramified, we have $\bar{\alpha} = \alpha \bmod \mathfrak{p}$ and $\mathfrak{p}$ is a simple zero of $f(T) = \bar{f}(T) \bmod \mathfrak{p}$. In this case $f'(\alpha) \in \mathcal{O}_K^*$ and $s = 0$. □

Corollary 5.13. *The prime factors of the discriminant d_K are the primes in $\mathbb{Q}$ that ramify in K.*

Proposition 5.14. *Let K be a number field and A an order in K. The volume of the fundamental domain $\mu(A)$ of the lattice $\sigma(A)$ given by the embedding $\sigma\colon K \longrightarrow \mathbb{R}^n$ where*

$$\sigma(a) = (\sigma_1(a), \dots, \sigma_{r_1}(a),\\ , Re(\sigma_{r_1+1}(a)), Im(\sigma_{r_1+1}(a)), \dots, Re(\sigma_{r_1+r_2}(a)), Im(\sigma_{r_1+r_2})(a))$$

is $\mu(A) = |d_A|^{1/2}2^{-r_2}$.

Proof. Consider a basis $\{a_1, a_2, \dots, a_n\}$ of A over $\mathbb{Z}$. If we denote the matrices $D = (\sigma_j(a_i))$ and $C = (\sigma(a_1), \sigma(a_2), \dots, \sigma(a_n))$. The two matrices are related by the equation $C^t = DE$ where E is almost diagonal, with diagonal entries equal 1 for the first r_1 diagonal entries and then r_2 diagonal blocks with the 2×2 matrix $\begin{pmatrix} 1/2 & 1/2i \\ 1/2 & -1/2i \end{pmatrix}$. Taking determinants we get

$$\mu(A) = |\det(C)| = |-\frac{1}{2i}|^{r_2}|\det(D)| = |d_A|^{1/2}2^{-r_2},$$

which is the identity we wanted to prove. □

Definition 5.15. *Let $K \subset K'$ be a finite extension of number fields, A an order of K and B the integral closure of A in K'. For an integral basis $\{b_1, \dots, b_n\} \subset B$ of K' over K, let us consider the discriminant with respect to that basis $d_{B/A}(\bar{b}) = \det(Tr(bibj))$. The* **relative discriminant** *$d_{B/A}$ is the ideal of A generated by $d(\bar{b})$, where $\{b_1, \dots, b_n\}$ is running over all integral basis of K' over K. For $A = \mathcal{O}_K$, we denote $d_{B/A}$ simply by $d_{K'/K}$.*

Remark 5.16. Let K'/K be a finite extension of number fields. The relative discriminant $d_{K'/K}$ is not always a principal ideal, on the other hand, for $K = \mathbb{Q}$, $d_{K'/\mathbb{Q}}$ is the principal ideal (d_K) generated by the discriminant of K.

Proposition 5.17. *In a tower of number fields $K \subset K' \subset L$ we have the identity of differents*

$$\mathcal{D}_{L/K} = \mathcal{D}_{K'/K}\mathcal{D}_{L/K'}$$

Proof. Consider $A = \mathcal{O}_K$ and the integral closures B and C in K' and L respectively. We are going to prove the equivalent statement for the co-different, namely

$$(C/A)^\vee = (C/B)^\vee(B/A)^\vee.$$

To prove the inclusion $(C/B)^\vee(B/A)^\vee \subset (C/A)^\vee$ we observe that

$$\begin{aligned} Tr_{L/K}((C/B)^\vee(B/A)^\vee C) &= Tr_{K'/K}Tr_{L/K'}((C/B)^\vee(B/A)^\vee C) \\ &= Tr_{K'/K}((B/A)^\vee Tr_{L/K'}(C/B)^\vee C) \subset A \end{aligned}$$

On the other hand $BC = C$, therefore

$$Tr_{L/K'}((C/A)^\vee C) = Tr_{L/K'}((C/A)^\vee BC) = Tr_{K'/K}(BTr_{L/K'}(C/A)^\vee C) \subset A$$

and we have $Tr_{L/K'}((C/A)^\vee C) \subset (B/A)^\vee$. As a consequence

$$((B/A)^\vee)^{-1}Tr_{L/K'}((C/A)^\vee C) = Tr_{L/K'}(((B/A)^\vee)^{-1}(C/A)^\vee C) \subset B$$

and then $((B/A)^\vee)^{-1}(C/A)^\vee \subset (C/B)^\vee$, which gives the reverse inclusion $(C/A)^\vee \subset (C/B)^\vee(B/A)^\vee$. □

Proposition 5.18. *(transitivity formula of the discriminant) Let K'/K be a finite extension of order n between number fields K and K'. Then $d_{K'} = (d_K)^n \operatorname{Norm}_{K'/K}(d_{K'/K})$.*

Proof. We consider the tower of field extensions $\mathbb{Q} \subset K \subset K'$ and apply the norm identity $\operatorname{Norm}_{K'} = \operatorname{Norm}_K \circ \operatorname{Norm}_{K'/K}$ to the relation between the differents $\mathcal{D}_{K'} = \mathcal{D}_{K'/K}\mathcal{D}_K$ to obtain

$$d_{K'} = \operatorname{Norm}_{K'/K}(d_{K'/K}) \operatorname{Norm}_K(\mathcal{D}_K^n) = d_K^n \operatorname{Norm}_{K'/K}(d_{K'/K}),$$

which is the relation wanted. □

6. The classic theorems of the algebraic number theory

We have introduced in the precedent chapters, the necessary information to understand the proofs of the principal theorems in algebraic number theory. The proofs presented however will not be the classical proofs.

