AUTOUR DES ANNEAUX DE DEDEKIND, ASPECTS GÉOMÉTRIQUES ET ARITHMÉTIQUES

Sandrine Henri
sous la direction de Marco A. Garuti,
professeur à l'Université de Padoue

19 mai au 13 juillet 2008

Table des matières

Partie 1

Généralités

1.1 Clôture intégrale et anneaux de Dedekind

Dans tout ce document, les anneaux sont supposés commutatifs et unitaires, et les extensions de corps sont algébriques. Dans cette partie, nous introduisons différentes notions d'algèbre commutative, notamment celles de clôture intégrale, d'anneau de Dedekind et de ramification. Les parties suivantes ont pour but de donner des exemples de tels objets en théorie des nombres et en géométrie algébrique. Certains résultats sont admis dans ce document. Le lecteur pourra en trouver les démonstrations dans [1].

Définition 1.1.1 (entier sur un anneau, anneau entier). Soient L un anneau et A un sous-anneau de L. Si $\alpha \in L$ est racine d'un polynôme unitaire à coefficients dans A, on dit que α est un *entier sur* A.
Si tout élément de L est entier sur A, on dit que L est un *anneau entier sur* A.

Proposition 1.1.2. *Soient L un corps et A un sous-anneau de L. Soit $\alpha \in L$. Alors les propositions suivantes sont équivalentes :*

(i) *L'élément α est entier sur A.*

(ii) *Le sous-anneau $A[\alpha]$ de L est un A-module finiment engendré.*

(iii) *Il existe un A-sous-module M de L finiment engendré tel que $\alpha M \subset M$.*

Démonstration. (i) $\Rightarrow$ (ii). Soit $\alpha \in L$ un entier sur A. Soit $X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ un polynôme annulateur de α, avec $a_i \in A$ pour $i = 0, \ldots, n-1$. Montrons que le A-module $A[\alpha]$ est engendré par $1, \alpha, \ldots, \alpha^{n-1}$. Pour cela, il suffit de montrer que pour tout $i \geqslant n$, α^i est une combinaison linéaire de $1, \ldots, \alpha^{n-1}$ à coefficients dans A. Or, on a la relation

$$\alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1},$$

et une récurrence immédiate permet de conclure.

(ii) $\Rightarrow$ (iii). Il suffit de choisir $M = A[\alpha]$.

(iii) $\Rightarrow$ (i). Considérons une famille génératrice du A-module M, $(e_1, \ldots, e_n)$. Comme $\alpha e_i \in M$ pour tout i entre 1 et n, il existe des éléments $c_{ij} \in A$ tels que

$$\alpha e_i = \sum_{j=1}^{n} c_{ij} e_j.$$

Notons C la matrice $(c_{ij})_{1 \leqslant i,j \leqslant n}$, et E la transposée de la matrice $(e_1, \ldots, e_n)$. La relation précédente s'écrit sous forme matricielle $\alpha E = CE$, soit $(\alpha I_n - C)E = 0$, autrement dit, le noyau

de $\alpha I_n - C$ n'est pas réduit à 0. Les coefficients de $\alpha I_n - C$ étant dans un corps, à savoir L, ceci implique que le déterminant de $\alpha I_n - C$ est nul. Celui-ci est de la forme

$$\det(\alpha I_n - C) = \alpha^n + \sum_{k=0}^{n-1} a_k \alpha^i,$$

où les a_k s'expriment comme polynômes en les c_{ij}, donc sont des éléments de A. Ainsi, α est racine d'un polynôme unitaire à coefficients dans A, donc est entier sur A. □

Corollaire 1.1.3. *Soient L un corps et A un sous-anneau de L. Soit B l'ensemble des entiers de L sur A. Alors B est un sous-anneau de L.*

Démonstration. Bien entendu, $1 \in B$. Soient α et β deux éléments de B. Il s'agit de montrer que $\alpha + \beta$ et $\alpha\beta$ sont également des éléments de B.

D'après la proposition précédente, $A[\alpha]$ et $A[\beta]$ sont finiment engendrés comme A-modules. Notons $(e_1, \ldots, e_r)$ une famille génératrice de $A[\alpha]$ et $(f_1, \ldots, f_s)$ une famille génératrice de $A[\beta]$. Le A-module $A[\alpha, \beta]$ est engendré par la famille $(e_i f_j, 1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s)$, et donc est finiment engendré. Or, $(\alpha + \beta)A[\alpha, \beta] \subset A[\alpha, \beta]$ et $(\alpha\beta)A[\alpha, \beta] \subset A[\alpha, \beta]$. On conclut par l'implication (iii) $\Rightarrow$ (i) de la proposition précédente. □

Définition 1.1.4 (clôture intégrale). Soient L un corps et A un sous-anneau de L. L'anneau B des entiers de L sur A est appelé *clôture intégrale* de A dans L.

Définition 1.1.5 (anneau intégralement clos). On dit qu'un anneau intègre A est *intégralement clos* s'il est égal à sa clôture intégrale dans son corps de fractions.

Proposition 1.1.6. *Soient A un anneau intègre, K son corps des fractions, L une extension de K et B la clôture intégrale de A dans L. Alors*

(i) *Si $\alpha \in L$, il existe $b \in B$ et $a \in A$ tels que $\alpha = b/a$. En particulier, L est le corps des fractions de B.*

(ii) *L'anneau B est intégralement clos.*

(iii) *Si A est intégralement clos, alors $B \cap K = A$.*

Démonstration. (i) Soient $\alpha \in L$ et $g \in K[X]$ un polynôme annulateur. Comme K est le corps des fractions de A, on peut écrire

$$g = X^n + \frac{c_{n-1}}{d_{n-1}} X^{n-1} + \cdots + \frac{c_0}{d_0}$$

avec $c_i, d_i \in A$ et $d_i \neq 0, \forall i = 0, \ldots, n-1$. Posons $d = \prod_{i=0}^{n-1} d_i$. On a $d^n g(\alpha) = 0$, c'est-à-dire :

$$(d\alpha)^n + \frac{c_{n-1}}{d_{n-1}} d(d\alpha)^{n-1} + \cdots + \frac{c_0}{d_0} d^n = 0.$$

Par construction, $\frac{c_i}{d_i} d \in A$, $\forall i = 0, \ldots, n-1$, et donc $d\alpha$ est racine d'un polynôme unitaire à coefficients dans A. Ainsi, $b = d\alpha \in B$, et $\alpha = b/d$, ce qui conclut.

(ii) Soit B' la clôture intégrale de B dans L. Il s'agit de montrer que tout élément de B' est entier sur A. Soit $\alpha \in B'$. Comme α est entier sur B, il existe

$$g(X) = X^n + b_{n-1} X^{n-1} + \cdots + b_0 \in B[X]$$

tel que $g(\alpha) = 0$. Considérons le sous-anneau $A[b_0, \ldots, b_{n-1}]$ de B'. Alors $A[b_0, \ldots b_{n-1}]$ est un A-module finiment engendré. En effet, les b_i sont tous entiers sur A. D'après la proposition

1.1.2, $A[b_0]$ est un A-module finiment engendré. Supposons par récurrence que $A[b_0, \ldots, b_i]$ est engendré par des éléments $e_1, \ldots, e_r$. Comme b_{i+1} est entier sur A, $A[b_{i+1}]$ est engendré par un nombre fini d'éléments $f_1, \ldots, f_s$. Finalement, $A[b_0, \ldots, b_{i+1}]$ est engendré par les $e_i f_j$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. Et donc, par récurrence, $A[b_0, \ldots b_{n-1}]$ est finiment engendré. Le A-module $A[b_0, \ldots, b_{n-1}, \alpha]$ est lui-aussi finiment engendré, par l'ensemble

$$\{u_i \alpha^k, 1 \leqslant i \leqslant m, 0 \leqslant k \leqslant n-1\}$$

où $(u_i)_{1 \leqslant i \leqslant m}$ est une famille génératrice de $A[b_0, \ldots, b_{n-1}]$. De plus, $\alpha A[b_0, \ldots, b_{n-1}, \alpha] \subset A[b_0, \ldots, b_{n-1}, \alpha]$. La proposition 1.1.2 assure alors que α est entier sur A.

(iii) Immédiat d'après les définitions de clôture intégrale et d'anneau intégralement clos. □

Définition 1.1.7 (anneau noethérien). On dit qu'un anneau est noethérien si tous ses idéaux sont engendrés par un nombre fini d'éléments.

Définition 1.1.8 (anneau de Dedekind). Soit A un anneau intègre qui n'est pas un corps. On dit que A est un anneau de Dedekind s'il vérifie les trois propriétés suivantes :

(i) A est noethérien,

(ii) tout idéal premier non nul de A est maximal,

(iii) A est intégralement clos.

Remarque. Tout anneau principal est un anneau de Dedekind. La propriété (i) est évidente ; montrons les propriétés (ii) et (iii).

Démonstration de (ii). Soit A un anneau principal, et $(p) \subset A$ un idéal premier non nul. Montrons que (p) est maximal. Soit (q) un idéal tel que $(p) \subset (q)$. Il existe $a \in A$ tel que $aq = p$. Comme (p) est premier, on a soit $a \in (p)$, soit $q \in (p)$.

Dans le premier cas, si $a \in (p)$, il existe $b \in A$ tel que $a = bp$. Donc $bpq = p$, et comme A est intègre et p non nul, $bq = 1$. Donc q est inversible et $(q) = A$.

Dans le deuxième cas, si $q \in (p)$, alors $(q) \subset (p)$ et donc $(q) = (p)$. □

Démonstration de (iii). On montre plus généralement que cette propriété est vraie pour tout anneau factoriel. Soit A un anneau factoriel, et notons K son corps des fractions. Soit $x \in K$ un élément entier. On écrit $x = \frac{b}{c}$, avec b et c deux éléments de A premiers entre eux, et $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, avec les a_i dans A. Ainsi,

$$-b^n = c(a_{n-1}b^{n-1} + \cdots + a_0 c^{n-1}).$$

Comme A est factoriel, tout facteur premier de c divise b. Or, b et c sont premiers entre eux, donc c est une unité, et $x \in A$. □

Dans la suite, nous aurons également besoin de la définition et du théorème suivant :

Définition 1.1.9 (extension séparable). Soient K un corps et L une extension de K. On dit que l'extension L/K est *séparable* si tout élément de L est racine d'un polynôme de $K[X]$ à racines simples dans $\overline{K}[X]$.

