Théorie algébrique des nombres

François Thilmany

Automne 2023

Ces notes accompagnent un cours donné à l'UCLouvain en Automne 2023.
Leur auteur remercie chaleureusement Justin Vast pour ses suggestions et corrections.

1. Quelques rappels d'algèbre commutative

Dans tout ce document, R est un anneau commutatif avec $1 \in R$. Sauf mention contraire, tous les anneaux sont unifères et commutatifs.

1.1. Idéaux maximaux et idéaux premiers. Nous rappelons les caractérisations suivantes pour P un idéal de R.

P est dit *premier* s'il satisfait l'une des conditions équivalentes suivantes :
(i) Si $P \supseteq J_1 J_2$ pour deux idéaux J_1, J_2 de R, alors $P \supseteq J_1$ ou $P \supseteq J_2$.
(ii) Si $ab \in P$, alors $a \in P$ ou $b \in P$.
(iii) Le complement $S_P = R \setminus P$ est clos pour la multiplication.
(iv) L'anneau R/P est intègre.

P est dit *maximal* s'il satisfait l'une des conditions équivalentes suivantes :
(i) Si $P \subseteq I \trianglelefteq R$, alors $P = I$ ou $I = R$.
(ii) L'anneau R/P est un corps.

En particulier, tout idéal maximal est premier, et R est premier mais n'est pas maximal.

1.2. Exercice. Démontrer les équivalences ci-dessus.

1.3. Exercice. Démontrer qu'un idéal principal propre (p) est premier si et seulement si son générateur p est un élément premier. Démontrer qu'un idéal principal propre (p) est maximal parmi les idéaux principaux si et seulement si son générateur p est irréductible. En déduire que si p est irréductible sans être premier, l'idéal (p) n'est contenu dans aucun idéal premier principal.

1.4. Théorème. Soit R un anneau. Le radical nilpotent N de R est l'intersection de tous les idéaux premiers minimaux de R.

Démonstration. Il est clair qu'un élément nilpotent est contenu dans tout idéal premier. Nous allons démontrer la réciproque.

Soit donc x un élément de R qui n'est pas nilpotent. Puisque l'ensemble $S = \{x^n \mid n \in \mathbb{N}\}$ ne contient pas 0, l'ensemble des idéaux disjoints de S est non-vide. De plus, si $I_1 \subseteq I_2 \subseteq \cdots$ est une chaine d'idéaux évitant S, leur union est aussi un idéal qui évite S. Par le lemme de Zorn, nous pouvons choisir un idéal I de R maximal pour la propriété d'être disjoint de S.

Il suffit maintenant de montrer que I est premier. Soient $a, b \in R$ tels que $ab \in I$ et supposons, pour rire, que $a, b \notin I$. Alors, par maximalité, les deux idéaux $I+(a)$ et $I+(b)$ contiennent disons respectivement x^m et x^n. Il suit que $x^{m+n} \in (I + (a))(I + (b)) \subseteq I$, absurde ! Nous concluons que I est premier. □

1.5. Dimension. La *dimension (de Krull)* de l'anneau R est la quantité

$$\dim_{\text{Krull}}(R) = \sup\{n \in \mathbb{N} \mid \text{il existe une chaine d'idéaux premiers } P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n \subsetneq R\}.$$

En théorie algébrique des nombres, les anneaux de dimension 1 sont prévalents.

1.6. Proposition. Un anneau intègre R satisfait $\dim_{\text{Krull}}(R) \leq 1$ ssi tout idéal premier propre et non-nul est maximal. Le cas $\dim_{\text{Krull}}(R) = 0$ correspond au cas où R est un corps.

Démonstration. Évidente. □

1.7. Exercice. Soit R un anneau fini, non nul. Montrer que R est de dimension (de Krull) 0.

1.8. Anneaux et modules noethériens. Un anneau qui satisfait la condition de chaîne ascendante (CCA) pour les idéaux (et l'inclusion) est appelé *noethérien*. Rappelons que la *condition de chaîne ascendante* dans un ensemble partiellement ordonné $(\mathcal{I}, \subseteq)$ est la propriété que toute suite croissante I_n d'éléments de $\mathcal{I}$ est stationnaire, c'est-à-dire qu'il existe un indice $n \in \mathbb{N}$ au delà duquel I_m $(m \geq n)$ est constant. Un module est dit noethérien s'il satisfait (CCA) pour les sous-modules (et l'inclusion). Un anneau est donc noethérien si et seulement s'il est noethérien comme module sur lui-même.

1.9. Proposition. Soit R un anneau noethérien et $N \subset M$ deux R-modules. Alors :
(i) M est noethérien si et seulement si N et M/N le sont.
(ii) Tout R-module finiment engendré est noethérien
(iii) Tout idéal de R est finiment engendré
De plus, les deux dernières propriétés impliquent que R soit noethérien.

Démonstration. (i) Regarder les chaines $M_i \cap N$ et $M_i + N$ de sous-modules de N et M/N.
(ii) Montrer que R^n est noethérien comme R-module.
(iii) Suit du point (ii) et est équivalent à R noethérien car les idéaux sont les sous-modules de R et R est engendré par 1. □

1.10. Exemples. (i) Tout anneau principal est clairement noethérien.
(ii) Si R est noethérien, alors $R[x]$ l'est aussi (c'est le *théorème de la base de Hilbert*).
(iii) Les sous-anneaux $x\mathbb{Q}[x] + \mathbb{Z} \subset \mathbb{Q}[x]$ et $\mathbb{Q}[xy, xy^2, xy^3, \dots] \subset \mathbb{Q}[x, y]$ ne sont pas noethériens.

Le lemme suivant est une bonne illustration de l'étendue des conséquences de la noethérianité.

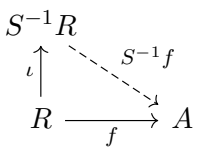
1.11. Lemme. Soit R un domaine noethérien et I un idéal non-nul de A. Alors I contient un produit $P_1 \cdots P_n$ d'idéaux premiers non-nuls P_i.

Démonstration. Puisque R est noethérien, il existe un idéal J de R qui ne contient pas de produits d'idéaux premiers non-nuls et qui est maximal pour cette propriété. Cet idéal J n'est pas premier, donc il existe $b, b' \in R \setminus J$ avec $bb' \in J$. Par choix de J, les deux idéaux $J + (b)$, $J + (b')$ contiennent chacun un produit $P_1 \cdots P_n$, $P'_1 \cdots P'_{n'}$ d'idéaux premiers non-nuls. Mais alors J contient le produit $P_1 \cdots P_n \cdot P'_1 \cdots P'_{n'}$. □

1.12. Lemme. Soit R un anneau noethérien et I un idéal de R. L'ensemble partiellement ordonné $\mathcal{P}_I$ des idéaux premiers qui contiennent I n'a qu'un nombre fini d'éléments minimaux.

Démonstration. Supposons qu'il existe un idéal I qui soit contenu dans une infinité d'idéaux premiers P minimaux pour la condition $I \subseteq P$. Puisque R est noethérien, nous pouvons supposer que I est maximal pour cette propriété. Bien sûr, I n'est pas premier, sinon I est l'unique élément minimal de $\mathcal{P}_I$. Dès lors, il existe $a, b \in R \setminus I$ tels que $ab \in I$. Tout idéal premier $P \in \mathcal{P}_I$ contient alors $I + (a)$ ou $I + (b)$. Ceci montre que $\mathcal{P}_I$ est l'union $\mathcal{P}_a \cup \mathcal{P}_b$ des ensembles $\mathcal{P}_a$ et $\mathcal{P}_b$ des idéaux premiers de R contenant $I + (a)$ ou $I + (b)$ respectivement. Évidemment, tout $P \in \mathcal{P}$ minimal reste minimal dans l'ensemble $\mathcal{P}_a$ ou $\mathcal{P}_b$ le contenant. Par maximalité de I, $\mathcal{P}_a$ et $\mathcal{P}_b$ n'ont qu'un nombre fini d'éléments minimaux, contradiction ! □

1.13. Localisation. Soit R un anneau et $1 \in S \subset R$ un sous-ensemble clos pour la multiplication. La *localisation de R en S* est l'anneau (unique à unique isomorphisme près) $S^{-1}R$, muni d'un morphisme $\iota : R \to S^{-1}R$ pour lequel les éléments de $\iota(S)$ sont inversibles, jouissant de la propriété universelle suivante : tout morphisme d'anneaux $f : R \to A$ pour lequel tout élément de $f(S)$ est inversible s'étend via ι de manière unique à un morphisme $S^{-1}f : S^{-1}R \to A$.



1.14. Lemme. Si $x \in S^{-1}R$, il existe $s \in S$ et $r \in R$ tels que $x\iota(s) = \iota(r)$. Autrement dit, $S^{-1}R = \iota(S)^{-1} \cdot \iota(R)$ comme ensembles.

Démonstration. En vertu de sa propriété universelle, $S^{-1}R$ est engendré comme anneau par $\iota(R)$ et $\iota(S)^{-1}$. Donc $x = \sum_i r_i s_i^{-1}$ avec $r_i \in \iota(R)$ et $s_i \in \iota(S)$. Mais alors $x \prod_i s_i = \sum_i (r_i \prod_{j \neq i} s_j) \in \iota(R)$. (Quitte à remplacer R par $\iota(R)$ et S par $\iota(S)$, nous aurions pu supposer que R est un sous-anneau de $S^{-1}R$ pour simplifier la notation.) □

1.15. Exercice. Montrer que l'anneau $S^{-1}R$ peut être construit ainsi. Munissons l'ensemble $R \times S$ de la relation d'équivalence

$$(r, s) \sim (r', s') \text{ s'il existe } t \in S \text{ tel que } rs't = r'st,$$

et notons $S^{-1}R$ l'ensemble quotient. Les opérations

$$(r, s) + (r', s') = (rs' + r's, ss'); \qquad (r, s) \cdot (r', s') = (rr', ss')$$

définissent sur $S^{-1}R$ une structure d'anneau unifère, pour laquelle $S^{-1}R$ est la localisation de R en S via le morphisme $\iota : r \mapsto (r, 1)$. La classe d'équivalence de (r, s) dans $S^{-1}R$ est dénotée $\frac{r}{s}$.

1.16. Exemples.
(i) Si R est intègre, alors $S = R \setminus \{0\}$ est clos pour la multiplication, et $S^{-1}R$ n'est autre que le corps de fractions de R. Plus généralement, le complément S des diviseurs de 0 dans R est multiplicativement clos, et la localisation $S^{-1}R$ est appelé *anneau (total) des fractions de R.*
(ii) À l'opposé, si S contient un élément nilpotent, alors $S^{-1}R$ est l'anneau nul.
(iii) Lorsque S est le complément d'un idéal premier P, la localisation de R en S est souvent notée R_P et appelée (abusivement) *localisation de R en P.*

1.17. Exercice. Montrer que l'anneau des fractions de R est la plus grande localisation de R dont le morphisme de structure ι est injectif.

Soit maintenant M un R-module. Le *localisé de M en S* est le $S^{-1}R$-module $S^{-1}R \otimes_\iota M$. Lorsque I est un idéal de R, la multiplication permet d'identifier $S^{-1}R \otimes_\iota I$ avec l'idéal $S^{-1}I$ de $S^{-1}R$ engendré par I. En effet, la multiplication $S^{-1}R \otimes_\iota R \to S^{-1}R$ est un isomorphisme d'anneaux, par lequel l'image de $S^{-1}R \otimes_R I$ est précisément l'idéal engendré par $\iota(I)$.

1.18. Exercice. Montrer que $S^{-1}M$ possède une description similaire à celle de l'exercice 1.15. L'utiliser pour expliciter l'identification $S^{-1}R \otimes_R I \cong S^{-1}I$.

1.19. Proposition (Structure des idéaux d'une localisation)**.** Soit $\iota : R \to S^{-1}R$ le morphisme canonique. Les applications $J \mapsto \iota^{-1}(J)$ et $I \mapsto S^{-1}I$, sont des bijections réciproques entre l'ensemble des idéaux premiers propres de $S^{-1}R$ et l'ensemble des idéaux premiers de R évitant S.

Démonstration. Puisque les éléments de $\iota(S)$ sont inversibles dans $S^{-1}R$, il est clair que si J est un idéal propre de $S^{-1}R$, alors $\iota^{-1}(J)$ est un idéal de R évitant S. Inversement, si $I \lhd R$ est premier et $xy \in S^{-1}I$, alors le lemme 1.14 implique l'existence de $s, t \in \iota(S)$ tels que $xs, yt \in \iota(R)$ et $xsyt \in \iota(I)$. Or $\iota(I)$ est un idéal premier de $\iota(R)$, donc $xs \in \iota(I)$ (disons) et $x = xss^{-1} \in S^{-1}I$. Il reste à montrer que les deux applications sont inverses l'une de l'autre.

Premièrement, si $J \lhd S^{-1}R$, alors $S^{-1}(\iota^{-1}(J))$ est contenu dans J puisque $\iota(\iota^{-1}(J))$ l'est. Inversement, si $x \in J$, alors il existe $s \in S$ tel que $x\iota(s) = \iota(r)$ en vertu du lemme 1.14. Ceci signifie d'une part que $r \in \iota^{-1}(J)$, et de l'autre que x est dans l'idéal engendré par $\iota(r)$ puisque $\iota(s)$ est inversible. Donc $J = S^{-1}(\iota^{-1}(J))$. (La primalité de J n'est pas nécessaire ici.)

Secondement, nous montrons que

$$\iota^{-1}(S^{-1}I) = \{r \in R \mid \text{il existe } s \in S \text{ t.q. } sr \in I\}.$$

Lorsque $P \lhd R$ est premier et évite S, il s'ensuivra que $\iota^{-1}(S^{-1}P) = P$. L'inclusion du membre de droite est claire. Pour l'autre inclusion, prenons $r \in R$ tel que $\iota(r) = x\iota(r')$ avec $r' \in I$. En vertu du lemme 1.14, il existe $s \in S$ tel que $x\iota(s) \in \iota(R)$, d'où $\iota(rs) = (x\iota(s))\iota(r') \in \iota(I)$. Donc $rs \in I + \ker \iota$ et l'égalité $\ker \iota = \{r \in R \mid \text{il existe } s \in S \text{ t.q. } sr = 0\}$ implique l'inclusion manquante. □

1.20. Corollaire. Si S est le complément d'un idéal premier P, alors $S^{-1}R$ est un anneau local dont l'unique idéal maximal est $S^{-1}P$.

1.21. Exercice. Démontrer les propriétés suivantes pour $I, J \lhd R$:
(i) $S^{-1}(I+J) = S^{-1}I + S^{-1}J$
(ii) $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$
(iii) $S^{-1}(IJ) = (S^{-1}I)(S^{-1}J)$.

1.22. Propriétés locales. Soit $(\mathcal{P})$ une propriété de la théorie des anneaux. Nous dirons que $(\mathcal{P})$ est une *propriété locale* si $(\mathcal{P})$ pour un anneau R est équivalente à $(\mathcal{P})$ pour tous les anneaux R_P, où P parcourt les idéaux premiers de R. Nous dirons que $(\mathcal{P})$ est une propriété *très locale* si $(\mathcal{P})$ pour un anneau R est équivalente à $(\mathcal{P})$ pour tous les anneaux R_M, où M parcourt les idéaux maximaux de M. Nous emploirons la même terminologie pour une propriété de la théorie des modules. Les propriétés (très) locales sont donc celles qui peuvent se vérifier équivalemment pour un R-module ou pour ses localisations en les idéaux premiers (resp. maximaux) de R.

1.23. Lemme (Trivial est locale)**.** Un R-module N est nul si et seulement si $S^{-1}N$ est nul pour tout choix S de complément d'un idéal maximal de R.

Démonstration. Il suffit de montrer que N est nul si toutes ses localisations le sont. Si N est non-nul, alors il admet un sous-module finiment engendré non nul ; on peut donc supposer que N est finiment engendré. Soit $I = \mathrm{Ann}_R(N)$ l'annulateur de N ; c'est un idéal de R. Supposons, pour rire, que I soit contenu dans un idéal maximal P dont S est le complément. Alors l'annulateur de $S^{-1}N$ est contenu dans $S^{-1}P$. En effet, si $\frac{r}{s} \in \mathrm{Ann}_{S^{-1}R} S^{-1}N$, nous avons $\frac{rn}{s} = 0$ pour tout $n \in N$. De là, il existe pour chaque générateur n_i de N un $t_i \in S$ tel que $t_i r n_i = 0$ dans N. Donc $(\prod t_i)r \in I \subset P$ et puisque P est premier et S multiplicativement clos, $r \in P$. Mais ceci est impossible puisque par hypothèse $\mathrm{Ann}_{S^{-1}R} S^{-1}N = S^{-1}R$ alors que $S^{-1}P$ est un idéal propre. □

1.24. Proposition (Exacte est locale)**.** Soit $L \to M \to N$ une suite exacte de R-modules. Alors la suite $S^{-1}L \to S^{-1}M \to S^{-1}N$ de $S^{-1}R$-modules est exacte. Autrement dit, $S^{-1}R$ est un R-module plat.

De plus, une suite $L \to M \to N$ est exacte si et seulement si ses localisations $S^{-1}L \to S^{-1}M \to S^{-1}N$ sont exactes pour tout choix S de complément d'un idéal maximal de R.

Démonstration. Si x est dans le noyau de $S^{-1}M \to S^{-1}N$, alors il en est de même pour xs pour tout $s \in \iota(S)$. En choisissant s comme dans le lemme 1.14, on voit que $xs \in \iota(M)$, donc xs est dans l'image de $\iota(L)$, et $x = xss^{-1}$ dans celle de $S^{-1}L$. L'autre inclusion est évidente.

Montrons maintenant l'exactitude de toute suite $L \xrightarrow{f} M \xrightarrow{g} N$ dont les localisations en les idéaux maximaux sont exactes. Notons f_S et g_S les applications induites par f et g après localisation en S. Premièrement, il est clair que $g \circ f = 0$. En effet, l'image de $g \circ f$ est un sous-R-module qui est localement nul par hypothèse. Le lemme 1.23 implique donc que l'image de $g \circ f$ est nulle. Pour vérifier l'exactitude, nous étudions le module quotient $(\ker g)/(\mathrm{im}\, f)$. Par la première partie, sa localisation en S est $(\ker g)_S/(\mathrm{im}\, f)_S = (\ker g_S)/(\mathrm{im}\, f_S)$. Mais par hypothèse, ce module est nul pour tout complément S d'un idéal maximal de R. Le lemme 1.23 conclut que $(\mathrm{im}\, f)/(\ker g)$ est nul, c'est-à-dire que la suite de départ est exacte. □

1.25. Corollaire. Pour un morphisme $f : M \to N$ de R-modules, être injectif, resp. surjectif, bijectif, est une propriété très locale.

Démonstration. Appliquer la proposition aux suites $0 \to M \to N$ et $M \to N \to 0$. □

1.26. Proposition (Être noethérien est presque très locale, Nagata)**.** Soit R un anneau ayant la propriété : chaque élément non-nul de R appartient à un nombre fini d'idéaux maximaux. Alors R est noethérien si et seulement si toutes ses localisations aux idéaux maximaux le sont.

L'hypothèse de la proposition 1.26 est nécessaire : l'anneau $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ n'est pas noethérien, alors que ses localisations aux idéaux maximaux sont toutes isomorphes à $\mathbb{Z}/2\mathbb{Z}$. Même avec l'hypothèse de la proposition 1.26, la condition d'être localement noethérien n'est pas toujours

satisfaite. En effet, l'anneau de séries formelles $K[[x_1, x_2 \dots]]$ est local (son unique idéal maximal est le noyau de l'évaluation en $(0, 0, \dots)$) mais n'est pas noethérien.

DÉMONSTRATION. La première implication est claire ; nous allons montrer que R est noethérien si ses localisations le sont. Soit $0 \neq I_1 \subseteq I_2 \subseteq \cdots$ une chaine d'idéaux de R. Par hypothèse, I_1 ne peut être contenu que dans un nombre fini d'idéaux maximaux $M_1, \dots, M_k$ de R. En conséquence, il existe un indice commun m à partir duquel

$$I_m R_{M_i} = I_{m+1} R_{M_i} = \cdots, \quad \text{pour } i = 1, \dots, k.$$

Mais cette égalité est aussi trivialement vérifiée pour les autres idéaux maximaux (qui ne contiennent pas I_1). Par localité de l'égalité, nous avons donc $I_m = I_{m+1} = \cdots$, ce qu'il fallait démontrer. □

1.27. Exercices.
(i) Montrer qu'être réduit est une propriété très locale (un anneau R est *réduit* si son seul élément nilpotent est 0).
(ii) Montrer qu'être un module cyclique n'est pas une propriété locale.
(iii) Montrer qu'être un module libre n'est pas une propriété locale.
(iv) Montrer qu'être un module projectif est une propriété locale.

1.28. Corollaire (Quotients d'une localisation)**.** Soit $I \lhd R$ et notons $\bar{S}$ l'image de S dans R/I. Alors $S^{-1}I$ est le noyau de l'application canonique $S^{-1}R \to \bar{S}^{-1}(R/I)$.

DÉMONSTRATION. Nous pouvons appliquer la proposition 1.24 à la suite exacte $0 \to I \to R \to R/I \to 0$ de R-modules. Alternativement, il est possible de montrer que $S^{-1}R/S^{-1}I$ jouit de la bonne propriété universelle. □

1.29. Extensions intégrales. Soit $f : R \to A$ un morphisme d'anneaux, équipant A d'une structure de R-algèbre unifère. Un élément $x \in A$ est dit *intégral sur* R (ou sur f s'il est nécessaire de préciser le morphisme) s'il satisfait une des trois conditions équivalentes suivantes :

(i) x est racine d'une polynôme monique à coefficients dans $f(R)$: il existe $a_0, \dots, a_{n-1} \in f(R)$ tels que
$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$
(ii) Le sous-anneau $f(R)[x]$ de A est finiment engendré comme R-module.
(iii) Il existe un sous-module M de A stable par x, qui soit finiment engendré comme R-module et fidèle comme $f(R)[x]$-module.

Si tout élément de A est intégral sur f, nous disons que f *est un morphisme intégral*, que l'extension $f : R \to A$ est une *extension intégrale*, ou encore que A *est intégral sur* R (quand il n'y a pas d'ambiguïté sur f).

Il est clair que si x satisfait la première condition, alors le R-module $f(R)[x]$ est engendré par $1, x, \dots, x^{n-1}$. De plus, l'anneau $f(R)[x]$ est toujours stable pour la multiplication par x et fidèle sur lui-même (puisque $1 \in f(R)[x]$).

Si maintenant $v_1, \dots, v_m$ engendrent un sous-module M de A stable par x et fidèle, nous pouvons écrire

$$\begin{cases} xv_1 = a_{11}v_1 + \dots a_{1m}v_m \\ \quad \vdots \qquad\qquad\qquad\qquad a_{ij} \in f(R). \\ xv_m = a_{m1}v_1 + \dots a_{mm}v_m, \end{cases}$$

La matrice (a_{ij}) à entrées dans $f(R)$ relève donc la multiplication par x à un endomorphisme $A : f(R)^m \to f(R)^m$,

$$\begin{array}{ccc} f(R)^m & \xrightarrow{A} & f(R)^m \\ \downarrow{\scriptstyle e_i \mapsto v_i} & & \downarrow \\ M & \xrightarrow{x\times} & M, \end{array}$$

auquel le théorème de Cayley–Hamilton s'applique : A annule le polynôme monique $p(X) = \det(X \cdot \mathrm{id} - A)$ à coefficients dans $f(R)$. Mais alors $p(x\times) = p(x)\times$ est aussi l'endomorphisme nul du $f(R)[x]$-module M. Puisque ce dernier est fidèle, $p(x) = 0$ et x satisfait la première condition.

1.30. Lemme. Supposons que A soit engendré comme R-algèbre par des éléments $x_1, \ldots, x_n$ intégraux sur R. Alors A est finiment engendré comme R-module.

Démonstration. Raisonnons par récurrence sur le nombre n de générateurs intégraux de A comme R-algèbre. Le cas $A = R[x_1]$ correspond à la définition d'intégralité.

Puisque $x_1, \ldots, x_n$ sont intégraux sur R, x_n est a fortiori intégral sur $A' = R[x_1, \ldots, x_{n-1}]$, ce qui signifie que A est un A'-module finiment engendré, disons par $v_1, \ldots, v_l \in A$. Par récurrence, A' est lui-même un R-module finiment engendré, disons par $w_1, \ldots, w_m \in A'$. Mis ensemble, tout élément $x \in A$ peut s'écrire comme une somme à coefficients dans R des $v_i w_j$, ce qu'il fallait démontrer. □

1.31. Proposition. Si $f : R \to A$ et $g : A \to B$ sont deux extensions intégrales, alors B est une extension intégrale de R (c.-à-d. $g \circ f$ est intégral).