6.1. Three technical lemmas.

The lemmas presented here have their exact parallel in the theory of "invertible fibre bundle" on projective curves.

Lemma 6.1. *Let $L \in \operatorname{Pic}_c(A)$ such that $\deg(L) < 0$. Then $H^0(L) = 0$.*

Proof. If $0 \neq s \in L$ is a non-zero element of L, we can compute the degree as $\deg(L) = \log \dfrac{\#(L/As)}{\prod_\sigma |s|_\sigma^{\epsilon_\sigma}}$. As the numerator $\#(L/As)$ is a positive integer, if $\prod_\sigma |s|_\sigma^{\epsilon_\sigma} \leq 1$ one has $\deg(L) > 0$. □

This lemma justify the "sign" that we have chosen for the degree. It will be a pity if, contrary to geometric analog, the existence of non-zero section would not force the degree to be positive or zero.

Lemma 6.2. *Let L be a compactified invertible A-module such that* $\deg(L) = 0$. *Then if $H^0(L) \neq 0$, L is equal to $A = (A, (1)_\sigma)$ as element of* $\mathrm{Pic}_c(A)$.

Proof. If $0 \neq s \in H^0(L)$ and $\deg(L) = 0$ then $\log \dfrac{\#(L/As)}{\prod_\sigma |s|_\sigma^{\epsilon_\sigma}} = 0$ then

(a) $L = As$
(b) $|s|_\sigma = 1$ for all σ

Condition (a) implies that L is the same as A as element of $\mathrm{Pic}(A)$. Condition (b) implies that the map $\varphi_s \colon A \longrightarrow L$ given by $\varphi_s(1) = s$ is an isometry. □

Definition 6.3. *Let us define a different normalization for the Euler characteristic* $\chi'(L) = \log \dfrac{2^{r_1}\pi^{r_2}}{2^n vol(L)}$.

Lemma 6.4. *(Minkowski) If $L \in$* $\mathrm{Pic}_c(A)$ *is such that* $\deg(L) \geq -\chi'(A)$ *then* $H^0(L) \neq 0$.

We observe that $\deg(L) \geq -\chi'(A)$ is equivalent using the global definition of degree 4.40 to $\chi'(L) \geq 0$. So we can express 6.4 in the form $\chi'(L) \geq 0 \Rightarrow H^0(L) \neq 0$. On the other hand we know that if d_A represents the discriminant of A over $\mathbb{Z}$.

$$-\chi'(A) = \log(|d_A|^{1/2}(\frac{2}{\pi})^{r_2}).$$

We find in this case the classic enunciate of Minkowski theorem on points on a lattice L in a compact symmetric convex domain B in $\mathbb{R}^n$ in the particular case of the unit ball: If B is the unit ball of $\oplus L \otimes K_\sigma \simeq \mathbb{R}^n$ and the volume $vol(B) > 2^n vol(L)$, then $L \cap B \neq \emptyset$.

Proof. (First Proof) The translations of $\mathbb{R}^n$ leave the Lebesgue measure invariant hence we have an induce measure on $\mathbb{R}^n/L$. If the map $\mathbb{R}^n \longrightarrow \mathbb{R}^n/L$ is injective one would have $vol(B) \leq vol(L)$. On the other hand if $vol(B) > 2^n vol(L)$ then the map $\frac{1}{2}B \longrightarrow \mathbb{R}^n/L$ is not injective and we will have $x \neq y \in B$ such that $\frac{1}{2}x - \frac{1}{2}y \in L$. Because B is symmetric $-y$ is also in B and by convexity of B, the linear combination $\frac{1}{2}x + \frac{1}{2}(-y) \in B$. □

Proof. (Second Proof) (Mordell) We have that the limit

$$\lim_{m\to\infty} 2^{-mn}(\#(2^m B \cap L)) = \frac{vol(B)}{vol(L)},$$

therefore if $vol(B) > 2^n vol(L)$ and m is sufficiently big, we will have $\#(2^m B \cap L) > 2^{n(m+1)}$. We note that $\#L/kL = k^n$ for all integers

k and deduce that the map $2^m B \cap L \longrightarrow L/2^{m+1}L$ is not injective. As a consequence there will be two points $x \neq y \in 2^m B$ such that $x - y \in 2^{m+1}L$. The element $\frac{1}{2}(\frac{x}{2^m}) - \frac{1}{2}(\frac{y}{2^m})$ is in $L \cap B$ by symmetry and convexity of B. $\square$

The two proofs above show the existence of $0 \neq s \in B \cap L$ in the case of the strict inequality $vol(B) > 2^n vol(L)$. Suppose that $vol(B) \geq 2^m vol(L)$ then, for all $\epsilon > 0$ we will have $vol((1+\epsilon)B) > 2^n vol(L)$ for all integer n. As a consequence we will have a sequence $0 \neq x_n \in (1+\frac{1}{n})B \cap L$. The x_n can be chosen to be in the finite set $2B \cap L$, which will give us a constant subsequence x_{n_i}. Putting $x = x_{n_i}$ we get $x \in L \cap (\cap(1+\frac{1}{n_i})B) = L \cap B$ because the sequence n_i is infinite.

6.2. **Finiteness of** $\mathrm{Pic}(A)$ **and simple connectness of** $\mathrm{Spec}(\mathbb{Z})$**.** We state here the finiteness theorem for the Picard group and the fact that orders in number fields must have a ramification locus.