Théorème 1.1.10 (élément primitif). *Soit L/K une extension finie séparable. Alors il existe $\alpha \in L$ tel que $L = K(\alpha)$ (on dit que l'extension est* monogène*).*

Théorème 1.1.11. *Soit A un anneau intègre noethérien et intégralement clos, de corps de fractions K. Soit L une extension finie séparable de K, et B la clôture intégrale de A dans L. Alors B est un A-module finiment engendré. En particulier, B est noethérien.*

Théorème 1.1.12. *Soit A un anneau de Dedekind. Soient K le corps des fractions de A et L une extension finie séparable de K. Alors la clôture intégrale B de A dans L est un anneau de Dedekind.*

Démonstration. On a déjà établi que l'anneau B est intégralement clos dans la proposition 1.1.6.

Montrons que tout idéal premier non nul de B est maximal. Soit $\mathfrak{P}$ un tel idéal. On pose $P = \mathfrak{P} \cap A$; on a $P \neq A$ car $\mathfrak{P} \neq B$. L'anneau A/P est intègre, car il s'injecte dans $B/\mathfrak{P}$ qui est intègre, et donc l'idéal P de A est premier. Montrons que $P \neq (0)$. Soit $\alpha \in \mathfrak{P}$, $\alpha \neq 0$. Comme tout élément de B est entier sur A, il existe un polynôme unitaire $f \in A[X]$ tel que $f(\alpha) = 0$. On choisit f de degré minimal, et on écrit

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0.$$

L'élément a_0 de A est non nul. En effet, si c'était le cas, on aurait

$$\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1) = 0,$$

et comme B est intègre et α non nul, $\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \cdots + a_1 = 0$. Ainsi, α serait annulé par un polynôme unitaire de degré strictement inférieur à celui de f, ce qui n'est pas possible puisqu'on a choisi f de degré minimal. Par ailleurs,

$$a_0 = -\alpha^n - a_{n-1}\alpha^{n-1} - \cdots - \alpha a_1 \in \mathfrak{P}$$

et comme a_0 est aussi dans A, il est dans P. On a montré que P contient un élément non nul, donc il est non nul. Or, l'anneau A est un anneau de Dedekind, et donc l'idéal P est maximal. Autrement dit, A/P est un corps. Montrons que $B/\mathfrak{P}$ est également un corps. Le fait que B soit un anneau entier sur A implique que $B/\mathfrak{P}$ est un anneau entier sur A/P. Soit $\gamma \in B/\mathfrak{P}$, non nul. On a une relation

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

avec les c_i dans A/P et n minimal, et de même que précédemment pour a_0, on montre que c_0 est non nul. C'est un élément du corps A/P, et il est donc inversible. Alors

$$\gamma(-c_0^{-1}\gamma^{n-1} - c_0^{-1}c_{n-1}\gamma^{n-2} - \cdots - c_0^{-1}c_1) = 1$$

et γ est inversible. Donc $B/\mathfrak{P}$ est un corps, et $\mathfrak{P}$ est maximal.

Le fait que B est noethérien est une conséquence du théorème 1.1.11. □

1.2 Propriétés de factorisation

1.2.1 Factorisation des idéaux

Rappel. On dit qu'un anneau intègre est factoriel si tout élément non nul peut s'écrire de manière unique (à l'ordre près des facteurs) comme le produit d'un inversible et d'éléments irréductibles.

Dans cette section, nous allons définir une autre propriété de factorisation, qui, elle, met en jeu des idéaux.

Définition 1.2.1 (produit d'idéaux). Soient I et J deux idéaux d'un anneau A. On note IJ l'idéal de A engendré par les produits xy pour $x \in I$ et $y \in J$. Ainsi,

$$IJ = \{x_1y_1 + \cdots + x_ny_n, n \in \mathbb{N}, x_i \in I, y_j \in J\}.$$

Définition 1.2.2 (factorisation des idéaux). Soit A un anneau intègre. On dit que A a *la propriété de factorisation unique des idéaux* si tout idéal I strict de A s'écrit $I = \mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_r$, où les $\mathfrak{P}_i$ sont des idéaux premiers, et où cette factorisation est unique au sens suivant : si $I = \mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}s$, alors $r = s$ et $\mathfrak{P}_i = \mathfrak{Q}_{\sigma(i)}$ pour une certaine permutation $\sigma \in \mathfrak{S}_r$.

Dans la suite, nous allons nous intéresser aux points clés de la démonstration du théorème suivant :

Théorème 1.2.3. *Soit A un anneau noethérien, dont tous les idéaux premiers non nuls sont maximaux. Alors A possède la propriété de factorisation unique des idéaux si et seulement si A est intégralement clos.*

Corollaire 1.2.4. *Tout anneau de Dedekind a la propriété de factorisation unique des idéaux.*

Démonstration du corollaire. Ceci est immédiat d'après la définition d'anneau de Dedekind et le théorème 1.2.3. □

1.2.2 Localisation

Définition 1.2.5 (partie multiplicative). Soit A un anneau. Une partie S de A est dite *multiplicative* si $1 \in S$ et si pour tous $a, b \in S$, le produit ab appartient à S.

On considère la relation $\mathcal{R}_S$ définie sur $A \times S$ par $(a, s)\,\mathcal{R}_S\,(b, t)$ si et seulement il existe $r \in S$ tel que $r(at - bs) = 0$.

Remarque. Si A est intègre, et $0 \notin S$, alors $(a, s)\,\mathcal{R}_S\,(b, t)$ si et seulement si $at - bs = 0$.

Lemme 1.2.6. *La relation $\mathcal{R}_S$ est une relation d'équivalence sur $A \times S$.*

Démonstration. Le fait que $\mathcal{R}_S$ soit réflexive et symétrique est évident.

Supposons que $(a, s)\,\mathcal{R}_S\,(b, t)$ et $(b, t)\,\mathcal{R}_S\,(c, u)$. Il existe q et r dans S tels que $q(at-bs) = 0$ et $r(bu - ct) = 0$. On a

$$qrt(au - cs) = qru(at - bs) + qrs(bu - ct) = 0,$$

et comme S est multiplicative, $qrt \in S$, ce qui conclut. □

Notation. On note $A[S^{-1}]$ l'ensemble quotient $A \times S/\mathcal{R}_S$. La classe de (a, s) est notée a/s.

On munit l'ensemble $A[S^{-1}]$ d'une structure d'anneaux de la manière suivante :

$$\begin{aligned} (a/s) + (b/t) &= (at + bs)/ts \\ (a/s)(b/t) &= ab/ts \\ 1/1 &= 1_{S^{-1}A} \end{aligned}$$

L'application

$$\begin{aligned} j_S \;:\; A &\longrightarrow A[S^{-1}] \\ a &\longmapsto a/1 \end{aligned}$$

est un morphisme d'anneaux. Pour tout $s \in S$, $j_S(s) = s/1$ est inversible d'inverse $1/s$.

Lemme 1.2.7. *Soient A un anneau et $\mathfrak{P}$ un idéal premier de A. Alors l'ensemble $S = A\backslash\mathfrak{P}$ est une partie multiplicative.*

Démonstration. Un idéal premier est strict, donc $1 \notin \mathfrak{P}$, donc $1 \in S$. Si $a, b \in S$, alors $a, b \notin \mathfrak{P}$; donc $ab \notin \mathfrak{P}$ car $\mathfrak{P}$ est premier. Donc $ab \in S$. □

Définition 1.2.8 (localisé). Soit $\mathfrak{P}$ un idéal premier de A. L'anneau $A[(A\backslash\mathfrak{P})^{-1}]$ est appelé *localisé de A en $\mathfrak{P}$* et est noté $A_{\mathfrak{P}}$.

Rappel. On dit qu'un anneau est local s'il a un unique idéal maximal.

Le terme de « localisé » est justifié par la proposition suivante :

Proposition 1.2.9. *Soient A un anneau et $\mathfrak{P}$ un idéal premier de A. Le localisé $A_{\mathfrak{P}}$ est un anneau local.*

Démonstration. Soit $\mathfrak{P}A_{\mathfrak{P}} = \{p/s, p \in \mathfrak{P}, s \notin \mathfrak{P}\}$. On vérifie facilement que $\mathfrak{P}A_{\mathfrak{P}}$ est un idéal strict, et que tout élément qui n'est pas dedans est inversible. Ceci implique que $\mathfrak{P}A_{\mathfrak{P}}$ est un idéal maximal et qu'il est unique. □

Proposition 1.2.10. *Soit A un anneau intègre. Alors dans le corps des fractions de A, on a*

$$A = \bigcap_{\mathfrak{P} \text{ premier}} A_{\mathfrak{P}}.$$

Démonstration. Notons $K = A_{(0)}$ le corps des fractions de A. Pour tout idéal premier $\mathfrak{P}$ de A, on a $A \subset A_{\mathfrak{P}} \subset K$. Ainsi,

$$A \subset \bigcap_{\mathfrak{P}} A_{\mathfrak{P}}.$$

Inversement, si $a/b \in A_{\mathfrak{P}}$ pour tout $\mathfrak{P}$, alors, quel que soit $\mathfrak{P}$, $b \notin \mathfrak{P}$, et donc b est inversible dans A (sinon l'idéal (b) serait inclus dans un idéal maximal, donc premier). Donc $a/b = ab^{-1} \in A$. □

Proposition 1.2.11. *Soit $\mathfrak{P}$ un idéal premier d'un anneau A. Alors l'ensemble des idéaux premiers de $A_{\mathfrak{P}}$ est en bijection avec l'ensemble des idéaux premiers de A inclus dans $\mathfrak{P}$.*

Démonstration. Notons $S = A\backslash\mathfrak{P}$. Considérons l'application qui a un idéal premier P de A inclus dans $\mathfrak{P}$ associe l'idéal $I = PA_{\mathfrak{P}}$ de $A_{\mathfrak{P}}$, et montrons qu'il s'agit d'une bijection entre les ensembles qui nous intéressent. Plus précisément, on montre qu'elle a pour réciproque l'application qui a un idéal premier J de $A_{\mathfrak{P}}$ associe $Q = j_S^{-1}(J) \cap A$.

