COURS DE GÉOMÉTRIE ARITHMÉTIQUE

Lucien SZPIRO

I – Le groupe de Picard

1 – Produit tensoriel et localisation.
2 – Schémas et schémas projectifs.
3 – Modules projectifs.
4 – Modules inversibles.
5 – Faisceaux inversibles sur les schémas.

II – Anneaux de dimension un

0 – Anneaux noethériens de dimension zéro.
1 – Anneaux principaux.
2 – Eléments entiers.
3 – Extensions algébriques de corps.
4 – Corps de nombres, ordre d'un corps de nombres, anneaux d'entiers algébriques.
5 – Anneaux de valuation discrète, anneaux de Dedekind.
6 – L'application cycle.
7 – L'application Div(A) $\to$ Pic(A).
8 – Points rationnels d'un schéma projectif sur un anneau de Dedekind.

III – Le groupe de Picard compactifié d'un ordre d'un corps de nombres

1 – Espaces vectoriels de dimension un sur $\mathbb{C}$.
2 – Le groupe de Picard compactifié.
3 – La norme d'un idéal.
4 – La norme d'un élément, formule du produit.
5 – La définition locale du degré sur $\mathrm{Pic}_c(A)$.
6 – Volume, définition globale du degré.
7 – Sections d'un module inversible compactifié, théorème de Riemann-Roch.

IV – Discriminant, différente, conducteur

V – Les théorèmes classiques de la théorie des nombres algébriques

1 – Trois lemmes techniques.
2 – Finitude de Pic(A) et simple connexité de $\mathrm{Spec}\,\mathbb{Z}$.
3 – Le théorème des unités de Dirichlet.
4 – Extensions à ramification donnée.

VI – Hauteur des points rationnels d'un schéma sur un corps de nombres

1 – Fibrés inversibles métrisés sur un schéma sur $\mathbb{C}$.
2 – Modèles entiers des schémas sur un corps.

II – Anneaux de dimension un

La **dimension** d'un anneau est le maximum des chaînes d'idéaux premiers contenus l'un dans l'autre. Par exemple $\mathbb{Z}$ est un anneau de dimension un.

Nous explicitons dans ce chapitre les anneaux fondamentaux de la géométrie arithmétique en dimension un : les anneaux d'entiers algébriques et les anneaux de fonctions algébriques sur une courbe affine.

0 – Anneaux noethériens de dimension zéro.

Pour faciliter l'étude des anneaux de dimension un nous établissons d'abord quelques faits en dimension 0.

Remarque 0.1. — Soit A un anneau intègre de dimension un et soit f un élément non nul de A, alors A/fA est de dimension zéro. En effet les seuls idéaux premiers de A sont (0) et les idéaux maximaux.

Remarque 0.2. — Soit A un anneau et soit M un **A-module simple** (i.e. un A-module **non nul** qui ne contient pas de sous-A-module propre), alors il existe un idéal maximal $\mathfrak{m}$ de A tel que $M \simeq A/\mathfrak{m}$. En effet si x est non nul dans M, x engendre M sur A donc $M \simeq A/I$ pour un idéal $I \cdots$

Proposition 0.3 (théorème de Jordan-Hölder). — *Soient A un anneau et M un A-module. Soient $(0) = M_0 \subset M_1 \subset \cdots \subset M_{n-1} \subset M_n = M$ et $(0) = M'_0 \subset M'_1 \subset \cdots \subset M'_0 = M$ deux filtrations finies de M telles que les quotients successifs M_{i+1}/M_i et M'_{j+1}/M'_j soient des A-modules simples. Alors $n = q$. De plus, il existe une permutation σ de $\{1, 2, \ldots, n\}$ telle que $M_i/M_{i-1} \simeq M'_{\sigma(i)}/M'_{\sigma(i)-1}$.*

Une filtration finie $(0) = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_n = M$ est dite de **longueur n**. Nous allons montrer par récurrence sur n qu'on a $q \leq n$. Les rôles de q et n étant les mêmes on aura ainsi la première partie de l'énoncé. Soit r le plus petit entier tel que $M'_r \supset M_1$. On a la filtration suivante dont au plus un des quotients successifs est nul, les autres étant simples :

$$(0) = M'_0 \subset M'_1 \subset \cdots \subset M'_{r-1} \subseteq M'_r/M_1 \subset M'_{r+1}/M_1 \subset \cdots \subset M'_q/M_1 = M/M_1 \ .$$

Le module M/M_1 ayant une filtration à quotients successifs simples, de longueur $n-1$, par récurrence on a $q \leq n-1$ ou $q-1 \leq n-1$ en tout cas $q \leq n$. □

Il nous reste à montrer qu'à l'ordre près les quotients successifs sont les mêmes. Soit $\mathfrak{m}$ un idéal maximal de A, si M est un A-module possédant une filtration comme dans l'énoncé, $M_\mathfrak{m}$ est un $A_\mathfrak{m}$ -module de longueur finie. En fait la filtration $(0) = M_0 \subset \cdots \subset M_i \subset \cdots \subset M_n = M$ tensorisée par $A_\mathfrak{m}$ donne une filtration de $M_\mathfrak{m}$ (I 1.7 b)). Les quotients successifs sont nuls s'ils sont isomorphes à $A/\mathfrak{m}'$ où $\mathfrak{m}'$ est un idéal maximal différent de $\mathfrak{m}$. Les quotients successifs isomorphes à $A/\mathfrak{m} = A\mathfrak{m}/\mathfrak{m}A_\mathfrak{m}$ restent inchangés. Appliquant la première partie de l'énoncé au $A_\mathfrak{m}$-module $M_\mathfrak{m}$, la deuxième partie de l'énoncé est prouvée.

La proposition 0.3 justifie la définition suivante.

Définition 0.4. — *Soient A un anneau et M un A-module. On dit que M est de* **longueur n** *s'il possède une filtration finie de longueur n dont les quotients successifs sont simples.*

Corollaire 0.5. — *Sur la catégorie des A-modules de longueur finie – la longuer – est une fonction additive. Un module est de longueur nulle si et seulement si il est lui-même nul.*

Les modules de longueur finie ont des propriétés bien spéciales, nous en montrons quelques-unes ci-dessous.

Corollaire 0.6. — *Soit M un module de longueur finie sur un anneau A. Soient $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ l'ensemble fini d'idéaux maximaux de A tels que $M_{\mathfrak{m}_i} \neq 0$. Alors l'application canonique :*

$$M \to \prod_{i=1}^{r} M_{\mathfrak{m}_i}$$

est un isomorphisme.

Ces deux modules sont de longueur finie comme A-modules car $(A/\mathfrak{m}_i)_{\mathfrak{m}_i} = A/\mathfrak{m}_i$ et $(A/\mathfrak{m}_i)_{\mathfrak{m}_j} = 0$ pour $j \neq i$. Par le corollaire 0.5 il nous suffit de montrer que l'application considérée est injective. Ce dernier point est clair car si x n'est pas nul x a une image non nulle dans au moins un localisé $M_{\mathfrak{m}_i}$ par I 1.7 e).

Corollaire 0.7. — *Soit A un anneau de longueur finie alors* $\mathrm{Pic}(A) = 0$.

Soit L un A-module inversible, si $\mathfrak{m}$ est un idéal maximal de A, $L_{\mathfrak{m}}$ est isomorphe à $A_{\mathfrak{m}}$ (I 3.9). Donc on a par 0.6

$$L \simeq \prod L_{\mathfrak{m}} \simeq \prod A_{\mathfrak{m}} \simeq A \ .$$

□

Remarquons que toute suite décroissante de sous-A-modules d'un A-module de longueur finie est stationnaire en vertu de 0.5. Cette propriété s'étudie pour elle-même.

Définition 0.8. — *Soient A un anneau et M un A-module, on dit que M est un* **A-module artinien** *si toute famille non vide de sous-A-modules de M possède un élément minimal pour l'inclusion. Si A lui-même est un A-module artinien on dit que A est un* **anneau artinien**.

Par le lemme de Zorn, M est artinien si et seulement si toute chaîne décroissante de sous-A-modules est stationnaire.

Exemple 0.9 : Soient A un anneau local $\mathfrak{m}$ son idéal maximal. Supposons que $\mathfrak{m}$ soit un A-module de type fini. Alors, pour tout entier n, l'anneau $A/\mathfrak{m}^n$ est artinien. En effet les $\mathfrak{m}^i/\mathfrak{m}^{n+1} \quad i \leq n-1$ donnent une filtration de $A/\mathfrak{m}^n$ dont les quotient successifs sont des espaces vectoriels de dimension finie sur $A/\mathfrak{m}$.

Exercice 0.10 : Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte de A-modules. Montrer que M est artinien si et seulement si M' et M'' le sont. Vérifier le même énoncé où "artinien" est remplacé par "de longueur finie".

Lemme 0.11. — *Soit A un anneau noethérien et soit M un A-module. Alors il existe un élément x non nul de M tel que son annulateur soit un idéal premier de A.*

Soit I un idéal maximal parmi ceux qui sont des annulateurs d'éléments non nuls de M. Alors $I \neq A$ sinon l'élément qu'il annule serait nul. Montrons que I est premier. Si a et b sont dans A, $abx = 0$ et $ax \neq 0$ alors $b \in \mathrm{ann}(bx) \supset I$, donc $b \in I$.

Corollaire 0.12. — *Soient A un anneau noethérien et M un A-module de type fini. Alors M possède une filtration finie $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ telle que M_{i+1}/M_i soit isomorphe à $A/\mathfrak{p}_i$ où $\mathfrak{p}_i$ est un idéal premier de A.*

Puisque M est noethérien, choisissons M' un sous-A-module maximal parmi ceux ayant une filtration telle que celle de l'énoncé. Le lemme 0.11 appliqué à M/M' montre que $M = M'$.

Proposition 0.13. — *Soit A un anneau. Les propositions suivantes sont équivalentes :*

(i) *A est un anneau noethérien de dimension zéro*

(ii) *A est de longueur finie*

(iii) *A est un anneau artinien.*

Il est clair que (ii) implique (i) et que (ii) implique (iii).

Sous les hypothèses de 0.13 (i) les idéaux premiers de A sont maximaux, et par 0.12 A est de longueur finie. Nous avons donc montré que (i) implique (ii).

Exercice 0.14 : Montrer que 0.13 (iii) implique 0.13 (ii)

Proposition 0.15. — *Soit A un anneau noethérien de dimension 1. Alors si f est un élément de A non contenu dans les idéaux premiers $\mathfrak{p}$ de A tels que $\dim A/\mathfrak{p} = 1$ le groupe $\mathrm{Pic}(A/fA)$ est nul.*

Par le corollaire 0.7 et la proposition 0.13 il nous suffit de montrer que $\dim A/fA = 0$. C'est clair par l'hypothèse sur les idéaux premiers contenant f.

Exemple 0.16 : Soit A un anneau noethérien intègre de dimension un et soit f un élément non nul de A alors, $\mathrm{Pic}(A/fA) = 0$.

Exercice 0.17 : Soit A un anneau **noethérien** et soit $\mathfrak{p}$ un idéal premier minimal de A.

a) Montrer que $A_{\mathfrak{p}}$ est artinien.

b) Montrer que dans une filtration de A comme celle considérée en 0.12, il existe toujours un quotient M_{i+1}/M_i qui soit isomorphe à $A/\mathfrak{p}$.

c) Montrer qu'il existe un élément x de A tel que annulateur$(x) = \mathfrak{p}$. (On pourra par exemple utiliser 0.14 dans $A_{\mathfrak{p}}$).

d) Montrer que **l'ensemble des idéaux premiers minimaux de A est fini**.

1 – Anneaux principaux.

Un anneau est dit **principal** s'il est intègre et si tout idéal est principal. Dans un anneau principal tout élément irréductible non inversible – i.e. non trivialement divisible – engendre un idéal premier.

Exercice 1.1 : Démontrer que $\mathbb{Z}$ et $k[X]$ (k un corps) sont des anneaux principaux. On notera les rôles similaires tenus par la "valeur absolue" et le "degré".

La proposition 1.2 qui suit est classique et se trouve dans tous les livres d'algèbre.

Proposition 1.2 (théorème des diviseurs élémentaires). — *Soit A un anneau principal. Soit M un A-module libre de rang n et soit M' un sous A-module de M. Alors il existe une base $e_1, \ldots, e_n$ de M, des éléments a_i de A tels que a_i divise a_{i+1}, tels que M' soit libre, que la suite des $(a_i e_i)$ qui sont non nuls forment une base de M'.*

Définition 1.3. — *Soit A un anneau intègre, un A-module M est dit* **sans torsion** *si un élément non nul de M n'est annulé que par zéro.*

Exemples 1.4 :

a) Un sous-module d'un A-module sans torsion est sans torsion.

b) Si M est un A-module alors $M^\vee$ est sans torsion car contenu dans $A^{(I)}$.

Lemme 1.5. — *Soit A un anneau intègre et noethérien et soit M un A-module de type fini sans torsion, alors l'homomorphisme canonique $M \to M^{\vee\vee}$ est injectif.*

On a le diagramme commutatif suivant :

$$M \longrightarrow M \otimes K \downarrow\downarrow M^{\vee\vee} \longrightarrow M^{\vee\vee} \otimes K$$

où toutes les flèches sont naturelles. Dire que M est sans torsion c'est exactement dire que $M \to M \otimes K$ est injectif. L'anneau A étant noethérien $M^\vee$ et $M^{\vee\vee}$ sont de type fini quand M l'est, il est alors clair que

$$M \otimes K \to M^{\vee\vee} \otimes K$$

est un isomorphisme car $(M^{\vee\vee} \otimes K)$ est isomorphe à $(M \otimes K)^{\vee\vee}$ (exercice). On en déduit que $M \to M^{\vee\vee}$ est injectif.

Note 1.6. Quand A n'est pas intègre on prend le lemme 1.5 comme "définition" de "sans torsion".

Corollaire 1.7. — *Soit A un anneau principal. Tout A-module de type fini sans torsion est libre. Pour tout A-homomorphisme de A-modules libres de rang fini $\varphi : M' \to M$ il existe des bases de M' et de M telles que φ soit diagonal.*

Un A-module qui est le dual d'un module de type fini est un sous-A-module d'un module libre de rang fini. Le lemme 1.5 et le théorème 1.2 impliquent donc la première

partie de l'énoncé du corollaire 1.7. Notons que sur un anneau principal si $\varphi : M \to A$ est une forme linéaire non nulle, alors il existe un facteur direct libre de rang 1 dans M. En effet $\mathrm{Im}\varphi = Ax$, $x \neq 0$. L'application surjective $M \to Ax$ se scinde puisque Ax est libre quand A est intègre. Par récurrence sur l'entier $\mathrm{rang}_K\ (M \otimes_A K)$ on a ainsi une démonstration de M sans torsion de type fini, alors M libre car, par le lemme 15, $M^\vee \neq 0$ si $M \neq 0$. Si $\varphi : M' \to M$ alors $\mathrm{Im}\varphi$ et $\mathrm{Ker}\,\varphi$ sont des sous-modules de modules libres appliquant 1.2 on a 1.7.

