IV
Discriminants

1. Norme d'un idéal

Soit A un anneau de Dedekind. Notons K son corps des fractions. Soit L une extension séparable et finie de K. Notons B la clôture intégrale de A dans L.

Pour $\mathcal{Q}$ idéal maximal de A, notons $B_{(\mathcal{Q})}$ le sous-anneau de L formé par les quotients d'éléments de B par des éléments de A premiers à $\mathcal{Q}$. C'est un anneau de Dedekind, dont les idéaux maximaux sont les diviseurs de $\mathcal{Q}$.

Proposition 1. — *Un anneau de Dedekind ne possédant qu'un nombre fini d'idéaux premiers est principal. En particulier, $B_{(\mathcal{Q})}$ est principal*
Démonstration. — Soit A un tel anneau. Notons K son corps des fractions. Soit I un idéal de A. Il s'écrit sous la forme $\prod_{\mathcal{P}} \mathcal{P}^{n_{\mathcal{P}}}$ où $\mathcal{P}$ parcourt les idéaux maximaux de A. Soit $(x_{\mathcal{P}})_{\mathcal{P}}$ une famille (finie) indexée par les idéaux maximaux de A d'éléments de A telle que $v_{\mathcal{P}}(x_{\mathcal{P}}) = n_{\mathcal{P}}$. D'après le lemme d'approximation, il existe $x \in K$ tel que $v_{\mathcal{P}}(x - x_{\mathcal{P}}) > n_{\mathcal{P}}$. On a donc $v_{\mathcal{P}}(x) = n_{\mathcal{P}}$ pour tout idéal maximal $\mathcal{P}$ de A ; cela entraîne que x est entier. L'idéal I est donc engendré par x. Tout idéal de A est donc principal.

Tout idéal premier maximal de $B_{(\mathcal{Q})}$ divise $\mathcal{Q}$. Ainsi $B_{(\mathcal{Q})}$ est principal.

Soit I un idéal de B. La *norme* $\mathrm{N}_{L/K}(I)$ de I est par définition l'idéal de A engendré par les normes $\mathrm{N}_{L/K}(b)$ des éléments b de I. En d'autres termes, on a

$$\mathrm{N}_{L/K}(I) = \sum_{b \in I} A\mathrm{N}_{L/K}(b).$$

Proposition 2. — *On a les formules suivantes :*
(ι) $\mathrm{N}_{L/K}(bB) = \mathrm{N}_{L/K}(b)A$, $b \in B$.
(ιι) $\mathrm{N}_{L/K}(IB_{(\mathcal{Q})}) = \mathrm{N}_{L/K}(I)A_{(\mathcal{Q})}$, *$I$ idéal de B et $\mathcal{Q}$ idéal premier non nul de A.*
(ιιι) $\mathrm{N}_{L/K}(I_1 I_2) = \mathrm{N}_{L/K}(I_1)\mathrm{N}_{L/K}(I_2)$, *$I_1$ et I_2 idéaux de B.*
(ιv) $\mathrm{N}_{L/K}(\mathcal{P}) = \mathcal{Q}^{f_{\mathcal{P}}}$, *$\mathcal{Q}$ idéal premier de A, $\mathcal{P}$ idéal de B au dessus de $\mathcal{Q}$.*
Démonstration. — La formule (ι) résulte de $\mathrm{N}_{L/K}(B) = A$ et de la multiplicativité de $\mathrm{N}_{L/K}$. On a l'inclusion $\mathrm{N}_{L/K}(I)A_{(\mathcal{Q})} \subset \mathrm{N}_{L/K}(IB_{(\mathcal{Q})})$. Démontrons l'inclusion inverse. Soit $x \in \mathrm{N}_{L/K}(IB_{(\mathcal{Q})})$. Il s'écrit $\sum_{b \in IB_{(\mathcal{Q})}} \lambda_b \mathrm{N}_{L/K}(b)$, cette somme étant finie avec $\lambda_b \in A$. Il suffit donc de prouver que $\mathrm{N}_{L/K}(b) \in \mathrm{N}_{L/K}(I)A_{(\mathcal{Q})}$ pour tout $b \in IB_{(\mathcal{Q})}$. Soit $s \in A - \mathcal{Q}$ tel que $sb \in I$. On a $\mathrm{N}_{L/K}(sb) = s^{[L:K]}\mathrm{N}_{L/K}(b)$. Comme $s^{[L:K]} \in A - \mathcal{Q}$, on a $\mathrm{N}_{L/K}(b) \in \mathrm{N}_{L/K}(I)A_{(\mathcal{Q})}$. Cela démontre l'inclusion cherchée et donc $(\iota\iota)$.