☞ L'idéal I est premier dans $A_{\mathfrak{P}}$. En effet, soient a/s et b/t dans $A_{\mathfrak{P}}$ tels que $(a/s)(b/t) = (ab)/(st) \in I$ (avec $a, b \in A$ et $s, t \in S$). Il existe $p \in P$ et $r \in S$ tels que $(ab)/(st) = p/r$. Par définition, il existe donc $u \in S$ tel que $u(abr - stp) = 0$. En particulier, $uabr \in P$. Or, $u, r \notin \mathfrak{P}$ et $P \subset \mathfrak{P}$ donc $u, r \notin P$. Comme P est premier, nécessairement $a \in P$ ou $b \in P$. Et par conséquent, $a/s \in I$ ou $b/t \in I$.

☞ L'idéal Q est premier dans A et inclus dans $\mathfrak{P}$. En effet, soient $x, y \in A$ tels que $xy \in Q$. Alors $(xy)/1 = (x/1)(y/1) \in J$ donc $x/1 \in J$ ou $y/1 \in J$, car J est premier. Par suite, $x \in Q$ ou $y \in Q$ et Q est premier. Soit $x \in Q$. En particulier, $x/1 \in J$ qui est un idéal strict car premier, donc $x/1$ n'est pas inversible dans $A_{\mathfrak{P}}$. Cela implique que x n'est pas dans S. Il est dans A, donc dans $\mathfrak{P} = A\backslash S$.

☞ On a $I \cap A = P$. L'inclusion $P \subset j_S^{-1}(I) \cap A$ est immédiate. Inversement, si $x \in j_S^{-1}(I) \cap A$, on a $x/1 = a/s$ avec $a \in P$ et $s \in S$. Par définition, il existe $r \in S$ tel que $r(xs - a) = 0$. Donc $rxs = ra \in P$, puis comme P est premier et que, en raison de l'inclusion $P \subset \mathfrak{P}$, $rs \notin P$, on en déduit $x \in P$.

☞ On a $J = QA_{\mathfrak{P}}$. Soit $a/s \in J$, avec $a \in A$ et $s \in S$. Alors $a/1 = (a/s)(s/1) \in J$, et donc $a \in j_S^{-1}(J) \cap A = Q$. Il s'ensuit que $a/s \in QA_{\mathfrak{P}}$. Soit maintenant $a/s \in QA_{\mathfrak{P}}$, avec $a \in Q$ et $s \in S$. En particulier, $a/1 \in J$ et donc $a/s = (a/1)(1/s) \in J$.

Notre proposition est démontrée. □

1.2.3 Points clés de la démonstration du théorème 1.2.3

Nous admettrons certaines étapes de la démonstration ; pour une preuve complète, le lecteur pourra se référer à [1].

Lemme 1.2.12. *Soit A un anneau intègre noethérien dont tous les idéaux premiers non nuls sont maximaux. Alors les affirmations suivantes sont équivalentes :*

(i) *A est intégralement clos.*

(ii) *A_P est intégralement clos pour tout idéal premier P de A.*

Démonstration. (i) $\Rightarrow$ (ii) Soit K le corps des fractions de A (et de A_P). Soit $x \in K$ non nul. On écrit $x = a/b$ avec $a, b \in A$. Supposons que x est entier sur A_P, et soit $f \in A_P[X]$ un polynôme unitaire tel que $f(x) = 0$. On écrit

$$f = X^n + \frac{a_{n-1}}{s_{n-1}} X^{n-1} + \cdots + \frac{a_0}{s_0}$$

avec $a_i \in A$ et $s_i \in A \backslash P$. Posons $s = \prod_{i=0}^{n-1} s_i$. Comme $s^n f(a/b) = 0$, on trouve que $sa/b \in K$ est entier sur A :

$$\left(\frac{sa}{b}\right)^n + \frac{a_{n-1}s}{s_{n-1}} \left(\frac{sa}{b}\right)^{n-1} + \cdots + \frac{a_0 s^n}{s_0} = 0.$$

L'hypothèse A intégralement clos, assure que $c = sa/b$ est un élément de A. Et donc $x = a/b = c/s$ est un élément de A_P. Donc A_P est intégralement clos.

(ii) $\Rightarrow$ (i) Soit x un entier sur A, et $f \in A[X]$ unitaire tel que $f(x) = 0$. Pour tout idéal P premier de A, $A \subset A_P$ donc x est entier sur A_P. Comme A_P est intégralement clos, $x \in A_P$. Par ailleurs, on a vu dans la proposition 1.2.10 que

$$\bigcap_P A_P = A$$

donc $x \in A$, et A est intégralement clos. □

Lemme 1.2.13. *Soit A un anneau noethérien dont tous les idéaux premiers non nuls sont maximaux. Alors pour tout idéal maximal M de A, A_M est noethérien et ses seuls idéaux premiers sont (0) et MA_M.*

Démonstration. Ceci est un corollaire de la proposition 1.2.11. □

Lemme 1.2.14. *Soit A un anneau local, noethérien, dont tous les idéaux premiers non nuls sont maximaux. Alors les affirmations suivantes sont équivalentes :*

(i) *A a la propriété de factorisation unique des idéaux.*

(ii) *A est principal.*

(iii) *A est intégralement clos.*

Lemme 1.2.15. *Soit A un anneau noethérien dont tous les idéaux premiers non nuls sont maximaux. Alors A a la propriété de factorisation unique des idéaux si et seulement si A_M a la propriété de factorisation unique des idéaux pour tout idéal maximal M de A.*

Le théorème 1.2.3 est un corollaire des lemmes 1.2.12, 1.2.13, 1.2.14 et 1.2.15

1.3 Ramification

1.3.1 Indice de ramification

Lemme 1.3.1. *Soient A un anneau de Dedekind, K son corps des fractions, L une extension finie de K et B la clôture intégrale de A dans L. Soit P un idéal maximal de A. Alors $PB \neq B$.*

Ainsi, l'idéal PB de B est non-trivial, et comme B est un anneau de Dedekind, il se factorise de manière unique en un produit d'idéaux maximaux

$$PB = M_1^{e_1} \cdots M_s^{e_s}$$

où les M_i sont distincts et les e_i des entiers strictement positifs.

Définition 1.3.2 (indice de ramification). L'entier e_i défini comme ci-dessus est appelé *indice de ramification de M_i au dessus de P* et est noté $e_{M_i/P}$. Si M n'intervient pas dans la décomposition au dessus de P on note $e_{M/P} = 0$.

Remarque. Les idéaux maximaux M_i sont exactement ceux vérifiant $P = M_i \cap A$.

Définition 1.3.3 (degré résiduel). Si B est un A-module finiment engendré[1], le corps B/M_i est une extension finie du corps A/P. On appelle *degré résiduel de M_i au dessus de P* et on note $f_{M_i/P}$ le degré de cette extension.

Théorème 1.3.4. *Soient A un anneau de Dedekind de corps de fractions K, L une extension finie de K, B la clôture intégrale de A dans L. Si B est un A-module finiment engendré, alors*

$$[L : K] = \sum_M e_{M/P} f_{M/P}$$

où la somme est prise sur l'ensemble des idéaux maximaux qui interviennent dans la décomposition de PB.

Définition 1.3.5 (idéal ramifié). Soient A un anneau de Dedekind, K son corps des fractions, L une extension finie de K, B la clôture intégrale de A dans L. On suppose que B est un A-module finiment engendré. Soit M un idéal maximal de B et $P = M \cap A$. On dit que l'idéal M est *ramifié au dessus de P* (ou au dessus de A) si, soit $e_{M/P} > 1$, soit l'extension B/M de A/P n'est pas séparable.

On dit qu'un idéal maximal P de A *se ramifie dans B* si l'idéal PB est contenu dans un idéal maximal M de B qui est ramifié au dessus de P.

Proposition 1.3.6. *Soit A un anneau de Dedekind. Soit $f \in A[Y]$ un polynôme irréductible unitaire. Soit α une racine de f dans une clôture algébrique du corps des fractions K de A. On note M un idéal maximal de $A[\alpha]$ et $P = M \cap A$. Enfin, on écrit $f(Y) = h(Y) + \prod_{i=1}^s g_i(Y)^{e_i}$ où $h \in PA[Y]$ et où les g_i sont tels que $\bar{f} = \prod_{i=1}^s \bar{g}_i^{e_i}$ est la factorisation en polynômes irréductibles dans $(A/P)[Y]$ de la réduction de f modulo P. Alors*

(1) *L'idéal M est engendré par les éléments de P et $g_{i_0}(\alpha)$ pour un certain $i_0 \in \{1, \ldots, s\}$ unique.*

(2) *Les propositions suivantes sont équivalentes :*

   (i) $f'(\alpha) \notin M$.

   (ii) $e_{i_0} = 1$ *et l'extension $A[\alpha]/M$ est séparable sur A/P.*

[1] D'après le théorème 1.1.11, c'est notamment le cas si l'extension L/K est séparable

(3) *Soit π un générateur de l'idéal maximal PA_P de A_P. L'anneau $A[\alpha]_M$ est un idéal principal si et seulement si $MA[\alpha]_M$ peut être engendré soit par π, soit par $g_{i_0}(\alpha)$.*

(4) *Si $e_{i_0} = 1$, alors l'anneau $A[\alpha]_M$ est un idéal principal, et l'idéal maximal $MA[\alpha]_M$ est engendré par π. En particulier, $e_{M/P} = 1$.*

(5) *L'anneau $A[\alpha]$ est un anneau de Dedekind si et seulement si l'anneau $A[\alpha]_M$ est un idéal principal pour tout idéal M contenant $f'(\alpha)$. Si f est un polynôme dont toutes les racines dans $\overline{K}$ sont simples, alors il n'y a qu'un nombre fini d'idéaux maximaux de $A[\alpha]$ qui contiennent $f'(\alpha)$.*

Corollaire 1.3.7. *Avec les notations de la proposition précédente,*

(i) *Si $f'(\alpha) \notin M$, alors $A[\alpha]_M$ est un anneau principal si et seulement si M n'est pas ramifié au dessus de A.*

(ii) *Si $A[\alpha]$ est un anneau de Dedekind, alors M est ramifié au dessus de A si et seulement si $f'(\alpha) \in M$.*

1.3.2 Discriminants

Définition 1.3.8 (résultant). Soit A un anneau, et soient $f = a_n X^n + \cdots + a_0$ et $g = b_m X^m + \cdots + b_0$ deux polynômes de $A[X]$ avec a_n et b_m non nuls. On appelle résultant de f et g, et on note $\mathrm{Res}(f, g)$, le déterminant de la matrice de l'application linéaire $A_{m-1}[X] \times A_{n-1}[X] \to A_{m+n-1}[X]$, $(u, v) \mapsto uf + vg$ (où $A_r[X]$ désigne l'espace des polynômes de degré inférieur où égal à r), dans les bases canoniques, à savoir :

$$\left.\begin{pmatrix} a_n & \cdots & a_1 & a_0 & & & \\ & a_n & \cdots & a_1 & a_0 & & \\ & & \ddots & & \ddots & \ddots & \\ & & & a_n & \cdots & a_1 & a_0 \\ b_m & \cdots & \cdots & b_1 & b_0 & & \\ & \ddots & & & \ddots & \ddots & \\ & & b_m & \cdots & \cdots & b_1 & b_0 \end{pmatrix}\right\} \begin{matrix} \} m \\ \\ \\ \\ \} n \\ \\ \\ \end{matrix}$$

Définition 1.3.9 (discriminant d'un polynôme). Soit A un anneau, et soit $f \in A[X]$, de degré n, de coefficient dominant a_n. On suppose que a_n est inversible dans A. On appelle discriminant de f l'élément

$$\mathrm{disc}(f) = a_n^{-1}(-1)^{n(n-1)/2} \mathrm{Res}(f, f').$$

Exemple 1.3.10. Supposons que $f = aX^2 + bX + c$. On a

$$\mathrm{Res}(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = 4a^2c - ab^2$$

et $\mathrm{disc}(f) = b^2 - 4ac$. On retrouve bien l'expression connue.