Corollaire 1.8. — *Soit G un sous-groupe fini du groupe des éléments non nuls d'un corps k. Alors G est cyclique.*

Le groupe G étant fini et commutatif il existe un entier n et une suite exacte :

$$0 \to \mathrm{Ker}\,\varphi \to \mathbb{Z}^n \to G \to 0\ .$$

Par la proposition 1.2 on peut donc écrire $G = \overset{n}{\oplus}\ \mathbb{Z}/a_i\mathbb{Z}$ où aucun des a_i n'est nul puisque G est fini. Si a est le pgcd des a_i il est facile de voir que a annule G, et que d'autre part l'élément $(1, 1, \ldots, 1)$ de $\overset{n}{\underset{i=1}{\oplus}}\ \mathbb{Z}/a_i\mathbb{Z}$ est d'ordre exactement a. L'équation $x^a = 1$ n'a que a solutions dans k, donc G est d'ordre au plus a. On en déduit que $(1, 1, \ldots, 1)$ engendre G (et que $n = 1$). □

Le corollaire suivant montre l'existence d'éléments primitifs pour les extensions de corps finis.

Corollaire 1.9. — *Soit k un corps fini de cararactéristique p, alors k est engendré par un élément comme algèbre sur le corps premier $\mathbb{F}_p$.*

Corollaire 1.10. — *Soit G un sous-groupe discret de $\mathbb{R}^n$, alors G est un $\mathbb{Z}$-module libre de rang au plus n. De plus une base de G sur $\mathbb{Z}$ est formée d'éléments linéairement indépendants sur $\mathbb{R}$.*

Démonstration : Soit r le cardinal maximum des ensembles d'éléments de G qui soient linéairement indépendants sur $\mathbb{R}$. Soient $x_1, \ldots, x_r, r$ éléments de G linéairement indépendants, et soit

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

Pour tout élément x de G il existe un ensemble fini de nombres réels λ_i tels que $x = \Sigma\lambda_i x_i$. Si $[\lambda]$ désigne la partie entière de λ on a : $x = \Sigma[\lambda_i]x_i + \Sigma(\lambda_i - [\lambda_i])x_i$. Donc $D \cap G$, qui est fini puisque G est discret, engendre G sur $\mathbb{Z}$. Le $\mathbb{Z}$-module G est donc de type fini et sans torsion, c'est donc un $\mathbb{Z}$-module libre. Son rang est au moins r. Il est au plus r car nous allons montrer qu'il existe $d \in \mathbb{Z}$, d non nul tel que dG soit dans le $\mathbb{Z}$-module libre engendré par les x_i. Considérons les éléments de $D \cap G$ suivants :

$$y_j = \sum_{i=1}^r (j\lambda_i - [j\lambda_i])x_i.$$

L'ensemble $D \cap G$ étant fini, il existe j et j' distincts tels que $y_j = y_{j'}$. On a donc $(j-j')x$ dans $\Sigma \mathbb{Z} x_i$. Le groupe G étant un $\mathbb{Z}$-module de type fini l'existence d'un d comme plus haut est prouvée.

Exercice 1.11 : Soit α un nombre réel irrationnel, montrer que pour tout $\varepsilon > 0$ il existe des entiers p et q tels que $|\alpha - \frac{p}{q}| < \frac{\varepsilon}{q}$.

Définitions 1.12. — *Les sous-groupes discrets de $\mathbb{R}^n$ de rang exactement n sont appelés des* **réseaux** *de $\mathbb{R}^n$. Si Λ est un réseau de $\mathbb{R}^n$ on appelle* **volume** *de Λ, et on note* $\mathrm{vol}(\Lambda)$*, le volume pour la mesure de Lebesgue du polytope construit sur une $\mathbb{Z}$ base de Λ.*

Il est clair que ce réel non nul est indépendant de la base choisie. La théorie des corps de nombres algébriques développée ci-dessous nous fournira de nombreux exemples de réseaux.

2 – Eléments entiers.

Nous étudions ici les "morphismes finis" au sens des variétés algébriques ou des schémas.

Définition 2.1. — *Soit B un anneau et soit A un sous-anneau de B. On dit qu'un élément x de B est* **entier sur A** *s'il satisfait une équation, dite équation de dépendance intégrale, de la forme :*

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

où les a_i sont dans A. On dit que B est entier sur A si tout élément de B satisfait une équation de dépendance intégrale à coefficients dans A.

Par exemple le corps des nombres complexes est entier sur le corps des réels. On sait que ce dernier corps n'est pas entier sur le corps des rationnels.

Proposition 2.2. — *Soit B un anneau et soit A un sous-anneau de B. Soit x un élément de B. Les propositions suivantes sont équivalentes :*

(i) *x est entier sur A*

(ii) *l'anneau $A[x]$ est un A-module de type fini*

(iii) *il existe un sous-anneau de B, contenant $A[x]$, et qui est un A-module de type fini.*

Démonstration : Soit x satisfaisant une équation unitaire de degré n comme dans la définition 2.1. On note que cette équation de dépendance intégrale multipliée par x^i donne une expression de x^{n+i} comme combinaison linéaire à coefficients dans A des x^{n+j} pour $j = i-1, i-2, \ldots, i-n$. Il nous reste à montrer que (iii) implique (i). Soient $x_1, \ldots, x_n$ des générateurs sur A d'un sous-anneau de B contenant $A[x]$. La multiplication par x dans cet anneau donne des expressions :

$$x x_i = \sum_{j=1}^{n} a_{ij} x_j$$

ou encore $\sum_{j=1}^{n}(\delta_{ij}x - a_{ij})x_j = 0$. Si d est le déterminant de la matrice $(\delta_{ij}x - a_{ij})$ on obtient $dx_j = 0$ pour tout j. Donc $d.1 = d = 0$ puisque les x_j engendrent B sur A. C'est bien une équation de dépendance intégrale de x sur A.

Corollaire 2.3. — *Soit B un anneau et soit A un sous-anneau. Alors l'ensemble des éléments de B qui sont entiers sur A est un sous-anneau de B appelé la* **clôture intégrale** *de A dans B.*

En effet si $A[x]$ et $A[y]$ sont des A-modules de type fini, $A[x, y]$ est un $A[x]$-module de type fini. Comme $A[x]$ est un A-module de type fini, $A[x, y]$ est un A-module de type fini. On en déduit que $x - y$ et xy sont entiers sur A.

Exemple 2.4 : Les nombres réels $\sqrt{2}$ et $\sqrt[3]{7}$ sont entiers sur $\mathbb{Z}$. On notera qu'il est assommant de trouver une équation pour $\sqrt{2} + \sqrt[3]{7}$.

Définition 2.5. — *Soient B un anneau, A un sous-anneau. On dit que A est intégralement fermé dans B si tout élément de B entier sur A, est déjà dans A.*

Le cas particulier suivant est d'un intérêt constant.

Définition 2.6. — *Si A est un anneau intègre on dit qu'il est* **intégralement clos** *s'il est intégralement fermé dans son corps de fractions.*

Exercice 2.7 a) : Montrer qu'un anneau principal est intégralement clos.

b) Soient A un anneau intègre, S une partie multiplicativement stable de A. Montrer que si A est intégralement clos alors $S^{-1}A$ l'est aussi.

Proposition 2.8. — *Soient B un anneau intègre et A un sous-anneau de B tel que B soit entier sur A. Pour que B soit un corps il faut et il suffit que A soit un corps.*

Si B est un corps et x est dans A, x^{-1} satisfait une équation

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

En multipliant par x^n on voit que

$$x(-a_1 - a_2x - a_3x^2 - \cdots - a_1x^{n-2} - a_nx^{n-1}) = 1 \ .$$

Réciproquement si A est un corps et B intègre entier sur A, tout élément x de B satisfait une équation $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$. Prenant une équation de degré minimum on voit que $a_n \neq 0$. Donc a_n est inversible et on a $xa_n^{-1}(-x^{n-1} - a_1x^{n-2} - \cdots - a_{n-1}) = 1$. □

Exercice 2.9 : Soient A un anneau et B un sur-anneau entier sur A. Montrer que l'application $\operatorname{Spec} B \to \operatorname{Spec} A$ est surjective.

Exercice 2.10 : Soit A un anneau contenu dans un anneau B de telle façon que B soit une A-algèbre de type fini.

a) Supposons que A soit local et B entier sur A. Montrer qu'un idéal premier de B dont l'intersection avec A est l'idéal maximal, est un idéal maximal de B.

b) Montrer que si B est entier sur A le morphisme $\operatorname{Spec} B \to \operatorname{Spec} A$ est surjectif à fibres finies.

3 – Extensions algébriques des corps.

Une extension entière d'un corps est dite algébrique. Si L est un corps contenant un sous-corps K de telle façon que L soit un espace vectoriel de dimension finie sur K alors L est algébrique sur K. Sa dimension comme K-espace vectoriel est appelée le degré de L sur K. On le note $[L : K]$. Si $K \subset L \subset M$ sont des corps on a $[M : L][L : K] = [M : K]$. Soient R un anneau, K un sous-corps de R et x un élément de R. Il existe un K-homomorphisme φ et un seul de l'anneau de polynômes $K[X]$ dans R tel que $\varphi(X) = x$. L'élément x est algébrique sur K si $\operatorname{Ker}\varphi \neq 0$. Dans ce cas l'idéal $\operatorname{Ker}\varphi$ est engendré par un polynôme unitaire non nul uniquement déterminé. Ce polynôme est appelé le **polynôme minimal** de x sur K.

Proposition 3.1. — *Soient K un corps et P un polynôme non constant à coefficients dans K. Alors il existe une extension algébrique K' de K de degré fini de K telle que $P(X)$ se décompose en facteurs du premier degré dans $K'[X]$.*

Par récurrence sur le degré d de $P(X)$, on peut supposer que P est irréductible. Par la proposition 2.8 $K[X]/(P(X)$, est un corps K_1 où l'image x de X est racine de $P(X) = 0$. Donc $(X - x)$ est facteur de $P(X)$ dans $K_1[X]$ et l'hypothèse de récurrence permet de conclure.

Lemme 3.2. — *Soient K un corps de caractéristique zéro ou un corps fini, $F(X)$ un polynôme unitaire de degré n irréductible. Alors ses n racines dans une extension finie K' de K sont distinctes.*

Comme $F(X)$ est irréductible c'est le polynôme minimal d'une quelconque de ses racines x. Si une racine était double la dérivée de $F'(X)$ s'annulerait aussi en x. Si K est de caractéristique zéro, F' est de degré un de moins que F et n'est pas nul (F est unitaire). Le fait que F devrait diviser F' est une contradiction. Donc F' est nul et la caractéristique est p nombre premier non nul. Le polynôme $F(X)$ est alors de la forme $X^{np} + a_1X^{(n-1)p} + \cdots + a_{n-1}X^p + a_n$. Il est classique de voir que **l'homomorphisme de Frobénius** $x \to x^p$ de K dans K est un homomorphisme d'anneaux réduits, donc injectif. Comme K est supposé fini cet homomorphisme est bijectif. Tout élément de K est une puissance p-ième et on peut écrire $a_i = b_i^p$. Le polynôme $F(X)$ est alors égal à $(X^n + b_1X^{n-1} + \cdots + b_{n-1}X + b_n)^p$ qui n'est pas irréductible. □

Lemme 3.3. — *Soient K un corps et σ un homomorphisme de corps de K dans un corps C, algébriquement clos. Soit K' un corps extension de degré fini de K alors σ se prolonge en un homomorphisme de corps σ' de K' dans C.*

Si K' est de la forme $K[x]$ le lemme est clair. Par récurrence sur $[K' : K]$ on se ramène à ce cas. □

PROPOSITION 3.4. — *Soit K un corps de caractéristique zéro ou un corps fini. Soit C un corps algébriquement clos contenant K et soit K', une extension de degré fini n de K. Alors il existe n K-homorphismes de corps distincts de K' dans C.*

L'énoncé est vrai quand l'extension K' de K est monogène par le lemme 3.2. En raisonnant par récurrence sur $[K' : K]$ on se ramène a la situation suivante : $K \subset K' \subset K''$, $[K' : K] = m < n$, $\sigma_i : K' \to C$ $i = 1, \ldots, m$, des K-homomorphismes distincts. Chaque σ_i se prolonge en $\sigma_i' : K'' \to C$ par le lemme 3.3. Il y a $[K'' : K']$ tels prolongements distincts par hypothèse de récurrence car $[\sigma_i(K'') : \sigma_i(K')] = [K'' : K']$. On a donc $m[K'' : K'] = n$ K-homomorphismes distincts de K'' dans C.

Exercice 3.5 : (théorème de l'élément primitif). Montrer que si K est un corps fini ou un corps de caractéristique zéro et si K' en est une extension finie, il existe x dans K' tel que $K' = K[x]$.

4 – Corps de nombres, ordre d'un corps de nombres, anneau d'entiers algébriques.

Nous introduisons ici le langage de la théorie algébrique des nombres.

DÉFINITION 4.1. — *Un corps K extension algébrique de degré fini du corps $\mathbb{Q}$ des nombres rationnels est appelé un* **corps de nombres**. *L'entier $[K : \mathbb{Q}]$ est appelé le* **degré** *de K.*

Par exemple $\mathbb{Q}[i]$ avec $i^2 = -1$ est un corps de nombres de degré 2 sur $\mathbb{Q}$.

DÉFINITION 4.2. — *Soit K un corps de nombres et soit A un anneau entier sur $\mathbb{Z}$, contenu dans K et dont le corps de fractions soit K. On dit que A est un* **ordre du corps de nombres K**.

Par exemple $\mathbb{Z}[\sqrt{5}]$ est un ordre du corps de nombres $\mathbb{Q}[\sqrt{5}]$. On notera cependant que $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ est aussi un ordre de $\mathbb{Q}[\sqrt{5}]$.

DÉFINITION 4.3. — *Soit K un corps de nombres. On appelle anneau des entiers algébriques de K, la clôture intégrale $\mathcal{O}_K$ de $\mathbb{Z}$ dans K.*

Exercice 4.4 : Montrer que $\mathcal{O}_K$ est un ordre de K.

Exercice 4.5 : (Anneaux des entiers des extensions quadratiques). Soit K une extension quadratique de $\mathbb{Q}$.

a) Montrer qu'il existe d dans $\mathbb{Z}$ sans facteurs carrés tel que $K = \mathbb{Q}[\sqrt{d}]$.

b) Si $d \equiv 2$ ou $d \equiv 3$ mod. 4 montrer que l'anneau $\mathcal{O}_K$ est égal à $\mathbb{Z} + \mathbb{Z}\sqrt{d}$.

c) Si $d \equiv 1$ mod. 4 montrer que $\mathcal{O}_K$ est égal à $\mathbb{Z} + \mathbb{Z}(\frac{1+\sqrt{d}}{2})$.

Définition 4.6. — *Soit K un corps de nombres. Les $\mathbb{Q}$-homomorphismes σ de K dans le corps des nombres complexes sont appelés les* **places à l'infini** *de K. Une place à l'infini σ de K est dite réelle (respectivement complexe) si $\sigma(K)$ est contenu dans $\mathbb{R}$ (respectivement n'est pas contenue dans $\mathbb{R}$). Si x est dans K, ses images $\sigma(x)$ s'appellent les* **conjugués** *de x.*

Si σ est une place complexe, la conjugaison complexe fournit une autre place $\bar{\sigma}$ distincte de σ. Il est classique de noter r_1 le nombre de places réelles de K, $2r_2$ le nombre des places complexes de K et n le degré $[K : \mathbb{Q}]$. On a $n = r_1 + 2r_2$. Soit ϕ un ensemble de $r_1 + r_2$ places à l'infini de K tel que si σ est complexe et σ est dans ϕ alors $\bar{\sigma}$ n'est pas dans ϕ.

Proposition 4.7. — *Soit K un corps de nombres A un ordre de K et soient n, r_1, r_2 et ϕ comme ci-dessus. L'application $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \simeq \mathbb{R}^n$ qui a un élément x de K associe*

$$(\sigma_i(x))_{\sigma_i \in \phi}$$

est telle que $\sigma(A)$ est un réseau de $\mathbb{R}^n$. En particulier un ordre d'un corps de nombres de degré n est un $\mathbb{Z}$-module libre de rang n.