Démonstration. Soit $b \in B$. Nous savons que le sous-anneau $g(A)[b]$ de B est finiment engendré comme A-module. Soit donc $b = b_1, \ldots, b_n$ un ensemble de générateurs pour celui-ci, et prenons $a_{ij}^k \in A$ tels que $b_i b_j = \sum_{i=1}^n g(a_{ij}^k) b_k$. Comme f est intégral, le sous-anneau $A' = f(R)[a_{ij}^k \mid 1 \leq i, j, k \leq n]$ de A est intégral sur R. Par le lemme précédent, puisque A' est engendrée comme R-algèbre par un nombre fini d'éléments intégraux, c'est aussi un R-module finiment engendré. Par construction, la multiplication par $b = b_1$ préserve le R-module finiment engendré $A'b_1 + \cdots + A'b_n$. Il s'ensuit que b est intégral sur R, ce qu'il fallait démontrer. □

1.32. Définition. Soit R un sous-anneau de A. L'ensemble des éléments de A qui sont intégraux sur R est appelé la *clôture intégrale de R dans A*. Nous dirons que R est *intégralement clos* s'il est sa propre clôture intégrale dans son anneau des fractions. [1]

La clôture intégrale de R dans A est bien un anneau : la somme et le produit de deux éléments intégraux $x, y \in A$ sont des éléments de la R-algèbre $R[x, y]$, qui est bien finiment engendrée comme R-module en vertu du lemme 1.30.

1.33. Proposition. Soient K le corps des fractions de R, et L une extension algébrique de K. Si $x \in L$ est intégral sur R, alors il en est de même pour $\sigma(x)$ (avec $\sigma \in \mathrm{Aut}(L/K)$), $\mathrm{Tr}_{L/K}(x)$, $\mathrm{N}_{L/K}(x)$, et tous les autres coefficients du polynôme caractéristique de x.

Démonstration. C'est clair pour $\sigma(x)$, qui satisfait le même polynôme monique que x. Après avoir plongé L dans sa clôture normale L^{n}, il reste à observer que $\mathrm{Tr}(x)$, $\mathrm{N}(x)$ et les autres coefficients du polynôme caractéristique de x sont respectivement somme, produit et fonctions symétriques de certains des conjugués $\sigma(x)$ de x (cette fois pour $\sigma \in \mathrm{Gal}(L^{\mathrm{n}}/K)$). □

1.34. Proposition. Si R est un anneau factoriel, alors R est intégralement clos.

Démonstration. Soit K le corps des fractions de R et $x \in K$ un élément intégral. Alors il existe $a_0, \ldots, a_{n-1} \in R$ tels que

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0.$$

Pour $s \in R \setminus \{0\}$ un dénominateur réduit de x, nous avons dans R l'égalité

$$(sx)^n + s a_{n-1}(sx)^{n-1} + \cdots + s^{n-1} a_1 (sx) + s^n a_0 = 0.$$

Si maintenant p est un facteur premier de s, alors p divise $(sx)^n$. En conséquence, tout facteur premier de s est un facteur de sx. Puisque s était réduit, il découle que $s \in R^\times$ et donc $x \in R$. □

1.35. Exemple. L'anneau $\mathbb{Z}[\sqrt{-3}]$ n'est pas intégralement clos. En effet, l'élément $\omega = \frac{1+\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3})$ satisfait l'équation $\omega^2 + \omega + 1 = 0$ mais n'appartient pas à $\mathbb{Z}[\sqrt{-3}]$. En conséquence, $\mathbb{Z}[\sqrt{-3}]$ n'est pas factoriel, fait illustré par l'égalité $(1 + \sqrt{-3})(1 - \sqrt{-3}) = 2^2$.

1. La plupart des auteurs réservent le terme 'intégralement clos' aux anneaux intègres.

1.36. Proposition. Soit S un sous-ensemble de R clos par multiplication. Si R est intégralement clos, alors $S^{-1}R$ l'est aussi. Si $f : R \to A$ est intégral, alors $S^{-1}f : S^{-1}R \to S^{-1}A$ l'est aussi.

En conséquence, si R est intègre et A est la clôture intégrale de R dans une extension L de son corps des fractions K, alors $S^{-1}A$ est celle de $S^{-1}R$ dans L.

1.37. Exercice. Démontrer la proposition 1.36.

La technique du point 1.29 peut aussi être utilisée pour prouver le lemme fondamental suivant.

1.38. Lemme (Nakayama)**.** Soit $I \lhd R$ un idéal et M un R module finiment engendré. Si $IM = M$, alors $R = \mathrm{Ann}(M) + I$. En conséquence, il existe $i \in I$ tel que $im = m$ pour tout $m \in M$, et il existe $r \in 1 + I$ tel que $rM = 0$.

Lorsque R est un anneau local, le lemme de Nakayama a la conséquence suivante :

1.39. Corollaire (Nakayama local)**.** Soit R un anneau local ayant I pour unique idéal maximal. Supposons que M soit un module finiment engendré, et que $f_1 + IM, \ldots, f_m + IM$ soit une base du R/I-module M/IM. Alors $f_1, \ldots, f_m$ forment un ensemble minimal de générateurs pour M.

Démonstration. Soit $v_1, \ldots, v_m$ des générateurs du R-module M. Par hypothèse, il existe des éléments $a_{ij} \in I$ tels que

$$\begin{cases} v_1 = a_{11}v_1 + \ldots a_{1m}v_m \\ \quad \vdots \\ v_m = a_{m1}v_1 + \ldots a_{mm}v_m, \end{cases}$$

L'argument du point 1.29 montre qu'il existe un polynôme monique $p \in R[x]$ qui, évalué en l'identité de M, donne $p(\mathrm{id}_M) = 0$, l'endomorphisme nul de M. De plus, par construction les coefficients non-dominants de p sont dans I. Donc $p(\mathrm{id}_M)$ est aussi l'endomorphisme 'multiplication par un élément r' de la forme $r = 1 - x$ avec $x \in I$, ce qui prouve la dernière assertion. Les deux autres s'ensuivent immédiatement, puisque $1 = r + x \in \mathrm{Ann}(M) + I$, et $x = 1 - r \in I$ est l'identité modulo $\mathrm{Ann}(M)$.

Si maintenant R est local et I est son idéal maximal, notons N le sous-R-module de M engendré par $f_1, \ldots, f_m$. Par hypothèse, $N + IM = M$ et donc

$$I \cdot (M/N) = (IM + N)/N = M/N.$$

Nous pouvons alors appliquer le lemme de Nakayama à M/N pour déduire l'existence de $r \in 1+I$ tel que $r \cdot M \subseteq N$. Puisque I est maximal, r est inversible et donc $M = N$, ce qu'il fallait démontrer. Si un sous-ensemble propre des f_i engendre M, alors son image modulo IM engendre certainement M/IM, ce qui est impossible si l'ensemble de départ est un ensemble minimal de générateurs de M/IM. □

2. Domaines de Dedekind

2.1. Anneaux de valuation discrète. Un anneau intègre R est appelé *anneau de valuation* si $K = \mathrm{Frac}(R)$ admet une valuation $v : K \to \Gamma \cup \{\infty\}$ à valeurs dans un groupe abélien totalement ordonné Γ pour laquelle $R = K_{v \geq 0}$.

Rappelons qu'une *valuation* $v : A \to \Gamma \cup \{\infty\}$ sur un anneau A à valeur dans un groupe abélien totalement ordonné Γ est définie par les propriétés :

(i) $v(x) = \infty$ si et seulement si $x = 0$ (non-dégénérescence)
(ii) $v(xy) = v(x) + v(y)$ pour tout $x, y \in A$ (multiplicativité)
(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ pour tout $x, y \in A$ (inégalité ultramétrique)

Dans ce cas, A est nécessairement un domaine, et si $v(x) < v(y)$, alors $v(x+y) = v(x)$.

Associés à une valuation v sur un anneau A sont *l'anneau de valuation* $A_{v\geq 0} = \{x \in A \mid v(x) \geq 0\}$, *l'idéal de valuation* $M_v = A_{v>0} = \{x \in A \mid v(x) > 0\}$ (qui est un idéal de $A_{v\geq 0}$), et l'*anneau résiduel* $k_v = A_{v\geq 0}/M_v$. Dans le cas où R est un anneau de valuation, $R_{v\geq 0} = R$, $R_{v>0} = M_v$ est l'unique idéal maximal (car tout élément de $R_{v=0}$ est inversible dans R), et k_v est le *corps résiduel* de R.

Un anneau de valuation R est appelé *anneau de valuation discrète (a.v.d.)* si sa valuation v prend valeurs dans le groupe ordonné $(\mathbb{Z}, \geq)$. Par convention, nous supposerons toujours que la valuation v d'un a.v.d. est surjective (dite *normalisée*) lorsque v n'est pas triviale (c.-à-d. lorsque R n'est pas un corps).

2.2. Exemple. La valuation p-adique $\mathrm{ord}_p : \mathbb{Z} \to \mathbb{Z} \cup \{\infty\} : a \mapsto \max\{n \in \mathbb{N} \mid p^n | a\}$ est une valuation à valeurs dans $\mathbb{N}$. Mais $\mathbb{Z}$ muni de v_p n'est pas un a.v.d. car l'idéal $(p) = \mathbb{Z}_{\mathrm{ord}_p>0}$ n'est pas l'unique idéal maximal de $\mathbb{Z}$. Autrement dit, $\mathbb{Z}$ est plus petit que l'anneau de valuation de ord_p dans $\mathbb{Q}$. Par la même formule, la valuation ord_p s'étend de façon unique à l'anneau $\mathbb{Z}_{(p)}$ localisé en (p), et cette fois $\mathbb{Z}_{(p)}$ a pour unique idéal maximal (p), est bien égal à $\mathbb{Q}_{\mathrm{ord}_p\geq 0}$, et donc est un a.v.d.

2.3. Remarque. Toute valuation sur un anneau intègre s'étend de façon unique à une valuation de son corps des fractions par la formule $v(\frac{x}{y}) = v(x) - v(y)$. À l'inverse, l'anneau de valuation $K_{v\geq 0}$ d'un corps K pour une valuation v à valeurs dans $\mathbb{Z}$ est toujours un anneau de valuation discrète, puisque tout élément de $K_{v=0} = K_{v\geq 0} \setminus K_{v>0}$ est inversible par construction.

2.4. Exercice. Démontrer que R est un anneau de valuation si et seulement si R est un anneau intègre dans lequel tout élément $x \in \mathrm{Frac}(R)$ satisfait $x \in R$ ou $x^{-1} \in R$.

2.5. Théorème (Caractérisation des a.v.d.)**.** Soit R un anneau intègre et K son corps des fractions. Les propriétés suivantes sont équivalentes.

(i) R est un anneau de valuation discrète (sans être un corps).
(ii) R satisfait la condition $x \in \mathrm{Frac}(R) \Rightarrow x \in R$ ou $x^{-1} \in R$, et le monoïde $(R \setminus \{0\})/R^\times$ ordonné par divisibilité est isomorphe à $(\mathbb{N}, \leq)$.
(iii) Il existe $\varpi \in R$ non-inversible pour lequel tout élément non-nul de R s'écrit de manière unique $u\varpi^n$ pour un certain $u \in R^\times$ et $n \in \mathbb{N}$.
(iv) R est principal et possède exactement une classe d'éléments irréductibles.
(v) R est principal et local (sans être un corps).
(vi) R est noethérien, local, intégralement clos et de dimension 1.
(vii) R est noethérien, local, et son idéal maximal est principal (sans que R soit un corps).

Démonstration. (i) $\Longrightarrow$ (ii). Il est clair que $x \in K_{v\geq 0}$ ou $x^{-1} \in K_{v\geq 0}$. Puisque $R = K_{v\geq 0}$, la condition est satisfaite. La valuation discrète $v : R \setminus \{0\} \to \mathbb{N}$ définit l'isomorphisme requis. En effet, le noyau de v est bien $K_{v=0} = \{x \in K^\times \mid x, x^{-1} \in R\} = R^\times$, et l'ordre est préservé puisque

$$x|y \iff yx^{-1} \in R \iff v(yx^{-1}) \geq 0 \iff v(x) \leq v(y).$$

(ii) $\Longrightarrow$ (iii). Soit v l'isomorphisme de l'énoncé et prenons ϖ un élément de R avec $v(\varpi) = 1$. Pour $x \in R$ et $n = v(x)$, nous avons $x\varpi^{-n} \in R$ ou $\varpi^n x^{-1} \in R$, donc $v(x\varpi^{-n}) + v(\varpi^n) = v(x)$ ou $v(\varpi^n x^{-1}) + v(x) = v(\varpi^n)$. Nous déduisons respectivement que $v(x\varpi^{-n}) = 0$ ou $v(\varpi^n x^{-1}) = 0$, donc que $x\varpi^{-n}$ ou $\varpi^n x^{-1}$ appartient à $R^\times$. Les deux cas impliquent $x = u\varpi^n$ avec $u \in R^\times$. L'unicité de la décomposition est évidente : $n = v(x)$ est uniquement déterminé puisque $v(u) = 0$, et il en est alors de même pour $u = x\varpi^{-n}$.

(iii) $\Longrightarrow$ (iv). Notons v l'application qui associe à $x = u\varpi^n \in R \setminus \{0\}$ l'exposant n donné par le point (iii), et à 0 la valeur $v(0) = \infty$. Soit I un idéal de R, et prenons $x \in I$ avec la propriété

$$v(x) = v(I) := \min\{v(y) \mid y \in I\};$$

ceci est possible car $(\mathbb{N}, \leq)$ est bien ordonné. Nous allons montrer que $I = (x)$. Si $y \in I$ est non-nul, alors $y = t\varpi^m$ avec $m \geq n$, d'où il découle que $y = x(tu^{-1}\varpi^{m-n})$ avec $tu^{-1}\varpi^{m-n} \in R$ puisque $u \in R^\times$ et $m \geq n$. Donc $y \in (x)$, ce qui démontre la première assertion.

La seconde est évidente, puisque $u\varpi^n$ est irréductible si et seulement si $n = 1$.

(iv) $\Longrightarrow$ (v). Soient (x) et (y) deux idéaux maximaux de R. Puisqu'ils sont principaux, x et y sont irréductibles donc associés. Il s'ensuit que $(x) = (y)$ et R est local.

(v) $\Longrightarrow$ (vi). Immédiat au vu de la proposition 1.34.

(vi) $\Longrightarrow$ (vii). Soit M l'unique idéal premier propre et non-nul de R (M est bien sûr maximal). Pour $I \lhd R$, notons $(R : I)$ le sous-module de K composé des éléments $x \in K$ tels que $x \cdot I \subseteq R$. Il est clair que $(R : I)$ contient R ; nous allons montrer que cette inclusion est stricte pour $I = M$.

Pour ce faire, considérons l'ensemble des idéaux I de R pour lesquels $R \subsetneq (R : I)$. Il est non-vide car tout idéal principal (x) donne $x^{-1} \in (R : (x))$. Soit J un idéal de cet ensemble, pris maximal pour l'inclusion (ce qui est possible parce que R est noethérien). Prenons $x, y \in R$ tels que $xy \in J$ et $x \notin J$, et $z \in (R : J) \setminus R$. Par maximalité, l'idéal $J + (x)$ de R satisfait $(R : J + (x)) = R$, donc $zy(J + (x)) \subseteq R$ implique $zy \in R$. Mais alors $z(J + (y)) \subseteq R$, et donc $J + (y) = J$ par maximalité. Ceci signifie que $y \in J$ et que J est premier. Puisque R est local de dimension 1 et que J est propre et non-nul, nous concluons que $J = M$.

La chaine d'inclusions $M \subseteq (R : M) \cdot M \subseteq R$ ne laisse que deux possibilités. La première, $M = (R : M) \cdot M$, contredit ce qui précède car elle implique l'existence d'un élément $z \notin R$ tel que $zM \subseteq M$. Un tel élément doit être intégral (puisqu'il préserve le sous-R-module M finiment engendré), or R est supposé intégralement clos. Donc $(R : M) \cdot M = R$.

Nous nous penchons maintenant sur l'idéal $\bigcap_{n\in\mathbb{N}} M^n$. Il est clair que $(R : M)$ préserve ce dernier. Puisque R est intégralement clos et que $(R : M) \supsetneq R$, nous devons avoir $\bigcap_{n\in\mathbb{N}} M^n = 0$.[2] Donc il existe un élément $\varpi \in M$ tel que $\varpi \notin M^2$. Alors d'une part $\varpi \cdot (R : M)$ est un idéal de R, d'autre part il ne peut pas être contenu dans M sinon $\varpi \in \varpi \cdot (R : M) \cdot M \subset M^2$. Nous concluons que $\varpi \cdot (R : M) = R$ et il en découle que $M = \varpi \cdot (R : M) \cdot M = \varpi \cdot R$ est engendré par ϖ.

(vii) $\Longrightarrow$ (iii). Soit ϖ un générateur de l'idéal maximal M de R. Montrons d'abord que $\bigcap_{n\in\mathbb{N}} M^n = \bigcap_{n\in\mathbb{N}} (\varpi^n) = 0$.[3] Si $x \in \bigcap_{n\in\mathbb{N}} (\varpi^n)$, alors pour tout $n \in \mathbb{N}$ nous trouvons $y_n \in R$ tel que $x = y_n\varpi^n$. De là, nous voyons que $y_n = y_{n+1}\varpi$, et donc que la suite d'idéaux (y_n) est croissante. Puisque R est noethérien, nous avons à terme que y_n et y_{n+1} sont associés. Or ϖ n'est pas inversible, donc $y_n = 0$ et $x = 0$.

Ensuite, nous montrons que tout idéal non-nul $I \lhd R$ est de la forme M^n pour $n \in \mathbb{N}$. Prenons le plus grand $n \in \mathbb{N}$ pour lequel $I \subseteq M^n$. Alors $I + M^{n+1}$ est un sous-module non nul de M^n/M^{n+1}. Puisque ce dernier est de dimension 1 sur R/M, l'image de n'importe quel élément de $x \in I \setminus M^{n+1}$ engendre M^n/M^{n+1} comme R-module. Par le lemme de Nakayama local (corollaire 1.39), nous déduisons qu'il en est de même pour x et M^n ; mais alors $M^n = I$.

Il en découle en particulier que si $x \in R$ est non-nul, $(x) = (\varpi^n)$ pour un certain n. L'unicité de la décomposition qui découle de cet égalité suit du fait que $M^n \neq M^{n+1}$.

(iii) $\Longrightarrow$ (i). En conséquence de l'hypothèse, tout $x \in K^\times$ s'écrit de façon unique $x = u\varpi^n$ pour $u \in R^\times$ et $n \in \mathbb{Z}$; posons $v(x) = n$. Alors v est une valuation discrète, dont R est bien l'anneau de valuation. □

2.6. Remarque. La condition 'intégralement clos' est indispensable. Soit K algébriquement clos avec $\operatorname{char} K \neq 2$ et P l'idéal premier de $K[x, y]$ engendré par le polynôme irréductible $x(x^2 + y^2) + x^2 - y^2$. L'anneau $A = K[x, y]/P$ est noethérien et de dimension 1 (puisque P n'est pas maximal). Sa localisation $A_{(x,y)}$ en l'idéal maximal engendré par x et y est donc un anneau noethérien local de dimension 1. Mais $A_{(x,y)}$ n'est pas intégralement clos, et en conséquence n'est pas un anneau de valuation discrète. $A_{(x,y)}$ n'est pas non plus principal.

2.7. Exemples. (i) $\mathbb{Q}_{\operatorname{ord}_p \geq 0} = \mathbb{Z}_{(p)}$ est un a.v.d., comme vu dans l'exemple précédent. Notons que $\mathbb{Z}[p^{-1}]$ n'est pas un anneau de valuation discrete : si q_1, q_2 sont premiers à p et entre-eux, alors ni $\frac{q_1}{q_2}$ et $\frac{q_2}{q_1}$ n'appartiennent à $\mathbb{Z}[p^{-1}]$.

2. Ceci est aussi une conséquence directe du théorème d'intersection de Krull, qui dit que dans un anneau noethérien, l'intersection $\bigcap_{n\in\mathbb{N}} I^n$ est nulle si et seulement si aucun élément de $1 + I$ ne divise 0.

3. Même remarque.

(ii) L'anneau $\mathbb{Z}_p$ des entiers p-adiques est un a.v.d. C'est le complété de $\mathbb{Z}$ pour la norme p-adique.
(iii) Si K est un corps, la valuation t-adique v_t sur le corps des fonctions rationnelles $K(t)$ est discrète. L'anneau $K(t)_{v_t \geq 0}$ est donc un a.v.d., qui admet $K[t]$ comme sous-anneau. Le degré $\deg_t$ en t définit lui aussi à une valuation discrete v_∞ sur $K(t)$, par la formule $v_\infty(\frac{f}{g}) = \deg_t(g) - \deg_t(f)$, pour $f, g \in K[t]$.
L'automorphisme $t \mapsto t^{-1}$ de $K(t)$ permute ces deux valuations discrètes.
(iv) L'anneau des series formelles $K[[t]]$ est un a.v.d. En effet, $K[[t]]$ a pour seul idéal maximal celui engendré par t (puisque toute série dont le terme constant est non-nul est inversible dans $K[[t]]$), et noethérien. L'anneau $K[[t]]$ contient $K(t)_{v_t \geq 0}$ comme sous-anneau ; il en est même la complétion t-adique.

2.8. Théorème (Ostrowski)**.** Toute valuation discrete sur $\mathbb{Q}$ est de la forme ord_p pour p premier. Les seules normes additionnelles sont les puissances de la valeur absolue $|\cdot|$ classique (archimédiennes).

Démonstration. Omise. □

2.9. Exercice (Un théorème d'Ostrowski pour $K(t)$)**.** Montrer que toutes les valuations discrètes de $K(t)$ qui sont triviales sur K sont de la forme v_f pour $f \in K[t]$ un polynôme irréductible monique, ou bien v_∞ (voir ci-dessus). Montrer au passage que ces valuations sont bien distinctes. (Noter que la condition de trivialité sur K est automatiquement satisfaite si K est un corps fini.)
Si de plus K est algébriquement clos, montrer que cet ensemble s'identifie de manière naturelle avec la droite projective $\mathrm{P}^1(K)$.

2.10. Exercice ($\mathcal{I}$-adique contre v-adique)**.** Soit A un anneau, et $\mathcal{I}$ une famille d'idéaux de A close pour l'intersection. Alors les quotients A/I pour $I \in \mathcal{I}$ forment un système inverse, dans lequel $A/I_1 \to A/I_2$ est l'application quotient lorsque $I_1 \subseteq I_2$. La limite $A_{\mathcal{I}} = \lim_{\mathcal{I}} A/I$ de ce système inverse est appelé la *complétion $\mathcal{I}$-adique de A*.

Soit maintenant R un a.v.d. ayant v pour valuation. La formule $\|x\|_v = \exp(-v(x))$ définit une norme non-archimédienne sur R. La complétion $\overline{R}$ de R pour cette norme est à nouveau un a.v.d., ayant pour valuation discrète l'unique extension de v, et est appelé la *complétion v-adique de R*.

Vérifier le bien-fondé de ces deux notions. Montrer que lorsque R est un a.v.d. et $\mathcal{I}$ est la collection de tous les idéaux de R, la complétion $\mathcal{I}$-adique et la complétion v-adique sont naturellement isomorphes.

2.11. La filtration du groupe multiplicatif d'un a.v.d. Le lemme suivant a été observé dans la preuve du théorème 2.5 :

2.12. Lemme. Soit R un a.v.d. ayant M pour idéal de valuation et k comme corps résiduel. Les k-modules k et M^n/M^{n+1} sont isomorphes.

Démonstration. Soit ϖ un générateur de M. La multiplication par ϖ^n induit un isomorphisme $R \to M^n$ de R-modules qui envoie M sur M^{n+1}. □

La valuation v d'un a.v.d. établit une suite exacte

$$0 \to U \xrightarrow{\text{incl.}} K^\times \xrightarrow{v} \mathbb{Z} \to 0.$$

De plus, nous pouvons détailler complètement la structure multiplicative du groupe $U = R^\times$ des unités de R. Notons $U_n = 1 + M^n$ le *n-ème sous-groupe de congruence de U*.

2.13. Proposition. Soit R un a.v.d. Les sous-groupes U_i forment une filtration de U. L'application canonique $R \to k$ induit un isomorphisme $U/U_1 \cong k^\times$. Pour tout $n \geq 1$, l'application $u \mapsto u - 1$ induit un isomorphisme $U_n/U_{n+1} \cong M^n/M^{n+1}$.

La preuve du théorème 2.5 a fait apparaître un objet important de l'étude des anneaux de nombres : l'inverse d'un idéal pour le produit de sous-modules. Cet inverse va à nouveau jouer un

rôle important dans le théorème suivant. Il s'agit d'un exemple primordial d'idéal fractionnaire, objet que nous examinons avant de poursuivre.

2.14. Idéaux fractionnaires. Soit R un anneau intègre et K son corps des fractions. Un *idéal fractionnaire de* R est un sous-R-module I de K jouissant de la propriété : il existe un élément $d \in R$ pour lequel $dI \subseteq R$.

Étant donné deux sous-R-modules I_1, I_2 de K, nous notons

$$(I_2 : I_1) = \{x \in K \mid xI_1 \subseteq I_2\}.$$

On montre facilement que $(I_2 : I_1)$ est un idéal fractionnaire lorsque I_1, I_2 le sont. Un idéal fractionnaire I_1 est dit *inverse d'un idéal fractionnaire* I_2 si $I_1 I_2 = R$; si un inverse de I_2 existe, I_2 est dit *inversible*.

2.15. Exercice. Montrer que si I_1, I_2 sont des idéaux fractionnaires de R, il en est de même pour $I_1 + I_2$, $I_1 I_2$, $I_1 \cap I_2$, et $(I_2 : I_1)$.

2.16. Lemme. Si R est un anneau noethérien intègre, alors un sous-R-module non-nul de $\mathrm{Frac}(R)$ est un idéal fractionnaire si et seulement si il est finiment engendré (comme R-module).