Proposition 6.5. *Let A be an order on a number field. The Picard group* $\mathrm{Pic}(A)$ *is a finite group.*

Proof. Let $L \in \mathrm{Pic}(A)$. By choosing a non-zero element of L and picking a norm at infinity for each σ, we can have metric at infinity on L such that $\deg(L) = \chi'(A)$. By Minkowski (6.4), there will $0 \neq s \in L$ such that $|s|_\sigma \leq 1$ for all σ. Using the formula in 4.40, the ideal $\mathfrak{a}_s$ from 3.101 has then the property $\log N(\mathfrak{a}_s) \leq \chi'(A)$. By the second finiteness lemma (lemma 4.22), the set of ideals of norm bounded by $e^{-\chi'(A)}$ is a finite set. This last set is sent surjectively onto $\mathrm{Pic}(A)$ because $\mathfrak{a} \in \mathrm{Div}(A)$ and we have a surjective map $\mathrm{Div}(A) \longrightarrow \mathrm{Pic}(A)$ for any integral domain by proposition 3.100. $\square$

Proposition 6.6. *(Theorem of Hermite and Minkowski) Let K be a number field of degree $n \geq 2$ and let A be an order in K. Then the discriminant d_A of A is not equal to* ± 1.

Proof. Combining lemma 6.1 and lemma 6.4 we get that $-\chi'(A) \geq 0$ because $\deg\colon \mathrm{Pic}_c(A) \longrightarrow \mathbb{R}$ is surjective. We have then $|d_A|^{1/2}(\frac{2}{\pi})^{r_2} \geq 1$. This proves the result when $r_2 > 0$. We will prove now that $-\chi'(A) > 0$ as long as K is not an imaginary quadratic field. Suppose that $\chi'(A) = 0$, by 6.4 every element of $\mathrm{Pic}_c(A)$ of degree zero possess a non-zero section and will be equal to A as element of $\mathrm{Pic}_c(A)$. We are going to show that if $r_1 + r_2 - 1 > 0$, then there exist $(x_\sigma) \in \mathbb{R}_+^\Phi$ such that $(A, (x_\sigma))$ is not equal to A while $\deg(A, (x_\sigma)) = 0$. The element $(A, (x)_\sigma)$ equals A if and only if there exist a unit $u \in A^\times$ such that $x_\sigma = |\sigma(u)|$ for all σ. It will enough to prove that there exist $(x)_\sigma \in \mathbb{R}_+^\Phi$ such that $\prod x_\sigma^{\epsilon_\sigma} = 1$ and $(x_\sigma) \notin \sigma(A^\times)$ as long as $r_1 + r_2 - 1 > 0$. We have that $\sigma(A^\times)$ is discrete in $\mathbb{R}^\Phi$ by the first finiteness lemma. Taking logarithms of the coordinates, one has a vector space of dimension r_1+r_2-1 over $\mathbb{R}$ in which $\sigma(A^\times)$ is discrete. □

Remark 6.7. One has seen before that the set of prime divisors of the discriminant of a number field K is exactly the prime numbers that are ramified in K, i.e. the support of $\Omega^1_{\mathcal{O}_K/\mathbb{Z}}$. The statement of the theorem is saying that a morphism $\operatorname{Spec}(A) \longrightarrow \operatorname{Spec}(\mathbb{Z})$, where $\operatorname{Spec}(A)$ is connected cannot be non-ramified, i.e. $\operatorname{Spec}(\mathbb{Z})$ **is simply connected**. This result is similar to the fact that the projective line $\mathbb{P}^1_k$ over any field is simple connected. For morphisms onto $\operatorname{Spec}(\mathbb{Z})$ of fibres of higher dimension (for example of dimension one (fibres are curves)) or even abelian varieties, analogous results can be obtained.

6.3. Dirichlet Units theorem.

Let W be the hyperplane at infinity defined by the equation $\sum_\sigma \epsilon_\sigma x_\sigma = 0$. We will denote by

$$\log\sigma\colon A^\times \longrightarrow \mathbb{R}^{|\Phi|}$$

the map that sends a unit u to the vector with coordinates $(\log|\sigma(u)|)_{\sigma\in\Phi}$. The image of the map falls into W and by the first finiteness lemma (lemma 3.81), the image of $A^\times$ is discrete. We state precisely:

Proposition 6.8. *The subgroup* $\log\sigma(A^\times)$ *of* W *is a lattice.*

Corollary 6.9. *(Dirichlet units theorem) Let A be an order in a number field K, then the group of units contains a finite subgroup $\mu(A)$ made of roots of unit in A and the quotient $A/\mu(A)$ is a free group of rank r_1+r_2-1.*