Pour montrer cette proposition décisive, nous allons d'abord prouver un lemme de finitude général.

Lemme 4.8. — **(premier lemme de finitude)**. *Soit $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$. Soient n un entier et h un nombre réel, alors, l'ensemble des éléments de $\overline{\mathbb{Q}}$, entiers sur $\mathbb{Z}$, de degré au plus n et dont les conjugués ont une valeur absolue bornée par h, est fini.*

Soit x comme dans l'énoncé. Le polynôme minimal de x sur $\mathbb{Q}$ est unitaire à coefficients dans $\mathbb{Z}$ et de degré au plus n. En effet x étant entier sur $\mathbb{Z}$ pour tout $\mathbb{Q}$-homomorphisme de corps $\rho : \mathbb{Q}[x] \to \mathbb{C}$, $\rho(x)$ est aussi entier sur $\mathbb{Z}$. Si m est égal à $[\mathbb{Q}[x] : \mathbb{Q}]$ le polynôme minimal s'écrit $\prod_{i=1}^{i=m} (X - \rho_i(x))$ il est donc à coefficients entiers sur $\mathbb{Z}$ et dans $\mathbb{Q}$. Comme $\mathbb{Z}$ est intégralement clos ces coefficients sont dans $\mathbb{Z}$. Par hypothèse on a $|\rho_i(x)| \leq h$. Donc x satisfait une équation

$$x^m + a_1 x^{m-1} + a_2 x^{m-2} + \cdots + a_m = 0$$

avec a_i entier, $|a_i| \leq \binom{m}{i} h^i$, $m \leq n$. La liste des coefficients est donc finie. Le degré étant borné, le nombre des solutions est fini. □

Démontrons maintenant la proposition 4.5. Le lemme 4.6 implique que $\sigma(A)$ est discret. Par le corollaire 1.10 c'est un $\mathbb{Z}$-module libre de rang au plus $[K : \mathbb{Q}]$. Comme $A \otimes_{\mathbb{Z}} \mathbb{Q} = K$ (proposition 2.8) A est de rang $[K : \mathbb{Q}]$ sur $\mathbb{Z}$ et $\sigma(A)$ est bien un réseau de $\mathbb{R}^n$.

Corollaire 4.9. — *Soit A un ordre d'un corps de nombres K de degré n sur $\mathbb{Q}$, et soit L un A-module inversible. Alors L est un $\mathbb{Z}$-module libre de rang n.*

En effet L est sans torsion car localement isomorphe à A, de plus il est de type fini et :

$$L \otimes_{\mathbb{Z}} \mathbb{Q} = L \otimes_A (A \otimes_{\mathbb{Z}} \mathbb{Q}) = L \otimes_A K \simeq K \ .$$

PROPOSITION 4.10. — *Un ordre d'un corps de nombres est un anneau noethérien de dimension* 1.

Démonstration : Puisque un ordre A d'un corps de nombres K de degré n sur $\mathbb{Q}$ est un $\mathbb{Z}$-module de type fini, c'est un anneau noethérien. De plus si $\mathfrak{p}$ est un idéal premier non nul de A, $\mathfrak{p} \otimes_A K = K$, donc $\mathfrak{p}$ est aussi un $\mathbb{Z}$-module libre de rang n (1.7). Le quotient $A/\mathfrak{p}$ est donc fini par 1.2. Un anneau intègre fini étant automatiquement un corps $\mathfrak{p}$ est maximal. □

Exercice 4.11 : La démonstration de 4.8 est had-hoc. En fait montrer que si $A \subset B$ est une extension entière d'anneaux, alors toute chaîne d'idéaux premiers de A se relève en une chaîne d'idéaux premiers de B. Montrer ensuite que $\dim(A) = \dim B$ (théorème de Cohen-Seidenberg).

5 – Anneaux de valuation discrète, anneaux de Dedekind.

Nous étudions ci-dessous les anneaux intègres, noethériens, locaux, de dimension 1. Les anneaux de séries formelles $k[[X]]$ par exemple sont de tels anneaux.

PROPOSITION 5.1. — *Soit A un anneau intègre et soit K son corps de fractions. Les deux propositions suivantes sont équivalentes*

(i) *A est local noethérien intégralement clos et de dimension 1.*

(ii) *Il existe une application surjective $v : K^\times \to \mathbb{Z}$ telle que $v(xy) = v(x) + v(y)$ et $v(x+y) \geq \inf(v(x), v(y))$, de manière que l'anneau A soit l'ensemble des x de K tels que $v(x) \geq 0$.*

Montrons d'abord que (ii) implique (i). Soit I un idéal de A, choisissons x non nul dans I tel que $v(x)$ soit minimum dans $v(I)$. Soit y dans I, $v(y/x) \geq 0$ donc $y = ax$ avec $a \in A$ et donc A est principal. Si $v(x) = 0$ il est clair que $v(x^{-1}) = 0$ et donc $x \in A^\times$. Soit $\mathfrak{m}$ l'ensemble des x dans A tels que $v(x) > 0$. On voit facilement que tout idéal de A est contenu dans $\mathfrak{m}$. L'implication est donc prouvée par l'exercice 2.7.

Pour montrer l'application inverse notons $\mathfrak{m}$ l'idéal maximal de A, nous allons montrer que $\mathfrak{m}$ est principal. Dans ce cas soit π un générateur de $\mathfrak{m}$. L'anneau A étant intègre et n'étant pas un corps l'élément π est non nul. Montrons d'abord que $\bigcap_n \mathfrak{m}^n = 0$. Si x est dans $\bigcap_n \mathfrak{m}^n$ on a des éléments x_n tels que $\pi^n x_n = \pi^{n+1} x_{n+1}$ donc (A est intègre) $x_n = \pi x_{n+1}$. La suite croissante d'idéaux Ax_n de l'anneau noethérien A est stationnaire pour n assez grand. On a donc $Ax_n = Ax_{n+1}$ pour $n >> 0$ donc $x_{n+1} = ax_n = a\pi x_{n+1}$. L'anneau A étant local $1 - a\pi$ est inversible donc x_{n+1} est nul et donc x est nul. On définit alors $v(x) = \sup\{n, x \in \mathfrak{m}^n\}$. Comme $\mathfrak{m}$ est principal il est clair que $v(xy) = v(x) + v(y)$.

L'inégalité $v(x+y) \geq \inf(v(x), v(y))$ est vraie pour tout idéal $\mathfrak{m}$ et tout v définit comme ci-dessus. La fonction v se prolonge à $K^\times$ par $v(\frac{x}{y}) = v(x) - v(y)$. Comme il est clair que pour x et y dans A , $v(x) \geq v(y)$ implique $x = ay$ avec $a \in A$, (ii) sera montré dès qu'on sait que $\mathfrak{m}$ est principal. Pour montrer ceci définissons $\mathfrak{m}' = \{x \in K | x\mathfrak{m} \subset A\}$. Nous allons montrer les trois points suivants :

a) $\mathfrak{m}' \neq A$

b) $\mathfrak{m}\mathfrak{m}' = A$

c) $\mathfrak{m}$ est principal.

démonstration de a) : Si x est dans $\mathfrak{m}$ l'anneau de fractions $A_x = K$ (exercice I 1.8). Soit z un élément non nul de A on peut écrire $\frac{1}{z} = \frac{y}{x^n}$ pour un y dans A et un entier n, i.e. $x^n = yz$. Tout élément de $\mathfrak{m}$ a donc une puissance dans l'idéal Az. L'idéal $\mathfrak{m}$ étant de type fini il existe un entier n tel que $\mathfrak{m}^n$ soit contenu dans Az. Choisissons n minimum avec cette propriété et soit $y \in \mathfrak{m}^{n-1}$ et $y \notin Az$. On vérifie facilement que $\frac{y}{z} \in \mathfrak{m}'$ et $\frac{y}{z} \notin A$.

démonstration de b) : Soit x dans $\mathfrak{m}'$ on a soit que $x\mathfrak{m}$ est contenu dans $\mathfrak{m}$ soit que $x\mathfrak{m} = A$. Dans le premier cas x est un endomorphisme d'un A-module de type fini sans torsion, et par "l'astuce" du déterminant déjà utilisée plusieurs fois (I 1.4 et II 2.2) x est entier sur A. L'anneau A étant intégralement clos la partie a) montre que $\mathfrak{m}.\mathfrak{m}' = A$ sinon $\mathfrak{m}.\mathfrak{m}'$ est contenu dans $\mathfrak{m}$.

démonstration de c) : Puisque $\mathfrak{m}\mathfrak{m}' = A$ il existe un entier $n, x_1, \ldots, x_n$ dans $\mathfrak{m}$ et $y_1, \ldots, y_n$ dans $\mathfrak{m}'$ tels que $\Sigma x_i y_i = 1$. Chacun des $x_i y_i$ est dans A, cet anneau étant local il existe un i tel que $u = x_i y_i$ soit inversible dans A. Posons $x = u^{-1} x_i \in \mathfrak{m}$ et $y = y_i \in \mathfrak{m}'$ si z est dans $\mathfrak{m}$ on a $z = (yz)x$ avec $yz \in A$ par définition. On a ainsi montré que x engendre $\mathfrak{m}$. □

Exercice 5.2 : (**lemme d'Artin-Rees**)

Soient A un anneau noethérien, I un idéal de A et posons $R(I) = \bigoplus_{n \geq 0} I^n$.

a) Montrer que $R(I)$ est un anneau noethérien.

b) Soient M un A-module de type fini et N un sous-A-module de M. Montrer que $\bigoplus_{n \geq 0} I^n M \cap N$ est un $R(I)$-module de type fini.

c) En déduire qu'il existe un entier k tel que $I^n M \cap N = I^{n-k}(I^k M \cap N)$.

d) (**Séparation de la topologie $\mathfrak{m}$-adique**).

Supposons de plus que A soit local d'idéal maximal $\mathfrak{m}$ montrer que $\bigcap_{n \geq 0} \mathfrak{m}^n = 0$. (On pourra utiliser le lemme de Nakayama).

Définition 5.3. — *Un anneau vérifiant les conditions de la proposition 5.1 est appelé un* **anneau de valuation discrète**. *Un générateur de l'idéal maximal d'un anneau de valuation discrète est appelé une* **uniformisante**.

Proposition 5.4. — *Soit A un anneau noethérien intégralement clos de dimension un, alors tout idéal de A est localement principal. De plus tout idéal est globalement engendré par deux éléments.*

Le début de la proposition signifie exactement qu'un idéal non nul de A est un A-module inversible. Soit $\mathcal{I}$ un idéal de A et soit $\mathfrak{m}$ un idéal maximal de A. Par la démonstration de la proposition 5.1 l'idéal $\mathcal{I}_\mathfrak{m}$ est principal. Si x est dans $\mathcal{I}$ et engendre $\mathcal{I}_\mathfrak{m}$ sur $A_\mathfrak{m}$ par I 1.7 d) x engendre $\mathcal{I}$ sur un voisinage $D(f)$ de $\mathfrak{m}$ dans $\operatorname{Spec} A$. Ceci démontre la première partie de 5.4. Soit f dans A comme ci-dessus, A/fA est un anneau de dimension zéro noethérien. Par 0.16 $\mathcal{I} \otimes_A A/fA \simeq A/fA$. Par le lemme de Nakayama (I 1.4) il existe un élément y de $\mathcal{I}$ qui engendre $\mathcal{I}_\mathfrak{m}$ sur $A_\mathfrak{m}$ pour tout $\mathfrak{m}$ contenant f. On voit ainsi que $Ax + Ay$ est égal à $\mathcal{I}$ par I 1.7 e).

Définition 5.5. — *Un anneau noethérien intègre intégralement clos de dimension un est appelé un* **anneau de Dedekind**.

Exemple 5.6 : Soit K un corps de nombres, l'anneau des entiers $\mathcal{O}_K$ est un anneau de Dedekind.

Exercice 5.7 (**Polynôme d'Eisenstein**) : Soient A un anneau de valuation discrète, $\mathfrak{m}$ son idéal maximal, K son corps de fractions et $k = A/\mathfrak{m}$ son corps résiduel. On dit que $F(X) = X^n + a_1X^{n-1} + \cdots + a_n$ est un polynôme d'Eisenstein – sur A – si les a_i sont dans $\mathfrak{m}$ mais a_n n'est pas dans $\mathfrak{m}^2$. On pose $B = A[X]/(F(X))$ et on note x l'image de X dans B.

a) Montrer qu'un idéal premier non nul de B contient $\mathfrak{m}$.

b) Montrer que $B/\mathfrak{m}B = k[X]/(X^n)$, en déduire que B est un anneau local, noethérien de dimension 1, dont l'idéal maximal est engendré par x.

c) Déduire de b) que x n'est pas nilpotent.

d) Montrer (en utilisant c) ou à défaut 5.6) que $\bigcap_n (Bx^n) = 0$.

e) Montrer que B est un anneau de valuation discrète.

6 – L'application cycle.

Nous commençons ici l'étude des "sous-schémas" de codimension un dans un schéma affine.

Définition 6.1. — *Soit A un anneau. On appelle* **diviseur de Weil** *une combinaison linéaire à coefficients entiers de quotients $A/\mathfrak{p}$ par des idéaux premiers $\mathfrak{p}$ tels que $\dim A_\mathfrak{p} = 1$. En général si n est un entier on appelle* **cycles de codimension n** *et*

on note $Z^n(A)$ *les combinaisons linéaires* $\sum_{i=1}^{s} n_i[A/\mathfrak{p}_i]$ *où les* n_i *sont entiers et les* $\mathfrak{p}_i$ *des idéaux premiers de* A *tels que* $\dim A_{\mathfrak{p}_i} = n$. *Ainsi les diviseurs de Weil sont les cycles de codimension un.*

Exemple 6.2 : Si I est un idéal de A anneau noethérien, et si $\dim A_{\mathfrak{p}} \geq n$ pour tout idéal premier de I on peut lui associer un cycle de codimension n

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

cette somme est finie (0.17 d)). Ainsi si I est un A-module inversible (i.e. si I est localement engendré par un élément non diviseur de zéro) on obtient un diviseur de Weil.

Exercice 6.3 : Montrer que les idéaux qui sont des A-modules inversibles forment un monoïde pour le produit tensoriel.

Définition 6.4. — *Soit A un anneau. On appelle groupe des* **diviseurs de Cartier** *de A, et on note* **Div(A)** *le groupe engendré par le monoïde des idéaux qui sont des A-modules inversibles.*

On voit facilement que si I et J sont deux idéaux qui sont dans **Div(A)** alors $I \otimes J \to IJ$ est un isomorphisme (cf. I 3.8 a)).

Lemme 6.5. — *Si A est un anneau de Dedekind l'application cycle :* $\text{Div}(A) \to Z^1(A)$ *est surjective.*

Démonstration : Par la proposition 5.4 tout idéal premier non nul $\mathfrak{p}$ de A est localement engendré par un élément non nul de A. De plus A étant de dimension 1 (4.8), si $\mathfrak{q}$ est idéal premier non nul de A différent de $\mathfrak{p}$ alors $\mathfrak{p}A_{\mathfrak{q}} = A_{\mathfrak{q}}$. Donc $\text{cycle}(A/\mathfrak{p}) = [A/\mathfrak{p}]$. □

Exercice 6.6 : Montrer que si A est un anneau intègre noethérien de dimension 1 et si $\text{Div}(A) \to Z^1(A)$ est surjective alors A est intégralement clos. (Utiliser les idées de la démonstration de la proposition 5.1).