Démonstration. Une direction est évidente : $I \cong dI$ comme R-modules. Pour l'autre, choisir un dénominateur commun des générateurs de I. □

2.17. Proposition. Soit P un ideal premier de R et I_1, I_2 deux idéaux fractionnaires de R. Alors leur localisations en P sont des idéaux fractionnaires de R_P. De plus, l'opération de localisation en P commute avec la somme, le produit, l'intersection, l'opération $(- : -)$, et l'inversion.

Démonstration. Directe. □

2.18. Proposition (Unicité de l'inverse d'un idéal fractionnaire)**.** S'il existe, tout inverse I^{-1} d'un idéal fractionnaire I coincide avec $(R : I)$.

Démonstration. Il est clair que $I^{-1} \subseteq (R : I)$. Pour l'inclusion inverse, remarquons que

$$(R : I) = (R : I)II^{-1} \subseteq RI^{-1} = I^{-1}.$$ □

2.19. Théorème (Caractérisation des domaines de Dedekind)**.** Soit R un anneau intègre. Les conditions suivantes sont équivalentes.

(i) R est noethérien, intégralement clos et de dimension ≤ 1.
(ii) R est noethérien, et pour chaque idéal premier $P \triangleleft R$ propre et non nul, la localisation R_P est un anneau à valuation discrète
(iii) Tout idéal non nul de R se décompose de façon unique en un produit d'idéaux premiers.
(iv) Tous les idéaux fractionnaires non nuls de R sont inversibles.

2.20. Définition. Un anneau intègre qui satisfait aux conditions équivalentes du théorème 2.19 (et qui n'est pas un corps) est appelé *domaine de Dedekind*.

Démonstration du théorème 2.19.

(i) $\implies$ (ii). Nous avons vu dans la démonstration de la proposition 1.19 que les idéaux de R_P sont des extensions d'idéaux de R. Ceci implique immédiatement qu'ils sont finiment engendrés et que R_P est de dimension 1. R_P étant évidemment local, grâce au théorème 2.5 il ne reste à vérifier que la clôture intégrale. Si $x \in K = \mathrm{Frac}(R)$ est intégral sur R_P, c'est-à-dire si

$$x^n + \frac{a_{n-1}}{b}x^{n-1} + \cdots + \frac{a_0}{b} = 0, \quad a_i \in R, b \in R \setminus P,$$

alors bx est intégral sur R, donc $bx \in R$ et $x \in R_P$.

(ii) $\implies$ (iii). Puisque $\dim_{\mathrm{Krull}}(R) = \sup\{\dim_{\mathrm{Krull}}(R_M) \mid M \text{ idéal maximal de } R\}$, nous avons d'emblée $\dim_{\mathrm{Krull}}(R) = 1$.

Prenons I un idéal non nul de R. Le lemme 1.12 implique que I est contenu dans un nombre fini d'idéaux premiers propres (tous nécessairement minimaux et maximaux pour cette propriété).

Pour chaque idéal premier P propre et non nul, R_P est un a.v.d. par hypothèse, et l'idéal IR_P de R_P coincide avec $P^{n_P}R_P$ pour un certain $n_P \in \mathbb{N}$. L'entier n_P est précisément $\min\{v_P(x) \mid x \in I\}$, et est non nul précisément quand P contient I (ce qui n'arrive que pour un nombre fini d'idéaux premiers P).

Nous allons montrer que

$$I = \prod_{P \text{ premier avec } n_P > 0} P^{n_P}.$$

Puisque ses deux membres sont des idéaux de R, cette égalité peut être vérifiée localement (appliquer le corollaire 1.25 à l'inclusion d'un membre dans la somme des deux). Par construction, nous avons pour chaque P l'égalité $IR_P = P^{n_P}R_P$.

(iii) $\implies$ (iv). Il suffit de montrer que les idéaux premiers non nuls sont inversibles. En effet, tout idéal fractionnaire I se factorise $(d)^{-1}P_1^{n_1}\cdots P_k^{n_k}$ par hypothèse.

Premièrement, observons l'inverse : si un idéal inversible I se factorise $P_1\cdots P_n$, alors chacun des P_i est inversible. En effet, P_i a pour inverse $I^{-1}\cdot P_1\cdots \not{P_i}\cdots P_n$.

Deuxièmement, montrons que tout idéal premier propre inversible P de R est maximal. Sinon, prenons $a \in R \setminus P$ tel que $P+(a)$ soit un idéal propre. Par hypothèse, ce dernier se factorise $P+(a) = P_1\cdots P_m$ et il en est de même pour $P+(a^2) = Q_1\cdots Q_n$. Dans l'anneau quotient R/P, les idéaux $P+(a)$ et $P+(a^2)$ sont principaux. Par l'observation précédente, nous en déduisons que les P_i/P et les Q_j/P sont tous inversibles. De plus,

$$\prod_{i=1}^{m}(P_i/P)^2 = (P+(a^2))/P = \prod_{j=1}^{n}(Q_j/P).$$

L'unicité de cette factorisation dans R/P ne peut pas être déduite directement de l'hypothèse ; néanmoins, elle découle du principe général suivant. Si I est un idéal d'un domaine R qui se factorise en produit d'idéaux premiers inversibles, alors cette factorisation est nécessairement unique. En effet, si I se factorise $P_1\cdots P_m = Q_1\cdots Q_n$, nous pouvons supposer sans perte de généralité que Q_1 est minimal pour l'inclusion. Il s'ensuit que $P_1\cdots P_m \subseteq Q_1$ implique disons $P_1 \subseteq Q_1$. Du coup, $Q_1\cdots Q_n \subseteq P_1$ implique $Q_j \subseteq P_1 \subseteq Q_1$, et donc $Q_1 = P_1$ par minimalité. En inversant P_1, nous déduisons que $P_2\cdots P_m = Q_2\cdots Q_n$ et par récurrence que la factorisation est unique.

Il suit maintenant de l'unicité de cette factorisation que $n = 2m$ et que chaque P_i/P apparaît deux fois parmi les Q_j/P ; de là, nous déduisons que $P+(a^2) = P_1^2\cdots P_n^2 = (P+(a))^2$. Donc si $x \in P$, nous pouvons écrire $x = y + ra$ avec $y \in P^2$ et $r \in R$. Alors $ra \in P$, d'où $r \in P$ puisque P est premier. Nous concluons que

$$P \subseteq P^2 + Pa \subseteq P \quad \text{et donc} \quad P = P^2 + Pa = P(P+(a)).$$

Puisque P est inversible (ou bien par unicité de la factorisation), ceci implique que $R = P+(a)$, contradiction.

Finalement, déduisons qu'un idéal premier P quelconque est inversible. Prenons $a \in P$. Par hypothèse, (a) se factorise $P_1\cdots P_m$. Par la première observation, les P_i sont tous inversibles, et par la deuxième observation, les P_i sont maximaux. Mais $P_1\cdots P_m \subseteq P$ implique disons $P_1 \subseteq P$; donc $P_1 = P$ et P est inversible.

(iv) $\implies$ (i). Montrons d'abord que R est noethérien ; ceci découle du fait que tout idéal fractionnaire inversible est finiment engendré. En effet, si I est un idéal de R et I^{-1} son inverse, alors il existe $a_i \in I, b_i \in I^{-1}$ tels que $1 = \sum_i a_i b_i$. Mais alors pour $x \in I$ quelconque, nous voyons que $x = \sum_i a_i(xb_i)$ avec $xb_i \in R$ puisque $b_i \in I^{-1}$. Ceci signifie que I est engendré par les a_i.

Soit maintenant $x \in K$ un élément intégral sur R. Alors $A = R[x]$ est un idéal fractionnaire de R qui satisfait $A^2 = A$ puisque c'est un anneau. En utilisant que A est inversible,

$$A = AR = AAA^{-1} = AA^{-1} = R,$$

et R est intégralement clos.

Il ne reste qu'à vérifier que R est de dimension 1. Si $0 \subsetneq P \subsetneq M \subsetneq R$ est une chaine d'idéaux premiers de R, alors PM^{-1} est un idéal de R (par définition de M^{-1}) et $PM^{-1}M = P$. Donc

$PM^{-1} \subseteq P$ (puisque P est premier et $M \not\subseteq P$), ce qui implique que $M^{-1} \subseteq R$, d'où $R \subseteq M$, absurde.

(ii) $\implies$ (iv). Soit I un idéal fractionnaire de R. Nous allons montrer que $(R : I)$ est bien son inverse. Puisque $(R : I)I$ est un idéal de R, il suffit de montrer qu'il n'est pas contenu dans un idéal maximal. Soient $a_1, \ldots, a_n$ des générateurs pour I, et P un idéal maximal de R. Sans perte de généralité, nous pouvons supposer que $v_P(a_1)$ est minimal, autrement dit que $I_P = (a_1)R_P$. En conséquence, $\frac{a_i}{a_1} = \frac{x_i}{y_i}$ avec $y_i \notin P$. Mais alors, $\frac{(\prod_i y_i)a_i}{a_1} = x_i \in R$ pour tout i, donc $\frac{\prod_i y_i}{a_1} \in (R : I)$ et $\prod_i y_i \in (R : I)I$. Or $\prod_i y_i \notin P$, ce qui montre que $(R : I)I \not\subset P$ comme souhaité.

(iv) $\implies$ (iii). Nous avons déjà montré que le point (iv) implique que R est noethérien.

Dès lors, s'il existe un idéal J qui ne soit pas le produit d'idéaux premiers, nous pouvons choisir J maximal pour cette propriété. Puisque J n'est pas lui-même maximal, J est contenu proprement dans un idéal maximal P. Ce derner étant inversible par hypothèse, nous avons que $P^{-1}J$ est un idéal propre de R qui contient J. Il s'ensuit que $P^{-1}J$ a une factorisation $P_1 \cdots P_n$ en produit d'idéaux premiers, et donc $J = P \cdot P_1 \cdots P_n$ aussi.

L'unicité de la factorisation se démontre comme dans le point (iii) $\implies$ (iv).

(ii) $\implies$ (i). Nous faisons usage de la caractérisation des a.v.d. (théorème 2.5).

Être de dimension ≤ 1 est une condition locale, et de même pour être intégralement clos. En effet, si $x \in K$ est intégral sur R, alors il l'est aussi sur R_P. Par hypothèse, $x \in R_P$ pour tout P premier, ce qui implique que $x \in R$ (en localisant le R-module $R + Rx \supseteq R$). □

2.21. Remarque. On peut extraire de la preuve du théorème 2.19 les principes généraux suivants :

(i) Être intégralement clos et être de dimension n sont des propriétés très locales.

(ii) Si $P \subsetneq Q$ sont deux idéaux premiers d'un anneau intègre R, un seul peut être inversible. (En effet, si P, Q sont inversibles, PQ^{-1} est un idéal de R, et $(PQ^{-1})Q = P$. Comme P est premier, il suit $PQ^{-1} \subseteq P$, et donc $PQ = P$.)

(iii) Un idéal fractionnaire non-nul I d'un domaine noethérien A est inversible si et seulement si il est très localement principal. (En effet, dans un domaine local tout idéal inversible doit être principal.) En conséquence, tout idéal premier inversible est de codimension 1. Ceci confirme le point précédent.

Récoltons immédiatement les fruits du théorème 2.19.

2.22. Corollaire. Les a.v.d. sont précisément les domaines de Dedekind locaux. Être de Dedekind est une propriété locale.

2.23. Corollaire. Si R est un domaine de Dedekind, toute valuation non-triviale sur $\mathrm{Frac}(R)$ et positive sur R est l'une des valuations P-adiques de R.

Démonstration. Soit v une valuation non-triviale sur $\mathrm{Frac}(R)$ et $K_{v\geq 0}$ son anneau de valuation. Par hypothèse, $R \subseteq K_{v\geq 0}$, et donc $P = R \cap K_{v>0}$ est un idéal premier propre de R. Puisque v est non-triviale, il existe $x, y \in R$ non nuls tels que $v(\frac{x}{y}) = v(x) - v(y) \neq 0$. Du coup, $v(x)$ ou $v(y)$ est non nul, et il en est de même pour P.

La restriction de v à R_P est positive, et l'idéal de valuation de R_P est PR_P. Fixons maintenant $\varpi \in P \setminus P^2$. Tout élément non nul de K s'écrit $u\varpi^n$ avec $u \in R_P^\times = R_P \setminus PR_P$ et $n \in \mathbb{Z}$, d'où $v(u\varpi^n) = v(u) + nv(\varpi) = nv(\varpi)$. Donc v est équivalente à la valuation P-adique. □

2.24. Corollaire. Toute localisation d'un domaine de Dedekind est un domaine de Dedekind ou son corps de fractions. De plus, si $S \subset R$ est un ensemble multiplicativement clos d'un domaine de Dedekind, l'application

$$\mathcal{I}_R \to \mathcal{I}_{S^{-1}R} : I \mapsto S^{-1}I$$

est un morphisme surjectif du groupe des idéaux fractionnaires non nuls de R à celui de $S^{-1}R$, dont le noyau est l'ensemble des idéaux fractionnaires de R qui rencontrent S.

DÉMONSTRATION. La première assertion découle immédiatement de la condition (ii). La seconde résulte de la proposition 1.19. □

2.25. Corollaire. Tout quotient non trivial d'un domaine de Dedekind est un anneau artinien.

DÉMONSTRATION. Notons que tout quotient non trivial R d'un domaine de Dedekind est un anneau noethérien de dimension 0. Nous montrons ci-après que dans ce cas R est artinien.

Par le lemme 1.12, R n'a qu'un nombre fini d'idéaux premiers propres $P_1, \dots, P_n$, qui sont d'ailleurs tous maximaux. En particulier, ils sont deux à deux comaximaux et leur intersection est le radical nilpotent N de R. Puisque R est noethérien, il existe un entier l tel que $N^l = 0$ et donc $\prod_{i=1}^n P_i^l \subseteq (\bigcap_{i=1}^n P_i)^l = N^l = 0$. Le théorème des restes chinois garantit alors que l'application canonique

$$R \to \prod_{i=1}^n R/P_i^l : x \mapsto (xP_i^l)_{i=1}^n$$

est un isomorphisme d'anneaux. Finalement, R/P_i^l est artinien vu qu'il admet la filtration

$$0 = P_i^l \subseteq P_i^{l-1} \subseteq \cdots \subseteq P_i^2 \subseteq P_i \subseteq R$$

dont les quotient successifs sont des modules artiniens, puisque ce sont des modules finiment engendrés sur le corps R/P_i. □

2.26. Corollaire. Dans un domaine de Dedekind, la relation de contenance entre les idéaux coincide avec la relation de divisibilité (pour le produit d'idéaux).

DÉMONSTRATION. Si $I_1 I_2 = I_3$, il est clair que $I_1 \supseteq I_3$. Nous allons montrer la réciproque.

Soit donc $I \supseteq J$ deux idéaux, et $I = P_1 \cdots P_m$, $J = Q_1 \cdots Q_n$ leur factorisation en produit d'idéaux premiers. Puisque $P_1 \supseteq Q_1 \cdots Q_n$, il existe un facteur, disons Q_1, contenu dans P_1. Puisque Q_1 est maximal, nous déduisons que $P_1 = Q_1$, que $P_2 \cdots P_m \supseteq Q_2 \cdots Q_n$, et puis par récurrence que $P_i = Q_i$ pour $i = 1, \dots, m$ (à un réarrangement des Q_i près). Ceci implique que $I \cdot Q_{m+1} \cdots Q_n = J$. □

2.27. Corollaire. Tout idéal I d'un anneau de Dedekind R est un module projectif sur R.

DÉMONSTRATION. Rappelons qu'un module P est projectif si et seulement si le foncteur $\mathrm{Hom}(P, -)$ est exact à droite. Puisque I est finiment présenté (car R est noethérien), l'application canonique

$$\mathrm{Hom}(I, M)_P \to \mathrm{Hom}(I_P, M_P) : \frac{f}{s} \mapsto \left(\frac{x}{t} \mapsto \frac{f(x)}{st} \right)$$

est un isomorphisme de R_P-modules, pour tout R-module M. Nous pouvons donc vérifier l'exactitude de $\mathrm{Hom}(I, -)$ localement. Or localement, I_P est un module libre de rang 1, donc $\mathrm{Hom}(I_P, -)$ est exact. □

2.28. Remarque. Réciproquement, on peut montrer qu'un anneau intègre noethérien qui satisfait la conclusion du corollaire 2.26 est un domaine de Dedekind (ou un corps). Idem pour un anneau intègre qui satisfait la conclusion de 2.27.

2.29. Corollaire. Un domaine de Dedekind R est un anneau factoriel si et seulement si il est principal.

DÉMONSTRATION. Il suffit de montrer que si R est factoriel, il est principal. Puisque les idéaux de R se factorisent en produit d'idéaux premiers, il suffit de montrer que tout idéal premier P est principal. Soit $x \in P$ non nul, et y un des facteurs irréductibles de x appartenant à P (ce dernier existe car P est premier). Alors (y) est premier par le lemme d'Euclide et contenu dans P. Il s'ensuit que $P = (y)$ est principal. □

2.30. Le groupe des classes d'idéaux. Notons $\mathcal{P}$ l'ensemble des idéaux maximaux de R, et $\mathcal{I}$ l'ensemble des idéaux fractionnaires inversibles de R. L'ensemble $\mathcal{I}$ muni du produit d'idéaux fractionnaires est un groupe abélien, appelé le *groupe d'idéaux de R*. Puisque tout idéal principal non-nul est inversible, les idéaux principaux non-nuls forment un sous-groupe $\mathcal{R}$ de $\mathcal{I}$, qui s'identifie à $(R \setminus \{0\})/R^\times$. Le quotient

$$\mathrm{Cl}(R) = \mathcal{I}/\mathcal{R}$$

est appelé le *groupe de classes d'idéaux de R*, souvent abrévié *groupe de classes*, parfois aussi appelé le *groupe de Picard de R*. Ses éléments sont donc des classes d'équivalences d'idéaux (fractionnaires) de R pour la relation $I_1 \sim I_2 \iff$ il existe $x \in \mathrm{Frac}(R)$ tel que $I_1 = xI_2$.

2.31. Corollaire (du théorème 2.19)**.** Soit R un domaine de Dedekind. Pour $I \subseteq \mathrm{Frac}(R)$ et P un idéal maximal de R, écrivons $v_P(I) = \inf\{v_P(x) \mid x \in I\}$, où v_P dénote la valuation discrete dont R_P est l'anneau de valuation. L'application

$$(v_P)_{P\in\mathcal{P}} : \mathcal{I}_R \to \bigoplus_{P\in\mathcal{P}} \mathbb{Z} : I \mapsto (v_P(I))_{P\in\mathcal{P}}$$

induite par les valuations locales est un isomorphisme de groupes abéliens, ayant pour inverse l'application $(n_P)_{P\in\mathcal{P}} \mapsto \prod_{P\in\mathcal{P}} P^{n_P}$. Cet isomorphisme est la composée de l'application canonique $\mathcal{I}_R \xrightarrow{\sim} \bigoplus_{P\in\mathcal{P}} \mathcal{I}_{R_P}$ avec les identifications $\mathcal{I}_{R_P} \xrightarrow{\sim} \mathbb{Z}$ induites par les v_P.

Démonstration. Le point (iii) du théorème 2.19 montre que l'ensemble $\mathcal{I}$ muni du produit d'idéaux est un groupe abélien libre de base $\mathcal{P}$. En effet, si $I \in \mathcal{I}$ et $d \in R$ est tel que dI est un idéal de R, nous pouvons factoriser $dI = P_1 \cdots P_n$ et $(d) = Q_1 \cdots Q_n$ pour déduire $I = P_1 \cdots P_n \cdot Q_1^{-1} \cdots Q_n^{-1}$. Le fait que les éléments de $\mathcal{P}$ soient indépendants est équivalent à l'unicité de la factorisation.

Pour obtenir l'isomorphisme énoncé, il suffit de repêcher la factorisation d'un idéal $I = \prod_{P\in\mathcal{P}} P^{v_P(I)}$ démontrée dans la preuve de l'implication (ii) $\implies$ (iii). □

2.32. Corollaire. L'application $v_P : \mathcal{I}_R \to \mathbb{Z}$ du corollaire 2.31 satisfait les propriétés suivantes :

(i) $v_P(IJ) = v_P(I) + v_P(J)$;
(ii) $v_P(I^{-1}) = -v_P(I)$;
(iii) $v_P(I + J) = \min\{v_P(I), v_P(J)\}$;
(iv) $v_P(I \cap J) = \max\{v_P(I), v_P(J)\}$.

Démonstration. Puisque $v_P(I) = v_P(I_P)$, les formules peuvent être vérifiés localement. Elles sont triviales dans un a.v.d. □

Nous retrouvons facilement le résultat suivant, qui découle en réalité du fait que R est intégralement clos.

2.33. Corollaire. Soit R un domaine de Dedekind. Un idéal fractionnaire I de R est un idéal si et seulement si $v_P(I) \geq 0$ pour tout $P \in \mathcal{P}$. En conséquence,

$$R = \{x \in \mathrm{Frac}(R) \mid v_P(x) \geq 0 \text{ pour tout } P \in \mathcal{P}\}.$$

Démonstration. La première assertion est une conséquence directe de la factorisation explicite du corollaire 2.31. Si x appartient au membre de droite, alors par examination de sa factorisation l'idéal fractionnaire (x) est un idéal de R. A fortiori, son générateur x appartient à R. □

2.34. Corollaire. Soit R un domaine de Dedekind. Si R n'a qu'un nombre fini d'idéaux premiers, alors R est principal.

Démonstration. Il suffit de démontrer que chacun des idéaux premiers non nuls $P_1, \ldots, P_n$ de R est principal. Le théorème des restes chinois établit une surjection

$$R \to \prod_{i=1}^{n} R/P_i^2 : x \mapsto (xP_i^2)_{i=1}^n$$

dont le noyau est le produit $P_1^2 \cdots P_n^2$. Il existe donc $x \in R$ tel que $x \in P_j \setminus P_j^2$ et $x \notin P_i$ pour $i \neq j$. Par construction, l'idéal (x) a pour valuations $v_{P_j}(x) = 1$ et $v_{P_i}(x) = 0$ pour $i \neq j$. Par le corollaire 2.31, $P_j = (x)$ est donc principal. □

Le mieux que l'on puisse faire quand $\mathcal{P}$ est infini est le théorème d'approximation suivant.

2.35. Théorème (Approximation forte)**.** Soient $\mathcal{S}$ un sous-ensemble fini de $\mathcal{P}$, et pour chaque $P \in \mathcal{S}$, soient $a_P \in \mathrm{Frac}(R)$ et $n_P \in \mathbb{N}$. Il existe un élément $x \in \mathrm{Frac}(R)$ tel que $v_P(x - a_P) = n_P$ pour $P \in \mathcal{S}$ et $v_P(x) \geq 0$ pour $P \notin \mathcal{S}$.

Démonstration. Prenons un élément $s \in R$ tel que $sa_P \in R$ pour tout $P \in \mathcal{S}$. Quitte à agrandir $\mathcal{S}$ (et poser $a_P = 0$, $n_P = 0$ pour les ajouts), nous pouvons supposer que $\mathcal{S}$ contient tous les facteurs premiers de (s). Nous allons trouver $y \in R$ tel que

$$\begin{cases} v(y - sa_P) = n_P + v_P(s) & P \in \mathcal{S} \\ v_P(x) \geq 0 & P \notin \mathcal{S}. \end{cases}$$

L'énoncé s'en suivra en prenant $x = \frac{y}{s}$.

Le théorème des restes chinois établit une surjection

$$R \to \prod_{P \in \mathcal{S}} R/P^{n_P + v_P(s) + 1} : y \mapsto (yP^{n_P + v_P(s)+1})_{P \in \mathcal{S}},$$

et il suffit de prendre y dans la préimage de $\prod_{P \in \mathcal{S}} \left(sa_P + P^{n_P + v_P(s)} \setminus sa_P + P^{n_P + v_P(s)+1}\right)$. □

2.36. Corollaire. Tout idéal fractionnaire d'un domaine de Dedekind peut être engendré par deux éléments.

Démonstration. Sans perte de généralité, nous pouvons supposer que I est un idéal du domaine de Dedekind R. Par le théorème 2.35, nous pouvons d'abord prendre un élément $x \in R$ tel que $v_P(x) = v_P(I)$ pour tout $P \in \mathcal{P}$ qui divise I. En applicant une fois de plus le théorème 2.35, nous choisissons ensuite un élément $y \in R$ tel que $v_P(y) = v_P(I)$ pour tout $P \in \mathcal{P}$ qui contient x. Nous calculons alors

$$v_P((x,y)) = \min\{v_P(x), v_P(y)\} = \begin{cases} v_P(I) & \text{pour } P \in \mathcal{P} \text{ qui divise } I \\ v_P(y) = 0 & \text{pour } P \in \mathcal{P} \text{ qui divise } (x) \text{ sans diviser } I \\ v_P(x) = 0 & \text{pour } P \in \mathcal{P} \text{ qui ne divise pas } (x). \end{cases}$$

Dès lors, $v_P((x,y)) = v_P(I)$ pour tout $P \in \mathcal{P}$ et le corollaire 2.31 permet de conclure l'égalité des idéaux. □

2.37. Exemples.

(i) Tout domaine principal est de Dedekind. En particulier, tout a.v.d. est de Dedekind.

(ii) $\mathbb{Z}$ est de Dedekind.