En vertu de $(\iota\iota)$ on peut procéder par localisation pour démontrer $(\iota\iota\iota)$. D'après la proposition 1, l'anneau $B_{(\mathcal{Q})}$ est principal puisque c'est un anneau de Dedekind qui a pour seuls idéaux maximaux les idéaux engendrés par les idéaux maximaux de B au-dessus de

$\mathcal{Q}$ qui sont en nombre fini. On se ramène donc au cas où A est un anneau de valuation discrète et où B est un anneau principal. On utilise alors (ι).

On démontre d'abord (ιv) dans le cas d'une extension $L|K$ galoisienne. Soit $b \in \mathcal{P}$. On a $\mathrm{N}_{L/K}(b) \in \mathcal{P} \cap K \subset \mathcal{Q}$. On a donc $\mathrm{N}_{L/K}(\mathcal{P}) \subset \mathcal{Q}$. De plus $\mathrm{N}_{L/K}(\mathcal{P})$ n'est contenu dans aucun idéal premier non nul distinct de $\mathcal{Q}$ en raison de $(\iota\iota)$. Par localisation on se ramène au cas où A est un anneau de valuation discrète. Posons $\mathrm{N}_{L/K}(\mathcal{P}) = \mathcal{Q}^{m_\mathcal{P}}$ pour un certain entier $m_\mathcal{P}$. On a la décomposition de $\mathcal{Q}$ donnée par $\mathcal{Q} = \prod_{\mathcal{P}'|\mathcal{Q}} \mathcal{P}'^{e_{\mathcal{P}'}}$. Pour $\sigma \in \mathrm{Gal}(L/K)$, on a $\mathrm{N}_{L/K}(\sigma(\mathcal{P})) = \mathrm{N}_{L/K}(\mathcal{P})$, si bien que $m_\mathcal{P}$ ne dépend que de $\mathcal{Q}$ et on peut poser $m_\mathcal{P} = m_\mathcal{Q}$. De plus $\mathrm{N}_{L/K}(\mathcal{Q}B) = \mathcal{Q}^{[L:K]}$ (en effet, $\mathcal{Q}$ est principal, et la norme d'un élément a de K est $a^{[L:K]}$)

De plus on a

$$\prod_{\mathcal{P}'|\mathcal{Q}} \mathcal{Q}^{e_{\mathcal{P}'} m_{\mathcal{P}'}} = \mathrm{N}_{L/K}(\mathcal{Q})B = \mathcal{Q}^{[L:K]}B = \prod_{\mathcal{P}'|\mathcal{Q}} \mathcal{Q}^{e_{\mathcal{P}'} f_{\mathcal{P}'}}$$

et donc, en notant $g_\mathcal{Q}$ le nombre de diviseurs premiers de $\mathcal{Q}B$ et $f_\mathcal{Q}$ le degré résiduel en $\mathcal{P}$, on a $\mathcal{Q}^{g_\mathcal{Q} m_\mathcal{Q} e_\mathcal{Q}} = \mathcal{Q}^{g_\mathcal{Q} e_\mathcal{Q} f_\mathcal{Q}}$. En comparant ces formules, on obtient $m_\mathcal{P} = m_\mathcal{Q} = f_\mathcal{Q} = f_\mathcal{P}$.