Proposition 6.7 (Définition usuelle des anneaux de Dedekind). — *Soit A un anneau de Dedekind alors l'application cycle* $\text{Div}(A) \to Z^1(A)$ *est un isomorphisme.*

Soit $\text{Div}_+(A)$ le monoïde des idéaux de A qui sont dans $\text{Div}(A)$. Par la démonstration de 6.4 nous savons que les générateurs de $Z^1(A)$ sont dans l'image de $\text{Div}_+(A)$. Il nous suffit donc de montrer que $\text{Div}_+(A) \to Z^1(A)$ est injective. Si I et J sont deux idéaux distincts de A, il existe $\mathfrak{p}$ tel que $I_{\mathfrak{p}}$ soit distinct de $J_{\mathfrak{p}}$ (sinon $I + J/I$ serait nul). Dans l'anneau de valuation discrète $A_{\mathfrak{p}}$ si π est une uniformisante $I_{\mathfrak{p}} = \pi^n A_{\mathfrak{p}}$ $J_{\mathfrak{p}} = \pi^m A_{\mathfrak{p}}$ où n et m sont des entiers distincts. Or, par 0.9, la longueur de $(A/I)_{\mathfrak{p}}$ vaut n et celle de $(A/J)_{\mathfrak{p}}$ vaut m donc, $\text{cycle}\ (A/I) \neq \text{cycle}(A/J)$.

7 – L'application Div(A) → Pic(A).

Soit I un idéal de A qui soit un A-module inversible, on lui associe la classe de son dual $\mathrm{Hom}_A(I, A)$ dans $\mathrm{Pic}(A)$.

Définition 7.1. — *Soit A un anneau. On appelle* **diviseurs principaux de A**, *et on note $Pr(A)$ le sous-groupe de* $\mathrm{Div}(A)$ *engendré par les idéaux fA où f est non-diviseur de zéro. Ce groupe est canoniquement isomorphe à $K^\times/A^\times$.*

Exemple 7.2 : Si A est un anneau de Dedekind, K son corps de fractions et f un élément de K, alors $(f) = \sum_{\dim A_\mathfrak{p}=1} v_\mathfrak{p}(f)[A/\mathfrak{p}]$ est un élément de $Z^1(A)$ qui est dans l'image de $Pr(A)$ ($v_\mathfrak{p}$ est la valuation associée à $A_\mathfrak{p}$ définie dans 5.1).

Proposition 7.3. — *Avec les notations introduites ci-dessus si A est intègre on a la suite exacte*

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

Si f est non nul dans A, l'idéal fA est un A-module libre de rang 1, donc son image dans $\mathrm{Pic}(A)$ est nulle. Tout élément de $\mathrm{Div}(A)$ est "différence" de deux éléments de $\mathrm{Div}_+(A)$, il nous faut donc montrer que si I et J sont deux idéaux de $\mathrm{Div}(A)$ tels que $\mathrm{Hom}_A(I, A) \simeq \mathrm{Hom}_A(J, A)$ alors il existe a et b non nuls dans A tels que $aI = bI$. On a les isomorphismes $I \otimes_A K \simeq K$ et $J \otimes_A K \simeq K$, où K est le corps de fractions de A. On a donc $\mathrm{Hom}_A(I, J) = \{ftK | fI \hookrightarrow J\}$ ce qui montre l'assertion.

Il nous reste à montrer la surjectivité de $\mathrm{Div}(A) \to \mathrm{Pic}(A)$. En fait, on a le lemme suivant qui sera d'un usage constant dans la suite.

Lemme 7.4. — *Soient A un anneau intègre et L un A-module inversible. Pour tout élément s non nul de L considérons l'application*

$$\varphi_s : A \to L$$

qui envoie 1 *sur s. Alors φ_s est injective et l'application duale $L^{\otimes -1} \to A$ identifie $L^{\otimes -1}$ à un idéal $\mathfrak{a}_s$ de A tel que $\mathfrak{a}_s = \mathrm{annulateur}(L/A_s)$.*

L'injectivité découle de l'exercice I 4.7, l'application duale $\varphi_s^\vee : L^{\otimes -1} \to A$ étant non nulle (car $\varphi_s^{\vee\vee} = \varphi_s$) le même exercice identifie $L^{\otimes -1}$ à un idéal $\mathfrak{a}_s$ de A. Pour montrer la fin de l'assertion il suffit de la prouver localement. Quand L est isomorphe à A, φ_s s'identifie à $\lambda : A \to A$, la multiplication par un élément λ de A. La duale est aussi la multiplication par λ et l'énoncé est démontré.

Remarque 7.5. — Quand A est un anneau de Dedekind $Z^1(A)/Pr(A)$ est classiquement appelé le **groupe de classes de diviseurs** noté **Cl(A)**.

Exemple 7.6 : Un exemple : $\mathrm{Pic}(\mathbb{Z}[\sqrt{-5}] \neq 0$.

Soit $A = \mathbb{Z}[i\sqrt{5}]$. Pour tout élément $x = a + bi\sqrt{5}$ de A on note $N(x) = a^2 + 5b^2$. La norme $N(x)$ est le carré du nombre complexe x. On a $N(xy) = N(x)N(y)$. Par l'exercice 4.5 l'anneau A est intégralement clos. Si le groupe $\mathrm{Pic}(A)$ était nul, l'anneau A serait

principal. Alors tout élément irréductible engendrerait un idéal premier. Montrons que l'élément $1+i\sqrt{5}$ est irréductible. Notons que $(1+i\sqrt{5})(1-i\sqrt{5})=6$ et $N(1+i\sqrt{5})=N(1-i\sqrt{5})=6$, $N(2)=4$, $N(3)=9$. Si x est non inversible $N(x)$ est un entier non égal à ± 1. Si de plus x divise $1+i\sqrt{5}$ et n'est pas $\pm(1+i\sqrt{5})$, $N(x)=2$ ou $N(x)=3$. Or les équations $a^2+5b^2=2$ ou $a^2+5b^2=3$ n'ont pas de solution entière car seuls 1 et 4 sont des carrés modulo 5. Si l'idéal engendré par $1+i\sqrt{5}$ était premier 2 ou 3 lui appartiendrait car 6 lui appartient, on aurait alors en prenant les normes $\frac{4}{6}$ ou $\frac{9}{6} \in \mathbb{Z} \cdots$ □

La version ci-dessous de la proposition 7.3 est souvent utile. La démonstration qui n'utilise pas d'idée nouvelle par rapport à 7.3 et 7.4 est laissée au lecteur.

Proposition 7.7. — *Soient A un anneau intègre et L un A-module inversible. Soient s et t deux éléments non nuls de A alors il existe des éléments non nuls a et b de A tels que $as=bt$. De plus si $\mathfrak{a}_s$ et $\mathfrak{a}_t$ sont les éléments de* $\mathrm{Div}(A)$ *définis en 7.4 alors $a\mathfrak{a}_s = b\mathfrak{a}_t$.*

Quand l'anneau A est noethérien et de dimension 1 le lemme 7.4 prend une forme plus attrayante.

Proposition 7.8. — *Soient A un anneau intègre noethérien et de dimension* 1 *et L un A-module inversible. Alors pour tout élément s non nul de L on a $L/A_s \simeq A/\mathfrak{a}_s$ où $\mathfrak{a}_s$ est l'idéal défini en 7.4.*

Les A-modules L/A_s et $A/\mathfrak{a}_s$ sont de longueur finie. Il suffit donc de montrer 7.8 localement par 0.6. Si A est local, L est libre de rang 1 et $\mathfrak{a}_s$ est principal, le résultat découle alors de 7.4.

8 – **Points rationnels d'un schéma projectif sur un anneau de Dedekind**.

Nous établissons ci-dessous la partie qui nous sera utile du critère valuatif de propreté : un point rationnel d'un schéma projectif sur un corps K s'étend en un "point" entier sur un anneau de Dedekind de corps de fractions K et ceci de façon unique.

Définition 8.1. — *Si A est un anneau X un A-schéma et B une A-algèbre, on note $X(B)$ des* **points rationnels de X sur B** *i.e. l'ensemble* $\mathrm{Hom}_A(\mathrm{Spec}\, B, X)$.

Proposition 8.2. — *Soient A un anneau, K un corps, B un anneau de Dedekind de corps de fractions K qui soit une A-algèbre. Alors si X est un A-sous-schéma fermé de $\mathbb{P}^n_A$ on a une bijection canonique : $X(B) \to X(K)$.*

Le morphisme $\mathrm{Spec}\, K \to \mathrm{Spec}\, B$ fournit l'application $X(B) \to X(K)$. Montrons d'abord la surjec tivité : un point de $X(K)$ est d'abord un point de $\mathbb{P}^n_A(K)$ donc la donnée d'un K-homomorphisme surjectif $K^{n+1} \to K \to 0$. Quitte à "chasser les dénominateurs" on peut considérer que cet homomorphisme vient d'un B-homomorphisme : $B^{n+1} \to B$. Celui-ci n'est plus forcément surjectif mais son image est un idéal non nul de B. Par la proposition 5.4 tout idéal de B est un B module inversible, donc on a construit par (I

5.9) un élément de $\mathrm{Hom}_{A-sch}(\mathrm{Spec}\, B, \mathbb{P}^n_A)$. Cet homomorphisme restreint à $\mathrm{Spec}\, K$ se factorise par X par hypothèse. Le schéma X étant fermé dans $\mathbb{P}^n_A$ il est défini par des équations homogènes (F_i) à coefficient dans A. Si $a_0 \cdots a_n$ sont des éléments de B tels que $F_i(a) = 0$ dans K alors $F_i(a) = 0$ dans B aussi. Donc on a construit un morphisme de $\mathrm{Spec}\, B \to X$ qui a pour image celui choisi dans $\mathrm{Hom}_A(\mathrm{Spec}\, K, X)$.

Pour montrer l'injectivité, il suffit de le faire quand $B = V$ est un anneau de valuation discrète. Soient $(x_0 \cdots x_n)$ et $(y_0, \ldots, y_n)$ dans V^{n+1} tel que l'un des x_i et l'un des y_i soit inversible dans V. Si les éléments correspondants dans $\mathrm{Hom}(\mathrm{Spec}\, K, X)$ sont les mêmes, c'est, par I 5.10, qu'il existe $\lambda \neq 0$ dans K tel que $x_i = \lambda y_i$ pour tout i. L'anneau V étant de valuation discrète λ ou λ^{-1} est dans V. Supposons que ce soit λ. Il existe i tel que λy_i est inversible dans V donc λ est inversible dans V. Les $(n+1)$-uples (x) et (y) donnent ainsi le même élément de $\mathrm{Hom}(\mathrm{Spec}\, V, X)$ (par I 5.10).

Remarque 8.3. — Soient A un anneau et $X \xrightarrow{f} \mathrm{Spec}\, A$ un A-schéma projectif alors, par définition, un élément de $\mathrm{Hom}_A(\mathrm{Spec}\, A, X)$ est une **section** de f. Ainsi, si A est un anneau de Dedekind de corps de fraction K on a par 8.2 une bijection canonique $X(K) \leftarrow \{\text{sections de } f : X \to \mathrm{Spec}\, A\}$.

Définition 8.4. — *Si A est un anneau de Dedeking de corps de fraction K et si X est un A-schéma projectif on note s_P la* **section de $X \to \mathrm{Spec}\, \mathrm{H}$, correspondant à un point rationnel** *P de X sur K.*

On a ainsi défini un accouplement $X(K) \times \mathrm{Pic}(X) \to \mathrm{Pic}(A)$ qui à (P, L) fait correspondre $s_P^* L$.

III – Le groupe de Picard compactifié d'un ordre d'un corps de nombres

Nous introduisons ici "l'invention" d'Arakelov : mettre des métriques hermitiennes aux places à l'infini.

1 – Espaces vectoriels de dimension un sur $\mathbb{C}$.

Un espace vectoriel V sur le corps des complexes $\mathbb{C}$ est dit muni d'un **produit scalaire hermitien** si on a une application biadditive $(.,.) : V \times V \to \mathbb{C}$ telle que $(\lambda x, y) = \lambda(x, y)$ et $(x, y) = \overline{(y, x)}$ pour tout λ dans $\mathbb{C}$ et tous x et y dans V. Un tel produit scalaire est dit positif non dégénéré si $(x, x) = \|x\|^2 \geq 0$ pour tout x et si $\|x\| = 0$ implique $x = 0$.

Exemple 1.1 : Soit V un espace vectoriel de dimension un sur $\mathbb{C}$. Il revient au même de se donner un produit scalaire hermitien sur V positif non dégénéré ou de se donner la longueur $\|x\| \neq 0$ d'un élément x non nul de V. En effet si y et z sont dans V, on a $y = \lambda x$, $z = \mu x$ et donc $(y, z) = \lambda\bar{\mu}\|x\|^2$. Cette remarque facile va nous être d'un usage constant.

Proposition 1.2. — *L'ensemble des produit scalaires hermitiens positifs non dégénérés sur un espace vectoriel V de dimension un sur $\mathbb{C}$ est un espace principal homogène sous $\mathbb{R}_+^\times$.*

En effet si $(,)$ et $(,)_1$ sont des produits scalaires hermitiens sur V et si $x \neq 0$, $x \in V$ on a $\|x\| = \lambda\|x\|_1$ pour un nombre réel λ. S'ils sont positifs non dégénérés $\lambda \in \mathbb{R}_+^\times$.

Remarque 1.3. — Si V_1 et V_2 sont deux espaces vectoriels de dimension un munis de produits scalaires hermitiens positifs non dégénérés $(,)_1$ et $(,)_2$, le **produit tensoriel** $V_1 \otimes_{\mathbb{C}} V_2$ est muni canoniquement d'un produit scalaire hermitien positif non dégénéré tel que $\|x_1 \otimes x_2\| = \|x_1\|_1.\|x\|_2$ où $x_i \neq 0$ et $x_i \in V_i$. De même le **dual** $V^\vee$ d'un tel espace vectoriel est muni de la norme $\|\varphi\| = \dfrac{|\varphi(x)|}{\|x\|}$ pour tout x non nul dans V, par l'exemple 1.1 est muni d'un produit scalaire hermitien positif non dégénéré.

Exercice 1.4 : Soit V un espace vectoriel sur $\mathbb{C}$ de dimension 1 muni d'un produit scalaire hermitien non dégénéré. Montrer que l'application trace : $V \otimes_{\mathbb{C}} V^\vee \to \mathbb{C}$ induit par 1.3 sur $\mathbb{C}$ le produit scalaire hermitien tautologique.

Vocabulaire 1.5 : Soit V un espace vectoriel de dimension un sur $\mathbb{C}$, nous utiliserons de manière équivalente les expressions

a) V est muni d'un produit scalaire hermitien positif non dégénéré.

b) V est muni d'une métrique hermitienne.

Définition 1.6. — *Soit V un espace vectoriel de dimension 1 sur $\mathbb{C}$ muni d'un produit scalaire hermitien.* **L'élément de volume canonique** *sur V est tel que le disque unité $\{z \in V \mid \|z\| \leq 1\}$ est de volume π.*

Il est à noter que la donnée d'un élément de volume sur V est la même chose que la donnée d'un élément non nul sur $\overset{2}{\underset{\mathbb{R}}{\Lambda}} V$. Ce dernier est un espace vectoriel de dimension 1 sur $\mathbb{R}$. On peut réécrire ce court paragraphe pour les espaces vectoriels de dimension 1 sur $\mathbb{R}$. Un produit scalaire défini positif nous fournit une "longueur" pour les vecteurs. L'élément de "volume" i.e. de longueur canonique est tel que le segment $\{x \mid \|x\| \leq 1\}$ est de longueur 2. Par exemple, si V est un espace vectoriel de dimension 1 sur $\mathbb{C}$ qui est égal à $V_0 \otimes_{\mathbb{R}} \mathbb{C}$ où V_0 est un espace vectoriel sur $\mathbb{R}$, un produit scalaire hermitien positif non dégénéré induit sur V_0 une telle structure.