Proof of 6.8: We will show that there are numbers $\alpha < \beta$ such that the application $[\alpha,\beta]^\Phi \cap W \longrightarrow W/\log\sigma(A^\times)$ is surjective. In this way $\log\sigma(A^\times)$ will be a compact for the quotient topology on $W \simeq \mathbb{R}^{r_1+r_2-1}$. If the rank of $\log\sigma(A^\times)$ were to be less than r_1+r_2-1 there will be a positive integer a such that $W/\log\sigma(A^\times)\otimes_{\mathbb{Z}}\mathbb{R} \simeq \mathbb{R}^a$ which is not compact.
Let us fix an element $L_0 = (A, x^0_\sigma) \in \operatorname{Pic}_c(A)$ of degree $-\chi'(A)$, or, in other words with $\prod (x^0_\sigma)^{\epsilon_\sigma} = e^{\chi'(A)}$. We know that the set of elements L of $\operatorname{Pic}_c(A)$ with underlying module A and of degree $\deg(L) = -\chi'(A)$ is the multiplicative translate of L_0 by the the group $\mathbb{R}^\Phi_{+,1}/\sigma(A^\times)$, where we have denoted by $\mathbb{R}^\Phi_{+,1}$ the set of elements $(y_\sigma)_{\sigma\in\Phi} \in \mathbb{R}^\Phi_+$ such that $\prod_\sigma y_\sigma^{\epsilon_\sigma} = 1$. Let $\{(a_1A), (a_2A), \ldots, (a_sA)\}$ be the finite set of non-zero principal ideals of of A with norm at most $e^{\chi'(A)}$. Let $(A, x_\sigma) \in \operatorname{Pic}_c(A)$ such that $\prod x_\sigma^{\epsilon_\sigma} = e^{\chi'(A)}$ $(\deg((A, x_\sigma)) = -\chi'(A))$, by Minkowski theorem there exist $0 \neq a_x \in A$ such that $|\sigma(a_x)|x_\sigma| \leq 1$, meaning that

$a_x \in H^0((A, x_\sigma))$. One has $e^{-\chi'(A)} = \deg(\deg((A, x_\sigma)) \geq N(a_x A)$. Therefore $(a_x A)$ is equal to one of the ideals $(a_i A)$ and we can find a unit u_x such that $a_x = u_x a_i$, which gives $|\sigma(u_x)| \leq \frac{1}{|\sigma(a_i)}$ for all places σ. Puttin $c_1 = \sup_{i,\sigma}\left(\frac{1}{|\sigma(a_i)|}\right)$ and $c_0 = e^{-\chi'(A)} c_1^{1-n}$, the element $(y_\sigma = |\sigma(u_x)| x_\sigma)_{\sigma\in\Phi}$ is in $[c_0, c_1]^\Phi$ due to $\prod_\sigma y_\sigma^{\epsilon_\sigma} = e^{-\chi'(A)}$. One notices that $c_1 \geq 1$ because the ideal $(1A)$ is of norm $\leq e^{-\chi'(A)}$. As elements of $\mathrm{Pic}_c(A)$ we have $(A, x_\sigma) = (A, y_\sigma)$ and the elements $\left(\frac{y_\sigma}{x_\sigma^0}\right)_{\sigma\in\Phi}$ are in $\mathbb{R}^\Phi_{+,1} \cap [\frac{c_0}{\sup_\sigma x_\sigma^0}, \frac{c_1}{\inf_\sigma x_\sigma^0}]^\Phi$. The map

$$\mathbb{R}^\Phi_{+,1} \cap [\frac{c_0}{\sup_\sigma x_\sigma^0}, \frac{c_1}{\inf_\sigma x_\sigma^0}]^\Phi \longrightarrow \mathbb{R}^\Phi_{+,1}/\sigma(A^\times)$$

is surjective. Putting $\alpha = \log \frac{c_0}{\sup_\sigma x_\sigma^0}$ and $\beta = \frac{c_1}{\inf_\sigma x_\sigma^0}$ and taking logarithms we observe that the canonical map $W \cap [\alpha, \beta]^\Phi \longrightarrow W/\log\sigma(A^\times)$ is surjective as well and $W/\log\sigma(A^\times)$ will be a compact set.

Exercise 6.10. *Find a generator $A^\times/\pm 1$ for the free $\mathbb{Z}$-module of rank one $A = \mathbb{Z}[\sqrt{2}]$. Relate your answer to the solution of Pell's equation $x^2 - 2y^2 = 1$.*

Exercise 6.11. *Describe the group of units $A^\times$ in the order $A = \mathbb{Z}[\sqrt{2}, \sqrt{3}]$ of $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.*

6.4. **Extensions with fixed ramification.** The aim of this part is to show that if one fixes the support of the discriminant and the degree of the number field K, then there are at most finitely many possible K. This results is close to a classical theorem of Riemann: There are at most finitely many finite covers of fixed degree of the sphere minus a given finite set of points.

Proposition 6.12. *Let K be a number field of degree n and A an order in K of discriminant d_A. Then $4d_A^2 \geq (\frac{\pi}{2})^n$.*

Proof. If we have r_2 complex places, we saw that $|d_A|^{1/2} \geq (\frac{\pi}{2})^{r_2}$ (because $-\chi(A)' \geq 0$). If $n = 2r_2$ (i.e. $r_1 = 0$) we obtained our proof already. On the other hand if $r_1 \neq 0$, the complex number i such that $i^2 = -1$ is not in K and we put $L = K(i)$ and $B = A[i]$. By the transitivity formula of the discriminant we have $d_B = d_A^2 \operatorname{Norm}(d_{B/A})$. The norm $\operatorname{Norm}(d_{B/A}) = 4$ and we can use the preceding case for the order B of L to get $4d_A^2 \geq (\frac{\pi}{2})^n$. □

Proposition 6.13. *(Theorem of Hermite) There is a a finite number of number fields with given discriminant.*

Proof. Let us consider the element $(A, (2^{1-r_1-r_2}e^{\chi'(A)}, 2, \ldots, 2)) \in \mathrm{Pic}_c(A)$ of degree precisely $-\chi'(A)$. There exist by Minkowski theorem an element $x \in A$ such that

$$|\sigma_1(x)| \leq 2^{r_1+r_2-1}e^{-\chi'(A)}$$
$$|\sigma_i(x)| \leq \frac{1}{2} \quad \forall i > 1$$