(iii) $\mathbb{Z}[\sqrt{-3}]$ n'est pas de Dedekind, mais sa clôture intégrale $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_3]/(\zeta_3^2 + \zeta_3 + 1)$ est de Dedekind : c'est un domaine euclidien.

(iv) $\mathbb{Z}[\sqrt{-5}]$ est de Dedekind, étant la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}[\sqrt{-5}]$ (cf. 4.1). Mais $\mathbb{Z}[\sqrt{-5}]$ n'est pas principal ! S'il l'était, il aurait factorisation unique, or $2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.
Les idéaux $P_2 = (2, 1 + \sqrt{-5}) = (2, 1 - \sqrt{-5})$, $P_3 = (3, 1 + \sqrt{-5})$ et $P_3' = (3, 1 - \sqrt{-5})$ ne sont pas principaux. Nous avons les factorisations d'idéaux

$$\begin{aligned} (2) &= (2, 1 + \sqrt{-5})^2 \\ (3) &= (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) \\ (1 + \sqrt{-5}) &= (2, 1 + \sqrt{-5})(3, 1 + \sqrt{-5}). \end{aligned}$$

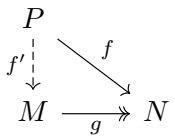
De là, nous déduisons $v_{P_2}(2) = 2$, $v_{P_2}(1 + \sqrt{-5}) = 1$ et $v_{P_3}(3) = v_{P_3}(1 + \sqrt{-5}) = 1$. De plus, dans le groupe de classes, $P_2 = P_3 = P_3'$ est d'ordre 2.

(v) Soit K un corps. L'anneau des polynômes $K[t]$ est un domaine de Dedekind. En effet, c'est un domaine principal. Les idéaux premiers sont donc ceux engendré par un polynôme irréductible f. La valuation associée à (f) est la valuation v_f de l'exercise 2.9. La valuation v_∞ de 2.9 n'apparaît pas : elle n'est pas positive sur $K[t]$, qui ne peut donc pas être contenu dans l'anneau de valuation de v_∞.
(vi) L'anneau $K[t, t^{-1}]$ des polynômes de Laurent est un domaine de Dedekind, étant le localisé de $K[t]$ en $S = \{1, t, t^2, \ldots\}$.

3. Modules sur un domaine de Dedekind

Ce chapitre contient une brève étude des modules et des formes bilinéaires sur un domaine de Dedekind. Dans tout ce chapitre, R est un domaine de Dedekind et $K = \operatorname{Frac} R$ est son corps de fractions.

3.1. Modules projectifs. Rappelons qu'un module P sur un anneau A est projectif s'il satisfait une des conditions équivalentes suivantes :
(i) Tout morphisme surjectif $M \to P$ de A-modules admet une section.
(ii) Dans toute suite exacte $0 \to K \to M \to P \to 0$ de A-modules, $M \cong K \oplus P$.
(iii) P est sommant d'un module libre, c.-à.-d. qu'il existe m et Q tel que $P \oplus Q \cong A^m$.
(iv) Le foncteur $\operatorname{Hom}(P, -)$ est exact (à droite).
(v) Étant donné une surjection $g : M \twoheadrightarrow N$, tout morphisme $f : P \to N$ se relève en un morphisme $f' : P \to M$ tel que $g \circ f' = f$.



3.2. Théorème (Classification des modules projectifs sur un domaine de Dedekind)**.** Soit R un domaine de Dedekind et M un R-module projectif finiment engendré et non nul. Alors il existe un entier $r \in \mathbb{N}_0$ et un idéal I non-nul de R tel que

$$M \cong R^{r-1} \oplus I.$$

De plus, l'entier r est le rang de M, et la classe de I dans $\operatorname{Cl}(R)$ est uniquement déterminée.

3.3. Lemme. Soient I, J deux idéaux fractionnaires non nuls du domaine de Dedekind R. Nous avons les isomorphismes de R-modules

$$I \oplus J \cong R \oplus IJ \qquad \text{et} \qquad I \otimes J \cong IJ.$$

Démonstration. En utilisant l'approximation forte (théorème 2.35), nous pouvons trouver $a, b \in R$ tels que aI^{-1} et bJ^{-1} soient des idéaux de R premiers entre-eux. En effet, il suffit de prendre $a \in R$ tel que aI^{-1} est un idéal, puis de choisir $b \in R$ pour arranger que bJ^{-1} ait valuation nulle pour tout diviseur de aI^{-1} et valuation positive ailleurs. Notons qu'alors, $a \in I$ et $b \in J$.

Puisque aI^{-1} et bJ^{-1} sont premiers entre-eux, ils sont comaximaux (localiser leur somme et utiliser la formule de 2.32). Il existe donc $c \in J^{-1}, d \in I^{-1}$ tels que $ad + bc = 1$. Mais alors l'application linéaire

$$R \oplus IJ \to I \oplus J : (x, y) \mapsto (x, y) \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ax + cy, bx + dy)$$

est un isomorphisme, d'inverse

$$I \oplus J \to R \oplus IJ : (x, y) \mapsto (x, y) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (dx - cy, -bx + ay).$$

Alternativement, nous aurions pu choisir $a, b \in K$ tels que aI et bJ soient des idéaux premiers entre-eux et déduire de la suite exacte

$$0 \to abIJ = aI \cap bJ \to aI \oplus bJ \xrightarrow{+} R \to 0$$

l'isomorphisme $aI \oplus bJ \cong R \oplus abIJ$.

La multiplication $\mu : I \otimes J \to IJ$ est un morphisme surjectif de R-modules par définition de IJ. Il ne reste qu'à vérifier qu'elle est injective. Ceci peut par exemple se vérifier localement, auquel cas μ devient une application surjective entre deux modules libres de rang 1, nécessairement injective puisque R est noethérien. De façon alternative, I, J et R sont des modules plats (car ils sont projectifs). Les applications canoniques $I \otimes J \to R \otimes J \to R \otimes R \xrightarrow{\sim} R$ sont donc toutes injectives. La multiplication μ est alors injective, étant la corestriction de la composition ci-dessus. □

Au passage, le premier isomorphisme du lemme 3.3 donne une preuve alternative que les idéaux d'un domaine de Dedekind sont des modules projectifs : $I \oplus I^{-1} \cong R \oplus R$ implique que I est sommant d'un module libre (de rang 2).

En général, on peut montrer qu'un idéal fractionnaire non nul d'un anneau intègre est projectif si et seulement si il est inversible. En conséquence, les idéaux fractionnaires inversibles sont précisément les modules projectifs de rang 1 de l'anneau.

Démonstration du théorème 3.2. Puisque M est projectif et non-nul, il existe un morphisme non trivial $f : M \to R$. L'image I de f est un idéal de R, donc est projectif et la suite exacte

$$0 \to N = \ker f \to M \xrightarrow{f} I \to 0$$

se scinde. Le noyau N est évidemment projectif, de rang strictement inférieur à M. Par induction sur le rang de M, nous déduisons que $M = \bigoplus_{i=1}^{r} I_i$ est une somme d'idéaux de R. En utilisant $r-1$ fois le lemme 3.3, il suit que $M \cong R^{r-1} \oplus \prod_{i=1}^{r} I_i$.

Finalement, r est bien le rang de M, et si $R^n \oplus I \cong R^n \oplus J$ pour un quelconque $n \in \mathbb{N}$, alors

$$R^{n+2} \cong R^n \oplus I \oplus I^{-1} \cong R^n \oplus J \oplus I^{-1} \cong R^{n+1} \oplus JI^{-1}.$$

Ceci implique que

$$R \cong \bigwedge^{n+2} R^{n+2} \cong \bigwedge^{n+2} (R^{n+1} \oplus JI^{-1}) \cong \left(\bigwedge^{n+1} R^{n+1}\right) \otimes \left(\bigwedge^{1} JI^{-1}\right) \cong JI^{-1},$$

et nous concluons que JI^{-1} est libre de rang 1, donc principal. □

3.4. Remarque. La dernière étape de la preuve du théorème 3.2 fonctionne pour les modules plats de rang 1 d'un anneau intègre A quelconque : si $M_1 \oplus \cdots \oplus M_m \cong N_1 \oplus \cdots \oplus N_m$ comme A-modules, la formule de Künneth permet de calculer

$$M_1 \otimes \cdots \otimes M_m \cong \bigwedge^{m} (M_1 \oplus \cdots \oplus M_m) \cong \bigwedge^{m} (N_1 \oplus \cdots \oplus N_m) \cong N_1 \otimes \cdots \otimes N_m,$$

car $\bigwedge^2 M_i = \bigwedge^2 N_i = 0$ grâce à la platitude et au rang. Si de plus les M_i, N_i sont des idéaux fractionnaires (toujours supposés plats), alors les produits tensoriels s'identifient au produit d'idéaux fractionnaires comme dans le lemme 3.3, et $M_1 \cdots M_m \cong N_1 \cdots N_m$. Cette dernière conclusion est vraie même sans supposer que les M_i sont plats. [4] Elle se démontre en étudiant le déterminant du changement de variables entre $M_1 \oplus \cdots \oplus M_m$ et $N_1 \oplus \cdots \oplus N_m$ dans A^m.

3.5. Définition (Anneau de Grothendieck)**.** Le *groupe de Grothendieck* d'un anneau R est le groupe des différences $K_0(R)$ du monoïde des R-modules projectifs finiment engendrés, muni de la somme directe. Supplémenté du produit tensoriel, $K_0(R)$ devient un anneau commutatif appelé l'*anneau de Grothendieck de R*, dont le neutre pour $\oplus$ est le module nul et le neutre pour $\otimes$ est le module libre de rang 1.

4. Lemma 1 dans I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. AMS (1952).

3.6. Corollaire (Anneau de Grothendieck d'un domaine de Dedekind)**.** Soit R un domaine de Dedekind. L'application

$$\psi = \operatorname{rank} \oplus \operatorname{cl} : K_0(R) \xrightarrow{\sim} \mathbb{Z} \oplus \operatorname{Cl}(R) : M \mapsto (r, I), \quad \text{avec } r,\ I \text{ extraits du théorème 3.2}$$

est un isomorphisme depuis l'anneau de Grothendieck $K_0(R)$ de R vers l'anneau ayant pour groupe additif le groupe abélien $\mathbb{Z} \oplus \operatorname{Cl}(R)$ et pour multiplication la formule $(r, I) \cdot (s, J) = (rs, I^s J^r)$.

De plus, le monoïde des modules projectifs finiment engendrés est simplifiable, autrement dit, il s'injecte dans $K_0(R)$.

Démonstration. Pour s'assurer que ψ est un morphisme de groupes, il suffit de vérifier que ψ est additive sur les R-modules. Soit donc $M = R^{r-1} \oplus I$, $N = R^{s-1} \oplus J$ deux R-modules projectifs non nuls. Par le lemme 3.3, nous avons bien

$$\psi(M \oplus N) = \psi(R^{r+s-2} \oplus I \oplus J) = \psi(R^{r+s-1} \oplus IJ) = (r + s, IJ) = \psi(M) + \psi(N).$$

La surjectivité de ψ est évidente. Son injectivité (sur le monoïde engendré par les modules projectifs, et donc sur $K_0(R)$) est la conséquence de l'unicité dans le théorème 3.2 et du fait que deux idéaux de même classe sont isomorphes comme R-modules. En conséquence, nous notons que le monoïde des modules projectifs finiment engendrés est simplifiable.

Il reste à vérifier que ψ préserve le produit, ce qui suit du calcul :

$$\psi((R^{r-1} \oplus I) \otimes (R^{s-1} \oplus J)) = \psi(R^{(r-1)(s-1)} \oplus I^{s-1} \oplus J^{r-1} \oplus IJ) = (rs, I^s J^r) = \psi(M) \cdot \psi(N). \ \square$$

Une conséquence majeure du théorème 3.2 est le bien-fondé de la classe d'un module projectif.

3.7. Définition (Classe d'un module)**.** Soit M un module projectif finiment engendré sur R. Les deux composantes de l'image de M par le morphisme ψ du corollaire 3.6 sont le *rang* $\operatorname{rank}(M) \in \mathbb{N}$ et la *classe (de Steinitz)* $\operatorname{cl}(M) \in \operatorname{Cl}(R)$ *de* M. Ces deux invariants sont additifs, et comme nous l'avons vu, ensemble déterminent M à isomorphisme près.

3.8. Corollaire (Groupe de classes comme quotient additif de K_0)**.** La classe induit un isomorphisme $\operatorname{cl} : K_0(R)/L \xrightarrow{\sim} \operatorname{Cl}(R)$ de groupes abéliens, où L désigne le sous-groupe de $K_0(R)$ engendré par les modules libres.

3.9. Corollaire (Groupe de classes comme sous-groupe multiplicatif de K_0)**.** Le groupe multiplicatif de $K_0(R)$ s'identifie à $\{\pm 1\} \times \operatorname{Cl}(R)$ via l'application ψ du corollaire 3.6. En particulier, $\operatorname{Cl}(R)$ est un sous-groupe d'indice 2 de $K_0(R)^\times$ via l'inclusion $I \mapsto I = \psi^{-1}(1, I)$.

Démonstration. Pour que $(m, I) \in \mathbb{Z} \oplus \operatorname{Cl}(R)$ soit inversible, il faut et suffit que $m \in \mathbb{Z}^\times = \{\pm 1\}$. Son inverse est alors $(\pm 1, I^{-1})$. $\square$

3.10. Sous-modules de K^n. Pour le reste de ce chapitre, soient V un espace vectoriel sur K de dimension $d < \infty$, et M, N deux sous-R-modules finiment engendrés de V qui sont *pleins*, c.-à.-d. que $KM, KN = V$. Nous souhaitons déterminer quel type d'isomorphisme de R-modules peut apparaître comme quotients de M.

Par hypothèse M et N sont sans torsion, de rang d. Nous allons voir dans la section suivante qu'alors M et N sont projectifs, et donc leur type d'isomorphisme est donné par le théorème 3.2. Dans la présente section, nous nous concentrons sur la position relative de M et N dans V et sur le quotient $(M + N)/N$. Puisqu'il est de rang nul, un tel quotient est de torsion.

3.11. Théorème (Classification des modules de torsion finiment engendrés sur un domaine de Dedekind)**.** Soit R un domaine de Dedekind, M un R-module projectif de rang s, et N un sous-module de M de même rang. Il existe une chaîne $J_1 \supseteq \cdots \supseteq J_s \supsetneq 0$ d'idéaux de R, unique parmi les chaînes de longueur s d'idéaux non nuls, telle que le quotient M/N est isomorphe au R-module $R/J_1 \oplus \cdots \oplus R/J_s$.

En conséquence, tout R-module de torsion T engendré par s éléments est isomorphe à $R/J_1 \oplus \cdots \oplus R/J_s$, pour une chaine $J_1 \supseteq \cdots \supseteq J_s \supsetneq 0$ d'idéaux de R uniquement déterminée.

3.12. Définition (Facteurs invariants)**.** Les idéaux $J_1 \supseteq \cdots \supseteq J_s \supsetneq 0$ du théorème 3.11 sont appelés les *facteurs invariants de* M/N.

Démonstration. Puisque M et N sont de même rang s, il existe un élément non nul $d \in R$ tel que $dM \subseteq N$ (autrement dit, M/N est de d-torsion). Soit $\mathcal{S}$ l'ensemble des idéaux maximaux de R qui contiennent d, et S le complément de l'union des éléments de $\mathcal{S}$. L'anneau localisé $S^{-1}R$ a pour idéaux maximaux les (extensions des) éléments de l'ensemble fini $\mathcal{S}$. Par le corollaire 2.34, $S^{-1}R$ est principal. Du coup, le théorème de classification pour les anneaux principaux établit que le module $S^{-1}(M/N) = S^{-1}M/S^{-1}N$ est somme directe

$$S^{-1}(M/N) \cong S^{-1}(R/J_1) \oplus \cdots \oplus S^{-1}(R/J_s) \cong S^{-1}\left(R/J_1 \oplus \cdots \oplus R/J_s\right)$$

pour les idéaux $J_1 \supseteq \cdots \supseteq J_s \supseteq (d)$ de R qui sont les préimages des facteurs invariants de $S^{-1}R$. Nous allons montrer que $M/N \cong R/J_1 \oplus \cdots \oplus R/J_s$ comme R-modules.

À cette fin, observons d'abord que $S^{-1}(R/J_i) \cong R/J_i$ comme R-algèbres. En effet, les idéaux maximaux de R/J_i descendent d'idéaux maximaux de R qui contiennent (d), c.-à.-d. qui appartiennent à $\mathcal{S}$. Dès lors, tout élément de l'image de S dans R/J_i n'est dans aucun idéal maximal de R/J_i, donc est inversible, et R/J_i est alors la localisée d'elle-même en S. Du coup, comme R-modules,

$$S^{-1}(M/N) \cong R/J_1 \oplus \cdots \oplus R/J_s.$$

Vérifions maintenant que l'application canonique $M/N \to S^{-1}(M/N)$ est aussi un isomorphisme de R-modules. Ceci peut se vérifier localement (comme aurait pu l'être l'étape précédente, d'ailleurs). Si $P \in \mathcal{S}$, alors l'isomorphisme est clair, puisque localiser en S puis en P revient à localiser directement en P. Si par contre P est un idéal maximal ne contenant pas d, nous avons

$$(M/N)_P = 0 = \left(R/J_1 \oplus \cdots \oplus R/J_s\right)_P,$$

car la multiplication de ce module par $d \in R_P$ est à la fois inversible et nulle.

Il reste à montrer que cette décomposition est unique. Si ce n'est pas le cas, la différence entre deux décompositions s'observera encore après localisation en un idéal maximal P. Mais puisque R_P est principal, ses facteurs invariants sont uniques et il ne peut y avoir de différence.

Finalement, si T est un module de torsion engendré par s éléments, alors T est le quotient du module libre R^s par un sous-module N. Puisque T est de rang 0, N est forcément de rang s, et la dernière assertion découle immédiatement de la première. □

3.13. Remarque. En utilisant la surjectivité de $\mathrm{SL}_s(R) \twoheadrightarrow \mathrm{SL}_s(R/I)$ (une forme de l'*approximation forte pour* SL_s, qui n'est pas valable pour GL_s), on peut montrer qu'il existe un automorphisme de $M = R^s$ identifiant N au sous-module $J_1 \oplus \cdots \oplus J_s$ de R^s, induisant ainsi l'isomorphisme du théorème 3.11. Qu'en est-il si M n'est pas libre ?

3.14. Définition (Indice modulaire)**.** *L'indice modulaire* $[M : N]$ *de* N *dans* M est l'idéal fractionnaire de R engendré par $\langle \det \alpha \mid \alpha \in \mathrm{GL}(V), \alpha(M) \subseteq N \rangle$.

Supposons un instant que M et N soient des sous-R-modules libres de V (ou plus généralement, que $M \cong N$ comme R-modules). Alors pour tout $\alpha \in \mathrm{GL}(V)$ tel que $\alpha(M) \subseteq N$, il existe $\beta \in \mathrm{GL}(V) \cap \mathrm{End}_R(N)$ tel que $\alpha(M) = \beta(N)$. Ayant posé $\alpha' = \beta^{-1} \circ \alpha$, il suit que $\alpha'(M) = N$ et $\det(\alpha') = \det(\beta) \cdot \det(\alpha)$ divise $\det(\alpha)$. De plus, si $\alpha'' \in \mathrm{GL}(V)$ est tel que $\alpha''(M) = N$, alors $\alpha'' \circ \alpha'^{-1} \in \mathrm{Aut}_R(M)$, d'où $\det(\alpha') \in \det(\alpha'') \cdot R^\times$. En conséquence, dans ce cas, l'idéal fractionnaire $[M, N]$ est principal, engendré par $\det(\alpha'')$ pour n'importe quel $\alpha'' \in \mathrm{GL}(V)$ tel que $\alpha''(M) = N$. Ceci prouve le premier point de la proposition suivante.

3.15. Proposition. Soient M, N, L trois sous-R-modules pleins d'un espace V de dimension d sur K. L'indice modulaire jouit des propriétés suivantes :

(i) Si M, N sont libres, alors $[M : N]$ est principal, engendré par $\det \alpha$ pour $\alpha \in \mathrm{GL}(V)$ vérifiant $\alpha(M) = N$.
(ii) L'indice modulaire commute avec la localisation : $[M : N]_P = [M_P : N_P]$ pour tout $P \in \mathcal{P}$.
(iii) $[M : N][N : L] = [M : L]$ et $[M : N]^{-1} = [N : M]$.
(iv) Si $N \subseteq M$ et $[M : N] = 1$, alors $M = N$.

(v) Si I est un idéal fractionnaire inversible de R, alors $[IM, IN] = [M, N]$.
(vi) Si I, J sont deux idéaux fractionnaires inversibles de R, alors $[I : J] = (J : I) = JI^{-1}$.
(vii) Si $N \subseteq M$, alors $[M : N]$ est le produit $J_1 \cdots J_d$ des facteurs invariants du théorème 3.11.
En particulier, c'est un idéal de R.
(viii) La classe de $[M : N]$ dans $\mathrm{Cl}(R)$ est $\mathrm{cl}(N)cl(M)^{-1}$.
En conséquence, $M \cong N$ comme R-modules si et seulement si $[M, N]$ est principal. Aussi, les classes de $\mathrm{Hom}(M, N)$ et $[M : N]^d$ dans $\mathrm{Cl}(R)$ coincident.

DÉMONSTRATION. (i) Voir la discussion précédant l'énoncé.
(ii) L'inclusion $[M : N] \subseteq [M_P : N_P]$ est évidente. Montrons que $[M_P : N_P] \subseteq [M : N]_P$. Si $m_1, \ldots, m_k$ engendrent M sur R, et que $\det(\alpha)$ est un des générateurs de $[M_P : N_P]$ donnés en 3.14, alors par définition $\alpha(m_i) = \frac{n_i}{s_i}$ pour certains $n_i \in N$, $s_i \notin P$. Ceci implique que l'application $s_1 \cdots s_k \cdot \alpha \in \mathrm{GL}(V)$ satisfait $(s_1 \cdots s_k \cdot \alpha)(M) \subseteq N$, et donc que $(s_1 \cdots s_k)^d \det(\alpha) \in [M : N]$.
(iii) La deuxième égalité découle de la première et du fait que $[M : M] = R$. La première égalité suit de la multiplicativité du déterminant quand les modules en question sont libres, et en général, est vérifiée localement en vertu du point (ii).
(iv) Clair localement, donc globalement en vertu du point (ii).
(v) Idem.
(vi) Par définition.
(vii) Pour tout $P \in \mathcal{P}$, la forme normale sur R_P de $\alpha \in \mathrm{GL}(V)$ tel que $\alpha(M_P) = N_P$ est diagonale, avec pour entrées les générateurs locaux de $J_1, \ldots, J_s$. Le déterminant de α engendre alors clairement l'idéal $(J_1 \cdots J_s)R_P$ de R_P. Les points (i) et (ii) permettent de conclure.
(viii) Quitte à multiplier N par un scalaire $r \in R$ bien choisi, nous pouvons supposer que $N \subseteq M$. Le théorème 3.11 montre que le R-module $T = R/J_1 \oplus \cdots \oplus R/J_s$ possède les deux résolutions projectives suivantes.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & J_1 \oplus \cdots \oplus J_s & \longrightarrow & R^s & \longrightarrow & T & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & T & \longrightarrow & 0 \end{array}$$

Le lemme de Schanuel affirme alors que $N \oplus R^s \cong M \oplus (J_1 \oplus \cdots \oplus J_s)$, autrement dit que $\mathrm{cl}(N)\,\mathrm{cl}(M)^{-1} = \mathrm{cl}(J_1 \oplus \cdots \oplus J_s) = \mathrm{cl}(J_1 \cdots J_s)$. L'énoncé suit donc du point (vii). □

3.16. Exercice. Montrer que les conditions imposées sur M, N au points (i) et (iv) sont nécessaires.

3.17. Théorème (Structure des modules finiment engendrés sur un domaine de Dedekind)**.** Soit R un domaine de Dedekind. Tout module M finiment engendré sur R se décompose

$$M \cong T \oplus M/T = (R/J_1 \oplus \cdots \oplus R/J_s) \oplus (I_1 \oplus \cdots \oplus I_r),$$

en somme directe du sous-module T de torsion de M (lui-même somme directe de quotients de R par des idéaux $J_1 \supseteq \cdots \supseteq J_s \supsetneq 0$) et du module quotient projectif M/T (lui-même somme directe de $r = \mathrm{rank}\, M$ idéaux inversibles de R).

Le module M/T est donc le plus grand quotient projectif de M (car tout module projectif est sans torsion), et la *classe* $\mathrm{cl}(M)$ *de* M se définit comme la classe de M/T. Vu le théorème 3.17, $\mathrm{cl}(M) = \mathrm{cl}(M/T) = I_1 \cdots I_r$ dans la notation de l'énoncé. Nous appellerons encore *facteurs invariants de* M les facteurs invariants de T. Nous appelerons *norme de* M l'idéal $\mathrm{N}_R(M) = J_1 \cdots J_s$ de R, et *coclasse de* M la classe $\mathrm{cl}(J_1 \cdots J_s)$ de sa norme.

DÉMONSTRATION. Nous allons montrer que tout R-module N finiment engendré et sans torsion est projectif, somme directe de $r = \mathrm{rank}\, N$ idéaux inversibles de R. Comme le quotient M/T est clairement sans torsion et de même rang que M, ceci impliquera que $M \cong T \oplus M/T \cong$

$T \oplus (I_1 \oplus \cdots \oplus I_r)$. L'énoncé s'ensuit après application du théorème 3.11 à T. Nous raisonnons par récurrence sur le rang r de N.