2 – Modules inversibles métrisés sur un ordre d'un corps de nombres.

Soit K un corps de nombres. Soient $n = [K : \mathbb{Q}]$ son degré, r_1 son nombre de places réelles $2r_2$ son nombre de places complexes. **On fixera pour la suite un ensemble ϕ de places à l'infini** contenant r_1 places réelles, r_2 places complexes qui ne sont pas conjuguées l'une de l'autre (cf. II 4.4). On se donne aussi un anneau A qui est un ordre de K.

Définition 2.1. — *Un module inversible L sur un ordre A muni pour toute place σ dans ϕ d'un produit scalaire hermitien non dégénéré $(,)_\sigma$ sur $(L \otimes_A \sigma(A)) \otimes_{\sigma(A)} \mathbb{C}$ est appelé un* **module inversible métrisé** *sur A. Si $\|.\|_\sigma$ est la norme associée à $(,)_\sigma$ on notera $(L, \|.\|_\sigma)$ un A-module inversible métrisé.*

On a une notion d'isomorphisme pour ces objets :

Définition 2.2. — *Une* **isométrie** *entre $(L_1, \| \ \|_{1,\sigma})$ et $(L_2, \| \ \|_{2,\sigma})$, deux modules inversibles métrisés sur l'ordre A, est un A-isomorphisme $\varphi : L_1 \xrightarrow{\sim} L_2$ tel que $\|\varphi(x)\|_{2,\sigma} = \|x\|_{1,\sigma}$ pour tout x dans L_1.*

Lemme 2.3. — *Soient $(L, \| \ \|_{1,\sigma})$ et $(L, \| \ \|_{2,\sigma})$ deux modules inversibles métrisés sur A ayant le même module inversible sous-jacent. Alors ils sont isomètres si et seulement si il existe une unité u de A telle que $\|x\|_{1,\sigma} = |\sigma(u)|\|x\|_{2,\sigma}$ pour tout x dans L et tout σ dans ϕ.*

En effet $\mathrm{Hom}_A(L, L) = A$ et donc $\mathrm{isom}_A(L, L) = A^\times$. On a $\|ux\|_{2,\sigma} = |\sigma(u)|\|x\|_{2,\sigma}$, ce qui prouve l'assertion.

Proposition 2.4. — *Le produit tensoriel induit sur l'ensemble des classes d'isométrie de A-modules inversibles métrisés une loi de composition interne qui en fait un groupe commutatif. Ce groupe est appelé le* **groupe de Picard compactifié de A**. *On le note* $\mathbf{Pic_c(A)}$.

Nous avons vu en 1.3 la loi de composition à l'infini. Par l'exercice 1.4 A muni du produit scalaire hermitien tel que $\|1\|_\sigma = 1$ pour tout σ est un élément neutre et le dual, muni des métriques duales est un inverse. □

Exemple 2.5. — Soient x_σ des nombres réels positifs, on notera $(A, (x_\sigma))$ l'élément de $\mathrm{Pic}_c(A)$ qui a pour module sous-jacent A et tel que $\|1\|_\sigma = x_\sigma$. Ainsi $(A, (1))$ est l'élément neutre de $\mathrm{Pic}_c(A)$.

Exercice 2.6 : Montrer que l'application $(\mathbb{R}_+^\times)^\phi \to \mathrm{Pic}_c(A)$ qui à $(x_\sigma)_{\sigma\in\phi}$ associe $(A, (x_\sigma))$ est un homomorphisme de groupe.

Exercice 2.7 : Montrer que l'application "oubli de l'infini" est un homomorphisme de $\mathrm{Pic}_c(A)$ dans $\mathrm{Pic}(A)$.

Proposition 2.8 (**première suite exacte fondamentale**). — *On a la suite exacte suivante :*

$$0 \to (A) \to A^\times \to (\mathbb{R}_+^\times)^\phi \to \mathrm{Pic}_c(A) \to \mathrm{Pic}(A) \to 0$$

où (A) est l'ensemble des racines de l'unité dans A, $|\sigma(u)|$ est la valeur absolue de l'image par σ de l'unité u dans $\mathbb{C}$ et $\sigma : A^\times \to (\mathbb{R}_+^\times)^\phi$ est l'application qui à $u \in A^\times$ fait correspondre $(|\sigma(u)|)_{\sigma\in\phi}$.

Par l'exemple 1.1 l'application $\mathrm{Pic}_c(A) \to \mathrm{Pic}(A)$ est surjective. Son noyau est l'ensemble des "structures hermitiennes à l'infini" sur A. Par 1.1 et 2.6 c'est l'image de $(\mathbb{R}_+^\times)^\phi$. En appliquant le lemme 2.3 on voit que $(A, (x_\sigma))$ est isomètre à $(A, (1))$ si et seulement si il existe une unité u dans $A^\times$ telle que $x_\sigma = |\sigma(u)|$ pour tout σ. Il nous reste donc à prouver le lemme qui suit :

Lemme 2.9. — *Soient K un corps de nombres, A un ordre de K alors pour un élément x de A les énoncés suivants sont équivalents :*

(i) *x est une racine de l'unité*

(ii) *pour tout homomorphisme de corps $\sigma : K \to \mathbb{C}$, $\sigma(x)$ est de valeur absolue 1. De plus l'ensemble (A) des racines de l'unité dans A est un groupe fini.*

Il est clair qu'un élément de (A) est de valeur absolue 1 dans tout plongement complexe i.e. (i) implique (ii). Dans l'autre sens : le premier lemme de finitude (II 4.6) montre que

si x dans $\mathfrak{a}$ a tous ses conjugués de valeur absolue un, alors l'ensemble $(x^n)_{n\in\mathbb{N}}$ est fini i.e. x est dans (A).

Pour finir de montrer l'énoncé il suffit d'appliquer encore une fois le premier lemme de finitude (II 4.6).

3 – La norme d'un idéal.

Nous commençons par mettre en évidence quelques anneaux finis construits à partir d'un ordre.

Proposition 3.1. — *Soit $\mathfrak{a}$ un ordre d'un corps de nombres et soit $\mathfrak{a}$ un idéal non nul de $\mathfrak{a}$ alors $A/\mathfrak{a}$ est fini. De plus si $(\mathfrak{p}_i)_{=1\cdots r}$ sont les idéaux premiers de $\mathfrak{a}$ contenant $\mathfrak{a}$ on a* $\#(A/\mathfrak{a}) = \prod_{i=1}^{r} \#(A_{\mathfrak{p}_i}/\mathfrak{a}A_{\mathfrak{p}_i})$ *et* $\log(\#(A_{\mathfrak{p}_i}/\mathfrak{a}A_{\mathfrak{p}_i})) = \mathrm{long}(A_{\mathfrak{p}_i}/\mathfrak{a}A_{\mathfrak{p}_i})\log(\#(A/\mathfrak{p}_i))$.

Pour montrer le début de 3.1 il suffit de montrer que A/xA est fini pour tout x non nul de $\mathfrak{a}$. Si $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ est une équation de dépendance intégrale de degré minimum sur $\mathbb{Z}$, on a $a_n \neq 0$ car x n'est pas diviseur de 0. Alors A/xA, qui est un $\mathbb{Z}/a_n\mathbb{Z}$ module de type fini, est fini. On peut comparer cette démonstration à celle de II 4.8. L'anneau $A/\mathfrak{a}$ est artinien et la fin de 3.1 se déduit de II 0.6 et du fait que sur un anneau local artinien le seul module simple est le corps résiduel.

Définition 3.2. — *Soit $\mathfrak{a}$ un ordre d'un corps de nombres et soit $\mathfrak{a}$ un idéal non nul de $\mathfrak{a}$. On nomme* **norme de a**, *et on note* $\mathbf{N}(\mathfrak{a})$, *le cardinal de $A/\mathfrak{a}$.*

Exemple 3.3 : Soit n un entier, $N(n\mathbb{Z}) = |n|$.

Proposition 3.4. — *L'application norme :* $\mathrm{Div}_+(A) \to \mathbb{N}$ *est multiplicative.*

Soient I et J deux idéaux dans $\mathrm{Div}_+(A)$ il nous faut montrer $\#A/IJ = (\#A/I).(\#A/J)$.

Prouvons d'abord le lemme suivant :

Lemme 3.5. — *Soient B un anneau, x un élément non diviseur de zéro dans B. Soit J un idéal de B, alors on a une suite exacte de B-modules :*

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

Le noyau de l'application canonique $B/xJ \to B/xB$ est xB/xJ. Calculons le noyau de l'homomorphisme surjectif $\varphi : B \to xB/xJ$ défini par $\varphi(1) = [x]$. Si λ, z sont dans B tels que $\lambda x = xz$ alors $\lambda = z$, car x est non diviseur de 0. Donc $\ker\varphi = J$. Appliquant le lemme 3.5 à un anneau $A_{\mathfrak{p}}$, où I et J sont engendrés par un élément, on obtient

$$\mathrm{long}\ A_{\mathfrak{p}}/IJA_{\mathfrak{p}} = (A_{\mathfrak{p}}/IA_{\mathfrak{p}}).(A_{\mathfrak{p}}/JA_{\mathfrak{p}}).$$

On déduit alors la proposition 3.4 de la deuxième partie de la proposition 3.1.

Corollaire 3.6. — *L'application norme se prolonge en un homomorphisme de groupes* $N : \mathrm{Div}(A) \to \mathbb{Z}$.

On aimerait avoir un homomorphisme de groupe partant de $\mathrm{Pic}(A)$ au lieu de $\mathrm{Div}(A)$, pour cela il nous faut étudier la norme des diviseurs principaux. On verra plus loin qu'on peut obtenir un homomorphisme à valeurs dans $\mathbb{R}$ (au lieu de $\mathbb{Z}$) sur le groupe $\mathrm{Pic}_c(A)$ (au lieu de $\mathrm{Pic}(A)$).

Nous établissons maintenant que la norme permet une première classification des idéaux d'un ordre.

Lemme 3.7 (**deuxième lemme de finitude**). — *Soit* $\mathfrak{a}$ *un ordre d'un corps de nombres et soit* r *un entier. Alors l'ensemble des idéaux de* $\mathfrak{a}$ *de norme au plus* r *est fini.*

Tout élément d'un groupe fini étant annulé par l'ordre du groupe, si $\mathfrak{a}$ est un idéal de $\mathfrak{a}$ tel que $N(\mathfrak{a}) \leq r$, $r!$ annule $A/\mathfrak{a}$ donc $r! \in \mathfrak{a}$. L'ensemble des idéaux de norme au plus r est donc contenu dans l'ensemble des sous-ensembles de $A/(r!)A$. □

4 – La norme d'un élément d'un corps de nombres.

Soit x est un élément d'un corps de nombres K et, soit d le degré de $\mathbb{Q}[x]$ sur $\mathbb{Q}$. Alors $(-1)^d$ multiplié par le déterminant de la multiplication par x dans l'espace vectoriel $\mathbb{Q}[x]$ sur $\mathbb{Q}$ est le coefficient constant du polynôme minimal de x. En effet le polynôme caractéristique est égal au polynôme minimal dans ce cas.

Proposition 4.1. — *Soient* K *un corps de nombres et* x *un élément de* K*. Alors le déterminant de* m_x*, la multiplication par* x *dans* K*, est un nombre rationnel qui satisfait à :*

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

Nous venons de voir ci-dessus que la proposition est vraie si $K = \mathbb{Q}[x]$. Si K est un espace vectoriel de dimension m sur $\mathbb{Q}[x]$ on a $m[\mathbb{Q}[x] : \mathbb{Q}] = [K : \mathbb{Q}]$. La matrice de m_x peut s'écrire avec m blocs égaux à la matrice de m_x restreint à $\mathbb{Q}[x]$. Donc $\mathrm{dét}(m_x) = \prod_{\sigma : \mathbb{Q}[x] \to \mathbb{C}} \sigma(x)^m$, comme il y a exactement m $\mathbb{Q}$-homomorphismes distincts de K dans $\mathbb{C}$ prolongeant un homomorphisme $\sigma : \mathbb{Q}[x] \to \mathbb{C}$ (II 3.4), la formule 4.1 est montrée.

Définition 4.2. — *Soient* K *un corps de nombres et* x *un élément de* K*, on appelle* **norme de x** *et on note* $\mathbf{N(x)}$ *le nombre rationnel* $\prod_{\sigma : K \to \mathbb{C}} \sigma(x)$.

Les conjugués d'un élément entier étant entiers eux aussi, si x est dans $\mathcal{O}_K$, $N(x)$ est dans $\mathbb{Z}$.

Remarque 4.3. — Il est clair que $N : K^\times \to \mathbb{Q}^\times$ est un **homomorphisme de groupe** défini par la même formule 4.2. La norme d'un élément inversible u de $\mathfrak{a}$ étant un élément inversible de $\mathbb{Z}$ elle vaut ± 1. En composant la norme avec la valeur absolue on obtient un homomorphisme de groupe $|N| : K^\times/A^\times \to \mathbb{Q}_+^\times$. Comme nous avons vu au chapitre II 7.4 $K^\times/A^\times = Pr(A)$. On peut donc essayer de comparer l'application induite par la norme sur $\mathrm{Div}(A)$ et celle que nous venons d'obtenir.

Proposition 4.4 (formule du produit). — *Soient K un corps de nombres, $\mathfrak{a}$ un ordre de K et x un élément de $\mathfrak{a}$. Alors la norme de l'idéal engendré par x dans $\mathfrak{a}$ est égale à la valeur absolue de la norme de l'élément x.*

Autrement dit il nous faut montrer

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

Pour ceci notons que le déterminant de la multiplication par x dans K est égal au déterminant de la multiplication par x dans $\mathfrak{a}$. Pour calculer celui-ci nous allons utiliser le lemme suivant :

Lemme 4.5. — *Soit $\varphi : \mathbb{Z}^n \to \mathbb{Z}^n$ un homomorphisme injectif de $\mathbb{Z}$-modules libres alors $\#(\operatorname{Coker}\varphi) = \#(\operatorname{Coker}\det\varphi) = \#(\mathbb{Z}/\det\varphi\mathbb{Z})$.*

Puisqu'on peut diagonaliser φ (II 1.2) le lemme est clair (notons que puisque φ est injective si $a_1 \cdots a_n$ sont les termes de la diagonale de la matrice de φ dans des bases had-oc, aucun des a_i n'est nul).