Proposition 1.3.11. *Soit A un anneau intègre et $f \in A[X]$ un polynôme unitaire. Soit $\overline{K}$ une clôture algébrique du corps des fractions de A, et soient $\alpha_1, \ldots \alpha_n \in \overline{K}$ les racines de f. Alors*

$$\mathrm{disc}(f) = \prod_{i=1}^{n} \prod_{j>i} (\alpha_j - \alpha_i)^2.$$

Définition 1.3.12 (discriminant d'une base). Soient A un anneau intégralement clos, de corps de fractions K, L une extension finie de K de degré n et B la clôture intégrale de A dans L. Soit $(b_1, \ldots, b_n)$ une K-base de L. On appelle discriminant de $(b_1, \ldots, b_n)$ l'élément

$$\mathrm{disc}(b_1, \ldots, b_n) = \det(\mathrm{Tr}_{L/K}(b_i b_j)_{i,j})$$

où $\mathrm{Tr}_{L/K}(\alpha) \in K$, pour $\alpha \in L$, désigne la trace de l'application K-linéaire de multiplication par α dans L.

Remarque. Avec les notations de la définition précédente, si les b_i sont dans B, alors $\mathrm{disc}(b_1, \ldots, b_n)$ est dans A car $B \cap K = A$.

Ces deux notions de discriminant sont liées par la relation suivante :

Proposition 1.3.13. *Soit L/K une extension finie séparable, et $\alpha \in L$ tel que $L = K(\alpha)$. Soit $f \in K[X]$ le polynôme minimal de α, et n le degré de f. Alors*

$$\mathrm{disc}(f) = \mathrm{disc}(1, \alpha, \ldots, \alpha^{n-1}).$$

Définition 1.3.14 (idéal discriminant, différente). Soient A un anneau de Dedekind, K son corps de fractions, L une extension finie de K et B la clôture intégrale de A dans L.
On note $\mathcal{D}_{A/B}$ l'idéal de B

- engendré par les éléments de la forme $f'(\alpha)$, avec α tel que $L = K(\alpha)$ et f le polynôme de minimal de α, si un tel α existe,
- (0) sinon.

Cet idéal est appelé *différente* de B/A.
On note $\Delta_{B/A}$ l'idéal de A engendré par les éléments de la forme $\mathrm{disc}(b_1, \ldots, b_n)$, pour les K-bases $(b_1, \ldots, b_n)$ de L contenues dans B. Cet idéal est appelé *idéal discriminant* de B/A.

Le lemme suivant est utile pour des calculs explicites de $\Delta_{B/A}$:

Lemme 1.3.15. *Avec les notations précédentes, on suppose en outre qu'il existe α tel que $B = A[\alpha]$. Alors $\Delta_{B/A} = (\mathrm{disc}(f))$ où f est le polynôme minimal de α. Plus précisément,* $\mathrm{disc}(f) = \mathrm{disc}(1, \alpha, \cdots, \alpha^{n-1})$.

Théorème 1.3.16. *Soient A un anneau de Dedekind, K son corps de fractions, L une extension finie séparable de K et B la clôture intégrale de A dans L.*

(i) *Soit M un idéal maximal de B. Alors M est ramifié au dessus de A si et seulement si $\mathcal{D}_{B/A} \subset M$.*

(ii) *Soit P un idéal maximal de A. Alors P se ramifie dans B si et seulement si $\Delta_{B/A} \subset P$.*

Corollaire 1.3.17. *Il n'y a qu'un nombre fini d'idéaux maximaux de B ramifiés au dessus de A, et un nombre fini d'idéaux de A qui se ramifient dans B.*

Nous admettons la partie (i) du théorème. On peut montrer en utilisant la notion de *norme* qu'elle est équivalente à la partie (ii).

1.3.3 Démonstration du théorème 1.3.16 (ii)

Commençons par démontrer le théorème dans le cas où l'anneau A est principal. Dans ce cas, B est un A-module libre de rang n. Soit $(b_1, \ldots, b_n)$ une base. Alors $\Delta_{B/A} = \mathrm{disc}(b_1, \ldots, b_n)A$. L'application bilinéaire

$$\begin{array}{rcl} \mathrm{Tr} : L \times L & \longrightarrow & K \\ (x, y) & \longmapsto & \mathrm{Tr}_{L/K}(xy) \end{array}$$

induit une application $\mathrm{Tr} : B \times B \to A$. Soit P un idéal maximal de A. Notons $\bar{x}$ la classe d'un élément $x \in A$ dans A/P (resp. d'un élément $x \in B$ dans B/PB). On vérifie aisément que B/PB est un A/P-espace vectoriel de dimension n dont une base est $(\bar{b}_1, \ldots, \bar{b}_n)$. Soit

$$\begin{array}{rcl} \overline{\mathrm{Tr}} : B/PB \times B/PB & \longrightarrow & A/P \\ (u, v) & \longmapsto & \mathrm{Tr}_{(B/PB)/(A/P)}(uv) \end{array}.$$

On trouve que pour tout $x, y \in B$, $\overline{\mathrm{Tr}(xy)} = \overline{\mathrm{Tr}}(\overline{xy})$ dans A/P. Il s'ensuite que la matrice $\overline{T}$ de la forme bilinéaire $\overline{\mathrm{Tr}}$ dans la base $(\bar{b}_1, \ldots \bar{b}_n)$ est la réduction modulo P de la matrice T de la forme Tr dans la base $(b_1, \ldots, b_n)$. En particulier,

$$\begin{array}{rcl} \Delta_{B/A} \subset P & \Leftrightarrow & \mathrm{disc}(b_1, \ldots, b_n) \in P \\ & \Leftrightarrow & \det(T) \in P \\ & \Leftrightarrow & \overline{\det(T)} = 0 \text{ dans } A/P \\ & \Leftrightarrow & \det(\overline{T}) = 0 \text{ dans } A/P. \end{array}$$

Soit $PB = M_1^{e_1} \cdots M_s^{e_s}$ la factorisation de PB dans B. Alors par le lemme chinois,

$$B/PB \simeq B/M_1^{e_1} \times \cdots \times B/M_s^{e_s}.$$

Posons maintenant

$$\begin{array}{rcl} \overline{\mathrm{Tr}}_i : B/M_i^{e_i} \times B/M_i^{e_i} & \longrightarrow & A/P \\ (\alpha, \beta) & \longmapsto & \mathrm{Tr}_{(B/m_i^{e_i})/(A/P)}(\alpha\beta) \end{array}.$$

Si l'on choisit pour tout i une A/P-base $\mathcal{B}_i$ de $B/M_i^{e_i}$, et que l'on considère la A/P-base « concaténée » $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_s$ de B/PB, on remarque que la matrice de la forme bilinéaire $\overline{\mathrm{Tr}}$ dans $\mathcal{B}$ est formée de blocs diagonaux représentants les formes $\overline{\mathrm{Tr}}_i$ dans la base $\mathcal{B}_i$. Il s'ensuit que

$$\det(\overline{\mathrm{Tr}}) = \prod_{i=1}^{s} \det(\overline{\mathrm{Tr}}_i).$$

En particulier, $\det(\overline{\mathrm{Tr}}) = 0$ si et seulement si il existe $i \in \{1, \ldots, s\}$ tel que $\det(\overline{\mathrm{Tr}}_i) = 0$. Ainsi, pour prouver le théorème 1.3.16 (ii) lorsque A est principal, il reste à montrer que

$$\det(\overline{\mathrm{Tr}}_i) \neq 0 \Leftrightarrow e_i = 1 \text{ et } B/M_i \text{ est une extension séparable de } A/P.$$

Commençons par montrer que si $\det(\overline{\mathrm{Tr}}_i) \neq 0$, alors $e_i = 1$. En effet, si $e_i > 1$, l'algèbre $B/M_i^{e_i}$ contient des éléments nilpotents : tout $z \in M_i/M_i^{e_i}$ est nilpotent car $z^{e_i} = 0$ dans $M_i/M_i^{e_i}$. Le lemme suivant montre que dans ce cas, $\det(\overline{\mathrm{Tr}}_i)$ est nécessairement nul.

Lemme 1.3.18. *Soit $\mathcal{A}$ une k-algèbre de dimension n. Si $\mathcal{A}$ contient un élément nilpotent non nul a, alors le discriminant de la forme bilinéaire $\mathrm{Tr} : \mathcal{A} \times \mathcal{A} \to k$ est égal à 0.*

Démonstration. Comme a est nilpotent, son polynôme caractéristique dans $k[X]$ est égal à X^n. En particulier, $\mathrm{Tr}_{\mathcal{A}/k}(a) = 0$. L'algèbre $\mathcal{A}$ étant commutative, tout multiple de a est également nilpotent. Soit $(a, a_2, \ldots, a_n)$ une base de $\mathcal{A}$ sur k. Alors la matrice de la forme bilinéaire Tr dans la base $(a, a_2, \ldots, a_n)$ a sa première colonne nulle, et donc est de déterminant nul. □

Nous allons maintenant montrer que si $e_i = 1$, alors $\det(\overline{\mathrm{Tr}}_i) \neq 0$ si et seulement si B/M_i est séparable sur A/P, ce qui achèvera la démonstration du théorème lorsque A est principal.