Soit $x \in N \setminus \{0\}$ et posons

$$I_1 = \{y \in N \mid \text{ il existe } a \in R \text{ tel que } ay \in Rx\}.$$

I_1 est un sous-module de N de rang 1, et N/I_1 est sans torsion, de rang $r-1$ par construction. Par l'hypothèse de récurrence, $N/I_1 = I_2 \oplus \cdots \oplus I_r$ est projectif. En conséquence, $N \cong I_1 \oplus (I_2 \oplus \cdots \oplus I_r)$ et il ne reste qu'à montrer que I_1 est isomorphe à un idéal de R. Puisque N est finiment engendré (et R est noethérien), il en est de même pour I_1. Prenons $y_1, \ldots, y_m$ engendrant I_1, et $a_1, \ldots, a_m \in R$ tels que $a_i y_i \in Rx$. Le module $(a_1 \cdots a_m)I_1 \cong I_1$ est alors contenu dans le module Rx, et est donc isomorphe à un sous-module non nul de R. (Nous avions vu précédemment que ceci impliquait que I_1 est projectif.) □

3.18. Modules duaux. Le dual du R-module $M = T \oplus R^{r-1} \oplus I$ (dans la décomposition du théorème 3.17) s'identifie à $R^{r-1} \oplus I^{-1} = R^{2r} \ominus M/T$. En terme de l'invariant ψ du corollaire 3.6, nous avons $\psi(\mathrm{Hom}(M, R)) = (r, I^{-1})$ quand $\psi(M) = (r, I)$.

En effet, $\mathrm{Hom}(-, R)$ commute avec les sommes directes, $\mathrm{Hom}(T, R) = 0$ car R est intègre, et l'appariement $\mathrm{Hom}(I, R) \otimes I \xrightarrow{\sim} R$ (dont l'injectivité est garantie quand I est un idéal fractionnaire et la surjectivité est équivalente à l'invertibilité de I) donne lieu à l'isomorphisme

$$\mathrm{Hom}(I, R) \cong \mathrm{Hom}(I, R) \otimes I \otimes I^{-1} \cong I^{-1}.$$

Le même genre d'argument montre que pour deux idéaux fractionnaires inversibles I, J, le R-module $\mathrm{Hom}(I, J)$ s'identifie au module $JI^{-1} = (J : I)$ de la section 2.14.

3.19. Formes bilinéaires et duaux. Donnons-nous à présent une forme K-bilinéaire symétrique non dégénérée b sur V. Pour M un sous-R-module plein de V, le *module b-dual à M dans V* est le R-module

$$M^b = \{x \in V \mid b(x, M) \subseteq R\}.$$

3.20. Proposition. Soient M, N deux modules pleins de V. Le b-dual jouit des propriétés suivantes :

(i) Si $N \subseteq M$, alors $M^b \subseteq N^b$.
(ii) Si M est libre de base $v_1, \ldots, v_d$, alors M^b est le R-module libre engendré par la base duale $v_1^b, \ldots, v_d^b$ (définie par $b(v_i, v_j^b) = \delta_{ij}$).
(iii) Pour tout $P \in \mathcal{P}$, $(M^b)_P = (M_P)^b$ (où il est entendu que le deuxième b-dual est pris comme R_P-module).
(iv) $M^b = \bigcap_{P \in \mathcal{P}} (M_P)^b$.
(v) $(M^b)^b = M$.
(vi) $[M^b : N^b] = [N : M]$.

3.21. Exercice. Démontrer la proposition 3.20.

3.22. Définition. Le *discriminant de M par rapport à b* est l'idéal fractionnaire $\Delta_b(M) = [M^b : M]$.

3.23. Proposition. Soient M, N deux modules pleins de V. Le discriminant par rapport à b jouit des propriétés suivantes :

(i) $\Delta_b(N) = \Delta_b(M)[M : N]^2$. En conséquence, si $N \subseteq M$, alors $\Delta_b(M)$ divise $\Delta_b(N)$ avec égalité si et seulement si $M = N$.
(ii) Pour tout $P \in \mathcal{P}$, $\Delta_b(M_P) = \Delta_b(M)_P$.
(iii) Si M est libre de base $v_1, \ldots, v_d$, alors $\Delta_b(M)$ est l'idéal fractionnaire engendré par $\det(b(v_i, v_i)_{i,j})$.

Démonstration. Les trois point résultent immédiatement de la proposition 3.20. □

L'usage principal du dual et du discriminant d'un R-module se fait dans la situation suivante : S est la clôture intégrale d'un domaine de Dedekind R dans une extension L de $K = \mathrm{Frac}(R)$, vu comme R-module et muni de la forme trace $\mathrm{tr}_{L/K}$ de L sur K. Cette trame nous mène au chapitre suivant.

4. Extensions de domaines de Dedekind

Le but de ce chapitre est d'étudier les extensions d'anneaux d'entiers des corps de nombres. Nous allons tirer parti du formalisme de Dedekind. La première étape est donc de montrer (enfin !) que l'anneau $\mathcal{O}_{\mathbb{K}}$ des entiers du corps de nombres $\mathbb{K}$ est un domaine de Dedekind.

Dans tout ce chapitre, sauf indication contraire, R est un domaine de Dedekind, K son corps de fractions, L une extension finie séparable de K, et S la clôture intégrale de R dans L.

4.1. Proposition. La clôture intégrale S d'un domaine de Dedekind R dans une extension finie séparable L de $K = \mathrm{Frac}(R)$ est un domaine de Dedekind. En particulier, les anneaux d'entiers des corps globaux sont de Dedekind.

Démonstration. Il est clair que S est intégralement clos. Nous allons vérifier les autres conditions du point (i) du théorème 2.19.

Tout élément $x \in L$ étant algébrique sur K, il existe $r \in R$ tel que xr est intégral sur R, c.-à.-d. appartient à S. Du coup, S vu comme R-module est plein dans L, et L est le corps de fractions de S. Notons $d = \deg_K L$. Comme L/K est séparable, la forme trace $\mathrm{tr} : (x, y) \mapsto \mathrm{tr}_{L/K}(xy)$ est non dégénérée. Nous pouvons donc tirer parti des résultats de la section 3.19.

Soient $v_1, \ldots, v_d$ une base de L contenue dans S, et notons N le R-module qu'elle engendre. Par la proposition 3.20, N^{tr} est un module libre qui contient S^{tr}. Puisque S est intégral sur R, les traces des éléments de S appartiennent à R. En conséquence, nous avons la chaîne de R-modules pleins

$$N \subseteq S \subseteq S^{\mathrm{tr}} \subseteq N^{\mathrm{tr}}.$$

Ceci implique immédiatement que tout idéal de S est finiment engendré comme R-module (puisque N^{tr} l'est et R est noethérien). En particulier, tout idéal de S est finiment engendré comme S-module, et S est noethérien.

Il reste à vérifier que tout idéal premier Q propre et non nul de S est maximal. Soit P l'idéal premier $R \cap Q$ de R. Il est évidemment propre, et si $x \in Q$ a pour équation intégrale minimale

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

alors a_0 est non nul et appartient à $R \cap Q$. Donc P est maximal et R/P est un corps. Mais alors S/Q est une algèbre intègre de dimension finie sur le corps R/P. C'est donc un corps, et Q est un idéal maximal. □

4.2. Remarque. La conclusion de la proposition 4.1 reste valable sans l'hypothèse de séparabilité faite sur L. Dans ce cas, S n'est plus nécessairement finiment engendré comme R-module, et on utilise le théorème de Krull–Akizuki pour démontrer que S est noethérien malgré tout.

La proposition suivante traite de l'extension et de la contraction des idéaux de R et S.

4.3. Proposition. Tout idéal maximal de S se contracte en un idéal maximal de R. Tout idéal maximal de R est contenu dans un idéal maximal de S.

L'application d'extension $e : \mathcal{I}_R \to \mathcal{I}_S : I \to IS$ est un morphisme injectif, ayant pour inverse à gauche l'application de contraction $c : \mathcal{I}_S \to \mathcal{I}_R : J \mapsto J \cap K$. L'application de contraction est surjective (mais n'est pas un morphisme de groupes !).

Démonstration. La première assertion découle de la dernière étape de la preuve de la proposition 4.1. La deuxième assertion est un cas particulier de la troisième, puisqu'un idéal I de R est contenu dans son extension IS.

Pour les deux dernières assertions, nous montrons directement que la contraction est inverse à gauche de l'application d'extension. Si par malheur $IS \cap K \supsetneq I$, alors en multipliant par I^{-1}

nous déduisons que $I^{-1}(IS \cap K) \supsetneq R$. Ceci est impossible, car $I^{-1}(IS \cap K) = (I^{-1}IS) \cap K = S \cap K = R$. □

4.4. Corollaire. Si tous les quotients propres de R sont finis, il en est de même pour S.

Démonstration. Tout quotient propre S/J de S est un module finiment engendré sur l'anneau fini $R/(J \cap R)$. □

4.5. Corollaire. Soit K un corps et L une extension finie séparable de K. Toute valuation discrète v sur K s'étend à une valuation discrète de L.

Démonstration. L'anneau de valuation R de v est un a.v.d. par définition ; soit P son idéal de valuation. La proposition 4.1 s'applique à la clôture intégrale S de R dans L : S est un anneau de Dedekind. La proposition 4.3 montre alors que la valuation Q-adique pour Q maximal contenant P, normalisée par l'exposant $v_Q(P)$ de Q dans la factorisation de PS, étend v. □

4.6. Remarque. Si de plus K est complet pour la norme induite par v, alors l'extension de v à L est unique. En effet, deux normes sur L qui coincident sur K doivent être équivalentes (c.-à.-.d. induisent la même topologie), par comparaison avec la norme L^∞ ou avec la topologie produit. Mais alors les deux valuations ont le même idéal de valuation, puisque c'est l'ensemble $\{x \in L \mid x^n \to 0 \text{ quand } n \to \infty\}$.

4.7. Définition. Soit S la clôture intégrale d'un domaines de Dedekind R dans une extension finie séparable L de $K = \mathrm{Frac}(R)$. Soit P un idéal premier de R. Nous disons qu'un idéal premier Q de S *est au-dessus de* P, ou que P *est sous* Q, lorsque $P = Q \cap R$ est la contraction de Q. En vertu de la proposition 4.3, les idéaux maximaux de S au-dessus de P sont précisément les facteurs premiers de l'extension PS de P à S ; ils sont donc en nombre fini.

4.8. Norme d'un idéal. Soit J un idéal fractionnaire de S. La *norme (idéale) de* J est l'idéal fractionnaire $\mathrm{N}_{L/K}(J) = [S : J]$ de R (calculé en voyant S comme un sous-R-module plein de L).

Si l'idéal $J = aS$ est principal, alors $\mathrm{N}_{L/K}(aS)$ est l'idéal principal $\mathrm{N}_{L/K}(a)R$ de R, engendré par la norme usuelle de a. En effet, $\mathrm{N}_{L/K}(a)$ est précisément le déterminant de la transformation $x \mapsto ax$ envoyant S sur aS.

4.9. Remarque. Lorsque $R = \mathbb{Z}$, $L = \mathbb{L}$ est un corps de nombres et $S = \mathcal{O}_\mathbb{L}$, il s'avère que la norme $\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(J) = [S : J]$ de $J \lhd S$ est l'idéal de $\mathbb{Z}$ engendré par la cardinalité de l'anneau fini S/J. En fait, l'indice $[M : N]$ de deux sous-$\mathbb{Z}$-modules de V est l'idéal engendré par l'indice de M dans N (en tant que groupes abéliens). En effet, par la proposition 3.15 (vii), $[M : N]$ est le produit $J_1 \cdots J_s$ des facteurs invariants de N dans M. Il est donc engendré par la cardinalité de l'anneau $\mathbb{Z}/(J_1 \cdots J_s)$, qui coincide avec celle du $\mathbb{Z}$-module $S/J \cong \mathbb{Z}/J_1 \oplus \ \cdots \oplus \mathbb{Z}/J_s$.

4.10. Proposition. La norme idéale est un morphisme de groupes $\mathrm{N}_{L/K} : \mathcal{I}_S \to \mathcal{I}_R$, et dans une tour d'extensions, $\mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$. La composition $\mathcal{I}_R \xrightarrow{e} \mathcal{I}_S \xrightarrow{\mathrm{N}} \mathcal{I}_R$ est l'application $I \mapsto I^{\deg_K(L)}$.

Démonstration. Pour montrer que la norme idéale est multiplicative, il suffit de montrer que pour deux idéaux I, J de S, nous avons $[I : IJ] = [S : J]$. Il en suivra que

$$\mathrm{N}_{L/K}(IJ) = [S : IJ] = [S : I][I : IJ] = [S : I][S : J] = \mathrm{N}_{L/K}(I) \cdot \mathrm{N}_{L/K}(J).$$

La même égalité pour les idéaux fractionnaires se déduit en multipliant IJ par un élément $s \in S$ bien choisi, modifiant les deux membres d'un facteur $\mathrm{N}_{L/K}(s)$.

Le point (vii) de la proposition 3.15 montre qu'en cas d'inclusion, l'indice modulaire ne dépend que du module quotient. Or, en les comparant localement (par exemple), nous voyons que I/IJ et S/J sont isomorphes comme S-modules, a fortiori comme R-modules.

La composition des normes dans une tour suit par exemple de l'unicité des facteurs invariants. L'assertion concernant $\mathrm{N}_{L/K} \circ e$ se vérifie facilement localement. □

4.11. Définition (Différent et discriminant)**.** Le *différent de S sur R* est l'idéal $\delta_{S/R}$ de S qui est inverse du dual S^{tr} de S pour la forme trace de L/K.

$$\delta_{S/R} = (S^{\mathrm{tr}})^{-1}$$

Le *discriminant de S sur R* est le discriminant $\Delta_{S/R}$ de la forme trace de L/K.

$$\Delta_{S/R} = [S^{\mathrm{tr}} : S]$$

C'est un idéal de R, et si S est intégralement clos, il coincide avec la norme idéale du différent $\delta_{S/R}$:

$$\mathrm{N}_{L/K}(\delta_{S/R}) = [S : (S^{\mathrm{tr}})^{-1}] = [S : S^{\mathrm{tr}}]^{-1} = [S^{\mathrm{tr}} : S].$$

4.12. Théorème (Différent et discriminant d'un anneau monogène)**.** Soient R un domaine de Dedekind, et L une extension finie séparable de $K = \mathrm{Frac}(R)$. Soit α un élément de la clôture intégrale S de R dans L tel que $R[\alpha]$ est plein, et notons g le polynôme minimal de α sur K, g' son dérivé. Alors :

(i) $(R[\alpha])^{\mathrm{tr}_{L/K}} = g'(\alpha)^{-1}R[\alpha]$
(ii) $\Delta_{\mathrm{tr}_{L/K}}(R[\alpha]/R) = \mathrm{N}_{L/K}(g'(\alpha))R = \mathrm{Disc}(g)R$
(iii) $S = R[\alpha] \iff \delta_{S/R} = g'(\alpha)S$

Démonstration. Remarquons d'emblée que si $\alpha = \alpha_1, \ldots, \alpha_n$ dénotent les racines de g dans une clôture algébrique de K, nous déduisons de la règle de Leibniz les identités

$$g'(\alpha) = \prod_{i=2}^{n}(\alpha - \alpha_i) \quad \text{et} \quad \mathrm{N}_{L/K}(g'(\alpha)) = \prod_{1\le i\neq j\le n}(\alpha_i - \alpha_j) = \mathrm{Disc}(g).$$

Notons $1 = a_n, a_{n-1}, \ldots, a_1, a_0$ les coefficients de g. Nous verrons dans le lemme suivant que les coefficients $b_{n-1}, \ldots, b_1, b_0 \in L$ du polynôme $g(X)/(X-\alpha)$ forment une base de $(g'(\alpha)^{-1}R[\alpha])^{\mathrm{tr}}$. Or, le module engendré par $b_{n-1}, \ldots, b_1, b_0$ est en fait $R[\alpha]$. En effet, par définition des b_i,

$$\alpha b_i = b_{i-1} - a_i \quad \text{pour } i = n-1, \ldots, 0 \text{ (entendu que } \alpha b_0 = -a_0).$$

Puisque $b_{n-1} = 1$, il en suit que la matrice de changement de base entre $1, \alpha, \ldots, \alpha^{n-1}$ et $b_{n-1}, \ldots, b_1, b_0$ est strictement triangulaire supérieure à coefficients dans R. En somme, $(g'(\alpha)^{-1}R[\alpha])^{\mathrm{tr}} = R[\alpha]$, ce qui prouve le point (i).

Le point (ii) découle du point (i) et de l'égalité $[g'(\alpha)^{-1}R[\alpha] : R[\alpha]] = \mathrm{N}_{L/K}(g'(\alpha))$.

Finalement, (iii) est une conséquence formelle de (i). D'une part, $S = R[\alpha]$ implique $\delta_{S/R} = g'(\alpha)S$ par (i). D'autre part, si $\delta_{S/R} = g'(\alpha)S$, alors par (i),

$$(R[\alpha])^{\mathrm{tr}} \supseteq S^{\mathrm{tr}} = g'(\alpha)^{-1}S \supseteq g'(\alpha)^{-1}R[\alpha] = (R[\alpha])^{\mathrm{tr}}.$$

Donc toutes les inclusions sont des égalités et $S = R[\alpha]$. □

Nous avons fait usage préemptif du lemme suivant, qui décrit la base duale à la base canonique d'une extension monogène.

4.13. Lemme (Euler ?)**.** Soit L une extension finie séparable d'un corps K, engendrée par un élément α de polynôme minimal g. Soient $b_{n-1}, \ldots, b_1, b_0 \in L$ les coefficients du polynôme $g(X)/(X-\alpha)$. Pour la forme $\mathrm{tr}_{L/K}$, la base $1, \alpha, \ldots, \alpha^{n-1}$ de L est duale à

$$b_0 g'(\alpha)^{-1}, b_1 g'(\alpha)^{-1}, \ldots, b_{n-1}g'(\alpha)^{-1}.$$

En particulier, puisque $b_{n-1} = 1$:

$$\mathrm{tr}_{L/K}\left(\alpha^i g'(\alpha)^{-1}\right) = \begin{cases} 0 & \text{si } i = 0, \ldots, n-2 \\ 1 & \text{si } i = n-1. \end{cases}$$

Démonstration. Pour chaque $j = 1, \ldots, n$, nous démontrons l'identité

$$\mathrm{tr}\left(\frac{g(X)}{(X-\alpha)}\frac{\alpha^j}{g'(\alpha)}\right) = \sum_{i=1}^{n}\frac{g(X)}{(X-\alpha_i)}\frac{\alpha_i^j}{g'(\alpha_i)} = X^j,$$

dans laquelle la trace est étendue aux anneaux de polynômes $L[X] \to K[X]$ en l'appliquant aux coefficients. Les deux membres de l'identité sont des polynômes de degré au plus $n-1$, et prennent les mêmes valeurs en $\alpha_1, \dots, \alpha_n$. (À vrai dire, le membre du milieu est l'interpolant de Lagrange des points (α_i, α_i^j).) Ils coincident donc ! L'énoncé du lemme est obtenu en comparant les coefficients des membres de l'identité. □

4.14. Corollaire. Soit $x \in L$ un élément intégral sur R et g son polynôme minimal. La clôture intégrale S de R dans L satisfait

$$R[x] \subseteq S \subseteq g'(x)^{-1} R[x].$$

4.15. Corollaire (Module des différentielles d'une extension de domaines de Dedekind)**.** Soient R un domaine de Dedekind, et L une extension finie séparable de $K = \mathrm{Frac}(R)$. Soit S la clôture intégrale de R dans L. Le différent $\delta_{S/R}$ est l'annulateur du module $\Omega_{S/R}$ des différentielles de S sur R.

Esquisse de démonstration. La construction du modules des différentielles de S/R et de l'annulateur commutent avec la localisation et la complétion. Nous pouvons donc supposer que R est local et complet. Alors, $S = R[\alpha]$ est monogène (cf. chapitre 6). D'une part le théorème 4.12 s'applique : $\delta_{S/R} = g'(\alpha)S$ pour g le polynôme minimal de α sur R. D'autre part, le module $\Omega_{S/R}$ des différentielles est cyclique, engendré par $d\alpha$, qui a pour annulateur précisément $g'(\alpha)S$ (car $g'(\alpha)d\alpha = dg(\alpha) = 0$). □

4.16. Lemme. Soient R un domaine de Dedekind, et L une extension finie séparable de $K = \mathrm{Frac}(R)$. Soit S la clôture intégrale de R dans L. Notons $\sigma_1, \dots, \sigma_d$ les différents plongements de L dans une clôture algébrique de K. Le discriminant $\Delta_{S/R}$ coincide avec l'idéal de R engendré par

$$\Delta_{S/R} = \langle \det(\sigma_i(b_j))_{ij}^2 \mid b_1, \dots, b_d \in S \rangle.$$

Si S est libre comme R-module, de base $b_1, \dots, b_d$, alors

$$\Delta_{S/R} = \det(\sigma_i(b_j))_{ij}^2 \cdot R.$$

Démonstration. La premiere assertion découle de la seconde, appliquée localement. Nous démontrons donc la seconde assertion. Quand S est libre de base $b_1, \dots, b_d$, S^{tr} est libre de base duale $b_1^{\mathrm{tr}}, \dots, b_d^{\mathrm{tr}}$. Dans ce cas, la transformation linéaire $b_i \to b_i^{\mathrm{tr}}$ a pour matrice $(\mathrm{tr}(b_i b_j)_{ij})$ (cf. 3.23 (iii)). Or

$$\mathrm{tr}(b_i b_j)_{ij} = \left(\sum_{k=1}^{d} \sigma_k(b_i)\sigma_k(b_i) \right)_{ij} = ((\sigma_k(b_i))_{ki})^{\top} (\sigma_k(b_j))_{kj}.$$

Donc $\Delta_{S/R} = \det(\mathrm{tr}(b_i b_j)_{ij}) \cdot R = \det(\sigma_k(b_i))_{ki}^2 \cdot R$. □

4.17. Proposition (Différent et discriminant d'une tour)**.** Soit $M/L/K$ une tour d'extensions finies séparables de K et T, S, R les clôtures intégrales de R correspondantes.

(i) $\delta_{T/R} = \delta_{T/S}\delta_{S/R}$ comme idéaux de T.

(ii) $\Delta_{T/R} = \mathrm{N}_{T/S}(\Delta_{S/R}) \cdot \Delta_{S/R}^{\deg_L M}$ comme idéaux de R.

Démonstration. Pour tout élément $x \in M$, nous avons

$$\begin{aligned} \mathrm{tr}_{M/K}(xT) = \mathrm{tr}_{L/K}\left(\mathrm{tr}_{M/L}(xT)S\right) \subseteq R &\iff \mathrm{tr}_{M/L}(xT) \subseteq S^{\mathrm{tr}_{L/K}} \\ &\iff \mathrm{tr}_{M/L}(xT\delta_{S/R}) \subseteq S \iff x\delta_{S/R} \subseteq T^{\mathrm{tr}_{M/L}} \iff x \in T^{\mathrm{tr}_{M/L}} S^{\mathrm{tr}_{L/K}}. \end{aligned}$$

Le point (ii) est conséquence du point (i) après application de $\mathrm{N}_{M/K}$. □

4.18. Proposition. Soit $\mathbb{L} = \mathbb{Q}(\beta)$ l'extension quadratique de $\mathbb{Q}$ engendré par un élément β de polynôme minimal $X^2 - d$, avec $d \in \mathbb{Z}$ sans facteur carré. Alors la clôture intégrale S de $\mathbb{Z}$ dans L est l'anneau

$$S = \mathbb{Z}[\alpha] \quad \text{avec} \quad \alpha = \begin{cases} \frac{1+\beta}{2} & \text{si } d = 1 \mod 4 \\ \beta & \text{sinon.} \end{cases}$$

De plus, le différent et le discriminant de S sont respectivement

$$\delta = \begin{cases} (2\alpha+1)S = \beta S & \text{si } d = 1 \mod 4 \\ (2\alpha)S = 2\beta S & \text{sinon} \end{cases} \qquad \Delta = \begin{cases} d & \text{si } d = 1 \mod 4 \\ 4d & \text{sinon.} \end{cases}$$

Démonstration. Premièrement, notons que supposer d entier sans facteur carré ne coute pas de généralité.

Soit $x+y\beta \in \mathbb{L}$ un élément intégral ($x, y \in \mathbb{Q}$). Nous voyons facilement que $2x = \mathrm{tr}(x+y\beta) \in \mathbb{Z}$ et $x^2 - dy^2 = \mathrm{N}(x+y\beta) \in \mathbb{Z}$. Les deux conditions ensemble impliquent que $2y \in \mathbb{Z}$ car d n'a pas de facteur carré. Par ailleurs, en étudiant le résidu modulo 4 de $(2x)^2 - d(2y)^2$, il apparaît que $2x$ et $2y$ ont même parité, et que d congru à 2 ou 3 modulo 4 force $x, y \in \mathbb{Z}$. À l'inverse, $\frac{1+\beta}{2}$ est intégral quand $d = 1 \mod 4$ car il satisfait $X^2 + X + \frac{d-1}{4}$.