Pour finir de montrer 4.4 on écrit en vertu de 4.1 et 4.5

$$\prod_{\sigma : K \to \mathbb{C}} |\sigma(x)| = |\det m_x| = \#\mathbb{Z}/\det m_x\mathbb{Z} = \#A/xA = N(xA).$$

Exercice 4.6 : Soit $\mathfrak{a}$ un anneau noethérien de dimension 1 et soit $\varphi : A^n \to A^n$ un $\mathfrak{a}$-homomorphisme.

a) Montrer que $\operatorname{Ker}\varphi$ et $\operatorname{Coker}\varphi$ sont annulés par $\det\varphi$.

b) Montrer que si $A/\det\varphi A$ est de dimension 0 la fonction $M \to \chi(M,\varphi) = \operatorname{long}\operatorname{Coker}(\varphi \otimes M) - \operatorname{long}(\operatorname{Ker}\varphi \otimes M)$ est additive, à valeur dans $\mathbb{N}$, sur les $\mathfrak{a}$-modules de type fini. Calculer $\chi(M)$ en fonction de $\chi(A)$ quand $\mathfrak{a}$ est intègre.

c) Montrer que $\chi(A,\varphi) = \chi(A,\det\varphi)$ (délicat, cet énoncé mérite le nom de théorème de **Riemann-Roch pour les anneaux noethériens de dimension 1**).

d) Soit $\mathfrak{a}$ un anneau noethérien de dimension 1 et de caractéristique un nombre premier positif p. Soit φ une matrice $n \times n$ à coefficients dans $\mathfrak{a}$, on note $\varphi^{(p)}$ la matrice $n \times n$ dont les coefficients sont les puissance p-ièmes des coefficients de φ sous les hypothèses de b), montrer que $\chi(M,\varphi^{(p)}) = p\chi(M,\varphi)$ pour tout A-module de type fini M.

Notation 4.7. — Soit $\mathcal{O}_K$ l'anneau des entiers du corps de nombres $\mathcal{O}_K$ on appelle **place à distance finie** de K une valuation v associée par II 5.1 à un idéal maximal $\mathfrak{p}_v$ de $\mathcal{O}_K$. Par abus de notation on note $N(v) = N(\mathfrak{p}_v)$. On voit facilement que la fonction $f \to N(v)^{-v(f)}$ est une **norme ultramétrique** sur K que nous noterons $|f|_v$.

Corollaire 4.8 (**formule du produit classique**). — *Avec les notations ci-dessus si f est un élément d'un corps de nombres K on a*

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

Les places de K sont celles à l'infini i.e. les plongements $\sigma : K \to \mathbb{C}$ **et** celles à distance finie. La formule se déduit aisément de 4.4 et 3.1 quand on note que sur l'anneau $\mathcal{O}_v$ de la valuation v : $\#\mathcal{O}_v/a\mathcal{O}_v = N(v)^{v(a)}$.

Exercice 4.9 *(formule du produit sur la droite projective* $\mathbb{P}^1$*)* : Soit $A = k[T]$ l'anneau de polynômes en une variable sur un corps k algébriquement clos. Soit P un point de la droite affine $\mathbb{A}^1(k)$ de coordonnée t et soit $\mathfrak{m}_p$ l'idéal maximal de $\mathfrak{a}$ engendré par $T - t$.

a) Soit f un élément de $\mathfrak{a}$ montrer que la valuation v_t associée à $\mathfrak{m}_P$ est telle que $v_t(f)$ est l'ordre du zéro de f en P.

b) Soit f un élément de $\mathfrak{a}$ de degré n montrer que f a un pôle d'ordre n à l'infini (i.e. $f(T) = \frac{1}{u^n} g(u)$ avec $u = \frac{1}{T}$ et $g(u)$ un polynôme en u tel que $g(0) \neq 0$).

c) Posons pour $f \in k(T)$, $v_\infty(f) =$–(ordre du pôle de f à l'infini). Montrer que v_∞ est une valuation sur $k(T)$.

d) Montrer que $\sum_{t \in k \cup \infty} v_t(f) = 0$ pour tout f dans $k(T)$.

Exercice 4.10 : Soit K un **corps de fonctions d'une variable sur un corps k** i.e. un corps qui est une extension finie du corps des fonctions rationnelles $k(T)$. On dira qu'un anneau $\mathfrak{a}$ est un **ordre de K** si $\mathfrak{a}$ est un $k[T]$ module de type fini contenu dans K tel que le corps de fractions de $\mathfrak{a}$ soit K.

a) Etablir que $A \simeq k[T]^n$ où $n = [K : k(T)]$.

b) Soit $\mathfrak{a}$ un idéal non nul de $\mathfrak{a}$ on pose $\deg(\mathfrak{a}) = \dim_k A/\mathfrak{a}$. Montrer que deg est un homomorphisme additif de $\mathrm{Div}_+(A)$ dans $\mathbb{N}$.

c) Supposons de plus que k est un corps fini. Montrer que l'ensemble des idéaux $\mathfrak{a}$ de A tel que $\deg(\mathfrak{a}) \leq r$, r donné, est fini.

5 – La définition locale du degré sur $\mathrm{Pic}_c(A)$.

Définition 5.1. — *On appelle* **groupe des 1-cycles compactifié de A**, *et on note* $Z^1_c(A)$ *le groupe* $Z^1(A) \times \mathbb{R}^\phi$. *On notera* $\sum_{\mathfrak{p} \in \mathrm{Spec}\, A} n_\mathfrak{p}[A/\mathfrak{p}] + \sum_{\lambda \in \phi} \lambda_\sigma[\sigma]$ *un élément générique de* $Z^1_c(A)$.

De même on définit le **groupe des diviseurs de Cartier compactifié de A**, et on note $\mathrm{Div}_c(A)$ le groupe $\mathrm{Div}(A) \times \mathbb{R}^\phi$. On a ainsi une injection $\mathrm{Div}(A) \to \mathrm{Div}_c(A)$.

On a clairement un homomorphisme de groupes : $\mathrm{Div}_c(A) \to Z^1_c(A)$ qui prolonge $\mathrm{Div}(A) \to Z^1(A)$ et garde "les composantes à l'infini".

Définition 5.2. — *On appelle* **degré du 1-cycle compactifié** $\Sigma n_\mathfrak{p}[A/\mathfrak{p}] + \Sigma\lambda_\sigma[\sigma]$ *le nombre réel*

$$\Sigma n_\mathfrak{p} \log N(\mathfrak{p}) + \Sigma \varepsilon_\sigma \lambda_\sigma$$

où $\varepsilon_\sigma = 1$ *si* σ *est une place réelle et* $\varepsilon_\sigma = 2$ *sinon.*

Par composition on a ainsi défini le **degré d'un diviseur compactifié**. On a l'énoncé évident suivant :

Proposition 5.3. — *L'application degré :* $\mathrm{Div}_c(A) \to \mathbb{R}$ *est un homomorphisme de groupes. On la note* **deg**. *Si* $\mathfrak{a}$ *est un élément de* $\mathrm{Div}_+(A)$ *on a, (en le considérant comme diviseur compactifié sans composante à l'infini) :*

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

Exemple 5.4 : Soit x un élément de $\mathfrak{a}$ définissons le diviseur $(x) = xA - \sum_{\sigma\in\phi} \varepsilon_\sigma \log|\sigma(x)|$. On a ainsi un homomorphisme du semi-groupe $A-\{0\}$ dans $\mathrm{Div}_c(A)$ qui se prolonge donc en un homomorphisme de groupes $K^\times \to \mathrm{Div}_c(A)$. Nous noterons (f) le diviseur compactifié associé ainsi à l'élément f de $K^\times$. On appelle **diviseurs principaux compactifiés** les éléments de l'image de $K^\times$ dans $\mathrm{Div}_c(A)$ par cette application. Ils forment un groupe que l'on note $Pr_c(A)$.

Proposition 5.5 (**l'homomorphisme** $\mathrm{Div}_c(A) \to \mathrm{Pic}_c(A)$). — *Il existe un homomorphisme naturel* $\mathrm{Div}_c(A) \to \mathrm{Pic}_c(A)$ *tel qu'on ait un diagramme commutatif de suites exactes :*

$$\mathbb{R}^\phi \to \mathrm{Div}_c(A) \to \mathrm{Div}(A) \to 0(\exp)^{-1}4mm4mm4mm(\mathbb{R}_+^\times)^\phi \to \mathrm{Pic}_c(A) \to \mathrm{Pic}(A) \to 04mm4mm00.$$

Soit $a + \Sigma x_\sigma[\sigma]$ un élément de $\mathrm{Div}_c(A)$ tel que $\mathfrak{a}$ soit un idéal – inversible – de A. On lui associe l'élément de $\mathrm{Pic}_c(A)$ suivant :

a) le module inversible est $\mathfrak{a}^{\otimes -1}$

b) en dualisant l'inclusion $\mathfrak{a} \hookrightarrow A$ on obtient un homomorphisme $A \to \mathfrak{a}^{\otimes -1}$ et on pose $|\mathrm{Im}(1)|_\sigma^{\varepsilon_\sigma} = e^{-x_\sigma}$.

Notons que si $L \in \mathrm{Pic}_c(A)$ et $0 \neq s \in L$ il provient de l'élément $(\mathfrak{a}_s - \Sigma \log|s|_\sigma[\sigma])$ de $\mathrm{Div}_c(A)$.

L'énoncé de 5.5 est alors clair, l'application $\mathrm{Div}(A) \to \mathrm{Pic}(A)$ est celle de II.7.

Exemple 5.6 : Soit x un élément de $\mathfrak{a}$ et (x) le diviseur compactifié qui lui est associé (5.4). Alors l'élément de $\mathrm{Pic}_c(A)$ associé à (x) est l'élément neutre $(A, (1)_\sigma)$.

Proposition 5.7. — *L'application* $\deg : \mathrm{Div}_c(A) \to \mathbb{R}$ *s'annule sur* $\mathrm{Pr}_c(A)$ *le groupe des diviseurs principaux compactifiés de* $\mathfrak{a}$. *Elle définit donc un homomorphisme de groupes que nous noterons toujours* $\deg : \mathrm{Pic}_c(A) \to \mathbb{R}$. *Si* L *est dans* $\mathrm{Pic}_c(A)$ *et si* $0 \neq s \in L$ *on a*

$$\deg\ L = \log \frac{\#L/As}{\prod_{\sigma\in\phi} |s|_\sigma^{\varepsilon_\sigma}}.$$

Démonstration : Si x est dans $\mathfrak{a}$ $\deg(x) = \log\ N(xA) - \Sigma\varepsilon_\sigma \log|\sigma(x)| = \log\ N(xA) - \log|N(x)|$ qui est nul par la formule du produit (4.4). Pour montrer la fin de 5.7 considérons l'idéal $\mathfrak{a}_s$ correspondant à s comme dans II 7.4. On a (II 7.8) $L/As \simeq A/\mathfrak{a}_s$ et donc $\deg\ L = \deg(\mathfrak{a}_s - \Sigma_{\sigma\in\phi}\varepsilon_\sigma \log|s|_\sigma)$ par 5.5. On en déduit la formule de 5.7.

Exercice 5.8 : Montrer que le noyau de l'application $K^\times \to \mathrm{Div}_c(A)$ définie en 5.4 est égal à (A).

Exemple 5.9 : Soit t un nombre réel positif et soit $L \in \mathrm{Pic}_c(A)$, on note L_t l'élément de $\mathrm{Pic}_c(A)$ obtenu à partir de L en multipliant les normes par t. C'est un corollaire de 5.7 que le degré de L_t vaut $\deg L - n \log t$.

Exemple 5.10 : Soit $(x_\sigma) \in \mathbb{R}_+^\phi$ et soit $(A,(x_\sigma))$ l'élément de $\mathrm{Pic}_c(A)$ défini en 2.5. La proposition 5.7 implique $\deg(A,(x_\sigma)) = -\Sigma\varepsilon_\sigma \log x_\sigma$.

6 – Volumes, définition globale du degré.

Si L est dans $\mathrm{Pic}_c(A)$ le $\mathbb{R}$-espace vectoriel $\underset{\sigma\in\phi}{\oplus} L\otimes_A K_\sigma$, où K_σ est égal à $\mathbb{R}$ ou $\mathbb{C}$ selon que σ est une place réelle ou une place complexe, est muni d'un élément de volume canonique, car chacun des $L\otimes_A K_\sigma$ l'est (1.6).

Proposition 6.1. — *Soit L un module inversible sur un ordre $\mathfrak{a}$ d'un corps de nombres de degré n. L'application diagonale $L \to \underset{\sigma\in\phi}{\oplus} L\otimes_A K_\sigma$ identifie L à un réseau dans un espace vectoriel de dimension n sur $\mathbb{R}$.*

On sait déjà que L est un $\mathbb{Z}$-module libre de rang n (II 4.7). Il nous faut montrer que L est discret dans $\oplus L\otimes_A K_\sigma$. Choisissons un élément non nul s de L, on a une application injective $\varphi_s : A \to L$ qui envoie 1 sur s. Donc $\varphi_s \otimes K_\sigma$ est un isomorphisme pour tout σ. On a un diagramme commutatif :

$$A\varphi_s 6mmL3mm3mm \oplus K_\sigma \sim 6mm \oplus L\otimes K_\sigma .$$

Soit $r = \#L/As$ et soit B un compact dans $\oplus L\otimes K_\sigma$, si x est dans $L\cap B$ alors rx est dans $A\cap rB$. Comme on sait que $\mathfrak{a}$ est discret dans $\oplus K_\sigma$, $A\cap rB$ est fini et donc $L\cap B$ aussi. □

Corollaire 6.2. — *L'application canonique $L\otimes_{\mathbb{Z}} R \to \underset{\sigma}{\oplus} L\otimes K_\sigma$ est un isomorphisme.*

Un élément L de $\mathrm{Pic}_c(A)$ possède donc un volume non nul par II 1.12. C'est le volume de $\oplus L\otimes K_\sigma/L$ mesuré avec l'élément de volume décrit au début de ce paragraphe. Nous le noterons **vol(L)**.

Proposition 6.3. — *Avec les notations définies ci-dessus on a pour L dans $\mathrm{Pic}_c(A)$:*

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

Choisissons un élément s non nul dans L. On a une suite exacte :

$$0 \to A \to L \to L/As \to 0\ .$$

Les applications $A\otimes K_\sigma \to L\otimes K_\sigma$ ne conservent pas forcément les volumes. L'image du disque unité à gauche est l'ensemble des éléments de $L\otimes K_\sigma$ tels que $|z|_\sigma \le |s|_\sigma$ et a donc pour mesure $\pi|s|_\sigma^2$ si σ est complexe et $2|s|_\sigma$ si σ est réelle. Le volume est donc multiplié par $\prod_{\sigma\in\phi} |s|_\sigma^{\varepsilon_\sigma}$ dans l'application $\oplus A\otimes K_\sigma \to \oplus L\otimes K_\sigma$. On a donc, par la suite exacte notée plus haut :

$$\mathrm{vol}(L).\#(L/As) = \mathrm{vol}(A).\prod_{\sigma\in\phi}(s)_\sigma^{\varepsilon_\sigma}.$$

Ceci montre 6.3 vu l'expression 3.7 du degré. On peut bien entendu se servir de 6.3 comme définition du degré sur $\mathrm{Pic}_c(A)$. C'est une **définition globale** par opposition à la définition locale 5.7. Il est moins évident sur 6.3 de montrer l'additivité du degré. Cette situation est celle qu'on retrouve dans le théorème de Riemann-Roch sur les courbes algébriques. Nous verrons plus bas une interprétation encore plus "Riemann-Roch" de la formule 4.3.

7 – Sections d'un module inversible compactifié, théorème de Riemann-Roch.

Nous rejoignons ici les problèmes de la "géométrie des nombres" chère à Minkowski.

Définition 7.1. — *Soit L un élément de* $\mathrm{Pic}_c(A)$ *on appelle* **section de L** *un élément s du module inversible sous-jacent tel que $|s|_\sigma \leq 1$ pour tout σ place à l'infini. L'ensemble des sections de L est noté $H^0(L)$. Si on note B la boule unité de $\oplus L \otimes K_\sigma$ on a $H^0(L) = B \cap L$.*

Remarque 7.2. — Un module inversible compactifié L étant discret dans $\oplus L \otimes K_\sigma$ (6.1), $H^0(L)$ est un **ensemble fini**.