Tout d'abord, supposons que B/M_i est une extension séparable de A/P. Soit $\alpha \in B/M_i$ tel que $B/M_i = A/P(\alpha)$, et soit $f \in A/P[X]$ le polynôme minimal de α. Comme l'extension est

séparable, les racines de f sont simples et d'après la relation donnée dans la proposition 1.3.11, $\mathrm{disc}(f) \neq 0$. Donc d'après la proposition 1.3.13, $\mathrm{disc}(1, \alpha, \ldots, \alpha^{\deg f - 1}) = \det(\overline{\mathrm{Tr}}_i) \neq 0$.

Réciproquement, supposons que l'extension n'est pas séparable. Remarquons tout d'abord que A/P a nécessairement pour caractéristique un nombre premier p. En effet, toute extension algébrique de caractéristique 0 est séparable : dans un corps de caractéristique 0, tout polynôme f irréductible est à racines simples dans une clôture algébrique. Si ce n'était pas le cas, les polynômes f et f' auraient une racine commune ; de plus, la caractéristique étant nulle, $f' \neq 0$. Par conséquent, le pgcd de f et f' serait de degré supérieur à 1 et strictement inférieur à $\deg f$, et constituerait un facteur non trivial de f. En particulier, le polynôme minimal de tout élément est à racine simples.

Notons $k_0 \subset B/M_i$ la plus grande extension séparable de A/P dans B/M_i. Par hypothèse, $k_0 \neq B/M_i$, donc $[B/M_i : k_0] = p^s$ pour un certain $s \geqslant 1$. Soit $\alpha \in B/M_i$ et soit $f = X^r + a_{r-1}X^{r-1} + \cdots + a_0$ son polynôme minimal ; on peut considérer l'extension $A/P(\alpha)$. Une A/P-base de cette extension est $(1, \alpha, \ldots, \alpha^{r-1})$. Soit $(f_1, \ldots, f_t)$ une base de B/M_i sur $A/P(\alpha)$. Alors la famille $(f_1, \alpha f_1, \ldots, \alpha^{r-1} f_1, \ldots, f_t, \alpha f_t, \ldots, \alpha^{r-1} f_t)$ est une base de B/M_i sur A/P, dans laquelle la matrice de multiplication par α est la matrice diagonale par bloc

$$\begin{pmatrix} C_\alpha & & \\ & \ddots & \\ & & C_\alpha \end{pmatrix}$$

avec

$$C_\alpha = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 & -a_{r-1} \end{pmatrix}.$$

On en déduit immédiatement que

$$\mathrm{Tr}_{(B/M_i)/(A/P)}(\alpha) = -[B/M_i : A/P(\alpha)] \cdot a_{r-1}.$$

Distinguons maintenant deux cas. Tout d'abord, si $\alpha \in k_0$, alors $[B/M_i : k_0]$ divise $[B/M_i : A/P(\alpha)]$, et en particulier p divise $[B/M_i : A/P(\alpha)]$. Alors $\mathrm{Tr}(\alpha) = 0$ dans A/P. Si $\alpha \notin k_0$, par définition de k_0, cela signifie que f n'est pas à racines simples. Comme il est irréductible, cela implique que f' est nul (sinon on trouverait un facteur non trivial comme dans le cas de la caractéristique nulle), et donc que f est de la forme $g(X^p)$ pour un certain g. En particulier, $a_{r-1} = 0$, ce qui entraîne à nouveau que $\mathrm{Tr}(\alpha) = 0$. Finalement, on en déduit que la forme $\overline{\mathrm{Tr}}_i$ est nulle, et donc son déterminant aussi.

Passons maintenant au cas général, où A est un anneau de Dedekind quelconque.

Lemme 1.3.19. *Soit S une partie multiplicative de A. Alors $\Delta_{B[S^{-1}]/A[S^{-1}]} = \Delta_{B/A}[S^{-1}]$.*

Démonstration. Toute base de l'extension L/K contenue dans B est bien entendue également contenue dans $B[S^{-1}]$ qui est la clôture intégrale de $A[S^{-1}]$, et donc $\Delta_{B/A}[S^{-1}] \subset \Delta_{B[S^{-1}]/A[S^{-1}]}$.

Toute base de L/K contenue dans $B[S^{-1}]$ est de la forme $(b_1/s, \ldots, b_n/s)$ (quitte à multiplier par un dénominateur commun qui est un élément de A) où $s \in S$ et $(b_1, \ldots, b_n)$ est une base de L/K contenue dans B. On en déduit que $\Delta_{B[S^{-1}]/A[S^{-1}]} \subset \Delta_{B/A}[S^{-1}]$. □

Lemme 1.3.20. *Soient A un anneau, P un idéal maximal de A et $S \subset A \backslash P$ une partie multiplicative de A. Les corps A/P et $A[S^{-1}]/P[S^{-1}]$ sont isomorphes.*

Démonstration. Tout d'abord montrons que $A[S^{-1}]/P[S^{-1}]$ n'est pas l'anneau nul. Soit $a/s \in A[S^{-1}]$, $a \in A$, $s \in S$. Supposons que $a/s \in P[S^{-1}]$. Alors il existe $p \in P$, $t, r \in S$ tels que $r(at - ps) = 0$, et en particulier, $rat \in P$. Comme P est premier et que $r, t \notin P$ (car $S \subset A\backslash P$), $a \in P$. Par contraposée, si $a \in A\backslash P$ et $s \in S$, alors $a/s \notin P[S^{-1}]$ et donc $A[S^{-1}]/P[S^{-1}]$ n'est pas l'anneau nul. On considère les applications naturelles $\pi : A \to A/P$, $j_s : A \to A[S^{-1}]$ et $\pi_S : A[S^{-1}] \to A[S^{-1}]/P[S^{-1}]$. Comme $(\pi_S \circ j_s)(P) = 0$, l'application $\pi_S \circ j_S$ se factorise par π, et on a donc un diagramme commutatif :

$$\begin{array}{ccc} A & \xrightarrow{j_s} & A[S^{-1}] \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi_S} \\ A/P & \xrightarrow{h} & A[S^{-1}]/P[S^{-1}] \end{array}$$

Il s'agit de montrer que h est un isomorphisme. Comme A/P est un corps et que $A[S^{-1}]/P[S^{-1}]$ n'est pas l'anneau nul, h est injective. Soit $x \in A[S^{-1}]/P[S^{-1}]$; x est de la forme $\pi_S(a/s)$ pour un certain $a/s \in A[S^{-1}]$ ($a \in A$, $s \in S$). Soit $t \in A$ tel que $ts - 1 \in P$ (c'est-à-dire un élément dont la classe dans A/P est l'inverse de la classe de s). Considérons l'élément $y = \pi(at)$. Alors

$$h(y) = h \circ \pi(at) = \pi_S \circ j_s(at) = \pi_S(at/1).$$

En outre, comme $ts - 1 \in P$, $a(ts - 1)/s = at/1 - a/s \in P[S^{-1}]$ donc

$$\pi_S(at/1) = \pi_S(a/s) = x$$

ce qui conclut. □

Lemme 1.3.21. *Soit P un idéal maximal de A. Soit $S = A\backslash P$. L'idéal P se ramifie dans B si et seulement si $PA_P \subset A_P$ se ramifie dans $B[S^{-1}]$.*

Démonstration. Soit $PB = M_1^{e_1} \cdots M_s^{e_s}$ la factorisation de PB dans B. Alors

$$(PB)[S^{-1}] = (M_1[S^{-1}])^{e_1} \cdots (M_s[S^{-1}])^{e_s}$$

est la factorisation de $(PA_P)B[S^{-1}] = (PB)[S^{-1}]$ dans $B[S^{-1}]$. En particulier,

$$e_{M_i/P} = e_{M_i[S^{-1}]/PA_P}.$$

En outre, d'après le lemme 1.3.20, le corps $B[S^{-1}]/M_i[S^{-1}]$ est isomorphe à B/M_i, et en particulier, ils sont soit tous deux séparables, soit tout deux non séparables sur $A/P = A_P/PA_P$. □

Il ne reste plus qu'à conclure. Soit P un idéal maximal de A et $S = A\backslash P$. Alors $\Delta_{B/A} \subset P$ si et seulement si $\Delta_{B/A}[S^{-1}] \subset PA_P$, c'est-à-dire d'après le lemme 1.3.19, si et seulement si $\Delta_{B[S^{-1}]/A[S^{-1}]} \subset PA_P$. Rappelons que les localisés d'un anneau de Dedekind sont des anneaux principaux, et le cas des anneaux principaux ayant été traité, on en déduit que cette dernière condition est équivalente au fait que PA_P se ramifie dans $B[S^{-1}]$. Enfin, d'après le lemme 1.3.21, ceci est encore équivalent au fait que P se ramifie dans B, ce qui conclut.

Partie 2

Théorie des nombres

Le but de cette partie est d'étudier des clôtures intégrales de $\mathbb{Z}$ en utilisant la notion d'anneau de Dedekind.

2.1 Définitions et premières propriétés

Définition 2.1.1 (entier algébrique). Soit L un anneau contenant $\mathbb{Z}$. On dit que $\alpha \in L$ est un *entier algébrique* s'il est entier sur $\mathbb{Z}$.

Définition 2.1.2 (corps de nombres). On dit qu'un corps L est un *corps de nombres* si c'est une extension finie de $\mathbb{Q}$.

Définition 2.1.3 (anneau d'entiers). Soit L un corps de nombres. On appelle *anneau des entiers de* L, et on note $\mathcal{O}_L$, la clôture intégrale de $\mathbb{Z}$ dans L.

L'anneau $\mathbb{Z}$ étant principal, donc de Dedekind, ce théorème 1.1.12, page 5, a pour corollaire la proposition suivante :

Proposition 2.1.4. *Soit L un corps de nombres. L'anneau $\mathcal{O}_L$ est de Dedekind.*

2.2 Exemples

2.2.1 Les corps cyclotomiques

Définition 2.2.1 (corps cyclotomique). Les corps de nombres $\mathbb{Q}(e^{2i\pi/n})$ avec $n \in \mathbb{N}^*$ sont appelés *corps cyclotomiques*.