Ne supposons plus que l'extension $L|K$ soit galoisienne pour démontrer (ιv). Soit $M|L$ une extension finie de corps telle que $M|K$ soit galoisienne. L'extension $M|L$ est alors galoisienne. Utilisons la transitivité de la norme et appliquons le résultat dans le cas galoisien. Soit $\mathcal{R}$ un idéal premier de M au dessus de $\mathcal{P}$. Pour lever toute ambiguïté, indiquons à quelle extension de corps le degré résiduel fait référence. On a

$$\mathcal{Q}^{f_\mathcal{R}(M/K)} = \mathrm{N}_{L/K}(\mathrm{N}_{M/L}(\mathcal{R})) = \mathrm{N}_{L/K}(\mathcal{P})^{f_\mathcal{P}(M/L)}.$$

Soient $k_2|k_1$ et $k_3|k_2$ deux extension finies de corps. Rappelons que le théorème de la *base télescopique* donne la formule suivante pour le degré de l'extension composée : $[k_3 : k_1] = [k_3 : k_2][k_2 : k_1]$. On en déduit la formule suivante pour les degrés résiduels $f_\mathcal{R}(M/K) = f_\mathcal{P}(L/K) f_\mathcal{R}(M/L)$, d'où la formule cherchée.

Dans le cas où $A = \mathbf{Z}$, $\mathrm{N}_{L/\mathbf{Q}}(I)$ est la *norme absolue* de I. On l'identifie à l'entier > 0 qui l'engendre comme idéal de $\mathbf{Z}$. Notons cet entier N_I.

Proposition 3. — *On a*

$$\mathrm{N}_{L/\mathbf{Q}}(I) = |B/I|\mathbf{Z}.$$

Démonstration. — Il suffit de le vérifier pour I premier car $|B/I_1I_2| = |B/I_1||B/I_2|$ lorsque I_1 et I_2 sont des idéaux premiers entre eux. On s'est donc ramené au cas où I est une puissance d'un idéal premier. Lorsque $I = \mathcal{P}$ est un idéal premier, $\mathcal{P}^k/\mathcal{P}^{k+1}$ est un espace vectoriel de dimension 1 sur $B/\mathcal{P}$. Par conséquent on a $|B/\mathcal{P}^k| = |B/\mathcal{P}|^k$. Il reste à vérifier le cas où $I = \mathcal{P}$ est premier. Cela résulte de la proposition 2 et de la formule

$$|B/\mathcal{P}| = p^{f_p}.$$

Remarque . — On généralise la notion de norme aux idéaux fractionnaires par la formule (où les fractions sont calculées dans le groupe des idéaux fractionnaires)

$$\mathrm{N}_{L/K}(I_1/I_2) = \mathrm{N}_{L/K}(I_1)/\mathrm{N}_{L/K}(I_2).$$

2. Discriminant d'un système

Reprenons les notations précédentes. Soit N un A-module libre de rang n contenu dans L.

Soit $v = (x_1, ..., x_n) \in N^n$. On appelle *discriminant* du système $(x_1, ..., x_n)$ l'élément de A donné par la formule :

$$D(v) = D(x_1, ..., x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j)),$$

où, par abus de notation, $\mathrm{Tr}_{L/K}(x_i x_j)$ est la matrice de $M_n(A)$ qui a pour coefficient (i, j) l'élément $\mathrm{Tr}_{L/K}(x_i x_j)$ de A.

Proposition 4. — *Soit $M \in \mathrm{M}_n(A)$. On a*

$$D(vM) = \det(M)^2 D(v).$$

Démonstration. — Posons $w = (y_1, ...y_n) = vM$. En prenant le déterminant, la proposition résulte de l'égalité :

$$\mathrm{Tr}_{L/K}(y_i y_j) = {}^{\mathrm{t}}M \mathrm{Tr}_{L/K}(x_i x_j) M.$$

Corollaire 1. — *Le discriminant de n'importe quelle base de N sur A ne dépend pas de la base à multiplication par un élément inversible de A près. En particulier l'idéal principal engendré par un tel discriminant ne dépend que de A et N.*

On appelle cet idéal principal *discriminant* de N sur A. On le note $\mathcal{D}_{N/A}$.