Exemple 7.3 : On a : $H^0(A) = \{0\} \cup (A)$. En fait pour tout L dans $\mathrm{Pic}_c(A)$, (A) agit sur $H^0(L)$, cette action est libre sur $H^0(L) - \{0\}$.

Définition 7.4. — *Soit L un élément de* $\mathrm{Pic}_c(A)$ *on pose* $\chi_s(L) = \log \dfrac{2^{r_1}\pi^{r_2}}{\mathrm{vol}(L)}$.

Nous allons montrer que $\chi_s(L)$ est une "approximation" de $\log(\#H^0(L))$ ce qui explique le nom de la remarque suivante.

Remarque 7.5 (**théorème de Riemann-Roch**). — On a la formule :

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

Cette remarque est équivalente à la proposition 6.3. Nous avons mis un indice s à χ_s pour spécifier que nous avons mis dans la "machine" le volume de la boule unité pour la norme "sup" : $2^{r_1}\pi^{r_2}$. On aurait une formule de Riemann-Roch avec n'importe quelle constante ajoutée à χ_s. Par exemple on peut prendre $\chi(L) = -\log \mathrm{vol}(L)$ ou $\chi'(L) = \log \dfrac{2^{r_1}\pi^{r_2}}{2^n \mathrm{vol}(L)}$ comme nous en aurons besoin plus bas.

Le nom de théorème de Riemann-Roch vient du cas des **courbes C projectives** et lisses sur un corps k. Si L est un fibré en droite sur C (i.e. localement un module inversible) on a une notion de degré pour L et on a une notion de section globale $H^0(C, L)$. On a aussi un $H^1(C, L)$, le théorème de Riemann-Roch sur C s'énonce : posant $\chi(L) = \dim_k H^0(C, L) - \dim_k H^1(C, L)$ on a

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

le terme $H^1(C, L)$ est le "terme d'erreur" (dû à Roch) dans $\chi(L)$. Il est nul quand $\deg\ L$ est assez grand et donc χ est une "approximation" de $\dim_k H^0$. Quant au "terme constant", $1 - \chi(\mathcal{O}_C)$ il s'interprète différentiellement sur C : c'est le nombre de différentielles globales k-linéairement indépendantes sur C. Nous verrons plus loin une interprétation "différentielle" du volume de A en passant par le discriminant et la différente.

V – Les théorèmes classiques de la théorie des nombres algébriques

Nous avons dans les chapitres précédents développé des notions qui vont nous permettre de comprendre avec aisance la démonstration des premiers théorèmes de la théorie des nombres algébriques. Les preuves présentées ici diffèrent parfois de celles données classiquement.

1 – Trois lemmes techniques.

Les lemmes ci-dessous ont des parallèles exactes pour les "fibrés inversibles" sur les courbes algébriques projectives.

LEMME 1.1. — *Soit* $L \in \mathrm{Pic}_c(A)$ *tel que* $\deg(L) < 0$. *Alors* $H^0(L) = 0$.

Si $0 \neq s \in L$ on a $\deg L = \log \dfrac{\#L/As}{\Pi |s|_\sigma^{\varepsilon_\sigma}}$ (III 5.7) comme $\#L/As$ est un entier, si $\Pi |s|_\sigma^{\varepsilon_\sigma} \leq 1$ (en particulier si chaque $|s|_\sigma \leq 1$) on a $\deg L \geq 0$.

Ce lemme justifie le "signe" que nous avons pris pour le degré ; il aurait été dommage, et contraire à l'analogue géométrique, que les sections non nulles ne forcent pas un degré positif ou nul.

LEMME 1.2. — *Soit* L *un* A*-module inversible compactifié tel que* $\deg L = 0$. *Alors si* $H^0(L) \neq 0$ L *est égal à* A *dans* $\mathrm{Pic}_c(A)$.

Regardons toujours la formule III 5.7 si $\log \dfrac{\#L/As}{\Pi |s|_\sigma^{\varepsilon_\sigma}} = 0$ et chaque $|s|_\sigma \leq 1$ on a :

a) $L = As$

b) $|s|_\sigma = 1 \ \forall \sigma$.

La condition a) implique que comme élément de $\mathrm{Pic}(A)$ L est égal à A. La condition b) dit que l'application $\varphi_s : A \to L$ telle que $\varphi_s(1) = s$, est une isométrie. □

Le troisième lemme est fameux, et dû à Minkowski. Nous en donnerons deux démonstrations.

Rappelons que nous avons défini au III 7.5 $\chi'(L) = \log \dfrac{2^{r_1}\pi^{r_2}}{2^n \operatorname{vol}(L)}$.

LEMME 1.3 (Minkowski). — *Soit* $L \in \mathrm{Pic}_c(A)$ *tel que* $\deg(L) \geq -\chi'(A)$ *alors* $H^0(L) \neq 0$.

REMARQUE 1.4. — D'après III 6.3 $\deg L \geq -\chi'(A)$ est équivalent à $\chi'(L) \geq 0$ ce qui rend 1.3 semblable à l'énoncé géométrique $\chi(L) > 0$ alors $H^0(L) \neq 0$. Notons d'autre part que nous savons par IV que si d_A est le discriminant de A sur $\mathbb{Z}$ on a

$$-\chi'(A) = \log(|d_A|^{1/2}\Big(\frac{2}{\pi}\Big)^{r_2}).$$

On reconnaîtra de cette façon l'énoncé classique du lemme de Minkowski sur les points d'un réseau L dans un convexe compact symétrique B : si $\operatorname{vol}(B) > 2^n \operatorname{vol}(L)$ alors $L \cap B \neq 0$. Dans 1.3 B est la boule "unité" dans $\oplus L \otimes K_\sigma$.

Nous donnons ci-dessous deux démonstrations de ce lemme sous cette dernière forme.

Première démonstration. Les translations dans $\mathbb{R}^n$ laissant invariante la mesure de Lebesgue, on a une mesure induite sur $\mathbb{R}^n/L$. Si $B \to R^n/L$ était injective on aurait $\mathrm{vol}(B) \leq \mathrm{vol}(L)$. Si $\mathrm{vol}(B) > 2^n \mathrm{vol}(L)$ c'est que l'application $\frac{1}{2}B \to \mathbb{R}^n/L$ n'est pas injective. Donc il existe x et y dans B, distincts tels que $\frac{1}{2}x - \frac{1}{2}y \in L$. Puisque B est symétrique $-y$ est dans B, et comme il est convexe $\frac{1}{2}x + \frac{1}{2}(-y) \in B$. □

Deuxième démonstration (Mordell). Par la proposition III 7.6 $2^{-mn}(\#(2^m B \cap L)) \xrightarrow[m\to\infty]{} \frac{\mathrm{vol}(B)}{\mathrm{vol}(L)}$. Si on a $\frac{\mathrm{vol}(B)}{\mathrm{vol}(L)} > 2^n$ et m assez grand on a $\#2^m B \cap L > 2^{n(m+1)}$. Notant que $\#L/kL = k^n$ pour tout entier k, on déduit que l'application $2^m B \cap L \to L/2^{m+1}L$ n'est pas injective. Il existe alors x et y dans L, $x \neq y$, $x \in 2^m B$, $y \in 2^m B$ et $x - y \in 2^{m+1}L$. Ecrivant $\frac{1}{2}(\frac{x}{2^m}) - \frac{1}{2}(\frac{y}{2^m}) \in L$ cet élément non nul appartient à B par symétrie et convexité. □

Ces deux démonstrations montrent que $B \cap L \neq 0$ dès que $\mathrm{vol}(B) > 2^n \mathrm{vol}(L)$. Pour passer à **l'inégalité large** supposons $\mathrm{vol}(B) \geq 2^n \mathrm{vol}(L)$ alors, pour tout $\varepsilon > 0$ $\mathrm{vol}((1+\varepsilon)B) > 2^n \mathrm{vol}(L)$ pour tout entier n on a donc un élément $0 \neq x_n \in (1+\frac{1}{n})B \cap L$. Chacun des x_n est dans $2B \cap L$ qui est fini, on a donc une sous-suite infinie x_{n_i} qui est constante (pincipe des tiroirs). Posant $x = x_{n_i}$ $\forall i$ on a $0 \neq x \in L \cap (\cap(1+\frac{1}{n_i})B)$. Comme la suite n_i est infinie $\bigcap\limits_i (1+\frac{1}{n_i})B = B$. □

2 – Finitude de Pic(A) et simple connexité de Spec $\mathbb{Z}$.

Proposition 2.1. — *Le groupe de Picard d'un ordre d'un corps de nombres est fini.*

Soit $L \in \mathrm{Pic}(A)$, munissons le de métriques à l'infini tel que $\deg L = -\chi'(A)$ (en prenant par exemple un élément non nul de L et en fixant ses normes en chaque place σ). Par 1.3 il existe $s \in L$ tel que $|s|_\sigma \leq 1$ $\forall \sigma$, l'idéal $\mathfrak{a}_s$ correspondant (II 7.4) est tel que $\log N(\mathfrak{a}_s) \leq -\chi'(A)$ par II 7.8. Par le deuxième lemme de finitude III 3.7 l'ensemble des idéaux de norme bornée par $e^{-\chi'(A)}$ est fini. Cet ensemble s'envoyant par II 7 surjectivement sur $\mathrm{Pic}(A)$ la démonstration est terminée.

Proposition 2.2 (Théorème d'Hermite et Minkowski). — *Soit K un corps de nombres de degré $n \geq 2$ et soit A un ordre de K. Alors son discriminant d_A n'est pas égal à ± 1.*

En opposant les lemmes 1.1 et 1.3 on voit que $-\chi'(A) \geq 0$ car $\mathrm{Pic}_c(A) \xrightarrow{\deg} \mathbb{R}$ est surjectif. Soit $|d_A|^{1/2}(\frac{2}{\pi})^{r_2} \geq 1$. Ceci prouve l'assertion 2.2 quand $r_2 > 0$. En fait l'autre partie de la démonstration que nous donnons ci-dessous prouve $-\chi'(A) > 0$ dès que K n'est pas un corps quadratique imaginaire. Comme on a $-\chi'(A) \geq 0$, supposons $-\chi'(A) = 0$. Par 1.3 tout élément de $\mathrm{Pic}_c(A)$ de degré zéro aurait une section non nulle, et par 1.2 serait égal à A dans $\mathrm{Pic}_c(A)$. Nous allons montrer ci-dessus que si $r_1 + r_2 - 1 > 0$ alors il existe $(x_\sigma) \in \mathbb{R}_+^\phi$ tel que (A, x_σ) (notation III 2.5) ne soit pas égal à A dans $\mathrm{Pic}_c(A)$ bien que $\deg(A, (x_\sigma)) = 0$. Par III 2.3 $(A, x_\sigma) = A$ si et seulement si il existe une unité $u \in A^\times$ telle que $x_\sigma = |\sigma(u)|$ pour tout σ. Il nous reste à montrer qu'il existe $(x_\sigma) \in \mathbb{R}_+^\phi$

tel que $\Pi x_\sigma^{\varepsilon_\sigma} = 1$ (i.e. $\deg(A, x_\sigma) = 0$) et $(x_\sigma) \notin \sigma(A^\times)$ dès que $r_1 + r_2 - 1 > 0$. Or $\sigma(A^\times)$ est discret dans $\mathbb{R}^\phi$ (premier lemme de finitude II 4.8). En prenant les logarithmes des coordonnées on a un espace vectoriel sur $\mathbb{R}$ de dimension $r_1 + r_2 - 1 > 0$ dans lequel $\log \sigma(A^\times)$ est discret, la proposition est donc démontrée.

Exercice 2.3 : Montrer que pour tout ordre A d'un corps de nombres K de degré $n \geq 2$ once $-\chi'(A) > 0$.

Remarque 2.4. — On a vu au chapitre IV que l'ensemble des diviseurs premiers du discriminant de K est exactement l'ensemble des nombres premiers qui se ramifient dans K, i.e. c'est le support de $\Omega^1_{\mathcal{O}_K/\mathbb{Z}}$. L'énoncé 2.2 signifie donc qu'un morphisme $\operatorname{Spec} A \to \operatorname{Spec} \mathbb{Z}$, où $\operatorname{Spec} A$ est connexe ne peut être non ramifié i.e. **Spec$\mathbb{Z}$ est simplement connexe**. Ce résultat est à rapprocher du fait que la droite projective $\mathbb{P}^1_k$ – sur tout corps – est simplement connexe. Pour les morphismes à fibres de dimension plus grande – par exemple le cas où les fibres sont des courbes algébriques ou des variétés abéliennes des résultats analogues – parfois très difficiles – ont été obtenus ([F] sur $\operatorname{Spec} \mathbb{Z}$, [M-B] et [Sz] en caractéristique positive).

3 – Le théorème des unités de Dirichlet.

Soit W l'hyperplan de $\mathbb{R}^\phi$ défini par l'équation $\Sigma \varepsilon_\sigma x_\sigma = 0$, nous avons déjà vu que l'application $\log \sigma : A^\times \to \mathbb{R}^\phi$ qui envoie une unité u sur le vecteur de coordonnées $(\log |\sigma(u)|)_{\sigma \in \phi}$ envoie $A^\times$ dans W. Par le premier lemme de finitude II 4.8 l'image de $A^\times$ dans W est discrète. Nous allons préciser cet énoncé.

Proposition 3.1. — *Le sous-groupe* $\log \sigma(A^\times)$ *de* W *est un réseau.*

Corollaire 3.2 (théorème des unités de Dirichlet). — *Soit* A *un ordre d'un corps de nombres* K*, alors le groupe des unités contient un sous-groupe fini* (A) *formé des racines de l'unité dans* A *et le quotient est un groupe libre de rang* $r_1 + r_2 - 1$.

Nous montrerons 3.1 en montrant qu'il existe deux nombres réels $\alpha < \beta$ tels que l'application $[\alpha, \beta]^\phi \cap W \to W/\log \sigma(A^\times)$ soit surjective.

Ainsi $W/\log \sigma(A^\times)$ sera compact pour lo topologie quotient de celle sur $W \simeq \mathbb{R}^{r_1+r_2-1}$.Si le rang de $\log \sigma(A^\times)$ était plus petit que $r_1 + r_2 - 1$ on aurait un entier a non nul et un homéomorphisme $W/\log \sigma(A^\times) \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{R}^a$ qui n'est pas compact.