Théorème 2.2.2. *L'anneau des entiers de $\mathbb{Q}(e^{2i\pi/n})$ est $\mathbb{Z}[e^{2i\pi/n}]$.*

On peut montrer facilement que les anneaux $\mathbb{Z}[e^{2i\pi/3}]$ et $\mathbb{Z}[i]$ sont principaux, donc factoriels. Cependant, ce n'est pas le cas, en général, de l'anneau $\mathbb{Z}[e^{2i\pi/n}]$ (par exemple, l'anneau $\mathbb{Z}[e^{2i\pi/23}]$ ne l'est pas). Mais un tel anneau étant une clôture algébrique de $\mathbb{Z}$ dans une extension finie séparable de $\mathbb{Q}$, c'est un anneau de Dedekind, et en particulier il possède la propriété de factorisation unique des idéaux. Historiquement, c'est afin de palier au défaut de factorialité de ces anneaux qu'ont été introduites les notions de factorisations des idéaux, et développée la notion d'anneau de Dedekind.

Proposition 2.2.3. *Soit p un nombre premier. Alors (p) est le seul idéal maximal de $\mathbb{Z}$ qui se ramifie dans $\mathbb{Z}[e^{2i\pi/p}]$.*

Démonstration. Notons $\omega = e^{2i\pi/p}$ et $B = \mathbb{Z}[\omega]$. Le polynôme minimal de ω est le polynôme cyclotomique $X^{p-1} + \ldots + X + 1$ qui est de degré $p-1$, donc l'extension $\mathbb{Q}(\omega)/\mathbb{Q}$ est également de degré $p-1$. Une base de cette extension est $(1, \omega, \ldots, \omega^{p-2})$. On calcule $\Delta_{B/\mathbb{Z}}$ grâce à la relation $\Delta_{B/\mathbb{Z}} = (\mathrm{disc}(1, \omega, \ldots, \omega^{p-2}))$. Soit $j \in \mathbb{N}$; on établit facilement en écrivant le matrice de multiplication par ω^j dans cette base que $\mathrm{Tr}_{B/\mathbb{Z}}(\omega^j) = p-1$ si $j \equiv 0 \pmod{p}$ et $\mathrm{Tr}_{B/\mathbb{Z}}(\omega^j) = -1$ sinon. On a

$$
\begin{aligned}
\mathrm{disc}(1, \omega, \ldots, \omega^{p-2}) &= \begin{vmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\omega) & \cdots & \mathrm{Tr}(\omega^{p-2}) \\ \mathrm{Tr}(\omega) & \mathrm{Tr}(\omega^2) & \cdots & \mathrm{Tr}(\omega^{p-1}) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}(\omega^{p-2}) & \mathrm{Tr}(\omega^{p-1}) & \cdots & \mathrm{Tr}(\omega^{2p-2}) \end{vmatrix} \\
&= \begin{vmatrix} p-1 & -1 & \cdots & \cdots & \cdots & -1 \\ -1 & -1 & \cdots & \cdots & \cdots & -1 \\ \vdots & \vdots & & & \iddots & p-1 \\ \vdots & \vdots & & \iddots & \iddots & -1 \\ \vdots & \vdots & \iddots & \iddots & \iddots & \vdots \\ -1 & -1 & p-1 & -1 & \cdots & -1 \end{vmatrix} \\
&= \begin{vmatrix} p & -1 & 0 & \cdots & \cdots & 0 \\ 0 & -1 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & & \iddots & p \\ \vdots & \vdots & \vdots & \iddots & \iddots & 0 \\ \vdots & \vdots & 0 & \iddots & \iddots & \vdots \\ 0 & -1 & p & 0 & \cdots & 0 \end{vmatrix} \\
\text{(retirer la colonne 2 aux autres)} &= \begin{vmatrix} p & 0 & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & 0 & p \\ \vdots & \vdots & \iddots & \iddots & 0 \\ \vdots & \iddots & \iddots & \iddots & \vdots \\ 0 & p & 0 & \cdots & 0 \end{vmatrix} \\
\text{(développer selon la ligne 2)} &= p^{p-2}.
\end{aligned}
$$

Ainsi, $\Delta_{B/\mathbb{Z}} = (p^{p-2})$ et le théorème 1.3.16 (ii) permet de conclure. □

2.2.2 Les corps quadratiques

Définition 2.2.4 (corps quadratiques). On dit qu'un corps est un *corps quadratique* si c'est une extension de degré 2 de $\mathbb{Q}$.

Proposition 2.2.5. *Pour tout corps quadratique K, il existe un entier relatif d sans facteur carré tel que $K = \mathbb{Q}(\sqrt{d})$ (où $\sqrt{d}$ désigne une racine carré quelconque de d).*

Démonstration. Soit $z \in K \backslash \mathbb{Q}$. On a alors $\mathbb{Q} \subsetneq \mathbb{Q}(z) \subset K$, l'inclusion stricte implique que $[\mathbb{Q}(z) : \mathbb{Q}] \geqslant 2$. Comme de plus, $[K : \mathbb{Q}] = 2$, on en déduit que $\mathbb{Q}(z) = K$. En particulier, z est de degré 2 et son polynôme minimal est de la forme $X^2 + aX + b$, avec $a, b \in \mathbb{Q}$. Alors $(z + \frac{1}{2}a)^2 = -b + \frac{1}{4}a^2$. Posons $D = -b + \frac{1}{4}a^2$; c'est un nombre rationnel. Il n'est pas nul, sinon on aurait $z = -\frac{1}{2}a$, d'où $z \in \mathbb{Q}$, ce qui n'est pas le cas. On peut écrire une décomposition en

facteurs premiers $D = \varepsilon \prod p_i^{n_i}$ avec $\varepsilon = \pm 1$ et $n_i \in \mathbb{Z}^*$. Maintenant, posons $m_i = 1$ si n_i est pair et $m_i = 0$ si n_i impair, et soit $d = \varepsilon \prod p_i^{m_i}$. Alors, d est sans facteur carré, et de plus,

$$\frac{D}{d} = \prod p_i^{n_i - m_i} = \left(\prod p_i^{(n_i - m_i)/2} \right)^2$$

est un carré, car $n_i - m_i$ est pair. Posons $r^2 = D/d$ avec $r \in \mathbb{Q}$.

Posons $\delta = \sqrt{d}$ et vérifions maintenant que $K = \mathbb{Q}(\delta)$. Tout d'abord, $(z + \frac{1}{2}a)^2 = dr^2 = (\delta r)^2$. Par suite, $\delta = \pm(z + \frac{1}{2}a)/r$ appartient à K. En outre, $\delta \notin \mathbb{Q}$ car cela entraînerait $z = -\frac{1}{2}a \pm r\delta \in \mathbb{Q}$. Le même argument que celui appliqué au début à z nous donne $K = \mathbb{Q}(\delta)$. □

Remarque. Un tel entier d est unique, mais nous ne le démontrons pas. Il est assez immédiat de voir que $\mathbb{Q}(\sqrt{d}) = \{p + q\sqrt{d}, p, q \in \mathbb{Q}\}$. De plus, l'écriture $p + q\sqrt{d}$ avec $p, q \in \mathbb{Q}$ est unique, ce que nous admettons également.

Théorème 2.2.6. *Soit d un entier relatif sans facteur carré.*

- *Si $d \not\equiv 1 \pmod 4$, alors l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est $\mathbb{Z}[\sqrt{d}]$.*
- *Si $d \equiv 1 \pmod 4$, alors l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.*

Démonstration. Si $p + q\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ est un entier algébrique, alors dans le cas où $q \neq 0$, il est de degré 2 et il existe $a, b \in \mathbb{Z}$ tels que $(p + q\sqrt{d})^2 + a(p + q\sqrt{d}) + b = 0$. En développant, et en utilisant l'unicité de l'écriture, on obtient $p^2 + q^2 d + ap + b = 0$ et $2pq + aq = 0$. La deuxième égalité s'écrit $2p + a = 0$, et on obtient $a = -2p$ et $b = p^2 - q^2 d$. Ainsi, le fait que $p + q\sqrt{d}$ soit un entier algébrique est équivalent au fait que $2p$ et $p^2 - q^2 d$ soient des entiers relatifs. Si $q = 0$, les mêmes conditions conviennent aussi[1].

La première condition entraîne $p \in \mathbb{Z}$ ou $p + \frac{1}{2} \in \mathbb{Z}$. Commençons par étudier le premier cas. Dans ce cas, $q^2 d \in \mathbb{Z}$. Si l'on écrit $q = r/s$, avec r et s entiers premiers entre eux, et $q^2 d = n$ avec $n \in \mathbb{Z}$, on obtient $r^2 d = s^2 n$. Par suite, s^2 divise d et comme d est sans facteur carré, $s = \pm 1$ et $q \in \mathbb{Z}$. Inversement, si $p, q \in \mathbb{Z}$, alors $2p \in Z$ et $p^2 - q^2 d \in \mathbb{Z}$, donc $p + q\sqrt{d}$ est un entier algébrique.

Dans le deuxième cas, on a $p + \frac{1}{2} \in \mathbb{Z}$. Posons $n = p^2 - q^2 d$. On a $4n = (2p)^2 - d(2q)^2$, donc $d(2q)^2$ est entier, et comme d est sans facteur carré, comme précédemment on obtient $2q \in \mathbb{Z}$. Posons $P = 2p$ et $Q = 2q$; on est dans le cas où P est impair. Donc $dQ^2 = P^2 - 4n$ est également impair, et par suite, d et Q sont impairs. En particulier $\frac{P-1}{2} + \frac{Q-1}{2}\sqrt{d}$ est un entier algébrique, donc $(p + q\sqrt{d}) - (\frac{P-1}{2} + \frac{Q-1}{2}\sqrt{d}) = \frac{1+\sqrt{d}}{2}$ aussi. Or, le polynôme minimal de $\frac{1+\sqrt{d}}{2}$ est $X^2 - X + \frac{1-d}{4}$, il doit être à coefficients entiers, donc $d \equiv 1 \pmod 4$. Cela démontre que si $d \not\equiv 1 \pmod 4$, ce cas ne se produit pas, et l'ensemble des entiers algébriques de $\mathbb{Q}(\sqrt{d})$ est $\{p + q\sqrt{d}, p, q \in \mathbb{Z}\} = \mathbb{Z}[\sqrt{d}]$.