If $r_1 \neq 0$ and σ_1 is a real place, the element x is a primitive element of K. Otherwise there will be an index $i > 1$ with $\sigma_i(x) = \sigma_1(x)$, which is not possible because $|\sigma_i(x)| < 1$ for $i > 1$ and the product $\prod_j |\sigma_j(x)|^{\epsilon_j} = 1$. In this case then we have reduce the proof to the first finiteness lemma.
Now, if all places are complex places ($r_1 = 0$) then we know from the previous line that $\sigma_1(x) \neq \sigma_i(x)$ for $i > 1$ and therefore $\sigma_1(x) = \overline{\sigma_1(x)}$ and $[K : \mathbb{Q}(x)] = 2$. Again by the first finiteness lemma the fields $K_0 = \mathbb{Q}(x)$ belong to a finite list. If $K = K_0(i)$ for the root i of the equation $x^2 + 1 = 0$, the field K lies as well in a finite list of fields. On the other hand if $i \notin K$, we consider the extension $L = K(i)$ where $|d_L| \leq 4|d_K|^2$ because $d_{A[i]/A} = \mathrm{Norm}_{L/K}(2i)$ for $A = \mathcal{O}_K$. We repeat the way of thinking at the beginning, now for the field L, and we can find $y \in L$ integral over $\mathbb{Z}$ that is a primitive element of L over $\mathbb{Q}$ and with bounded absolute values of conjugates. If $L_0 = \mathbb{Q}(y)$ then $[L : L_0] = 2$. Then the element i is not in L_0 and $L = L_0(i)$. The fields $\mathbb{Q}(y)$ are in a finite list and so are the fields L. Because for each of these possibilities for L we have extension L/K such that $Aut(L/\mathbb{Q})$ is a finite group and K is the fixed field of an element in $Aut(L/\mathbb{Q})$, we have also a finite number of possibilities for K. □

7. Heights of rational points on a scheme over a number field

We are going to define the height of a rational point over K as the Arakelov degree of an associated element in $\mathrm{Pic}_c(\mathcal{O}_K)$. The interest of this presentation is that the functions obtained this way are well defined. We will present a few of their properties: Northcott theorem, and some counterexamples.

7.1. Invertible metrized fibre bundles on a scheme over $\mathbb{C}$.

If X is a scheme over $\mathbb{C}$ and $\mathcal{L}$ is an invertible sheaf on X, for every point $P \in X(\mathbb{C})$, the restriction $\mathcal{L}|_P$ is a vector space of dimension one over $\mathbb{C}$. We are going to extend to this global situation, our notions in 4.1.

Definition 7.1. *Let $f \colon X \longrightarrow \mathbb{C}$ an scheme over $\mathbb{C}$ and L an invertible sheaf on X. One says that $\mathcal{L}$ is* **metrized** *if:*

(a) *For all points $P \in X(\mathbb{C})$, the vector space $L|P$ is equipped with non-degenerate hermitian scalar product.*

(b) *For all opens sets $U \subset X$ and for all section $s \in \Gamma(U, \mathcal{L})$, the function $U(\mathbb{C}) \longrightarrow \mathbb{R}$ that to P associates $|s(P)|$ is continuous for the usual topology.*

Lemma 7.2. *Let X be a projective scheme over $\mathbb{C}$ and let $\mathcal{L}$ be an invertible sheaf on X. Then if $|.|_1$ and $|.|_2$ are two metrics on $\mathcal{L}$, there exist a constant C such that for all sections $s \in L$ on an open set U of X, $|s(P)|_1 \leq C|s(P)|_2$ for all $P \in U(\mathbb{C})$.*

Proof. Using proposition 4.2, for every point $P \in X(\mathbb{C})$ we have $|.|_1 = \lambda(P)|.|_2$ where $\lambda(P) \in \mathbb{R}_+^\times$ is a positive real number. When we choose a section on neighborhood of every $P \in X$, property (b) of metrized line bundles asserts that $\lambda\colon X(\mathbb{C}) \longrightarrow \mathbb{R}_+^\times$ is a continuous function for the usual topology on the projective scheme X over $\mathbb{C}$. The set $X(\mathbb{C})$ is compact because it is a closed set of $\mathbb{P}^n(\mathbb{C})$ which is compact for the usual topology (proper as scheme over Spec($\mathbb{C}$)) and therefore λ is bounded on $X(\mathbb{C})$. □

Example 7.3. Let n be an integer and $P = \mathbb{P}^n_{\mathbb{C}}$ the projective space of dimension n over $\mathbb{C}$. Let us put on $V = \Gamma(P, \mathcal{O}_P(1))$ a non-degenerated scalar product such that the $n+1$ canonical sections $x_0, \ldots, x_n$ form an orthonormal basis of V. The invertible sheaf $\mathcal{O}_P(1)$ being generated by those sections provides us with a surjective homomorphism of sheaf of $\mathcal{O}_P$-modules:

$$\varphi\colon \mathcal{O}_P \otimes_{\mathbb{C}} V \longrightarrow \mathcal{O}_P(1) \longrightarrow 0.$$