Ceci montre que la clôture intégrale de $\mathbb{Z}$ est bien celle énoncée. Les valeurs du différent et du discriminant découlent immédiatement du théorème 4.12 puisque S est monogène. □

4.19. Exemples. (i) $R = \mathbb{Z}$, $S = \mathbb{Z}[i] \subset \mathbb{Q}(i)$, $\delta = (2i)$, $\Delta = 4$.
(ii) $R = \mathbb{Z}$, $S = \mathbb{Z}[\zeta_3] \subset \mathbb{Q}(\sqrt{-3})$, $\delta = (\sqrt{-3})$, $\Delta = 3$.
(iii) $R = \mathbb{Z}$, $S = \mathbb{Z}[\phi] \subset \mathbb{Q}(\sqrt{5})$, $\delta = (\sqrt{5})$, $\Delta = 5$.
(iv) $R = \mathbb{Z}$, $S = \mathbb{Z}[\sqrt[3]{2}] \subset \mathbb{Q}(\sqrt{3})$, $\delta = (3\sqrt[3]{4})$, $\Delta = (108)$
(v) $R = \mathbb{Z}[\sqrt[3]{2}]$, $S = \mathbb{Z}[\zeta_3, \sqrt[3]{2}] \subset \mathbb{Q}(\sqrt{3}, \omega)$, $\delta = (\sqrt{-3})$, $\Delta = (3)$
(vi) $R = \mathbb{Z}$, $S = \mathbb{Z}[\zeta_3, \sqrt[3]{2}] \subset \mathbb{Q}(\sqrt{3}, \omega)$, $\delta = (\sqrt{-3} \cdot 3\sqrt[3]{4})$, $\Delta = (3^6 \cdot 4^2)$
(vii) $R = \mathbb{Z}$, $S = \mathbb{Z}[\zeta_p] \subset \mathbb{Q}(\zeta_p)$ (p premier), $\delta = \prod_{j=2}^{p-1}(\zeta_p - \zeta_p^j)$, $\Delta = p^{p-2}$

4.20. Exercice (Difficile)**.** Soit $d \geq 2$ un entier sans facteur carré et soit $q \geq 2$ un nombre premier congru à 3 modulo 4 qui ne divise pas d. Soient $\mathbb{K} = \mathbb{Q}(\sqrt{-dq})$, $\mathbb{L} = \mathbb{K}(\sqrt{-q}) = \mathbb{Q}(\sqrt{-dq}, \sqrt{-q})$, et soient R et S leurs anneaux d'entiers. Montrer que S n'est pas un module libre sur R. En particulier, S n'est pas une extension monogène.

5. Décomposition et ramification

Sauf indication contraire, dans tout ce chapitre R est un domaine de Dedekind, K son corps de fractions, L une extension finie séparable de K, et S la clôture intégrale de R dans L. Nous supposerons par facilité que toutes les extensions de corps résiduels sont séparables. Ceci est le cas, par exemple, quand ceux-ci sont des corps finis.

5.1. Définition (Décomposition de l'extension d'un idéal premier)**.** Nous avons vu dans la définition 4.7 que l'extension SP d'un idéal maximal P de R a pour facteurs premiers les idéaux maximaux $Q_1, \dots Q_r$ de S qui sont au-dessus de P, et que ces derniers se contractent tous en P. Soit Q un idéal maximal au-dessus de P.

Le corps résiduel $k_P = R/P$ de P se plonge dans $k_Q = S/Q$. Le *degré résiduel* (parfois *degré d'inertie*) *de Q sur P* est le degré de l'extension k_Q/k_P ; il est noté $f(Q|P)$.

L'idéal maximal P de l'anneau local R_P s'étend en un idéal de S_Q. L'*indice de ramification de Q sur P* est la valuation (normalisée !) $v_Q(PS)$; il est noté $e(Q|P)$.

L'idéal maximal P est dit :
(i) *totalement décomposé* lorsque $e(Q|P) = f(Q|P) = 1$ pour tout Q au-dessus de P.
(ii) *non ramifié* lorsque $e(Q|P) = 1$ et k_Q est une extension séparable de k_P pour tout Q au-dessus de P. (Sinon, nous dirons que Q ramifie P, ou que P est ramifié dans l'extension.)
(iii) *docilement ramifié* si $\mathrm{char}\, k_P$ ne divise pas $e(Q|P)$ pour tout Q au-dessus de P.
(iv) *totalement ramifié* lorsque $e(Q|P) = \deg_K(L)$ pour un (et donc tout) Q au-dessus de P.
(v) *inerte* lorsque $f(Q|P) = \deg_K(L)$ pour un (et donc tout) Q au-dessus de P.

5.2. Théorème. Soit R est un domaine de Dedekind, K son corps de fractions, L une extension finie séparable de K, et S la clôture intégrale de R dans L. Soit P un idéal maximal de R et $Q_1, \dots, Q_r$ les idéaux maximaux de S au-dessus de P. Alors

$$\deg_K L = \sum_{i=1}^{r} e(Q_i|P) f(Q_i|P).$$

DÉMONSTRATION. Notons par facilité $e_i = e(Q_i|P)$ et $f_i = f(Q_i|P)$.

Par définition des indices de ramification, l'extension de P à S se factorise $PS = \prod_{i=1}^{r} Q_i^{e_i}$. Puisque les idéaux $Q_i^{e_i}$ sont comaximaux, le théorème des restes chinois établit un isomorphisme d'anneaux

$$S/(PS) \cong \bigoplus_{i=1}^{r} S/Q_i^{e_i}.$$

D'une part, chaque anneau $S/Q_i^{e_i}$ est un module sur le corps $k_P = R/P$ qu'il contient (car $Q_i^{e_i} \cap R = P$). Comme k_P-module, il se filtre

$$0 = Q_i^{e_i}/Q_i^{e_i} \subset Q_i^{e_i-1}/Q_i^{e_i} \subset \cdots \subset S/Q_i^{e_i},$$

avec e_i quotients successifs isomorphes à S/Q_i comme k_P-modules. Or par définition, la dimension de S/Q_i sur k_P est f_i. Il suit que

$$\dim_{k_P}(S/(PS)) = \sum_{i=1}^{r} \dim_{k_P}(S/Q_i^{e_i}) = \sum_{i=1}^{r} e_i f_i.$$

D'autre part, la dimension de L/K est le rang de S comme R-module. Après localisation à R_P, $S \otimes_R R_P$ devient un R_P-module libre, de même rang. Mais alors

$$(S \otimes_R R_P) \otimes_{R_P} k_P \cong S \otimes_R k_P = S \otimes_R (R/P) \cong S/(PS)$$

est aussi de dimension $\deg_K(L)$ comme k_P-module. Le théorème est la combinaison de ces deux calculs. □

5.3. Proposition (Décomposition explicite dans une extension monogène)**.** Soit R un anneau de Dedekind, P un idéal maximal de R, et L une extension finite séparable de $K = \mathrm{Frac}(R)$. Supposons que la clôture intégrale S de R dans L soit monogène, de la forme $S = R[\alpha]$. Notons f le polynôme minimal de α sur R, et $\bar{f} = \bar{f}_1^{e_1}, \dots, \bar{f}_r^{e_r}$ la factorisation (monique) de la réduction $\bar{f}$ de f modulo P. Alors l'extension de P à S se factorise

$$PS = Q_1^{e_1} \cdots Q_r^{e_r},$$

avec $Q_i = PS + f_i(\alpha)S$, pour f_i un polynôme monique à coefficients dans R qui se réduit à $\bar{f}_i$ modulo P.

DÉMONSTRATION. Notons $\bar{R} = R/P$ et prenons $\bar{\alpha}_i$ une racine de $\bar{f}_i$ dans une extension de $\bar{R}$. Soit Q_i l'idéal maximal de S qui est noyau du morphisme

$$\phi_i : S = R[\alpha] \to \bar{R}[\bar{\alpha}_i] : r \mapsto r \bmod P, \quad \alpha \mapsto \bar{\alpha}_i.$$

Ce morphisme s'inscrit dans le diagramme commutatif de morphismes d'anneaux

$$\begin{array}{ccccc} R & \hookrightarrow & R[X] & \xrightarrow{X \mapsto \alpha} & S \\ \downarrow & \text{mod } P & \downarrow & & \downarrow \phi_i \\ \bar{R} & \hookrightarrow & \bar{R}[X] & \xrightarrow[X \mapsto \bar{\alpha}_i]{} & \bar{R}[\bar{\alpha}_i] \end{array}$$

Il est clair que $PS + f_i(\alpha)S \subseteq Q_i$, puisque $f_i(\alpha) \mapsto \bar{f}_i(\bar{\alpha}_i) = 0$. Inversement, soit x un élément arbitraire de Q_i, par hypothèse de la forme $x = g(\alpha)$ pour g un polynôme à coefficients dans R. Puisque $\bar{x} = 0$, la réduction $\bar{g}$ de g modulo P s'annule en $\bar{\alpha}_i$, et donc $\bar{g}$ se factorise $\bar{h}\bar{f}_i$ pour $\bar{h}$ un polynôme monique à coefficients dans $\bar{R}$. Ayant fait un choix de représentant h de $\bar{h}$, il suit que $g - hf_i$ est un polynôme à coefficients dans P, et après évaluation en α, que $g(\alpha) \in PS + f_i(\alpha)S$. Ceci prouve que $Q_i = PS + f_i(\alpha)S$.

Il reste à montrer que PS se factorise comme énoncé. Les Q_i sont évidemment au-dessus de P. De plus, $\deg \bar{f}_i$ est le degré résiduel $f(Q_i|P)$ de Q_i par construction, puisque $S/Q_i \cong \bar{R}[\bar{\alpha}_i]$. Toujours par construction, nous avons donc $\deg_K L = \deg_K f = \sum_{i=1}^r e_i f(Q_i|P)$.

Par ailleurs, $f_1(\alpha)^{e_1} \cdots f_r(\alpha)^{e_r} \in PS$. En effet, la réduction du polynôme $f_1^{e_1} \cdots f_r^{e_r} - f$ modulo P est nulle par choix des f_i, et $f(\alpha) = 0$. Ceci implique que $Q_1^{e_1} \cdots Q_r^{e_r} \subseteq PS + f_1(\alpha)^{e_1} \cdots f_r(\alpha)^{e_r} S = PS$; nous avons donc $e_i \geq e(Q_i|P)$ pour $i = 1, \ldots, r$. En particulier, tout Q au dessus de P apparaît parmi les Q_i, et finalement le théorème 5.2 force l'égalité $e_i = e(Q_i|P)$ puisqu'il établit qu'aussi $\sum_{i=1}^r e(Q_i|P) f(Q_i|P) = \deg_K L$. □

5.4. Exemple (Décomposition et ramification dans $\mathbb{Z}[i]$)**.** Nous avons vu dans la proposition 4.18 que $\mathbb{Z}[i]$ est bien la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}(i)$. Par la proposition 5.3, la décomposition de (p) dans $\mathbb{Z}[i]$ dépend uniquement de la factorisation de $X^2 + 1$ dans $\mathbb{F}_p$, autrement dit, de l'existence d'une racine primitive 4ème de l'unité dans $\mathbb{F}_p$. Notons σ l'unique automorphisme non trivial du corps $\mathbb{Q}(i)$. Nous avons

$$(p) = \begin{cases} Q_2^2 & \text{si } p = 2 \\ Q_p \cdot \sigma(Q_p) & \text{si } p = 1 \mod 4 \\ p\mathbb{Z}[i] & \text{si } p = 3 \mod 4, \end{cases}$$

où $Q_p = (a+bi)\mathbb{Z}[i] = p\mathbb{Z}[i] + (c-i)\mathbb{Z}[i]$ pour n'importe quels deux entiers positifs a, b satisfaisant $a^2 + b^2 = p$ et entier positif c satisfaisant $c^2 = -1 \mod p$ (ce qui n'est bien sûr possible que si $p \neq 3 \mod 4$). En particulier, nous observons que (2) est le seul idéal maximal de $\mathbb{Z}$ qui se ramifie dans $\mathbb{Z}[i]$ (conformément à ce que nous allons voir au théorème 5.15) ; il est même totalement sauvagement ramifié. L'idéal (p) se scinde complètement si $p = 1 \mod 4$, et est inerte dans les cas restant.

5.5. Exercice. Déterminer la décomposition des idéaux premiers de $\mathbb{Z}$ dans l'extension monogène $\mathbb{Z}[\alpha]$ où $\alpha^3 = 2$, en fonction du résidu de p modulo 3 et de la cubicité de 2 modulo p. (NB : il est facile de montrer que lorsque $p = 0, 2 \mod 3$, tout est un cube modulo p. Pour $p = 1 \mod 3$, il est possible de montrer que 2 est un cube modulo p si et seulement si $p = a^2 + 27b^2$ pour $a, b \in \mathbb{Z}$.)

5.6. Le cas local. Jusqu'à la section suivante, nous allons supposer en plus des hypothèses habituelles que R et S sont tous deux locaux, d'unique idéaux maximaux P et Q. Nous noterons par facilité $e = e(Q|P)$ et $f = f(Q|P)$.

5.7. Lemme. Pour tout $x \in S/P$, nous avons $\mathrm{tr}_{(S/P)/k_P}(x) = e \,\mathrm{tr}_{k_Q}(\overline{x})$ et $\mathrm{N}_{(S/P)/k_P}(x) = \mathrm{N}_{k_Q}(\overline{x})^e$, où $\overline{x}$ est l'image de x dans S/Q et les traces sont prises sur k_P.

Démonstration. Nous avons vu dans la preuve du théorème 5.2 que S/P se filtre

$$0 = Q^e/Q^e \subset Q^{e-1}/Q^e \subset \cdots \subset S/Q^e,$$

comme k_P-module, et que les quotients successifs Q^{j-1}/Q^j sont isomorphes à k_Q. De plus, ces isomorphismes identifient la multiplication par x à celle par $\overline{x}$.

Soit maintenant $b_1, \ldots, b_f$ une base de $Q^{e-1}/Q^e \cong k_Q$ sur k_P. Nous pouvons la relever à une base $\{b_{i,j} \mid i = 1, \ldots, f, j = 1, \ldots, e\}$ de S/P telle que $b_{i,j} \in Q^{j-1}$ a pour image b_i modulo Q^j. La multiplication par x dans cette base est block-triangulaire inférieure, avec pour blocks diagonaux e copies de la matrice de multiplication par $\overline{x}$ dans la base $b_1, \ldots, b_f$. Le lemme découle immédiatement du calcul de la trace et de la norme de x dans cette base. □

5.8. Proposition. Nous avons

$$v_Q(\delta_{S/R}) \geq e - 1 \quad \text{et} \quad v_P(\Delta_{S/R}) \geq (e-1)f.$$

Démonstration. Soit $\{b_{i,j} \mid i = 1, \ldots, f, j = 1, \ldots, e\}$ la base de S/Q^e donnée dans la preuve du lemme 5.7. Par le lemme de Nakayama, elle se relève en une base de S sur R (notée identiquement). Dans cette base, $b_{i,j} \in Q$ lorsque $j \geq 2$. Donc les $(e-1)f$ premiers rangs de la matrice $\mathrm{tr}(b_{i,j} b_{i',j'})_{(i,j),(i',j')}$ sont des éléments de P, en vertu du lemme 5.7. Il s'ensuit que le

discriminant $\Delta_{S/R}$ est divisible par $P^{(e-1)f}$, ce qui démontre la deuxième inégalité. En calculant la norme, nous déduisons que

$$v_Q(\delta_{S/R}) = \frac{1}{f} v_P(\mathrm{N}_{L/K}(\delta_{S/R})) = \frac{1}{f} v_P(\Delta_{S/R}) \geq \frac{(e-1)f}{f} = e-1,$$

la première égalité venant de

$$e \cdot v_P(\mathrm{N}_{L/K}(Q)) = v_Q(\mathrm{N}_{L/K}(Q)) = v_Q(\mathrm{N}_{L/K}(\varpi_Q)) = \deg_K(L) = ef \cdot v_Q(Q). \qquad \square$$

5.9. Théorème. *Q/P est non-ramifié si et seulement si $\Delta_{S/R} = R$.*

Démonstration. Si $\Delta_{S/R} = R$, alors $e = 1$ par la proposition 5.8. Nous démontrons la réciproque. Supposons donc que $e = 1$, et soit $\{b_1, \ldots, b_d\}$ une base de S comme R-module. Par le lemme 5.7, $\mathrm{tr}_{S/P}(b_i b_j) = \mathrm{tr}_{k_Q/k_P}(\overline{b_i b_j})$. Puisque k_Q est séparable sur k_P, la trace associée est non-dégénérée, et $\det(\mathrm{tr}_{k_Q/k_P}(\overline{b_i b_j}))$ est non-nul. Ceci signifie que $\det(\mathrm{tr}_{L/K}(b_i b_j))$ n'appartient pas à P, et donc $\Delta_{S/R} = R$. $\square$

5.10. Théorème. Les conditions suivantes sont équivalentes :

(i) Q/P est docilement ramifié
(ii) La trace $\mathrm{tr}_{L/K} : S \to R$ est surjective.
(iii) $v_Q(\delta_{S/R}) = e - 1$.

Démonstration. Si Q/P est docilement ramifié, alors les inversibles de R sont dans $\mathrm{tr}_{L/K}(S)$ par le lemme 5.7. Puisque la trace est R-linéaire, $\mathrm{tr}_{L/K}(S)$ est un idéal et donc $\mathrm{tr}_{L/K}(S) = R$. La réciproque suit aussi du lemme 5.7 : si $\mathrm{char}\, k_P$ divise e, alors la trace prend image dans P.

Montrons que (ii) $\iff$ (iii). Notons d'abord que puisque la trace est K-linéaire,

$$\delta_{S/R}^{-1} \cap K = \mathrm{tr}_{L/K}(S)^{-1}.$$

En effet, si $x \in K$ est tel que $\mathrm{tr}_{L/K}(xS) \in R$, alors $x \,\mathrm{tr}_{L/K}(S) \in R$, et réciproquement. Comparons les valuations de $\delta_{S/R}$ et $\mathrm{tr}_{L/K}(S)$:

$$v_P(\mathrm{tr}_{L/K}(S)) = \frac{v_Q(\mathrm{tr}_{L/K}(S)S)}{e} \leq \frac{v_Q(\delta_{S/R})}{e} < v_P(\mathrm{tr}_{L/K}(S)) + 1.$$

Donc, si $v_P(\mathrm{tr}_{L/K}(S)) = 0$, alors $v_Q(\delta_{S/R}) < e$ et $v_Q(\delta_{S/R}) = e - 1$ par la proposition 5.8. À l'inverse, $v_Q(\delta_{S/R}) = e - 1$ force $v_P(\mathrm{tr}_{L/K}(S)) < 1$. $\square$

En complément des résultats précédents, notons qu'une extension intégrale locale d'un domaine de Dedekind est toujours monogène. Cette proposition permet de prendre quelques raccourcis dans les développements de cette section, que le lecteur intéressé peut explorer.

5.11. Proposition. *Supposons que l'extension k_Q/k_P est séparable. Alors S est monogène sur R.*

Démonstration. Puisqu'elle est séparable, l'extension k_Q est monogène. Soit donc $\bar{\alpha}$ tel que $k_Q = k_P(\bar{\alpha})$, et notons $\bar{f}$ le polynôme minimal de $\bar{\alpha}$ sur k_P. Soit f un polynôme monique à coefficients dans R, qui se réduit à $\bar{f}$ modulo P et qui est de même degré.

Il existe un élément α de S se réduisant à $\bar{\alpha}$ modulo Q, tel que $f(\alpha)$ engendre Q. En effet, soit α' un élément quelconque de S qui se réduit à $\bar{\alpha}$ modulo Q. Clairement, $f(\alpha') \in Q$. Si $f(\alpha') \in Q^2$, alors pour tout choix de générateur $\varpi_Q \in Q$, $\alpha = \alpha' + \varpi_Q$ engendre Q. Nous vérifions en utilisant la formule de Taylor que

$$f(\alpha) = f(\alpha' + \varpi_Q) = f(\alpha') + f'(\alpha')\varpi_Q + Q^2 = Q + Q^2,$$

puisque $f'(\alpha') \notin Q$ car $\bar{f}$ est séparable.

Nous allons montrer que $B = \{\alpha^i f(\alpha)^j \mid i = 0, \ldots, f-1,\ j = 0, \ldots, e-1\}$ est une base de S comme R-module. Ceci implique immédiatement que $S = R[\alpha]$. L'argument s'inspire de celui du lemme 5.7. Soit M le R-module engendré par B, et N celui engendré par $\{\alpha^i \mid i = 0, \ldots, f-1\}$. Clairement, $M = N + f(\alpha)N + \cdots + f(\alpha)^{e-1}N$ (la somme est même directe par comparaison

des valuations des sommants). De plus, $S = N + f(\alpha)S$ puisque par construction, N se surjecte sur k_Q. Nous calculons alors

$$S = N + f(\alpha)S = N + f(\alpha)(N + f(\alpha)S) = \cdots = N + f(\alpha)N + \cdots + f(\alpha)^{e-1}N + f(\alpha)^e S.$$

Donc $S = M + PS$ et le lemme de Nakayama 1.39 permet de conclure que $M = S$ et que B est bien une base de S sur R. □

5.12. Retour au cas global. Ne supposons désormais plus que R et S sont locaux. Le théorème suivant est une version globale de la proposition 5.8 et du théorème 5.9, mais nous aurons besoin des méthodes du chapitre suivant pour le démontrer.

La raison est que si $Q_1, \ldots, Q_r$ sont au-dessus de P, le localisé S_{Q_i} n'est pas intégral sur R_P, et le localisé de S au complément de SP n'est pas local. Il est nécessaire de compléter R et S pour garantir ces deux conditions simultanément, et pouvoir appliquer la proposition 5.8. La conséquence de cette complétion est que le degré de l'extension complétée L_{Q_i}/K_P est possiblement plus petit que celui de L/K. Heureusement, tout ceci est controlé par le corollaire 6.14.

Nous faisons appel de façon anticipé à la notation du chapitre 6 et aux conséquences du théorème 6.10. Le lecteur vérifiera que ceci ne cause pas de dépendance logique dans la suite.

5.13. Lemme. Soit R un domaine de Dedekind, L une extension finie séparable de $K = \mathrm{Frac}(R)$ et S la clôture intégrale de R dans L. Soit P un idéal maximal de R et Q un idéal maximal de S au-dessus de P. L'extension du différent $\delta_{S/R}$ de S à la complétion $\overline{S}^Q$ est le différent local $\delta_{\overline{S}^Q/\overline{R}^P}$. L'extension du discriminant $\Delta_{S/R}$ à $\overline{R}^P$ est le produit des discriminants locaux $\prod_{Q \text{ au-dessus de } P} \Delta_{\overline{S}^Q/\overline{R}^P}$.

5.14. Exercice. Démontrer le lemme 5.13, en se servant des résultats du chapitre 6.

5.15. Théorème. Soit R un domaine de Dedekind, L une extension finie séparable de $K = \mathrm{Frac}(R)$ et S la clôture intégrale de R dans L. Un idéal maximal P de R se ramifie dans S si et seulement si il existe Q_i au dessus de P qui divise le différent $\delta_{S/R}$, si et seulement si P divise le discriminant $\Delta_{S/R}$. En particulier, seul un nombre fini d'idéaux maximaux de R se ramifient dans S.

Démonstration. Un idéal Q_i au-dessus de P divise $\delta_{S/R}$ si et seulement si dans la complétion L_{Q_i}, l'idéal de valuation divise l'extension $\delta_{\overline{S}^{Q_i}/\overline{R}^P}$ de $\delta_{S/R}$ (voir le lemme 5.13). La proposition 5.8 s'applique alors à l'extension $\overline{S}^{Q_i}$ sur $\overline{R}^P$, et montre que ceci équivaut à $e(Q_i|P) > 1$, autrement dit, au fait que Q_i ramifie P.

L'assertion concernant le discriminant se démontre en employant le même argument et le théorème 5.9 en lieu de la proposition 5.8. Elle est aussi une conséquence du fait que $\mathrm{N}_{L/K}(\delta_{S/R}) = \Delta_{S/R}$ et du corollaire 6.11. □

Il est possible d'être plus précis que l'énoncé du théorème 5.15, en ce sens que le lemme 5.13 peut être utilisé pour calculer localement les indices de ramification de chaque Q_i sur P. Par exemple, avec le théorème 5.10, il est possible de déterminer localement pour quels Q_i le couple $(Q_i|P)$ est sauvagement ramifié. Nous donnons une version globale du théorème 5.10.

5.16. Théorème. Soit R un domaine de Dedekind, L une extension finie séparable de $K = \mathrm{Frac}(R)$ et S la clôture intégrale de R dans L. Soit P un idéal maximal de R. Les conditions suivantes sont équivalentes :

(i) P est docilement ramifié
(ii) $v_{Q_i}(\delta_{S/R}) = e(Q_i|P) - 1$ pour tout Q_i au-dessus de P.

Démonstration. Par définition, P est docilement ramifié si et seulement si $(Q_i|P)$ est docilement ramifié pour tout Q_i au dessus de P. En vertu de la proposition 6.2, du lemme 5.13 et du théorème 5.10, $v_{Q_i}(\delta_{S/R}) = v_{Q_i}(\delta_{\overline{S}^{Q_i}/\overline{R}^P}) = e(Q_i|P) - 1$ si et seulement si $(Q_i|P)$ est docilement ramifié. □

6. Complétions et corps locaux

En supplément des techniques de localisation que nous avons déjà bien exploités, il est possible de compléter I-adiquement un anneau de Dedekind (ici I est un idéal quelconque, mais l'intérêt principal réside bien sûr là où I est maximal). Compléter un anneau permet de simplifier considérablement la théorie de ses extensions intégrales, via le lemme de Hensel par exemple.