Ne supposons plus que N est libre sur A. Appelons *discriminant de N sur A* et notons $\mathcal{D}_{N/A}$ l'idéal engendré par les discriminants des systèmes formés par les bases de L sur K qui sont dans N. Cette définition est compatible à la précédente lorsque N est libre sur A. La proposition suivante permet de déterminer localement le discriminant.

Pour $\mathcal{Q}$ idéal maximal de A, on note $N_{\mathcal{Q}}$ le $A_{\mathcal{Q}}$-module formé par les quotients des éléments de N par les éléments de $A - \mathcal{Q}$.

Proposition 5. — *Soit $\mathcal{Q}$ un idéal premier de A. On a*

$$\mathcal{D}_{N/A} A_{(\mathcal{Q})} = \mathcal{D}_{N_{(\mathcal{Q})}/A_{(\mathcal{Q})}}.$$

Démonstration. — Une base de L sur K qui est contenue dans N est contenue dans $N_{(\mathcal{Q})}$. On a donc une inclusion

$$\mathcal{D}_{N/A} A_{(\mathcal{Q})} \subset \mathcal{D}_{N_{(\mathcal{Q})}/A_{(\mathcal{Q})}}.$$

Démontrons l'inclusion inverse. Soit $(x_1, ..., x_n)$ une base de $N_{(\mathcal{Q})}$ comme $A_{(\mathcal{Q})}$-module (il en existe puisque $A_{(\mathcal{Q})}$ est principal et donc $N_{(\mathcal{Q})}$ est libre sur $A_{(\mathcal{Q})}$). Il existe $s \in A - \mathcal{Q}$ tel

que $(sx_1, ..., sx_n) \in N^n$. Le n-uplet $(sx_1, ..., sx_n)$ est une base de L sur K qui est contenue dans N. On a

$$D(sx_1, ..., sx_n) = s^{2n} D(x_1, ..., x_n).$$

On a donc, puisque s est inversible dans $A_{(\mathcal{Q})}$,

$$\mathcal{D}_{N_{(\mathcal{Q})}/A_{(\mathcal{Q})}} \subset s^{-2n} \mathcal{D}_{N/A} A_{(\mathcal{Q})} = \mathcal{D}_{N/A} A_{(\mathcal{Q})}.$$

Corollaire 1. — *On a*

$$\mathcal{D}_{N/A} = \prod_{\mathcal{Q}} (\mathcal{D}_{N_{(\mathcal{Q})}/A_{(\mathcal{Q})}} \cap A),$$

où $\mathcal{Q}$ parcourt les idéaux premiers et non nuls de A.

Supposons désormais que l'extension $L|K$ est séparable.

Proposition 6. — *L'idéal $\mathcal{D}_{N/A}$ est non nul. Plus précisément le discriminant de toute base de L sur K est non nul.*
Démonstration. — On utilise d'abord le lemme suivant.

Lemme 1. — *Soit $(x_1, ..., x_n) \in N^n$. Soit $\bar{K}$ un corps algébriquement clos qui contient K. Notons σ_1, ..., σ_n les n plongements distincts de L dans $\bar{K}$ qui sont l'identité sur K. On a*

$$D(x_1, ..., x_n) = \det(\sigma_j(x_i))^2.$$

Démonstration. — Cela résulte de la formule (en utilisant la séparabilité de l'extension $L|K$) :

$$D(x_1, ..., x_n) = \det(\mathrm{Tr}_{L/K}(x_i x_j)) = \det(\sum_k (\sigma_k(x_i)\sigma_k(x_j)))$$

$$= \det((\sigma_k(x_i)) \det((\sigma_k(x_j)) = \det(\sigma_j(x_i))^2.$$

Cela achève de prouver le lemme.