For each $Q \in P(\mathbb{C})$ one has also a surjective homomorphism $f = \varphi_Q\colon V \longrightarrow \mathcal{O}(1)|_Q \longrightarrow 0$ of vectors spaces over $\mathbb{C}$. One equips $\mathcal{O}_P(1)|_Q$ with the hermitian scalar product obtained when we say that $\mathcal{O}_P(1)|_Q$ is orthogonal to the kernel of φ_Q. In other words the length of an element of $\mathcal{O}_P(1)|_Q$ is the distance from its lift in V to the kernel of φ_Q. Let $s_0, \ldots, s_n$ an orthonormal basis of V, if x is a basis of $\mathcal{O}_P(1)|_Q$ over $\mathbb{C}$, the number x_i defined by $x_i e = \varphi_Q(s_i)$ are the homogeneous coordinates of the point Q. A unitary vector normal to the hyperplane $Ker(\varphi_Q)$ is then $\overrightarrow{n}_Q = \left(\frac{x_0}{(\sum_i |x_i|^2)^{1/2}}, \ldots, \frac{x_n}{(\sum_i |x_i|^2)^{1/2}}\right)$. To obtain the distance of $s = \sum_i \lambda_i s_i$ to this hyperplane, one does the scalar product $(s.\overrightarrow{n}_Q)$ and obtain the formula:

$$|\varphi_Q(s)| = |s(Q)| = \frac{|\sum_i \lambda_i s_i|}{(\sum_i |x_i|^2)^{1/2}},$$

which is a continuous function on $\mathbb{P}^n(\mathbb{C})$.

Definition 7.4. *A metric $\|.\|$ on $\mathcal{L}$ will be called smooth if for every local section s, the function $\|s(.)\|^2$ is smooth. Given a smooth metric $\|.\|$ and a local section s of $\mathcal{L}$ on an open set U of X_σ, the first Chern form of $(\mathcal{L}, \|.\|)$ is defined as the $(1,1)$-form*

$$c_1(\mathcal{L}, \|.\|) = \partial\bar{\partial} \log \|s\|_v^2.$$

It does not depend on our choice of local section and can be extended to a closed global form on X.

Definition 7.5. *Let $(\mathcal{L}, \|.\|)$ be a smooth metrized line bundle on X and $\mathbb{D} = \{z \in \mathbb{C} \,|\, |z| \leq 1\}$. We say that $(\mathcal{L}, \|.\|)$ is semipositive if, for any holomorphic map $\varphi \colon \mathbb{D} \longrightarrow X^{an}$*

$$\frac{1}{2\phi i} \int_{\mathbb{D}} \varphi^* c_1(\mathcal{L}, \|.\|) \geq 0.$$

Example 7.6. The Fubini-Study is a smooth semi-positive metric on $\mathbb{P}^n(\mathbb{C})$ because the first Chern form is positive.

7.2. **Integral models of schemes over a field.** There are several ways to clear out the denominators in the equations defining a scheme over a field. There are also several ways to write a projective scheme as a closed set of a projective space $\mathbb{P}^n_K$ or an affine space $\mathbb{A}^n_K$. The notion of model will take care of that phenomenon.

Definition 7.7. *Let A be an integral domain and K the field of fractions. If $X_K \xrightarrow{f} \operatorname{Spec}(K)$ is a K-scheme, one calls* **model of f over A**, *to an A-scheme $X \xrightarrow{g} \operatorname{Spec}(A)$ such that $g \times_A \operatorname{Spec}(K) = f$. A model of f over A is also called* **a model of X_K over A**. *A* **model is flat** *if $X \xrightarrow{g} \operatorname{Spec}(A)$ is flat. A* **model is proper** *if $X \xrightarrow{g} \operatorname{Spec}(A)$ is proper.*

Example 7.8. $\mathbb{P}^n_A$ is a model of $\mathbb{P}^n_K$ over A. This is not the only projective model of $\mathbb{P}^n_K$. Indeed the blow-up of a closed subscheme $Y \subset \mathbb{P}^n_A$ such that $Y \times_{\operatorname{Spec}(A)} \operatorname{Spec}(K)$ is empty is another model of $\mathbb{P}^n_K$.

Example 7.9. (Clearing out denominators) If X_K is a closed subscheme of $\mathbb{P}^n_K$ defined by homogeneous equations $F_i(X_0, \ldots, X_n) = 0$ with coefficients in K we can multiply all equations by an element of A to have equations defined over A and therefore a model of X_K over A as a closed subscheme of $\mathbb{P}^n_A$. In the same way we can find a model of the line bundle $\mathcal{O}_{X_K}(1)$ over $\operatorname{Spec}(A)$.

Definition 7.10. *Let A be an integral domain, K its fraction field and $X \xrightarrow{f} \operatorname{Spec}(A)$ an A-scheme. If $\mathcal{F}_K$ is a sheaf of $\mathcal{O}_{X_K}$-modules on X_K one calls model of $\mathcal{F}_K$ over A to a sheaf $\mathcal{F}$ of $\mathcal{O}_X$-modules such that*

$\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_{X_K} = \mathcal{F}_K$. A model of the pair $(X_K, \mathcal{F}_K)$, where X_K is a K-scheme and $\mathcal{F}_K$ is a sheaf of $\mathcal{O}_{X_K}$-modules is a pair $(X, \mathcal{F})$, where X is a model of X_K over Spec(A) *and $\mathcal{F}$ is a model of $\mathcal{F}_K$ over A.*

7.3. **Heights associated to metrized line bundles.** Let K be a number field and X a proper variety over K. To build heights we need a integral structure on $\mathcal{O}_K$ and hermitian metrics at places over infinity. Let $\tilde{X}$ a proper model of X over $\mathrm{Spec}(\mathcal{O}_K)$, L a line bundle on X with extension $\tilde{L}$ on $\tilde{X}$. We are going to assume that L_σ on X_σ is equipped of a hermitian metric $|.|_\sigma$ for every place σ at infinity. Let $P \in X(K)$ be a point of X over K. By the valuative criterion of properness, the point corresponds bijectively to a section ε_P of $f\colon \tilde{X} \longrightarrow \mathrm{Spec}(\mathcal{O}_K)$. The invertible sheaf $\varepsilon_P^*(\tilde{L}) = \varepsilon_P^*(\tilde{L}, |.|_\sigma)$ on $\mathcal{O}_K$ is in $\mathrm{Pic}_c(\mathcal{O}_K)$ and we can define its degree.