Rappelons (cf. 2.10) qu'étant donné un idéal maximal P d'un anneau de Dedekind R, la *complétion v_P-adique* (que nous abrévions souvent *P-adique*) $\overline{R}^P$ de R est le complété de R_P pour la norme non-archimédienne $|x|_P = e^{-v_P(x)}$ définie par v_P. Quand le corps résiduel k_P est fini, disons de cardinalité q_P, nous préférerons la normalisation $|x|_P = q_P^{-v_P(x)}$ (qui est bien sûr équivalente).

6.1. Définition. Un corps topologique K est dit *local* si K est localement compact, sans être discret.

6.2. Proposition. La complétion P-adique d'un anneau de Dedekind R est un a.v.d. complet, de même groupe de valuation et de même corps résiduel k_P que R_P. Son corps de fractions, que nous noterons K_P, est le complété de K pour $|\cdot|_P$. C'est un corps topologique complet, qui est local si et seulement si k_P est fini (et R n'est pas un corps).

Démonstration. Le fait que le complété $\overline{R}^P$ de R_P soit un a.v.d. de même groupe de valuation est conséquence du fait que v s'étend en une valuation $\overline{R}^P \to \mathbb{Z}$ par continuité. L'application quotient $\overline{R}^P \to \overline{R}^P/P\overline{R}^P$ est continue (ici $\overline{R}^P/P\overline{R}^P$ est muni de la topologie discrète). Sa restriction à R_P est donc d'image dense, donc surjective. Son noyau est bien évidemment PR_P, ce qui montre que $\overline{R}^P/P\overline{R}^P = k_P$.

Il est clair que le corps des fractions K_P de $\overline{R}^P$ est un sous-corps dense du complété de K pour $|\cdot|_P$. Il suffit donc de montrer que K_P est fermé pour cette norme. Soit $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy d'éléments de K_P. En particulier, $|x_n|_P$ est bornée supérieurement. Il existe donc $y \in \overline{R}^P$ tel que $|yx_n|_P \leq 1$ pour tout $n \in \mathbb{N}$; puisque $\overline{R}^P$ est un a.v.d., ceci signifie que $yx_n \in \overline{R}^P$. Or $\overline{R}^P$ est complet, donc la suite $(yx_n)_{n\in\mathbb{N}}$ converge dans $\overline{R}^P$ vers une limite $z \in \overline{R}^P$. Par continuité de la multiplication, la suite $(x_n)_{n\in\mathbb{N}}$ converge donc vers $y^{-1}z \in K_P$, ce que nous voulions montrer.

Finalement, si K_P est localement compact et non discret, la base $\{K_{v\geq n} \mid n \in \mathbb{N}\}$ de voisinages fermés (et ouverts) de 0 doit contenir un compact $K_{v\geq n}$. Mais $K_{v\geq n}$ est l'union disjointe des $a + K_{v\geq n+1}$ pour a parcourant un système de représentants de $K_{v\geq n}/K_{v\geq n+1} \cong K_{v\geq 0}/K_{v\geq 1} \cong k_P$. Ceci force k_P à être fini. À l'inverse, si k_P est fini nous montrons que l'ouvert $\overline{R}^P = K_{v\geq 0}$ est compact. Il s'ensuivra que $K_{v\geq n} = \varpi^n \overline{R}^P$ est compact-ouvert pour tout $n \in \mathbb{Z}$. Soit $\mathcal{U} = \{U_i \mid i \in I\}$ un recouvrement de $K_{v\geq 0}$ par des ouverts, qui n'admet pas de sous-recouvrement fini. Puisque k_P est fini, au moins une des classes $a_0 + K_{v\geq 1}$ ($a_0 \in +K_{v\geq 0}$) n'admet pas de sous-recouvrement fini par des ouverts de $\mathcal{U}$. De la même façon, une des classes $a_1 + K_{v\geq 2}$ congrues à a_0 modulo $K_{v\geq 1}$ n'admet pas de recouvrement fini. Ainsi de suite, nous construisons des éléments $(a_i)_{i\in\mathbb{N}}$ de $\overline{R}^P$, tous congrus au précédent modulo $K_{v\geq i}$, dont les classes $a_i + K_{v\geq i+1}$ n'admettent pas de sous-recouvrement fini. La suite $(a_i)_{i\in\mathbb{N}}$ converge par construction vers un élément $a \in \overline{R}^P$, qui doit appartenir à l'un des ouverts $U \in \mathcal{U}$. Puisque U est ouvert, il contient un ouvert de base $b_i + K_{v\geq i+1}$ qui contient a, ce qui revient à dire que la classe $a_i + K_{v\geq i+1}$ est recouverte par l'ouvert U de $\mathcal{U}$ seul, contradiction ! □

6.3. Exercice. Montrer que si un corps K équipé d'une norme ultramétrique $|\cdot|$ est localement compact pour la topologie induite par cette norme, alors K est complet, $|\cdot|$ est équivalente à la norme induite par une valuation discrete v sur K, et le corps résiduel de cette valuation est fini. (La proposition précédente donne la dernière conclusion.)

6.4. Exemple. Les complétions adiques locales de $R = \mathbb{Z}$ sont les anneaux $\mathbb{Z}_p$ des entiers p-adiques. Leurs corps de fractions sont bien entendu les corps de nombres p-adiques $\mathbb{Q}_p$.

L'utilité première des corps complets est de pouvoir trouver plus facilement des racines ou des factorisations de polynômes. C'est justement le contenu du célèbre lemme de Hensel. Nous en donnons deux versions, la première pour les racines, la seconde pour les factorisations.

6.5. Lemme (Lemme de Hensel pour les racines)**.** Soit K un corps complet pour une valuation discrete v. Soit f un polynôme à coefficients dans l'anneau $K_{v\geq 0}$ de valuation de K. Supposons qu'il existe un élément $x_0 \in K_{v\geq 0}$ tel que

$$|f(x_0)|_v < |f'(x_0)|_v^2.$$

Alors la suite $(x_i)_{i\in\mathbb{N}}$ définie récursivement par $x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$ converge vers une racine x_∞ de f dans $K_{v\geq 0}$. De plus, $|x_\infty - x_0|_v \leq \left|\frac{f(x_0)}{f'(x_0)^2}\right|_v < 1$.

Démonstration. Posons $c = \left|\frac{f(x_0)}{f'(x_0)^2}\right|_v < 1$. Il s'agit de montrer que

$$\left|\frac{f(x_i)}{f'(x_i)^2}\right|_v \leq c^{2^i} \qquad \text{et} \qquad |x_i - x_0|_v \leq c.$$

La première condition garantit que la suite $(x_i)_{i\in\mathbb{N}}$ soit de Cauchy, donc converge puisque K est complet. Les autres conclusions de l'énoncé découlent alors de ces deux conditions par continuité de la norme.

Nous démontrons ces deux inégalités par récurrence sur i ; elles sont évidents pour $i = 0$. Premièrement,

$$|x_{i+1} - x_0|_v = \left|x_i - \frac{f(x_i)}{f'(x_i)} - x_0\right|_v \leq \max\left\{|x_i - x_0|_v, \left|\frac{f(x_i)}{f'(x_i)}\right|_v\right\} \leq \max\{c, c^{2^i}|f'(x_i)|_v\} = c.$$

Ensuite, pour tout $x \in K$ et tout i, nous avons l'expansion de Taylor

$$f(x) = f(x_i) + f'(x_i)(x - x_i) + \frac{f''(x_i)}{2!}(x - x_i)^2 + \cdots.$$

Remarquons que le terme $\frac{f^{(n)}(x_i)}{n!}$ appartient toujours à $K_{v\geq 0}$. Donc

$$\begin{aligned} f(x_{i+1}) = f\left(x_i - \frac{f(x_i)}{f'(x_i)}\right) &= f(x_i) - f'(x_i)\frac{f(x_i)}{f'(x_i)} + \frac{f''(x_i)}{2!}\frac{f(x_i)^2}{f'(x_i)^2} - \frac{f^{(3)}(x_i)}{3!}\frac{f(x_i)^3}{f'(x_i)^3} + \cdots \\ &= \frac{f(x_i)^2}{f'(x_i)^2}\left(\frac{f^{(2)}(x_i)}{2!} - \frac{f^{(3)}(x_i)}{3!}\frac{f(x_i)}{f'(x_i)} + \cdots\right) \in \frac{f(x_i)^2}{f'(x_i)^2}\cdot K_{v\geq 0}, \end{aligned}$$

ce que permet d'estimer $|f(x_{i+1})|_v \leq \left|\frac{f(x_i)^2}{f'(x_i)^2}\right|_v$. D'autre part, l'expansion de Taylor de f' donne

$$f'(x_{i+1}) = f'(x_i) - f''(x_i)\frac{f(x_i)}{f'(x_i)} + \frac{f^{(3)}(x_i)}{2!}\frac{f(x_i)^2}{f'(x_i)^2} + \cdots \in f'(x_i) + K_{v>0},$$

ce qui donne l'égalité $|f'(x_{i+1})|_v = |f'(x_i)|_v$. Ensemble, $\left|\frac{f(x_{i+1})}{f'(x_{i+1})^2}\right|_v \leq \left|\frac{f(x_i)^2}{f'(x_i)^4}\right|_v \leq c^{2^{i+1}}$. □

La preuve du lemme montre aussi que $|f'(x_i)|_v$ est constante, donc égale à $|f'(x_\infty)|_v$.

6.6. Lemme (Lemme de Hensel pour les factorisations)**.** Soit K un corps complet pour une valuation discrete v. Soit f un polynôme à coefficients dans l'anneau $K_{v\geq 0}$ de valuation de K. Si la réduction $\bar{f}$ de f modulo $K_{v\geq 1}$ admet une factorisation $\bar{f} = \bar{g}\bar{h}$ avec $\bar{g}$, $\bar{h}$ premiers entre-eux, alors il existe deux polynômes h et g à coefficients dans $K_{v\geq 0}$ tels que $f = gh$ et $\deg(g) = \deg(\bar{g})$.

6.7. Exercice. Démontrer le lemme 6.6.

6.8. Corollaire. Soit K un corps complet pour une valuation discrete v. Soit $f = a_dX^d + \cdots + a_1X + a_0$ un polynôme à coefficients dans K, irréductible et de degré d. Alors $\min\{v(a_0), \ldots, v(a_d)\} = \min\{v(a_0), v(a_d)\}$. En particulier, si $v(a_0), v(a_d) \geq 0$ alors f est à coefficients dans $K_{v\geq 0}$.

Démonstration. Quitte à multiplier f par une constante, nous pouvons supposer sans perte de généralité que $\min\{v(a_0),\dots,v(a_d)\} = 0$. Pour i le plus petit indice pour lequel ce minimum est atteint, la réduction de f se factorise

$$\bar{f} = X^i(a_i + a_{i+1}X + \cdots + a_dX^{d-i}).$$

S'il s'avérait que $0 < i < d$, les deux facteurs seraient non-triviaux et premiers entre-eux. Le lemme de Hensel pour les factorisations (lemme 6.6) affirmerait qu'alors f se factorise non-trivialement, ce qui est contraire à l'hypothèse. Nous concluons que $i = 0$ ou $i = d$, comme souhaité. □

6.9. Théorème. Soit K un corps complet pour une valuation discrete v, et soit L une extension finie de K. Il existe une unique valuation sur L étendant v. Elle est discrète et complète, et induit l'unique topologie pour laquelle L est un corps topologique et l'inclusion $K \to L$ est un plongement.

Esquisse de démonstration. La formule $x \mapsto \frac{1}{\deg_K L} v(\mathrm{N}_{L/K}(x))$ définit une valuation discrète (non normalisée) sur L qui étend clairement v. Il est immédiat qu'ainsi équipé, L est un corps topologique et l'inclusion $K \to L$ est un plongement.

La seule difficulté réside en la vérification de l'inégalité ultramétrique. Il suffit de vérifier que pour tout $x \in L$, $v(\mathrm{N}_{L/K}(x)) \geq 0$ implique $v(\mathrm{N}_{L/K}(1+x)) \geq 0$. Soit f le polynôme minimal de x sur K. Le corollaire 6.8 implique que f a ses coefficients dans $K_{v\geq 0}$. En particulier, $\mathrm{N}_{L/K}(1+x) = f(-1) \in K_{v\geq 0}$.

L'unicité de la topologie sur L étendant celle de K est un cas particulier de l'unicité de la topologie sur un espace vectoriel topologique Hausdorff de dimension finie sur K (qui est elle-même conséquence du fait que les applications linéaires entres espaces vectoriels topologiques Hausdorff sont toujours continues).

Quant à l'unicité de v, l'unicité de la topologie sur L implique que tout autre valuation v' étendant v possède le même idéal de valuation et le même anneau de valuation que v. En effet, ce sont les ensembles $L_{v>0} = \{x \in L \mid (x^n)_{n\in\mathbb{N}} \text{ converge vers } 0\}$ et $L_{v\geq 0} = \{x \in L \mid x^{-1} \notin L_{v>0}\}$. La valuation v' est donc discrète à son tour (car $L_{v>0}$ est fermé) et coincide avec v après renormalisation. □

6.10. Théorème (Décomposition de l'extension d'une complétion)**.** Soit K un corps muni d'une valuation discrete v, et soit K_v le complété de K pour v. Soit L une extension finie séparable de K. Les extensions différentes de v à L viennent en nombre fini $v_1,\dots,v_r$. Chaque complétion respective L_{v_i} de L est une extension finie séparable de K_v. Nous avons un isomorphisme de L-algèbres et de K_v-algèbres topologiques

$$L \otimes_K K_v \cong \bigoplus_{i=1}^{r} L_{v_i}.$$

(Dans le membre de droite, L se plonge comme sous-corps dense diagonalement via les applications de complétion $L \to L_{v_i}$, et K_v se plonge diagonalement.) En particulier, ces deux algèbres sont étales sur K_v et complètes. De plus, si $e(v_i|v)$ dénote l'indice de ramification et $f(v_i|v)$ le degré résiduel de l'extension L_{v_i} sur K_v, alors $\deg_K L = \sum_{i=1}^{r} e(v_i|v)f(v_i|v)$.

Démonstration. Puisque L est séparable, le théorème d'Artin garantit l'existence d'un générateur α de L sur K. Soit f le polynôme minimal de α, de sorte que $L \cong K[X]/(f)$. Disons que f se factorise sur K_v en produit d'irréductibles $f = g_1 \cdots g_r$, et notons L_i le corps $K_v[X]/(g_i)$. Alors les g_i sont premiers entre-eux car f est séparable, et le théorème des restes chinois donne le dernier isomorphisme de la série

$$L \otimes_K K_v \cong K[X]/(f) \otimes_K K_v \cong K_v[X]/(f) \cong \bigoplus_{i=1}^{r} K_v[X]/(g_i) = \bigoplus_{i=1}^{r} L_i.$$

Vu que L_i est une extension finie de K_v, le théorème 6.9 indique que L_i est un corps complet pour l'unique extension v_i de v à L_i. Munissons aussi l'algèbre $L \otimes_K K_v$, finie sur K_v, de l'unique

extension de la topologie de K_v qui en fasse une algèbre topologique sur K_v. Cette topologie coincide avec la topologie produit sur $\bigoplus_{i=1}^r L_i$ via l'isomorphisme ci-dessus.

Par précomposition avec $L \to L \otimes_K K_v$, le corps L se plonge dans $\bigoplus_{i=1}^r L_i$. De plus, puisque L contient K, sa clôture dans $L \otimes_K K_v$ contient L et K_v. L'image de L dans $L \otimes_K K_v$ et $\bigoplus_{i=1}^r L_i$ est donc dense ; il en est de même pour sa projection (continue) dans L_i. La restriction de v_i à L définit alors une valuation discrète sur L, pour laquelle L_i est la complétion de L par densité.

Montrons maintenant que toute valuation v' de L étendant v apparait parmi les v_i, et que les v_i se restreignent à des valuations non-équivalentes. Par continuité de v' et par densité de L, v' s'étend à une fonction $L \otimes_K K_v \to \mathbb{Z} \cup \{\infty\}$ (encore notée v') satisfaisant toujours

$$v'(xy) = v'(x)v'(y) \quad \text{et} \quad v'(x+y) \geq \min\{v'(x), v'(y)\}, \quad \text{pour tout } x, y \in L \otimes_K K_v.$$

Si la restriction de v' à l'un des sommants L_i est non-triviale, alors v' est une valuation discrète qui, restreinte à K_v, égale v. Par l'unicité dans le théorème 6.9, v' coincide avec v_i. La restriction de v' est non-triviale pour exactement un des sommants L_i. En effet, le calcul

$$\infty = v'(0) = v'(x_i x_j) = v'(x_i) + v'(x_j), \quad \text{pour } i \neq j \text{ et } x_i \in L_i,\ x_j \in L_j,$$

implique qu'au moins un parmi $v'(x_i)$, $v'(x_j)$ égale ∞, donc qu'au plus une des restrictions de v' aux différents L_i est non triviale. Toutes les restrictions ne peuvent être triviales, sinon $v'((x_i)_{i=1}^r) \geq \min\{v'(x_i) \mid i = 1, \dots, r\} = \infty$ et v' serait identiquement égale à ∞. Nous concluons que v' coincide avec précisément un des v_i, et en conséquence que les v_i doivent se restreindre à des valuations non-équivalentes sur L.

Finalement, le degré de L_i est $e(v_i|v)f(v_i|v)$ par le cas local du théorème 5.2, donc $\deg_K L = \deg_{K_v}(L \otimes_K K_v) = \sum_{i=1}^r \deg_{K_v} L_i = \sum_{i=1}^r e(v_i|v)f(v_i|v)$. □

6.11. Corollaire (Principe local-local pour la norme et la trace)**.** Dans la notation du théorème 6.10, soit $x \in L$.

$$\mathrm{tr}_{L/K}(x) = \sum_{i=1}^r \mathrm{tr}_{L_{v_i}/K_v}(x) \qquad \mathrm{N}_{L/K}(x) = \prod_{i=1}^r \mathrm{N}_{L_{v_i}/K_v}(x).$$

6.12. Corollaire (Formule locale du produit)**.** Dans la notation du théorème 6.10, soit $x \in L$.

$$\prod_{i=1}^r |x|_{v_i}^{\deg_{K_v} L_{v_i}} = |\mathrm{N}_{L/K}(x)|_v.$$

Démonstrations. Soit f le polynôme caractéristique sur K de la multiplication par x dans L, et g_i celui sur K_{v_i} de la multiplication par (l'image de) x dans L_{v_i}. Alors f (vu comme ayant coefficients dans K_v) est aussi le polynôme caractéristique sur K_v de la multiplication à gauche par x dans $L \otimes_K K_v$. L'isomorphisme du théorème 6.10 implique donc l'égalité $f = \prod_{i=1}^r g_i$, dont découle immédiatement le premier corollaire.

Le second corollaire est conséquence du premier et de la formule $v_i(x) = \frac{1}{\deg_{K_v} L_{v_i}} v(\mathrm{N}_{L_{v_i}/K_v}(x))$ démontrée dans la preuve du théorème 6.9. □

6.13. Remarque. Les théorèmes 6.9 et 6.10 restent vrais sous l'hypothèse plus faible que v soit une valuation à valeurs dans $\mathbb{R}$. Par contre, l'hypothèse de complétude est indispensable, comme nous le savons déjà.

Le corollaire suivant est une application directe du théorème 6.10 aux extensions intégrales des domaines de Dedekind.

6.14. Corollaire (Décomposition de la complétion d'un domaine de Dedekind)**.** Soit R un anneau de Dedekind, P un idéal maximal de R, et L une extension séparable finie de $K = \mathrm{Frac}(R)$. Soit S la clôture intégrale de R dans L, et $Q_1, \dots, Q_r$ les idéaux maximaux au-dessus de P. Nous avons l'isomorphisme de L-algèbres

$$L \otimes_K K_P \cong \bigoplus_{i=1}^r L_{Q_i}.$$

La clôture de l'image de S dans $\bigoplus_{i=1}^{r} L_{Q_i}$ est le sous-anneau $\bigoplus_{i=1}^{r} \overline{S}^{Q_i}$.

DÉMONSTRATION. En vertu de la proposition 6.2, L_{Q_i}/K_P a le même corps résiduel et indice de ramification que Q_i sur P. Donc $\deg_{K_P} L_{Q_i} = e(Q_i|P)f(Q_i|P)$ par le théorème 5.2.

Vu le théorème 6.10, il suffit de vérifier que toutes les extensions $v_1, \dots, v_{r'}$ de v à L sont de la forme v_{Q_i} pour un certain i. Il est clair que les v_{Q_i} (normalisées correctement) sont des extensions de v_P à L ; supposons que nous les ayons numérotées $v_1, \dots v_r$. Alors, par le point ci-dessus et par les théorèmes 5.2 et 6.10 successivement,

$$\sum_{i=1}^{r} e(v_i|v)f(v_i|v) = \sum_{i=1}^{r} e(Q_i|P)f(Q_i|P) = \deg_K L = \sum_{i=1}^{r'} e(v_i|v)f(v_i|v).$$

Il suit que $r = r'$, et que nous avons bien pris en compte toutes les extensions de v.

La dernière assertion découle du théorème 2.35 d'approximation forte. □

7. Automorphismes et groupes de ramification d'une extension

Le but de ce chapitre est d'étudier le groupe d'automorphismes d'une extension de domaines de Dedekind en termes de son action sur la décomposition des idéaux.

Nous commençons par énoncer quelques résultats généraux qui assurent le bien-fondé de la suite. Comme toujours, R est un domaine de Dedekind, et S est la clôture intégrale de R dans une extension finie séparable L de $K = \mathrm{Frac}(R)$. Nous notons $G = \mathrm{Aut}_K(L)$.

7.1. Proposition. La clôture intégrale S d'un domaine de Dedekind R dans une extension finie séparable L de $K = \mathrm{Frac}(R)$ est stable par tout automorphisme $\sigma \in \mathrm{Aut}_K(L)$. La restriction $\mathrm{Aut}_K(L) \to \mathrm{Aut}_R(S)$ est un isomorphisme de groupes. L'image par $\sigma \in \mathrm{Aut}_K(L)$ de tout idéal premier (resp. maximal) de S est un idéal premier (resp. maximal).

DÉMONSTRATION. La première assertion est claire, car si x est intégral sur R, $\sigma(x)$ satisfait la même équation monique. (Nous l'avions déjà observé à la proposition 1.33.) Puisque σ préserve S, sa restriction à S est un automorphisme d'anneaux. Par la formule $\sigma\left(\frac{a}{b}\right) = \frac{\sigma'(a)}{\sigma'(b)}$, tout automorphisme σ' de S fixant R s'étend de façon unique en un automorphisme σ de $L = \mathrm{Frac}(S)$ qui fixe bien sûr $K = \mathrm{Frac}(R)$. Cette opération d'extension $\mathrm{Aut}_R(S) \to \mathrm{Aut}_L(K)$ est l'inverse de la restriction ; tous deux sont donc des isomorphismes de groupes. La dernière assertion est évidente. □

7.2. Proposition. Soit P un idéal maximal de R. Si L est une extension normale de K, alors G agit transitivement sur l'ensemble des idéaux de S au-dessus de P.

DÉMONSTRATION. Supposons que Q, Q' soient deux idéaux de S au-dessus de P situés dans deux orbites différentes pour l'action de G. Par hypothèse, Q et les différents $\sigma(Q')$ sont premiers entre-eux. Nous pouvons donc trouver $a \in Q$ tel que $a \notin \sigma(Q')$ pour tout $\sigma \in G$. Or le produit $\mathrm{N}_{L/K}(a) = \prod_{\sigma\in G} \sigma(a)$ appartient à $Q \cap R = P \subset Q'$. Puisque Q' est premier, l'un des facteurs $\sigma(a)$ appartient à Q', contradiction ! □

7.3. Corollaire. Supposons que L soit une extension normale de K. Soit P un idéal maximal de R et $Q_1, \dots, Q_r$ les idéaux de S au-dessus de P. Alors $e = e(Q_i|P)$ et $f = f(Q_i|P)$ ne dépendent pas de i, et $\deg_K L = r \cdot e \cdot f$.

DÉMONSTRATION. Par les propositions 7.1 et 7.2 précédentes, il existe $\sigma \in \mathrm{Aut}_R(S)$ tel que $\sigma(Q_1) = Q_i$. Par factorisation unique de $PS = \sigma(P)S = \sigma(Q_1)^{e_1} \cdots \sigma(Q_r)^{e_r}$, il suit que $e(Q_i|P) = e(Q_1|P)$. De plus, σ induit un isomorphisme $S/Q_1 \to S/Q_i$ qui se restreint à l'identité sur R/P. Autrement dit, les corps résiduels k_{Q_1} et k_{Q_i} sont isomorphes sur k_P. En particulier, leurs degrés $f(Q_1|P)$ et $f(Q_i|P)$ coincident. La formule $\deg_K L = r \cdot e \cdot f$ découle maintenant du théorème 5.2. □

7.4. Proposition. Supposons que L soit une extension normale de K. Soit I un idéal fractionnaire de S. Alors $\mathrm{N}_{L/K}(I)$ est le produit des conjugués $\prod_{\sigma\in G}\sigma(I)$ de I.