Supposons maintenant que $d \equiv 1 \pmod 4$. Alors, comme vu précédemment, $\frac{1+\sqrt{d}}{2}$ est un entier algébrique, de polynôme minimal $X^2 - X + \frac{1-d}{4}$, ce qui implique que $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \subset \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. Par ailleurs, on a montré que les entiers algébriques de $\mathbb{Q}(\sqrt{d})$ étaient de la forme $\frac{P}{2} + \frac{Q}{2}\sqrt{d}$, avec $P, Q \in \mathbb{Z}$ et de même parité. Donc si $p + q\sqrt{d}$ est entier algébrique, alors $p - q = \frac{P-Q}{2}$ est un entier relatif ; rappelons qu'on a également $2q \in \mathbb{Z}$. Donc $p + q\sqrt{d} = (p - q) + 2q\frac{1+\sqrt{d}}{2} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Finalement, l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. □

Proposition 2.2.7. *Dans le cas où $d \not\equiv 1 \pmod 4$, les idéaux premiers de $\mathbb{Z}$ qui se ramifient dans $\mathbb{Z}[\sqrt{d}]$ sont (2) et les (p) pour tout facteur premier p de d.*

[1] Si $q = 0$, il s'agit de savoir si $p \in \mathbb{Q}$ est un entier algébrique, mais ceci est le cas si et seulement si $p \in \mathbb{Z}$. Or, on vérifie facilement que $p \in \mathbb{Z} \Leftrightarrow 2p \in \mathbb{Z}$ et $p^2 \in \mathbb{Z}$.

Dans le cas où $d \equiv 1 \pmod 4$, les idéaux premiers de $\mathbb{Z}$ qui se ramifient dans $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ sont les (p) pour tout facteur premier p de d.

Démonstration. Plaçons-nous d'abord dans le cas où $d \not\equiv 1 \pmod 4$, et notons $B = \mathbb{Z}[\sqrt{d}]$. On calcule $\Delta_{B/\mathbb{Z}}$ à l'aide du lemme 1.3.15. Le polynôme minimal de $\sqrt{d}$ est $X^2 - d$, et son discriminant est $4d$. Ainsi, $\Delta_{B/A} = (4d)$.

Maintenant, supposons que $d \equiv 1 \pmod 4$ et notons $B = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Le polynôme minimal de $\frac{1+\sqrt{d}}{2}$ est $X^2 - X + \frac{1-d}{4}$, dont le discriminant est d. Donc $\Delta_{B/A} = (d)$.

Dans les deux cas, le théorème 1.3.16 (ii) permet de conclure. □

Partie 3

Courbes algébriques

3.1 Définitions et premières propriétés

Définition 3.1.1 (espace affine). Soit k un corps. On note $\mathbb{A}^n(k)$, et on appelle *espace affine de dimension n à coordonnées dans k*, l'espace k^n. Les éléments de $\mathbb{A}^n(k)$ sont appelés *points*. L'espace affine de dimension 1 est appelé *droite affine*. L'espace affine de dimension 2 est appelé *plan affine*.

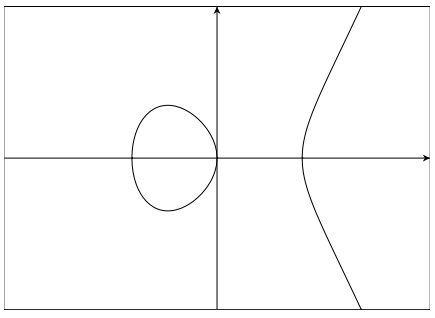
Définition 3.1.2 (sous-ensemble algébrique). Soit $S \subset k[X_1, \ldots, X_n]$ un ensemble de polynômes à n variables. L'ensemble

$$\mathcal{Z}_k(S) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n(k), \forall f \in S, f(x_1, \ldots, x_n) = 0\}$$

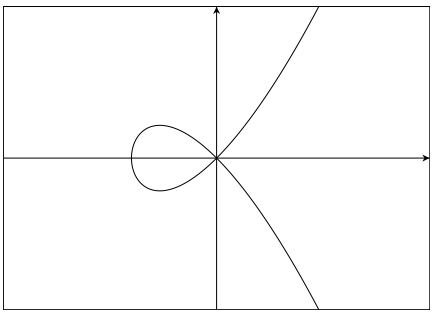
est appelé *ensemble des zéros communs de S*. On pourra le noter $\mathcal{Z}(S)$ s'il n'y a pas d'ambiguïté sur le corps. Si $S = \{f\}$ est un singleton, on notera plus simplement $\mathcal{Z}(\{f\}) = \mathcal{Z}(f)$.

Une partie V de $\mathbb{A}^n(k)$ telle qu'il existe $S \subset k[X_1, \ldots, X_n]$ vérifiant $V = \mathcal{Z}(S)$ est appelé *sous-ensemble algébrique* de $\mathbb{A}^n(k)$. Dans le cas où $n = 2$, on parle de *courbe algébrique*.

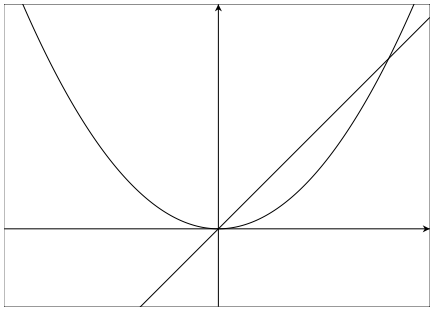
Exemple 3.1.3. On a $\mathbb{A}^n = \mathcal{Z}(0)$, et si $(x_1, \ldots, x_n) \in \mathbb{A}^n$ est un point, $(x_1, \ldots, x_n) = \mathcal{Z}(X_1 - x_1, \ldots, X_n - x_n)$. Voici quelques autres exemples d'ensembles algébriques avec $k = \mathbb{R}$.

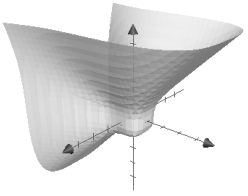


(A) $\mathcal{Z}(Y^2 - X(X^2 - 1)) \subset \mathbb{A}^2$



(B) $\mathcal{Z}(Y^2 - X^2(X + 1)) \subset \mathbb{A}^2$





(C) $\mathcal{Z}(Y^2 - XY - X^2Y + X^3)$ (D) $\mathcal{Z}(-Z^3 + X^4 + Y^3 - 1) \subset \mathbb{A}^3$

Propriétés 3.1.4. *On a les propriétés suivantes :*

(i) *Si I est l'idéal engendré par S, alors $\mathcal{Z}(S) = \mathcal{Z}(I)$. En particulier, tout ensemble algébrique est l'ensemble des zéros communs d'un idéal.*

(ii) *Si $\mathcal{E}$ est un ensemble quelconque d'idéaux, alors*

$$\mathcal{Z}\left(\bigcup_{I\in\mathcal{E}} I\right) = \bigcap_{I\in\mathcal{E}} \mathcal{Z}(I)$$

et en particulier, une intersection quelconque d'ensembles algébriques est un ensemble algébrique.

(iii) *Si $I \subset J$, alors $\mathcal{Z}(J) \subset \mathcal{Z}(I)$.*

(iv) *Si f et g sont deux polynômes, alors $\mathcal{Z}(fg) = \mathcal{Z}(f) \cup \mathcal{Z}(g)$. Plus généralement, si I et J sont deux idéaux de $k[X_1, \ldots, X_n]$, alors*

$$\mathcal{Z}(I) \cup \mathcal{Z}(J) = \mathcal{Z}(IJ)$$

et en particulier, toute union finie d'ensembles algébriques est un ensemble algébrique.

La démonstration de ces propriétés est immédiate.

Remarque. Si V est un ensemble algébrique, alors il existe en fait un ensemble S *fini* de polynômes tel que $V = \mathcal{Z}(S)$. En effet, l'anneau $k[X_1, \ldots, X_n]$ est noethérien, et comme tout ensemble algébrique est de la forme $\mathcal{Z}(I)$ pour un certain idéal I, il suffit de considérer une partie S finie qui engendre I.

Définition 3.1.5 (topologie de Zariski). Les propriétés précédentes montrent que les sous-ensembles algébriques de $\mathbb{A}^n(k)$ sont les fermés d'une topologie, appelée *topologie de Zariski*.

3.2 Points singuliers

Définition 3.2.1 (point singulier). Soit $f \in k[X, Y]$. On dit qu'un point $(a, b) \in \mathcal{Z}_k(f)$ est un *point singulier* si $\frac{\partial f}{\partial x}(a, b) = \frac{\partial f}{\partial y}(a, b) = 0$. On dit alors que la courbe $\mathcal{Z}_k(f)$ est *singulière* au point (a, b). Si une courbe ne contient aucun point singulier, on dit qu'elle est *non singulière*.

Exemple 3.2.2. Dans l'exemple 3.1.3, la courbe (A) est non singulière. La courbe (B) présente une singularité en $(0, 0)$, et la courbe (C) présente deux singularités, en $(0, 0)$ et en $(1, 1)$.

Notation. Si $f \in k[X, Y]$ est un polynôme, on considérera l'anneau quotient $k[X, Y]/(f)$, que l'on notera C_f.

Théorème 3.2.3. *Soit k un corps algébriquement clos, et soit $f \in k[X,Y]$ un polynôme irréductible. Alors l'anneau C_f est intégralement clos si et seulement si la courbe $\mathcal{Z}_k(f)$ est non singulière.*

Remarque. Par ailleurs, si f est irréductible, on peut montrer que l'anneau C_f est noethérien et que tous ses idéaux premiers non nuls sont maximaux.

3.3 Interprétation géométrique de la ramification

Soit k un corps algébriquement clos, et soit $f \in k[X,Y]$ un polynôme irréductible, avec $\deg_Y(f) = n > 0$, et unitaire en Y (on peut toujours se ramener à cette dernière condition par un changement de repère affine). On suppose que la courbe $\mathcal{Z}_k(f)$ est non singulière. Notons $A = k[X]$ et K le corps des fractions de A ; ainsi on peut voir f comme un polynôme unitaire et irréductible de degré n de $A[Y]$. On note L le corps des fractions de C_f. On identifie l'anneau C_f à $A[\alpha]$ où $\alpha \in \overline{K}$ est une racine de f comme polynôme de $A[Y]$, de sorte que l'on ait une inclusion $A \subset C_f$ (qui est en fait un morphisme injectif canonique). Comme f est unitaire en Y, l'anneau C_f est entier sur A. De plus, $\mathcal{Z}(f)$ est non singulière, donc C_f est intégralement clos, et par suite, est la clôture intégrale de A dans L.