Revenons à la démonstration de la proposition. Soit $(x_1, ..., x_n)$ une base de L sur K. On veut démontrer qu'on a

$$\det(\sigma_j(x_i)) \neq 0.$$

Supposons le contraire. Il existe une combinaison linéaire non triviale des σ_j qui annule tous les x_i et par conséquent tous les éléments de L puisque les x_i forment une base. Ecrivons cette combinaison linéaire à coefficients dans L sous la forme

$$\sum_{i=1}^{q} \alpha_i \sigma_i = 0,$$

avec $2 \leq q \leq n$. On peut supposer que les α_i sont tous non nuls et q est minimal. Soient x et y deux éléments de L^*. On a

$$\sum_{i=1}^{q} \alpha_i \sigma_i(x)\sigma_i(y) = \sum_{i=1}^{q} \alpha_i \sigma_i(xy) = 0.$$

En soustrayant à cette dernière identité l'égalité $\sigma_q(y)\sum_{i=1}^{q}\alpha_i\sigma_i(x)=0$, on obtient :

$$\sum_{i=1}^{q-1}\alpha_i\sigma_i(x)(\sigma_i(y)-\sigma_q(y))=0.$$

Comme cela est vérifié pour tout $x\in L$, on a obtenu une nouvelle combinaison linéaire des σ_i à coefficients dans L. Elle doit être triviale puisqu'on a choisi $q\geq 2$ minimal ou on a $q=2$. Dans chaque cas on en déduit que $\sigma_1(y)=\sigma_2(y)$ pour tout $y\in L$. Cela entraîne $\sigma_1=\sigma_2$, ce qui est absurde puisque les σ_i sont distincts.

Cela permet de démontrer une conséquence de la séparabilité à laquelle nous avons déjà fait référence.

COROLLAIRE 1. — *Lorsque qu'une extension de corps $L|K$ est séparable, la forme bilinéaire $L\times L\longrightarrow K$ donnée par $(x,y)\mapsto \mathrm{Tr}_{L/K}(xy)$est non dégénérée.*

3. Lien avec la ramification

Soient A un anneau de Dedekind de corps des fractions K. Soit $L|K$ une extension séparable finie. Notons B l'anneau des entiers de L. On pose $\mathcal{D}_{L/K}=\mathcal{D}_{B/A}$. Ce discriminant est bien défini puisque A et B sont déterminés par le fait que ce sont les anneaux des entiers de K et L.

On dit qu'un idéal premier $\mathcal{Q}$ de A *se ramifie* dans B s'il existe un idéal premier de B au dessus de $\mathcal{Q}$ qui n'est pas non ramifié.

Lorsque L est un corps de nombres, on peut considérer le cas $A=\mathbf{Z}$. Le discriminant $\mathcal{D}_L=\mathcal{D}_{L/\mathbf{Q}}$ est le *discriminant absolu* de L. Puisque c'est un idéal de $\mathbf{Z}$, on est souvent amené a considérer l'entier >0 qui l'engendre. On note souvent cet entier $|\mathcal{D}_L|$.

Revenons-en à une situation plus générale. Le théorème suivant fait le lien entre la ramification et la notion de discriminant.

THÉORÈME 1. — *Soit A un anneau de Dedekind de corps de fractions K. Soit L/K une extension finie et séparable. Notons B la clôture intégrale de A dans L. Les idéaux premiers de A qui se ramifient dans B coïncident avec les idéaux premiers de A qui divisent $\mathcal{D}_{B/A}$. En particulier il n'y a qu'un nombre fini d'idéaux premiers de A qui sont ramifiés dans B.*

Démonstration. — Cela se vérifie localement puisque le discriminant et la ramification peuvent se déterminer en localisant les anneaux d'après la proposition 2 et le théorème de décomposition en produit d'idéaux premiers dans les anneaux de Dedekind.

Supposons donc que A soit un anneau de valuation discrète. Notons $\mathcal{Q}$ son idéal maximal. L'anneau A est principal. Cela entraîne que B est libre sur A.