Definition 7.11. *With notation as in the previous paragraph, the height $h_L = h_{L,|.|_\sigma}$ of P associated to $(L, |.|_\sigma)$ is defined as*

$$h_L(P) = h_{L,|.|_\sigma}(P) = \frac{1}{[K(P) : \mathbb{Q}]} \deg \varepsilon_P^* \tilde{L}.$$

Example 7.12. (usual or naive height) Fix generators $X_0, \dots, X_r$ of the global sections of the line bundle $\mathcal{O}_{\mathbb{P}^r}(1)$ on $\mathbb{P}^r_{\mathbb{Z}}$. Let σ be a place at infinity. Let us define the usual metric on $\mathcal{O}_{\mathbb{P}^r}(1) \otimes_\sigma \mathbb{C}$ by the condition that for each section $s = \sum_i \lambda_1 X_i$ and each point $P = (x_0, \dots, x_n) \in \mathbb{P}^r(K)$,

$$\|s(P)\|_\sigma = \frac{|\sum_i \lambda_i x_i|}{\max_i\{|x_i|\}}.$$

The associated height will be called the naive or usual height on $\mathbb{P}^n_K$.

Exercise 7.13. *Check that the naive height of $P = (x_0, \dots, x_n)$ can be obtained as*

$$h(P) = h_n(P) = \frac{1}{[K : \mathbb{Q}]} \log \frac{\prod_\sigma \sup_i |\sigma(x_i)|^{\epsilon_\sigma}}{N(\sum x_i \mathcal{O}_K)}.$$

Exercise 7.14. *Show that the naive height of $P = (x_0, \dots, x_n)$ can be given by the formula*

$$h(P) = \frac{1}{[K : \mathbb{Q}]} \sum_v \log(\max(|x_0|_v, \dots |x_n|_v)),$$

where $|.|_v$ is running over all normalized absolute values on K.

Example 7.15. (Fubini-Study height) Let $P = (X_0, \dots, X_r) \in \mathbb{P}^r$ and suppose that we equip $\mathcal{O}_{\mathbb{P}^r}(1)$ with the metric of Fubini-Study, where

$$\|s(P)\|^2 = \frac{|\sum_i \lambda_i x_i|^2}{\sum_i |x_i|^2},$$

for $s = \sum \lambda_i x_i \in H^0(\mathbb{P}^r, \mathcal{O}_{\mathbb{P}^r}(1))$. The associated height will be called the Fubini-Study height h_{FS} on $\mathbb{P}^r$.

Exercise 7.16. *Check that the Fubini-Study height can be given by the formula:*

$$h_{FS}(P) = \frac{1}{[K:\mathbb{Q}]} \log \frac{\prod_\sigma (\sum_i x_i^2)^{(\epsilon_\sigma/2)}}{N(\sum_i \mathcal{O}_K x_i)}.$$

Exercise 7.17. *Show that the Fubini-Study differs from the naive usual height by a bounded amount by proving the formula:*

$$h_{FS}(P) = \frac{1}{[K:\mathbb{Q}]} \left(\sum_{v \textit{ finite}} \log \max_i |X_i(P)|_v + \sum_\sigma \frac{\epsilon_\sigma}{2} \log(\sum_i X_i^2(P)) \right).$$

Exercise 7.18. *Prove that the height $h_L(P)$ is independent of the base field K.*

Exercise 7.19. *Prove that for every integer $m > 0$ we have $h_{L^m}(P) = m h_L(P)$.*

Lemma 7.20. *If $|.|'_\sigma$ and $|.|_\sigma$ are two sets of metrics on L, there exist a constant C such that*

$$|h_{L,|.|}(P) - h_{L,|.|'}| < C.$$

Proof. Let $\sigma \colon K \longrightarrow \mathbb{C}$ be a place at infinity for K. On the compact space X_σ, we have a continuous function φ_σ such that $|.|_\sigma = \varphi_\sigma |.|'_\sigma$. The function φ_σ is bounded in X_σ and we can take $C = \sup_{P \in X_\sigma} \varphi_\sigma(P)$. On the other hand if K' is an extension of K and $\rho \colon K' \longrightarrow \mathbb{C}$ is a place at infinity extending σ, we have $\sup_{P \in X_\rho} \varphi_\rho = \sup_{P \in X_\sigma} \varphi_\sigma = C$. □