Démonstration. Par factorisation unique, il suffit de montrer l'égalité pour un idéal premier Q. Soit $P = Q\cap R$ et $Q = Q_1, \ldots, Q_r$ les idéaux de S au-dessus de R. Par la proposition 7.2, G agit transitivement sur $\{Q_1, \ldots, Q_r\}$. Le corollaire 7.3 indique donc que l'indice du stabilisateur de Q_1 dans G est ef. Nous calculons

$$\prod_{\sigma\in G}\sigma(Q) = Q_1^{ef}\cdots Q_r^{ef} = (Q_1^e\cdots Q_r^e)^f = P^f = [S:Q] = \mathrm{N}_{L/K}(Q),$$

la dernière égalité étant conséquence du fait que les facteurs invariants du R-module S/Q sont f copies de P. □

7.5. Définition (Groupe de décomposition)**.** Soit Q un idéal maximal de S au-dessus de P. Le *groupe de décomposition de Q (sur P)* est le stabilisateur

$$G_Q = \{\sigma\in G \mid \sigma(Q) = Q\}$$

de Q dans $G = \mathrm{Aut}_K(L)$.

7.6. Lemme. Soit Q un idéal maximal de S. Le groupe de décomposition G_Q coincide avec le fixateur $\{\sigma\in G \mid v_Q(\sigma(x)) = v_Q(x)$ pour tout $x\in L\}$ de la valuation v_Q. Le groupe G_Q est aussi l'ensemble des $\sigma\in G$ qui sont continus pour v_Q. Le groupe de décomposition de $\sigma(Q)$ est $G_{\sigma(Q)} = \sigma G\sigma^{-1}$.

Démonstration. Il est clair que si $\sigma\in G$ fixe v_Q, alors σ préserve Q. Inversement, si σ préserve Q, alors σ se restreint en un automorphisme du localisé R_Q, qui fixe forcément sa valuation discrete (puisque celle-ci est déterminée par la filtration par les puissances de Q).

Tout $\sigma\in G$ qui fixe v_Q est continu pour la topologie Q-adique. Inversement, si $\sigma\in G$ est continu pour v_Q, alors par densité de L, σ s'étend à un automorphisme de la complétion L_Q, qui fixe K_P puisque K y est dense. Par l'unicité de l'extension dans le théorème 6.9, σ fixe alors v_Q.

La dernière assertion est évidente. □

7.7. Proposition. Supposons que L soit une extension normale de K. Soit Q un idéal maximal de S au-dessus de P. L'extension des complétions respectives L_Q/K_P est normale. La restriction $\mathrm{Aut}_{K_P}(L_Q)\to G_Q$ est un isomorphisme.

Démonstration. Puisque L est normal sur K, L est stable par tout élément de $\mathrm{Aut}_{K_P}(L_Q)$. La restriction $\mathrm{Aut}_{K_P}(L_Q)\to\mathrm{Aut}_K(L)$ est donc bien définie. Par l'unicité de l'extension dans le théorème 6.9, tout $\sigma\in\mathrm{Aut}_{K_P}(L_Q)$ fixe v_Q (et la restriction de σ à L fixe celle de v_Q). Le lemme 7.6 montre alors que l'image de la restriction $\mathrm{Aut}_{K_P}(L_Q)\to\mathrm{Aut}_K(L)$ est contenue dans G_Q.

Inversement, tout $\sigma\in G_Q$ s'étend par continuité à un automorphisme de L_Q fixant K_P (voir la preuve du lemme 7.6). Il est clair que ces opérations de restriction et d'extension sont mutuellement inverses. □

La proposition précédente indique que pour l'étude du groupe de décomposition G_Q de Q, il n'y a pas de perte à supposer que le corps L est complet pour v_Q.

Nous le faisons dès le théorème suivant, qui établit une correspondence bijective entre les extensions séparables du corps résiduel et les extensions séparables non ramifiées de K.

7.8. Théorème (Classification des extensions non ramifiées)**.** Supposons que K soit complet pour v_P. Toute extension séparable k du corps résiduel k_P de K est le corps résiduel d'une unique extension séparable non ramifiée L de K. De plus, tout morphisme $\bar\phi : k\to k'$ d'extensions séparables de k_P induit un unique K-morphisme $\phi : L\to L'$ entre les extensions ainsi construites qui se réduit à $\bar\phi$ modulo les idéaux de valuation. Cette construction est inverse à la réduction modulo l'idéal de valuation.

En conséquence, les extensions séparables du corps résiduel k_P et les extensions séparables non ramifiées de K sont en correspondence fonctorielle bijective, préservant le degré, la normalité, et le groupe d'automorphisme sur le corps de base.

DÉMONSTRATION. Il suffit de montrer le théorème pour les extensions finies. L'énoncé général en découle en prenant les limites directes des sous-corps finis. (Il est entendu dans l'énoncé qu'une extension algébrique de degré possiblement infini sur K est dite non ramifiée si toutes ses extensions intermédiaires finies sont non-ramifiées.)

Soit k une extension séparable finie de k_P. Par le théorème de l'élément primitif, il existe $\bar{\alpha}$ tel que $k = k_P(\bar{\alpha})$. Soit $\bar{f}$ le polynôme minimal de $\bar{\alpha}$ sur k_P, et soit f un polynôme monique de même de degré à coefficients dans R. Le polynôme f est irréductible sur K par le lemme de Gauss : toute factorisation de f se fait par des polynômes moniques à coefficients dans R qui, réduits, donnent une factorisation de $\bar{f}$ sur k_P. Notons L l'extension obtenue en ajoutant à K une racine α de f, S son anneau de valuation et Q son idéal de valuation. L'extension L est séparable, car f est séparable puisque $f'(\alpha)$ se réduit à $\bar{f}'(\bar{\alpha}) \neq 0$.

Le corps résiduel de L est bien k. En effet, l'image $\tilde{\alpha}$ de α par le morphisme de réduction $S \to k_Q$ est racine du polynôme $\bar{f}$. Il y a donc un plongement $k_P(\bar{\alpha}) \to k_Q : \bar{\alpha} \mapsto \tilde{\alpha}$ fixant k_P. Or

$$\deg_{k_P} k_Q \leq \deg_K L = \deg f = \deg \bar{f} = \deg_{k_P} k_P(\bar{\alpha}) \leq \deg_{k_P} k_Q,$$

donc l'égalité a lieu partout, et en particulier $k_Q = k_P(\bar{\alpha}) = k$. Il s'agit aussi de vérifier que L n'est pas ramifiée sur K. Par le théorème 5.2,

$$e(Q|P) \cdot f(Q|P) = \deg_K L = \deg f = \deg \bar{f} = \deg_{k_P} k_Q = f(Q|P).$$

Donc $e = 1$ et L est non-ramifiée.

Tout morphisme $\bar{\phi} : k_P(\bar{\alpha}) = k \to k'$ induit un morphisme $\phi : K(\alpha) = L \to L'$ en envoyant α sur une racine dans L' de son polynôme minimal f qui se réduit à $\bar{\phi}(\bar{\alpha})$. Une telle racine existe par le lemme de Hensel, puisque $\bar{\phi}(\bar{\alpha})$ est une racine de $\bar{f}$ dans k'. Cette racine est bien unique : $\bar{f}$ étant séparable, deux racines distinctes de f ne peuvent avoir le même résidu dans k'. Le morphisme induit ϕ est continu puisqu'il est K-linéaire, et sa réduction est $\bar{\phi}$ par construction.

Dans l'autre sens, étant donné une extension séparable non ramifiée L de K, nous avons vu à la proposition 5.11 que l'anneau de valuation S de L est monogène sur R, l'anneau de K. Soit donc $\alpha \in S$ tel que $S = R[\alpha]$, et notons $\bar{\alpha}$ l'image de α dans k_Q ; il est clair que $k_Q = k_P(\bar{\alpha})$. Cette extension est séparable par hypothèse (L est supposé non-ramifié). Montrons qu'elle est de degré $\deg_K L$. Par le théorème 5.2, vu que L est non ramifiée,

$$f(Q|P) = \deg_{k_P} k_Q \leq \deg \bar{f} = \deg f = \deg_K L = f(Q|P).$$

L'égalité a donc lieu, et il suit aussi que $\bar{f}$ est irréductible.

Si $\phi : L \to L'$ est un K-morphisme, alors ϕ est continu (puisque K-linéaire) et donc induit une inclusion entre les anneaux et les idéaux de valuation de L et L', puis une inclusion $\bar{\phi} : k_Q = k \to k'$ entre leurs corps résiduels.

Il reste à verifier que les deux opérations $\bar{\phi} \mapsto \phi$ et $\phi \mapsto \bar{\phi}$ sont inverses l'une de l'autre. Ceci découle facilement de la construction donnée ci-dessus et de l'unicité de l'extension (et de la réduction). De plus, ces deux opérations préservent clairement la composition. L'assertion concernant le groupe d'automorphisme est alors immédiate, puisque la première partie du théorème s'applique bien sûr à tout automorphisme $L \to L$ ou $k_Q \to k_Q$. En comparant le degré et l'ordre du groupe d'automorphisme, nous voyons que la normalité d'une extension est préservée aussi par les deux opérations. □

7.9. Définition (Groupe d'inertie)**.** Soit Q un idéal maximal de S au-dessus de P. Le *groupe d'inertie de Q (sur P)* est le sous-groupe

$$G_0 = \{\sigma \in G \mid v_Q(\sigma(x) - x) > 0 \text{ pour tout } x \in S\}$$

de G_Q.

Il s'agit de vérifier que G_0 est bien sous-groupe de G_Q. En effet, si $x \in S \setminus Q$, la condition $v_Q(\sigma(x) - x) > 0$ implique que $v_Q(\sigma(x)) = v_Q(x)$. Donc σ préserve (le complément de) Q, et appartient à G_Q par le lemme 7.6. Le produit de $\sigma, \sigma' \in G_0$ satisfait

$$v_Q(\sigma(\sigma'(x))-x) \geq \min\{v_Q(\sigma(\sigma'(x))-\sigma(x)), v_Q(\sigma(x)-x)\} = \min\{v_Q(\sigma'(x)-x), v_Q(\sigma(x)-x)\} > 0,$$

donc appartient à G_0. En fait, G_0 est le noyau du morphisme de réduction $G_Q \to \mathrm{Aut}_{k_P} k_Q$; c'est donc un sous-groupe normal de G_Q.

7.10. Théorème (Corps inertiel)**.** Soit L une extension séparable du corps K supposé complet pour v_P. Il existe un unique corps intermédiaire L^{nr} jouissant de la propriété : les corps intermédiaires non-ramifiés de L/K sont précisément les corps intermédiaires de L^{nr}/K. En particulier, L^{nr} est le plus grand sous-corps de L non ramifié sur K.

Son corps résiduel est la clôture séparable de k_P dans le corps résiduel de L, et son fixateur dans $G = \mathrm{Aut}_K(L)$ est précisément le sous-groupe d'inertie G_0. De plus, L^{nr} est normal sur K quand L l'est.

Démonstration. Soit L^{nr} le corps associé par le théorème 7.8 à la clôture séparable k_P^{s} de k_P dans le corps résiduel k_Q de L. Si L_1 est un corps intermédiaire non ramifié, alors par le théorème 7.8, son corps résiduel k_1 est un sous-corps de k_P^{s}, et il existe un unique morphisme $L_1 \to L^{\mathrm{nr}}$ dont la réduction est l'inclusion $k_1 \to k_P^{\mathrm{s}}$. Par comparaison de L_1 avec son image, ce morphisme est l'inclusion de $L_1 \to L^{\mathrm{nr}}$ comme corps intermédiaires de L.

Inversement, tout sous-corps de L^{nr} est non-ramifié. En effet, il suit de la définition que deux extensions L_1/L_2 et L_2/K sont non-ramifiées si et seulement si l'extension L_1/K est non-ramifiée. Ceci montre la première partie de l'énoncé.

Tout automorphisme de L sur K préserve la propriété d'être non ramifié. Donc L^{nr} est stable par tout automorphisme de L sur K. Si L est une extension normale, ceci implique que L^{nr} est normal. Par la correspondence des morphismes dans le théorème 7.8, il suit que le fixateur de L^{nr} dans G est précisément le noyau du morphisme de réduction

$$G \to \mathrm{Aut}_{k_P} k_Q : \phi \mapsto \bar{\phi}.$$

Ce noyau est par définition le groupe d'inertie. □

7.11. Corollaire. Il existe une unique extension séparable non ramifiée maximale de K. Son corps résiduel est la clôture séparable de k_P, et son groupe de Galois sur K est naturellement isomorphe à celui de la clôture séparable de k_P sur k_P.

Démonstration. Il suffit de prendre l'extension K^{nr} associée par le théorème 7.10 à la clôture séparable K^{sep} de K. Elle est non-ramifiée et maximale pour cette propriété parmi toutes les extensions séparables de K, à nouveau par le théorème 7.10. La description de son groupe de Galois est conséquence du théorème 7.8. □

7.12. Corollaire. Le corps engendré par deux extensions non ramifiées sur K (dans une clôture séparable de K) est non-ramifié.

Démonstration. Tous deux sont des sous-corps de l'extension non ramifiée maximale du corps engendré. □

7.13. L'élément de Frobenius. Soit maintenant $\mathbb{K}$ est un corps global et $\mathbb{L}$ une extension finie séparable de $\mathbb{K}$. Prenons Q un idéal premier de $\mathcal{O}_{\mathbb{L}}$ au-dessus de $P \triangleleft \mathcal{O}_{\mathbb{K}}$. Alors k_Q est une extension finie du corps fini k_P. Son groupe de Galois $\mathrm{Aut}_{k_P}(k_Q)$ est cyclique engendré par une puissance ϕ_Q de l'automorphisme de Frobenius.

Par la proposition 7.7 combinée avec les théorèmes 7.8 et 7.10, le quotient $G_Q/G_{Q,0}$ est naturellement isomorphe à $\mathrm{Aut}_{k_P}(k_Q)$. Nous noterons (abusivement) ϕ_Q une image inverse de l'élément de Frobenius dans G_Q. Lorsque Q est non-ramifié, $G_{Q,0} = \{1\}$ et $G_Q \cong \mathrm{Aut}_{k_P}(k_Q)$. Dans ce cas, ϕ_Q est uniquement déterminé, et caractérisé par la propriété $\phi_P(x) \in x^{\#k_p} + Q$ pour tout $x \in \mathcal{O}_{\mathbb{L}}$.

Bien sûr, ϕ_Q dépend de Q, mais lorsque Q est non-ramifié et $\mathbb{L}$ est normal sur $\mathbb{K}$, nous avons vu à la proposition 7.2 que tous les idéaux au-dessus de P sont conjugués. Il en est de même

pour leurs groupes de décomposition. Du coup, ϕ_Q parcourt une unique classe de conjugaison dans $G = \mathrm{Aut}_{\mathbb{K}}(\mathbb{L})$, et est communément utilisé pour désigner cette classe de conjugaison, ou n'importe lequel de ses représentants.

La prochaine étape est d'obtenir une description des extensions intermédiaires docilement ramifiées.

7.14. Définition (Groupes de ramification)**.** Soit Q un idéal maximal au-dessus de P. Le *i-ème groupe de ramification de Q (sur P)* est le sous-groupe

$$G_i = \{\sigma \in G_Q \mid v_Q(\sigma(x) - x) > i \text{ pour tout } x \in S\}$$

de G_Q. Étant donné un élément $\sigma \in G_Q$, sa *valuation* est la quantité

$$i(\sigma) = \max\{i \mid \sigma \in G_{i-1}\}.$$

Les groupes de ramifications forment une filtration

$$G \geq G_Q = G_{-1} \trianglerighteq G_0 \trianglerighteq G_1 \trianglerighteq \cdots = \{1\}.$$

du groupe de décomposition $G_Q = G_{-1}$ de $G = \mathrm{Aut}_K(L)$. Nous avons vu au théorème 7.10 que le premier quotient G_{-1}/G_0 s'identifiait à $\mathrm{Aut}_{k_P}(k_Q)$. Cette filtration se termine en $\{1\}$ puisque G est un groupe fini (pour $x \in S$ fixé, la quantité $v_Q(\sigma(x) - x) > i$ est alors bornée).

7.15. Exercice. Supposons que K soit complet pour la valuation discrète v_P, et que L/K et k_Q/k_P soient des extension séparables finies, de sorte que $S = R[\alpha]$ pour $\alpha \in S$ (cf. 5.11). Montrer que les groupes de ramification peuvent être calculés par rapport à α, c'est-à-dire que

$$G_i = \{\sigma \in G_Q \mid v_Q(\sigma(\alpha) - \alpha) > i\}.$$

En conséquence, la valuation de $\sigma \in G_Q$ est $i(\sigma) = v_Q(\sigma(\alpha) - \alpha)$.

7.16. Théorème (Formule du différent)**.** Supposons que K soit complet pour v_P, que L soit une extension finie, normale et séparable de K, et que k_Q soit séparable sur k_P. Nous avons la formule

$$v_Q(\delta_{S/R}) = \sum_{\sigma \in G \setminus \{1\}} i(\sigma) = \sum_{i=0}^{\infty} (\#G_i - 1).$$

Démonstration. Par la proposition 5.11, nous pouvons écrire $S = R[\alpha]$. Soit g le polynôme minimal de α sur R. La proposition 4.12 indique que $\delta_{S/R}$ est l'idéal de S engendré par $g'(\alpha)$. En tenant compte de l'exercise 7.15, nous calculons

$$v_Q(\delta_{S/R}) = v_Q(g'(\alpha)) = v_Q\left(\prod_{\sigma \in G \setminus \{1\}} (\alpha - \sigma(\alpha))\right) = \sum_{\sigma \in G \setminus \{1\}} i(\sigma).$$

D'autre part,

$$\sum_{\sigma \in G \setminus \{1\}} i(\sigma) = \sum_{i=0}^{\infty} i \cdot (\#G_{i-1} - \#G_i) = \sum_{i=0}^{\infty} i \cdot ((\#G_{i-1} - 1) - (\#G_i - 1)) = \sum_{i=0}^{\infty} (\#G_i - 1). \quad \square$$

Dans le reste de ce chapitre, nous noterons U_i le i-ème sous-groupe de congruence du groupe $S^\times$ des unités de S (introduit à la section 2.11).

7.17. Théorème (Filtration par les groupes de ramification)**.** Supposons que K soit complet pour v_P, et que k_Q soit séparable sur k_P. Soit ϖ un générateur de Q. Pour $i \geq 1$, les conditions suivantes sur $\sigma \in G$ sont équivalentes :

(i) σ induit l'identité sur S/Q^{i+1}, (ii) $\sigma \in G_i$, (iii) $\dfrac{\sigma(x)}{x} \in U_i$ pour tout $x \in S \setminus \{0\}$.

De plus, pour $i \geq 0$, l'application

$$G_i \to U_i/U_{i+1} : \sigma \mapsto \frac{\sigma(\varpi)}{\varpi}$$

est un morphisme de groupes indépendant du choix de ϖ, et dont le noyau est précisément G_{i+1}.

DÉMONSTRATION. L'équivalence (i) $\iff$ (ii) est conséquence immédiate de la définition de G_i (et est valable pour $i = 0$).

Montrons (iii) $\implies$ (ii). Si $i \geq 1$ et $\frac{\sigma(x)}{x} \in U_i$ pour tout $x \in S \setminus \{0\}$, alors certainement $\sigma(x) \in x + Q$, et donc $\sigma \in G_0$. Soit $x \in S$ et prenons $y \in Q$ tel que $x - y \in S^\times \cap L^{\mathrm{nr}}$. Un tel y existe parce que L et L^{nr} ont le même corps résiduel par le théorème 7.10. Alors σ fixe $x - y$, et

$$v_Q(\sigma(x) - x) = v_Q(\sigma(y) - y) = v_Q\left(\frac{\sigma(y)}{y} - 1\right) + v_Q(y) \geq i + 1.$$

Inversement, prenons $i \geq 0$ et $\sigma \in G_i$. Pour tout $y \in U_0 = S^\times$,

$$v_Q\left(\frac{\sigma(y)}{y} - 1\right) = v_Q(\sigma(y) - y) \geq i + 1, \quad \text{i.e. } \frac{\sigma(y)}{y} \in U_{i+1}.$$

Pour ϖ un générateur de Q,

$$v_Q\left(\frac{\sigma(\varpi)}{\varpi} - 1\right) = v_Q(\sigma(\varpi) - \varpi) - 1 \geq i, \quad \text{i.e. } \frac{\sigma(\varpi)}{\varpi} \in U_i.$$

Soit maintenant $x \in S \setminus \{0\}$, et écrivons $x = y\varpi^n$. Alors

$$\frac{\sigma(x)}{x} = \frac{\sigma(y)}{y} \cdot \frac{\sigma(\varpi)^n}{\varpi^n} = \frac{\sigma(\varpi)^n}{\varpi^n} \mod U_{i+1}.$$

Donc $\frac{\sigma(x)}{x} \in U_i$, ce qui démontre (ii) $\implies$ (iii).

De plus, le dernier calcul montre que la classe de $\frac{\sigma(x)}{x}$ modulo U_{i+1} ne dépend que de $n = v_Q(x)$. L'application $\sigma \mapsto \frac{\sigma(\varpi)}{\varpi} \mod U_{i+1}$ ne dépend donc pas du choix de ϖ, et est bien un morphisme puisque pour $\sigma, \sigma' \in U_i$,

$$\frac{\sigma'(\sigma(\varpi))}{\varpi} = \frac{\sigma'(\sigma(\varpi))}{\sigma(\varpi)} \cdot \frac{\sigma(\varpi)}{\varpi} = \frac{\sigma'(\varpi)}{\varpi} \cdot \frac{\sigma(\varpi)}{\varpi} \mod U_{i+1}.$$

Finalement, par la première étape de la démonstration, son noyau est G_{i+1}. □

7.18. Remarque. Tenu compte de l'exercise 7.15, le théorème 7.17 peut être résumé ainsi : si $S = R[\alpha]$, l'application

$$G_0 \to U_0 : \sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$$

(qui dépend du générateur α et n'est pas un morphisme) relève la filtration $\{U_i\}_{i\in\mathbb{N}}$ de U_0 en la filtration $\{G_i\}_{i\in\mathbb{N}}$ de G_0, et induit des morphismes injectifs $G_i/G_{i+1} \to U_i/U_{i+1}$, le tout indépendamment du choix de α.

7.19. Corollaire. Soient R et S tels que dans le théorème 7.17. Les quotients G_i/G_{i+1} sont abéliens pour $i \geq 0$ et cyclique pour $i = 0$. En conséquence, G est l'extension de $\mathrm{Aut}_{k_P}(k_Q)$ par un groupe résoluble.

DÉMONSTRATION. Le théorème 7.17 montre que G_i/G_{i+1} est isomorphe à un sous-groupe de U_i/U_{i+1}, qui est abélien. L'isomorphisme $G/G_0 \to \mathrm{Aut}_{k_P}(k_Q)$ découle des théorèmes 7.8 et 7.10. □

7.20. Exemple. Nous aurions pu être plus précis dans le corollaire 7.19.

Si $\mathrm{char}\, k_Q = p > 0$ (en plus des hypothèses), alors G_{-1} est extension de $\mathrm{Aut}_{k_P}(k_Q)$ par un groupe cyclique-par-p. En effet, U_i/U_{i+1} est un p-groupe élémentaire pour $i \geq 1$, et $U_0/U_1 \cong k_Q^\times$ est cyclique, d'ordre premier à p. Nous voyons aussi que G_1 est l'unique sous-groupe p-Sylow de G_{-1}.

Si de plus le corps résiduel k_Q est fini, alors $\mathrm{Aut}_{k_P}(k_Q)$ est engendré par l'élément de Frobenius, et G_{-1} est extension d'un groupe cyclique par un groupe cyclique-par-p.

Si à la place $\mathrm{char}\, k_Q = 0$, alors U_1 est sans torsion et donc G_1 est trivial. Dans ce cas, G_0 est cyclique et G_{-1} est l'extension de $\mathrm{Aut}_{k_P}(k_Q)$ par un groupe cyclique.

7.21. Théorème (Corps de ramification)**.** Soit L une extension séparable finie du corps K supposé complet pour une valuation discrète v_P. Supposons que k_Q soit séparable sur k_P. Il existe un unique corps intermédiaire L^{dr} jouissant de la propriété : les corps intermédiaires docilement ramifiés de L/K sont précisément les corps intermédiaires de L^{dr}/K. En particulier, L^{dr} est le plus grand sous-corps de L docilement ramifié sur K.

Son fixateur dans $G = \mathrm{Aut}_K(L)$ est le groupe de ramification G_1. De plus, L^{dr} est normal sur K quand L l'est.

La preuve du théorème 7.21 est laissé comme exercise pour le lecteur, suffisamment aguerri pour être parvenu jusqu'ici.

8. Sujets à présentations

8.1. Le théorème d'Ostrowski et ses variantes / généralisations. Voir aussi le théorème de Gelfand–Tornheim. Peut être accompagné de la classification des corps locaux.

8.2. Les bornes de Minkowski pour le discriminant et le nombre de classes.

8.3. La construction du corps de classe de Hilbert.

8.4. La loi de réciprocité quadratique comme conséquence de la décomposition de (q) dans $\mathbb{Q}(\sqrt{p})$. Décrire comment le symbole d'Artin et la réciprocité d'Artin généralisent la réciprocité quadratique.

8.5. Le groupe de classe par la théorie des formes quadratiques binaires.