Supposons qu'il existe un idéal maximal $\mathcal{P}$ de B qui soit ramifié. Il existe $x\in B-\mathcal{Q}B$ et $k>1$ tel que $x^k\in\mathcal{Q}B$. La classe $\bar{x}$ de x dans $B/\mathcal{Q}$ est un élément non nul de $B/\mathcal{Q}$. Ce dernier est un $A/\mathcal{Q}$-espace vectoriel. On peut compléter $\bar{x}$ en une base $(\bar{x}_1=\bar{x},\bar{x}_2,...,\bar{x}_n)$de

$B/\mathcal{Q}$. Un représentant $(x_1 = x, x_2, ..., x_n)$ de cette base dans B^n donne une base de B comme A-module (cela se voit en identifiant B à A^n et en remarquant que la réduction modulo $\mathcal{Q}$ de $\det(x_1, ..., x_n)$ dans la base canonique de A^n est non nulle ; ce déterminant est donc inversible).

Soit $x_0 \in B$. Puisque B est un A-module libre, la trace de l'endomorphisme de $B/\mathcal{Q}$ donné par $y \mapsto x_0 y$ est l'image dans $A/\mathcal{Q}$ de la trace de l'endomorphisme $y \mapsto x_0 y$. On a $(x_1 x_i)^k \in \mathcal{Q}$ pour tout i. L'endomorphisme de $B/\mathcal{Q}$ donné par $y \mapsto y(x_1 x_i)$ est donc nilpotent. Sa trace est donc nulle. Le déterminant $\det(\mathrm{Tr}(x_i x_j))$ est donc dans $\mathcal{Q}$. On a donc $\mathcal{D}_{B/A} \subset \mathcal{Q}$.

Réciproquement, supposons que tout idéal premier de B divisant $\mathcal{Q}$ est non ramifié. On a alors un isomorphisme de A-modules

$$B/\mathcal{Q} \simeq B/\mathcal{P}_1 \oplus ... \oplus B/\mathcal{P}_n,$$

où $\mathcal{P}_1$,..., $\mathcal{P}_n$ sont les idéaux premiers de B qui divisent $\mathcal{Q}$. Soient β_1, β_2,...β_n des bases des $A/\mathcal{Q}$ espaces vectoriels $B/\mathcal{P}_1$,...,$B/\mathcal{P}_n$. Elles définissent, par l'isomorphisme ci-dessus, une base β de $B/\mathcal{Q}$. Dans cette base la matrice de l'endomorphisme $B/\mathcal{Q} \longrightarrow B/\mathcal{Q}$ qui à y associe $x_0 y$ est une matrice par blocs ($x_0 \in B$). Le discriminant du système formé par la base β est donc le produit des discriminants $\mathcal{D}_i$ des systèmes formés par les β_i. Chacun de ces discriminants est non nul (cela résulte de la proposition 6, puisque les extensions de corps résiduels sont séparables). Leur produit est donc non nul.

La base β est la réduction modulo $\mathcal{Q}$ d'une base de B sur A (voir ci-dessus). La réduction modulo $\mathcal{Q}$ du discriminant du système formé par cette base est donc égal au discriminant du système formé par la base β ; ce dernier discriminant est non nul. Le discriminant de B/A n'est donc pas contenu dans $\mathcal{Q}$. Cela achève la démonstration du théorème.

Remarque . — Pour démontrer qu'un idéal premier $\mathcal{Q}$ de A est non ramifié dans une extension $L|K$ il suffit donc de trouver un système d'éléments de B de discriminant premier à $\mathcal{Q}$. On va voir ci-dessous une méthode qui permet parfois de trouver de tels systèmes lorsque que l'extension est donnée par un polynôme explicite.

4. Exemple de calcul de discriminant

Soit K un corps et $L = K(x)$ ($x \in L$) une extension séparable de K de degré n. Soit P le polynôme minimal de x.