Lemma 7.21. *If $(\tilde{X}, \tilde{L})$ and $(\tilde{X}', \tilde{L}')$ are integral models of (X, L), there exist a constant C such that for all $P \in X(\bar{K})$ we have*

$$|h_{L'}(P) - h_L(P)| < C.$$

Proof. If we have two extensions $\tilde{L}$ and $\tilde{L}'$ over the same model $\tilde{X}$, we will have a vertical divisor E of $\mathrm{Div}(\tilde{X})$ with $\tilde{L} = \tilde{L}' \otimes \mathcal{O}(E)$. The metric on $\mathcal{O}(E)$ will be trivial for every place σ at infinity and the degree of the line bundle $\mathcal{O}(E)$ will be bounded by a constant C, i.e. $\deg(\mathcal{O}(E)) < C$. For the general case, we consider the fibre product $\tilde{X} \times \tilde{X}'$ to reduce the question to the case of a birrational morphism $\pi \colon \tilde{X}' \longrightarrow \tilde{X}$ such that π is the identity on the generic fibre and $\tilde{L}' = \pi^* \tilde{L}$ as metrized line bundles. In this last case we have a commutative diagram

$$\begin{tikzcd}
\operatorname{Spec}\mathcal{O}_K \arrow[r, "\varepsilon'_P"] \arrow[d, "|"] & \tilde{X}' \arrow[d, "\pi"] \\
\operatorname{Spec}\mathcal{O}_K \arrow[r, "\varepsilon_P"] & \tilde{X}
\end{tikzcd}$$

and $h_{\tilde{X}',\tilde{L}'}(P) = h_{\tilde{X},\tilde{L}}(P)$ for all $P \in X(\bar{K})$. □

Remark 7.22. If a map $\varphi\colon \mathbb{P}^r \longrightarrow \mathbb{P}^l$ is given by homogeneous polynomials $\varphi_0, \dots, \varphi_l$ of degree m in the variables $X_0, \dots, X_r$ and if P is a point in $\mathbb{P}^r$ where φ_i are not simultaneously zero, one has the following comparison between the naive heights on $\mathbb{P}^r$ and $\mathbb{P}^l$:

$$h(\varphi(P)) \leq mh(P) + h(\varphi),$$

where $h(\varphi) = \log(N) + \sum_\sigma \log\sup|\text{coefficients of } \varphi_i|$ and N is the maximum number of monomials in φ_i.

Theorem 7.23. *(Northcott) Let $f\colon \tilde{X} \longrightarrow \operatorname{Spec}(\mathcal{O}_K)$ a projective variety over $\mathcal{O}_K$ and $\tilde{L}$ a line bundle on $\tilde{X}$ such that $L = \tilde{L} \otimes K$ is ample and L_σ is equipped with a non-trivial hermitian metric for each σ. Then:*

1. *There exist a constant C such that $h_L(P) \geq C$ for all $P \in X(\bar{K})$.*
2. *For each real number A and each integer d, the set of points of $X(\bar{K})$ defined over a field of degree at most d over $\mathbb{Q}$ and of height h_L at most A, is a finite set.*

Proof. (1) The line bundle L is ample and therefore $L^{\otimes m}$ is very ample for some power $m > 0$. We have a map $\varphi\colon X \longrightarrow \mathbb{P}^N$ into some projective space $\mathbb{P}^n$ such that $L^m = \varphi^*\mathcal{O}(1)$. As a consequence of lemma 7.20, for some positive constant C' independent of the point $P \in X(K)$ we have

$$-C' < mh_{L,|.|}(P) - h(P) < C'.$$

Using that the naive height $h(P) \geq 0$, we get $h_L(P) \geq C$ for $C = -C'/m$.

(2) Consider the set $E_{r,d}$ of rational points of $\mathbb{P}^r$ over a field K with $[K : \mathbb{Q}] = d$. Let $\sigma\colon E_{r,d} \longrightarrow (\mathbb{P}^r(\mathbb{Q}))^d$ be the map associating to any $P \in E_{r,d}$ the point $(\sigma_i(P))_{1 \leq i \leq d}$ consisting of all conjugates. Let $X_{d,r}$ be the quotient of $\mathbb{P}^r \times \cdots \times \mathbb{P}^r$ by the action of the symmetric group S_d and denote by $q\colon \mathbb{P}^r \times \cdots \times \mathbb{P}^r \longrightarrow X_{d,r}$ the quotient map. We observe that the map $q \circ \sigma\colon E_{r,d} \longrightarrow X_{r,d}$ is well defined whenever $P \in X(K)$ and $[K : \mathbb{Q}] \leq d$. On the hand the assertion of part (2) is true for $d = 1$ and the naive height h. If will be enough to verify that one has a height

$h' = h_{L'}$ on $X_{r,d}$, where L' is ample, such that for certain constants C and m (m a natural number)

$$h'(q \circ \sigma(P)) \leq mh(P) + C,$$

is true for all $P \in E_{r,d}$. The conclusion of the theorem will be obtained when we embed $X_{r,d}$ in a projective space using homogeneous polynomials invariants under the action of S_d and use remark 7.22. □

References

[AtiM69] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Westview Press, (1969).

[Har77] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, Graduate Texts in Mathematics, vol. **52**, New York, (1977).

[Mum99] D. Mumford, *The red book of Varieties and Schemes*, Second expanded edition. Lectures Notes in Mathematics **1358**, (1999).

[Serr79] J. P. Serre, *Local fields*, Lectures Notes in Mathematics **67**, (1979).

[Szp82] L. Szpiro, *Cours de géométrie arithmétique*, Orsay preprint available at https://www.gc.cuny.edu/Page-Elements/Academics-Research-Centers-Initiatives/Doctoral-Programs/Mathematics/Faculty/Lucien-Szpiro.

[Zhang95] S. Zhang, *Small points and adelic metrics*, J. Algebraic Geometry **4** (1995), 281–300.