Fixons un élément $L_0 = (A, x^0_\sigma)$ de $\operatorname{Pic}_c(A)$ qui soit de degré $-\chi'(A)$ i.e. tel que $\Pi(x^0_\sigma)^{\varepsilon_\sigma} = e^{\chi'(A)}$. Dans III 2.8 et III 5.3 l'ensemble des éléments de $\operatorname{Pic}_c(A)$ dont le module inversible sous-jacent est A et dont le degré est $-\chi'(A)$ est le "translaté" multiplicatif de L_0 par $\mathbb{R}^\phi_{+,1}/\sigma(A^\times)$, où nous avons noté $\mathbb{R}^\phi_{+,1}$ l'ensemble des éléments $(y_\sigma)_{\sigma\in\phi}$ de $\mathbb{R}^\phi_+$ tels que $\Pi Y_\sigma^{\varepsilon_\sigma} = 1$. Soit $\{(a_1A), (a_2A), \ldots, (a_sA)\}$ l'ensemble fini des idéaux principaux non nuls de A dont la norme est au plus $e^{-\chi'(A)}$ (III 3.7). Soit (A, x_σ) dans $\operatorname{Pic}_c(A)$ tel que $\Pi x_\sigma^{\varepsilon_\sigma} = e^{\chi'(A)}$ i.e. $\deg(A, x_\sigma) = -\chi'(A)$, par 1.3 il existe $0 \neq a_x \in A$ tel que $|\sigma(a_x)|x_\sigma \leq 1$ quel que soit σ i.e. $a_x \in H^0((A, x_\sigma))$ on a : $e^{-\chi'(A)} = \deg(A, x_\sigma) \geq N(a_xA)$. Donc (a_xA) est égal à l'un des idéaux (a_iA). On a ainsi une unité $u_x \in A^\times$ telle que $a_x = u_x a_i$ et $|\sigma(u_x)|x_\sigma \leq \frac{1}{|\sigma(a_i)|}$ $\forall \sigma$. Posons $c_1 = \sup\limits_{i,\sigma} \left(\frac{1}{|\sigma(a_i)|}\right)$, l'élément $(y_\sigma = |\sigma(u_x)|x_\sigma)_{\sigma\in\phi}$ est dans $[c_0, c_1]^\phi$ où $c_0 = e^{-\chi'(A)} c_1^{1-n}$ puisque $\Pi y_\sigma^{\varepsilon_\sigma} = e^{-\chi'(A)}$. On notera que $c_1 \geq 1$ car l'idéal 1.A est de norme $\leq e^{-\chi'(A)}$. Par III 2.3 $(*)$ $(A, x_\sigma) = (A, y_\sigma)$ dans $\operatorname{Pic}_c(A)$. Les éléments

$\left(\frac{y_\sigma}{x_\sigma^0}\right)_{\sigma\in\phi}$ sont dans $\mathbb{R}_{+,1}^{\phi}\cap\left[\frac{c_0}{\sup x_\sigma^0},\frac{c_1}{\inf x_\sigma^0}\right]^{\phi}$. L'application $\mathbb{R}_{+,1}^{\phi}\cap\left[\frac{c_0}{\sup x_\sigma^0},\frac{c_1}{\inf x_\sigma^0}\right]^{\phi}\to\mathbb{R}_{+,1}^{\phi}/\sigma(A^\times)$ est surjective par $(*)$. Posant $\alpha=\log\frac{c_0}{\sup x_\sigma^0}$ et $\beta=\log\frac{c_1}{\inf x_\sigma^0}$ en prenant les logarithmes on voit que l'application canonique $W\cap[\alpha,\beta]^\phi\to W/\log\sigma(A^\times)$ est surjective. □

Exercice 3.3 : Soit $A=\mathbb{Z}[\sqrt{2}]$ trouver un générateur du $\mathbb{Z}$ module libre de rang 1 $A^*/(\pm1)$.

4 – Extensions à ramification donnée.

Le but de ce paragraphe est de montrer que si on fixe le support du discriminant et le degré d'un corps de nombres K, alors il n'y a qu'un ensemble fini de corps K possibles. Ce théorème est à rapprocher d'un théorème classique de Riemann : les revêtements finis de degré fixe, de la sphère privée d'un ensemble donné fini de points sont en nombre fini.

Montrons d'abord que le discriminant "borne" le degré

Proposition 4.1. — *Soient K un corps de nombres de degré n, A un ordre de K et d_A son discriminant. Alors on a $4d_A^2\geq(\frac{\pi}{2})^n$.*

S'il y a r_2 places complexes on a vu que $|d_A|^{1/2}\geq(\frac{\pi}{2})^{r_2}$. Donc si $n=2r_2$ (i.e. $r_1=0$) 4.1 est démontré. Si $r_1\neq0$ le nombre complexe i tel que $i^2=-1$ n'est pas dans K. Soit $L=K[i]$ et $B=A[i]$, par la formule de "transitivité des discriminants" on a $d_B=d_A^2\text{Norme}(d_{B/A})$. Or $\text{Norme}(d_{B/A})=4$ et appliquant le cas précédent à B ordre de L on a $4d_A^2\geq(\frac{\pi}{2})^n$. □

Proposition 4.2 (théorème d'Hermite). — *Il n'y a qu'un nombre fini de corps de nombres de discriminant donné.*

Considérons l'élément $(A,(2^{1-r_1-r_2}e^{\chi'(A)},2,\dots,2))$ de $\text{Pic}_c(A)$ (notation III 2.5). Son degré est exactement $-\chi'(A)$, il existe donc (lemme 1.3) un élément x de A tel que, en indexant les places à l'infini :

$$|\sigma_1(x)|\leq2^{r_1+r_2-1}e^{-\chi'(A)}$$

$$|\sigma_i(x)|\leq\frac{1}{2}\quad\forall i>1\ .$$

Si $r_1\neq0$ et σ_1 est une place réelle un tel élément est un élément primitif de K sur $\mathbb{Q}$. Sinon par II 3.4 il existerait $i>1$ $\sigma_1(x)=\sigma_i(x)$ ce qui n'est pas puisque $\Pi|\sigma_j(x)|^{\varepsilon_i}=1$ et $|\sigma_i(x)|<1$ pour $i\neq1$. L'énoncé 4.2 est alors démontré par le premier lemme de finitude II 4.8.

Si toutes les places sont complexes et si x n'est pas un élément primitif de K sur $\mathbb{Q}$, comme $\sigma_1(x)\neq\sigma_i(x)$ $i>1$ c'est que $\sigma_1(x)=\overline{\sigma_1(x)}$ et que $[K:\mathbb{Q}[x]]=2$ (toujours par II 3.4). On a donc un corps $K_0=\mathbb{Q}[x]$ qui est dans une liste finie par II 4.8. Si $K=K_0[i]$ avec $i^2=-1$, K est aussi dans une liste finie. Sinon $i\notin K$. Considérons alors $L=K[i]$, on a $|d_L|\leq4d_K^2$ car $d_{A[i]/A}=\text{Norme}_{L/L}(2i)$ où $A=\mathcal{O}_K$. Reprenant le raisonnement du début on trouve un élément y de L entier sur $\mathbb{Z}$, dont toutes les valeurs absolues sont bornées,

soit c'est un élément primitif de L sur $\mathbb{Q}$, soit $\mathbb{Q}[y] = L_0$ et $[L : L_0] = 2$. Alors l'élément i n'est pas dans L_0 et $L = L_0[i]$. Les corps $\mathbb{Q}[y]$ étant dans une liste finie les corps L aussi. Il nous reste à montrer que K est dans une liste finie. Pour ceci on peut par exemple, sachant que $\mathrm{Aut}(L/\mathbb{Q})$ est fini, remarquer que K est un corps fix par un automorphisme de L sur $\mathbb{Q}$. □

Remarque 4.3. — Les démonstrations habituelles de 4.2 utilisent quand K est imaginaire un autre convexe symétrique compact pour conclure (cf. par exemple P. Samuel [Sa]). Ici comme en 4.1 et en 2.2 nous avons conservé la technique : "un élément non nul dans $H^0(L)$ doit être significatif". Le prix que nous payons dans ces trois cas est de regarder de plus près des extensions quadratiques imaginaires. Dans mon esprit il est satisfaisant de penser que les corps quadratiques jouent le rôle spécial des courbes hyperelliptiques en géométrie algébrique.

VI – Hauteur des points rationnels d'un schéma sur un corps de nombres

Nous définissons dans ce chapitre la hauteur d'un point rationnel sur K comme le degré d'Arakelov (III.5) d'un élément qui lui est associé dans $\mathrm{Pic}_c(\mathcal{O}_K)$. L'intérêt de cette présentation sur celle classique d'A. Weil est que les fonctions obtenues sont bien définies et non plus à constante près. Nous montrons quelques propriétés des hauteurs : théorème de Northcott, contrexemples à des énoncés fâcheux$\cdots$

1 – Fibrés inversibles métrisés sur un schéma sur $\mathbb{C}$.

Si X est un schéma sur $\mathbb{C}$ et si L est un faisceau inversible sur X, pour chaque point $P \in X(\mathbb{C})$ la restriction $L_{|P}$ est un espace vectoriel de dimension un sur $\mathbb{C}$. Nous allons "étendre" à cette situation plus globale (!) les notions de III.1.

Définition 1.1. — *Soit $X \xrightarrow{f} \mathrm{Spec}\,\mathbb{C}$ un schéma sur $\mathbb{C}$ et L un faisceau inversible sur X. On dit que L est* **métrisé** *si :*

a) pour tout point P de $X(\mathbb{C})$, l'espace vectoriel L/P est muni d'un produit scalaire hermitien non dégénéré.

b) Pour tout ouvert U de X et toute section $s \in \Gamma(U, L)$ la fonction $U(\mathbb{C} \to \mathbb{R})$, qui à P associek $|s(P)|$, est continue pour la topologie usuelle.

Lemme 1.2. — *Soit X un schéma projectif sur $\mathbb{C}$ et soit L un faisceau inversible sur X. Alors si, $|\cdot|_1$ et $|\cdot|_2$ sont deux métrisations de L, il existe une constante C telle que pour toute section s de L sur un ouvert U de X $|s(P)|_1 \leq C|s(P)|_2$ pour tout point P de $U(\mathbb{C})$.*

Par la proposition III 1.2 pour tout point P de $X(\mathbb{C})$ $|\cdot|_1 = \lambda(P)|\cdot|_2$ où $\lambda(P) \in \mathbb{R}_+^\times$. En choisissant une section locale de L au voisinage de chaque point $P \in X(\mathbb{C})$, la propriété b) de 1.1 montre que $\lambda : X(\mathbb{C}) \to \mathbb{R}_+$ est une fonction continue pour la topologie usuelle. Le schéma X étant projectif sur $\mathbb{C}$, l'ensemble de $X(\mathbb{C})$ de ses points sur $\mathbb{C}$ est compact pour la topologie usuelle (c'est un fermé de $\mathbb{P}^n(\mathbb{C})$). La fonction $\lambda(P)$ est donc bornée sur $X(\mathbb{C})$.

Exemple 1.3 : (**Métrique de Fubini-Study**). Soient n un entier et $P = \mathbb{P}^n_{\mathbb{C}}$ l'espace projectif de dimension n sur $\mathbb{C}$. Munissons $V = \Gamma(D, \mathcal{O}_P(1))$ d'un produit scalaire

hermitien non dégénéré tel que les $n+1$ sections canoniques V (cf. I.5.6) forment une base orthonormale de V. Le faisceau inversible $\mathcal{O}_P(1)$ étant engendré par ses sections on a un homomorphisme surjectif de faisceaux de $\mathcal{O}_P$ -modules :

$$\varphi : \mathcal{O}_P \otimes_{\mathcal{C}} V \to \mathcal{O}_P(1) \to 0 \ .$$

Pour chaque point Q de $P(\mathbb{C})$ on a ainsi un homomorphisme surjectif $f : \varphi_Q : V \to \mathcal{O}_P(1)_{|Q} \to 0$ de $\mathbb{C}$-espaces vectoriels. On munit $\mathcal{O}_P(1)_{|Q}$ du produit scalaire hermitien obtenu en écrivant que $\mathcal{O}_P(1)_{|Q}$ est orthogonal au noyau de φ_Q. Autrement dit la longueur d'un élément de $\mathcal{O}_P(1)_{|Q}$ est la distance d'un relèvement dans V au noyau de φ_Q. Soit $s_0 \cdots s_n$ est une base orthonormale de V. Si e est une base de $\mathcal{O}_P(1)_{|Q}$ sur $\mathbb{C}$ les nombres x_i définis par : $x_i e = \varphi_Q(s_i)$, sont les coordonnées homogènes du point Q. Un vecteur normal un unitaire à l'hyperplan $\ker \varphi_Q$ est alors $\left(\dfrac{x_i}{(\Sigma|x_i|^2)^{1/2}}\right) = \vec{n}_Q$. Pour obtenir la distance de $s = \Sigma\lambda_i s_i$ à cet hyperplan, on prend le produit scalaire $(s \cdot \vec{n}_Q)$ ce qui donne la formule :

$$|\varphi_Q(s)| = |s(Q)| = \frac{|\Sigma\lambda_i x_i|}{(\Sigma|x_i|^2)^{1/2}} \ .$$

Cette fonction sur $\mathbb{P}^n(\mathbb{C})$ est bien continue (elle est même réelle analytique).

2 – **Modèles entiers des schémas sur un corps**.

Il y a plusieurs façons de "chasser les dénominateurs" dans les équations d'un schéma sur corps. Il y a aussi plusieurs façons d'écrire un schéma comme fermé d'un $\mathbb{P}^n_K$ ou d'un $\mathbb{A}^n_K$. La notion de "modèle" tient compte de ces phénomènes.

Définition 2.1. — *Soient A un anneau intègre et K son corps de fractions. Si $X_K \xrightarrow{f} \operatorname{Spec} K$ est un K-schéma on appelle* **modèle de f sur A**, *un A-schéma $X \xrightarrow{g} \operatorname{Spec} A$ tel que $g \times_{\operatorname{Spec} A} \operatorname{Spec} K = f$. Un modèle de f sur A est aussi appelé un* **modèle de X_K sur A**.

Exemple 2.2 : $\mathbb{P}^n_A$ est un modèle de $\mathbb{P}^n_K$ sur A. Ce n'est pas le seul modèle projectif de $\mathbb{P}^n_K$. En effet l'éclatement d'un sous schéma Y fermé de $\mathbb{P}^n_A$ tel que $Y \times_{\operatorname{Spec} A} \operatorname{Spec} K$ soit vide donne un autre modèle.

Exemple 2.3 : (**Chasser les dénominateurs**). Si X_K est un sous schéma fermé de $\mathbb{P}^n_K$ défini par les équations homogènes à coefficients dans K $(F_i(X_0, \ldots, X_4))_{i=1\cdots r}$. En multipliant les F_i par un élément de A de telle façon que les coefficients de ces polynômes soient dans A, on a construit un modèle X de X_K qui est un sous-schéma fermé de $\mathbb{P}^n_A$. On a donc trouvé par la même occasion un "modèle" de $\mathcal{O}_{X_K}(1)$. Formalisons cette notion par une définition :

Définition 2.4. — *Soient A un anneau intègre, K son corps de fractions et $X \xrightarrow{f} \operatorname{Spec} A$ un A-schéma. Si $\mathcal{F}_K$ est un faisceau de $\mathcal{O}_{X_K}$ -modules sur X_K on appelle* **modèle de $\mathcal{F}_K$ sur A** *un faisceau de $\mathcal{F}$ de $\mathcal{O}_X$-modules tel que $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_K = \mathcal{F}_K$.*

Remarque 2.5. — On a ainsi défini la notion de modèle d'un couple $(X_K, \mathcal{F}_K)$ où X_K est un K-schéma et $\mathcal{F}_K$ est un faisceau de $\mathcal{O}_{X_K}$-modules. De même on a la notion de modèle entier d'un K-morphisme de schémas.

Exemple 2.6 : Soient P un point rationnel sur K d'un schéma projectif X_K sur un anneau de Dedekind A. Alors la section $s_P : \operatorname{Spec} A \to X$ correspondant à P est un modèle entier du morphisme $\operatorname{Spec} K \to X_K$.

PROPOSITION 2.7. — *Soient K un corps de nombres des schémas, X_K un schéma projectif sur K et L_K un faisceau inversible sur X_K. Soient (X_1, L_1) et (X_2, L_2) deux modèles de (X_K, L_K) sur $\mathcal{O}_K$. Alors il existe un entier n, ne dépendant que des (X_i, L_i), tel que pour tout corps de nombres L contenant K.*