Proposition 7. — *Le discriminant du système* $(1, x, x^2, ..., x^{n-1})$ *est donné par la formule :*

$$D(1, x, ..., x^{n-1}) = (-1)^{n(n-1)/2} N_{L/K}(P'(x)).$$

Démonstration. — Notons x_1, x_2,..., x_n les conjugués de x. Utilisons le lemme 1. On a

$$D(1, x, ..., x^{n-1}) = (\det(x_i^j))^2,$$

où i parcourt les entiers entre 1 et n et j parcourt les entiers entre 0 et $n-1$. Ce déterminant est un déterminant de Van der Monde. Il est égal à

$$(-1)^{n(n-1)/2} \prod_{i_1 \neq i_2} (x_{i_1} - x_{i_2}).$$

En dérivant l'identité

$$P(X) = \prod_i (X - x_i),$$

on obtient la formule

$$P'(x_i) = \prod_{i' \neq i} (x_i - x_{i'}).$$

Or on a

$$N_{L/K}(P'(x_i)) = \prod_{i'} (P'(x_{i'})) = \prod_{i_1 \neq i_2} (x_{i_1} - x_{i_2}).$$

Cela nous donne la formule cherchée.

COROLLAIRE 1. — *Lorsque x est un élément de B (i.e. c'est un élément entier de L), le discriminant $\mathcal{D}_{L/K}$ contient l'idéal principal de A engendré par $N_{L/K}(P'(x))$.*
Démonstration. — Cela résulte immédiatement du fait que B contient $A[x]$ et donc le système $(1, x, x^2, ..., x^{n=1}) \in B^n$ est une base de L comme K-espace vectoriel.

5. Compléments

Reprenons la situation suivante. Soit K un corps et $L = K(x)$ $(x \in L)$ une extension séparable de K de degré n. Soit P le polynôme minimal de x. Supposons que x soit entier sur A. Notons A et B les anneaux des entiers de K et L. Supposons que ce soient des anneaux de Dedekind.

PROPOSITION 8. — *On a*

$$D(1, x, ..., x^{n-1})B \subset A[x] \subset B.$$

Démonstration. — La deuxième inclusion est évidente. Démontrons la première.

Lemme 2. — *Soit $\mathcal{Q}$ un idéal maximal de A. On a*

$$D(1, x, ..., x^{n-1})B_{(\mathcal{Q})} \subset A_{(\mathcal{Q})}[x].$$

Démonstration. — Le $A_{(\mathcal{Q})}$-module $B_{(\mathcal{Q})}$ est libre car $A_{(\mathcal{Q})}$ est principal. Considérons-en une base $(x_1, ..., x_n)$. Ecrivons la matrice M de passage de cette base à la base de L comme K-espace vectoriel donnée par $(1, ..., x^{n-1})$. Notons $a_{i,j}$ les coefficients de M. Ce sont des

éléments de A. Le déterminant d de cette matrice est non nul. Notons $b_{j,i}$ les coefficients de M^{-1}. Ce sont des éléments de $\frac{1}{d}A$. On a donc $dB_{(\mathcal{Q})} \subset A_{(\mathcal{Q})}[x]$. On en déduit

$$D(1, x, ..., x^{n-1})B_{(\mathcal{Q})} = d^2 D(x_1, ..., x_n)B_{(\mathcal{Q})} = (dB_{(\mathcal{Q})})(dD(x_1, ..., x_n)) \subset A_{(\mathcal{Q})}[x].$$

Cela prouve le lemme.

Pour déduire la proposition du lemme 2, utilisons la formule

$$M = \cap_{\mathcal{Q}} A_{(\mathcal{Q})} M,$$

qui est valide pour tout A-sous-module M contenu dans un K-espace vectoriel de dimension finie. Par application à $M = A[x]$ on obtient la proposition.

Proposition 9. — *Soient L_1 et L_2 des extensions finies et séparables de K qui sont contenues dans un corps M et qui sont linéairement disjointes (i.e. le sous-corps $L = L_1 L_2$ de M engendré par L_1 et L_2 est de degré $[L_1 : K][L_2 : K]$ sur K). Notons B_1, B_2 et B les clôtures intégrales de A dans L_1, L_2 et L. On a*

$$\mathcal{D}_{L_2/K} B \subset B_1 B_2.$$

Démonstration. — On le vérifie idéal maximal par idéal maximal en localisant. Supposons donc que A soit un anneau de valuation discrète.