Rappelons de plus que $A = k[X]$ est principal, donc de Dedekind. Les idéaux maximaux de $k[X]$ sont ceux engendrés par un polynôme irréductible, et comme k est algébriquement clos, les polynômes irréductibles sont ceux de degré 1. Ainsi, $k \simeq \mathbb{A}^1(k)$ est en bijection avec l'ensemble des idéaux maximaux de A par l'application $x \mapsto (X - x)$. Soit $P = (X - x)$ un idéal maximal de A. À quelle condition sur x l'idéal P se ramifie-t-il en C_f ?

Si M est un idéal maximal de C_f, il est engendré par les classes modulo f de $(X - x)$ et $(Y - y)$ pour un certain couple $(x, y) \in \mathcal{Z}_k(f)$. Par abus, on notera $M = (X - x, Y - y)$. À x fixé, les idéaux maximaux de C_f contenant $P = (X - x)$ sont les $M = (X - x, Y - y)$ pour y tel que $(x, y) \in \mathcal{Z}_k(f)$. On a, d'une part

$$C_f/M \simeq k[X,Y]/(X - x, Y - y) \simeq k,$$

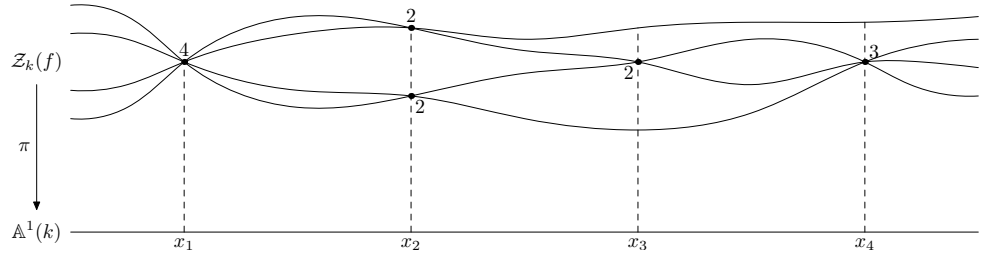
d'autre part, $A/P = k[X]/(X - x) \simeq k$. Ainsi l'extension C_f/M est séparable et de degré 1 sur A/P. Le fait qu'elle soit séparable implique que M est ramifié au dessus de P si et seulement si $e_{M/P} > 1$, par définition. D'autre part, le fait qu'elle soit de degré 1 signifie que $f_{M/P} = 1$, et le théorème 1.3.4 implique que

$$\sum_{M \supset P} e_{M/P} = [L : K] = [\mathrm{Frac}(A[Y]/(f)) : \mathrm{Frac}(A)] = \deg_Y(f) = n.$$

Ainsi, P se ramifie dans C_f si et seulement si il existe strictement moins de n idéaux maximaux de C_f contenant P.

Considérons l'application $\pi : \mathcal{Z}_k(f) \to \mathbb{A}^1(k)$, $(x, y) \mapsto x$. Comme k est algébriquement clos, cette application est surjective. De plus, $\deg_Y(f) = n$ donc pour $x \in \mathbb{A}^1$ fixé, $\pi^{-1}(\{x\})$ contient au plus n points. L'ensemble des idéaux maximaux de C_f contenant $P = (X - x)$ est en bijection avec $\pi^{-1}(\{x\})$ par l'application $(X - x, Y - y) \mapsto y$. Ainsi, d'après l'étude faite ci-dessus, $P = (X - x)$ se ramifie dans C_f si et seulement si $\pi^{-1}(\{x\})$ contient strictement moins de n points. D'après le corollaire 1.3.17, il n'y a qu'un nombre fini de tels idéaux.

La figure ci-dessous illustre les cas de ramification possible lorsque $n = 4$. Le terminologie *ramification* prend tout son sens dans cette vision géométrique des choses.



Remarque. Le dessin ci-dessus est trompeur, dû au fait que $\mathbb{R}$ n'est pas algébriquement clos, et que sur une courbe algébrique réelle, tout point n'a pas toujours n antécédents. En particulier, les points de ramification semblent singuliers, alors qu'en réalité ils ne le sont pas.

Dans la première partie, nous avons énoncé une proposition assez générale, la proposition 1.3.6, nous permettant d'obtenir des informations sur la ramification d'une extension d'anneaux de la forme $A[\alpha]/A$. Les courbes algébriques représentent un cas particulier, plus simple, de cette situation, avec $A = k[X]$ et $C_f \simeq A[\alpha]$. On se donne f vérifiant les mêmes conditions que ci-dessus, sauf que $\mathcal{Z}(f)$ n'est plus nécessairement supposée non-singulière.

Soit $M = (X-x, Y-y)$ avec $(x,y) \in \mathcal{Z}(f)$ un idéal maximal de C_f. Soit $P = (X-x) = M \cap k[X]$. On écrit $f = (X-x)h(X,Y) + \prod_{i=1}^{s}(Y-y_i)^{e_i}$. Dans cette situation, il est immédiat, grâce à l'égalité $f(x,y) = 0$, que $y = y_{i_0}$ pour un certain $i_0 \in \{1, \ldots, s\}$ unique, ce qui traduit l'affirmation (1) de la proposition 1.3.6. Ce que l'on avait alors noté f' est ici la dérivée partielle $\frac{\partial f}{\partial Y}$, qui s'écrit

$$\frac{\partial f}{\partial Y}(X,Y) = (X-x)\frac{\partial h}{\partial Y} + \sum_{i=1}^{s}\big(e_i(Y-y_i)^{e_i-1}\prod_{j\neq i}(Y-y_j)^{e_j}\big).$$

Savoir si « $f'(\alpha) \in M$ ou non » revient ici à savoir si $\frac{\partial f}{\partial Y}(x,y)$ est nul ou non. Or, $\frac{\partial f}{\partial Y}(x,y) = e_{i_0} \times 0^{e_{i_0}-1}$ et donc $\frac{\partial f}{\partial Y}(x,y) \neq 0$ si et seulement si $e_{i_0} = 1$ (on utilise la convention $0^0 = 1$). On retrouve l'affirmation (2) de la proposition 1.3.6 (les extensions, dans ce cas-là, sont toujours séparables comme on l'a remarqué plus haut). Si l'on se place maintenant dans le localisé $(C_f)_M$, on peut écrire

$$0 = \frac{(X-x)h(X,Y)}{\prod_{i\neq i_0}(Y-y_i)^{e_i}} + (Y-y_{i_0})^{e_{i_0}} \in (C_f)_M$$

autrement dit $(X-x)\tilde{h}(X,Y) = (Y-y_{i_0})^{e_{i_0}}$ avec $\tilde{h} \in (C_f)_M$. Soit $g \in M(C_f)_M$. Il existe $g_1, g_2 \in (C_f)_M$ telles que $g = (X-x)g_1(X,Y) + (Y-y_{i_0})g_2(X,Y)$. Dans le cas où $e_{i_0} = 1$, on a donc $g = (X-x)(g_1 + \tilde{h}g_2)$, et ainsi $M(C_f)_M$ est engendré par $X-x$. C'est l'affirmation (4) de la proposition 1.3.6. Enfin, rappelons que l'anneau C_f est de Dedekind si et seulement si $\mathcal{Z}(f)$ est non singulière (théorème 3.2.3). L'affirmation (5) de la proposition affirme quant à elle que C_f est un anneau de Dedekind si et seulement si $(C_f)_M$ est un anneau principal pour tout idéal maximal M de C_f. La proposition suivante établit directement ce lien :

Proposition 3.3.1. *Un point (x,y) de $\mathcal{Z}(f)$ est non-singulier si et seulement si l'anneau $(C_f)_M$, où $M = (X-x, Y-y)$, est principal.*

Exemple 3.3.2. Considérons le polynôme $f = Y^n - X$ pour un certain $n > 0$. Il est irréductible dans $k[X,Y]$. Soit $x \in k$. Le polynôme f s'écrit sous la forme

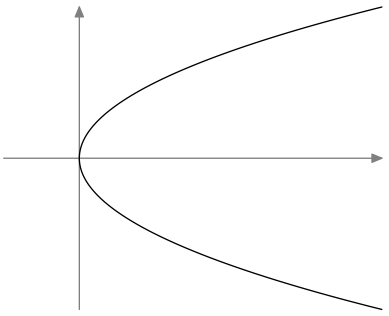
$$f = (x-X) + Y^n - x = (x-X) + \prod_{\omega\in\mu_n}(Y-\omega\xi)^{e_\omega}$$

où ξ désigne une racine n-ième de x dans k et μ_n l'ensemble des racines n-ièmes de l'unité dans k. Si la caractéristique de k est un nombre premier p, on se place uniquement dans le cas où n est premier avec p. Il y a alors exactement n racines n-ièmes de l'unité, et donc $e_\omega = 1$ pour tout ω.

- ☞ Si $x \neq 0$, alors $\mathrm{card}\{\omega\xi, \omega \in \mu_n\} = \mathrm{card}\,\mu_n = n$, et donc l'idéal maximal $(X - x)$ de $k[X]$ ne se ramifie pas dans C_f.
- ☞ Si $x = 0$, alors $f = (0 - X) + (Y - 0)^n$, l'idéal maximal (X) se ramifie et son indice de ramification est n.

Sur la courbe représentative de $\mathcal{Z}(f)$, on aura un seul point de ramification en $(0, 0)$, où convergent toutes les branches.

Intéressons-nous au cas simple $n = 2$ et $k = \mathbb{C}$. On peut représenter dans $\mathbb{R}^2$ la courbe $\mathcal{Z}(Y^2 - X)$:



Le point de ramification $(0, 0)$ est visible sur la figure. Les réels strictement positifs ont chacun deux antécédents réels. Représenter la courbe dans $\mathbb{C}^2$ nécessiterait quatre dimensions, ce qui demande un certain effort d'imagination. On peut par exemple la voir comme un plan que l'on aurait coupé le long d'un demi-axe partant de l'origine, puis que l'on aurait recollé après lui avoir fait faire un tour autour de l'origine.

Remarque. Si l'entier n n'est pas premier avec p, alors $e_\omega > 1$ pour tout ω. Plus généralement, si le degré n du polynôme considéré n'est pas premier avec la caractéristique du corps, l'étude de la ramification est plus compliquée. On parle de *ramification sauvage*.

Bibliographie

[1] Dino Lorenzini. *An Invitation to Arithmetic Geometry*. American Mathematical Society, 1997.

[2] William Fulton. *Algebraic Curves*. The Benjamin/Cummings Publishing Compagny, 1969.

[3] Jean-Pierre Serre. *Corps Locaux*. Hermann, 1962.

[4] Pierre Samuel. *Algebraic Theory of Numbers*. Hermann, 1971.