Soit $(y_1, ..., y_n)$ une base de B_2 sur A et donc une base de L sur L_1. Notons $(y'_1, ..., y'_n)$ la base duale de L_2 sur K vis-à-vis de la forme bilinéaire $(x, y) \mapsto \mathrm{Tr}_{L_1/K}(xy)$. C'est aussi une base de L sur L_1. Elle est dans $D(y_1, ..., y_n)^{-1} B_2 = \mathcal{D}^{-1}_{L_2/K} B_2$ puisque les matrices $\mathrm{Tr}_{L_2/K}(y_i y_j)$ et $\mathrm{Tr}_{L_2/K}(y'_i y'_j)$ sont inverses l'une de l'autre. Soit $x \in B$. Il s'écrit $\sum_i \alpha_i y'_i$ avec $\alpha_i \in L$. On a

$$\mathrm{Tr}_{L/L_1}(xy_i) = \sum_j \alpha_j \mathrm{Tr}_{L/L_1}(y'_j y_i) = \alpha_i$$

On a donc $\alpha_i = \mathrm{Tr}_{L/L_1}(xy_i) \in B_1$. On a donc

$$x = \sum_i \mathrm{Tr}_{L/L_1}(xy_i) y'_i \in \sum_i B_1 y'_i \subset \mathcal{D}^{-1}_{L_2/K} B_2 B_1.$$

Cela démontre le résultat cherché.

Corollaire 1. — *Supposons de plus que les discriminants $\mathcal{D}_{L_2/K}$ et $\mathcal{D}_{L_1/K}$ soient premiers entre eux. On a*

$$B = B_1 B_2.$$

De plus on a

$$\mathcal{D}_{B/A} = \mathcal{D}^{[L_2:K]}_{B_1/A} \mathcal{D}^{[L_1:K]}_{B_2/A}.$$

Démonstration. — On a $B_1 B_2 \subset B$ par définition de B.

Démontrons l'inclusion inverse. On a, d'après la proposition 8,

$$\mathcal{D}_{L_2/K}B + \mathcal{D}_{L_1/K}B \subset B_1B_2.$$

On conclut immédiatement puisque, par hypothèse, on a $B = \mathcal{D}_{L_2/K}B + \mathcal{D}_{L_1/K}B$.

Venons-en à la deuxième assertion. Par localisation on se ramène au cas où A est un anneau de valuation discrète. Choisissons des bases $(x_i)_{i=1,\dots,[L_1:K]}$ et $(y_j)_{j=1,\dots,[L_2:K]}$ de B_1 et B_2 sur A. Alors la famille (x_iy_j) forme une base de B sur A puisqu'on a $B = B_1B_2$. La matrice

$$\mathrm{Tr}_{L/K}(x_ix_{i'}y_jy_{j'}) = \mathrm{Tr}_{L_1/K}(x_ix_{i'})\mathrm{Tr}_{L_2/K}(y_jy_{j'})$$

est le produit tensoriel des matrices $\mathrm{Tr}_{L_1/K}(x_ix_{i'})$ et $\mathrm{Tr}_{L_2/K}(y_jy_{j'})$. En utilisant la formule donnant le déterminant du produit tensoriel de deux matrices on obtient le résultat.

Remarque . — En pratique ce corollaire est très utile pour déterminer les anneaux des entiers des corps de nombres.

La deuxième assertion du corollaire pourrait se déduire de la formule des tours :

$$\mathcal{D}_{M/K} = \mathcal{D}_{L/K}^{[M:L]}N_{L/K}(\mathcal{D}_{M/L}),$$

où $L|K$ et $M|L$ sont des extensions finies et où $N_{L/K}$ est la norme d'un idéal de L (voir la leçon suivante).