I. Discriminant et ramification.

$$(1)\quad \begin{cases} .\ K = \bigcup_{\alpha\in I} K_\alpha. \\ .\ \text{Si } \alpha \text{ et } \beta \text{ appartiennent à } I, \text{ le corps composé } K_\alpha\,.\,K_\beta \text{ appartient} \\ \quad \text{à l'ensemble } \{K_\gamma\}_{\gamma\in I}. \end{cases}$$

Il existe toujours au moins un sous-ensemble I, $\mathscr{F}$ lui-même. Lorsque D est dénombrable, nous pouvons prendre $\mathbf{N}$ comme sous-ensemble I:

$$K = \bigcup_{n\in\mathbf{N}} K_n$$

les corps K_n étant emboîtés.

Soit L une extension finie séparable de K. Si θ est un générateur de L/K, posons $L_\alpha = K_\alpha(\theta)$. *Nous ne considèrerons par la suite que les indices* α *pour lesquels* $[L_\alpha : K_\alpha] = [L : K] = n$.

Enfin les anneaux d'entiers de K, L, K_α et L_α seront notés respectivement A, B, A_α et B_α.

I. Discriminant et ramification.

1. *Discriminant.*

Définition 1.

Nous appellerons discriminant de l'extension L/K *l'idéal* Δ *de* A *engendré par les discriminants des bases de* L/K *à éléments dans* B.

Puisque L/K est séparable, Δ est un idéal entier non nul de A.

Proposition 1.

Soit I *un sous-ensemble de* $\mathscr{F}$ *possédant la propriété* (1). *Notons* Δ *le discriminant de* L/K, *et* Δ_α *celui de* L_α/K_α. *Alors*

$$\Delta = \bigcup_{\alpha\in I} \Delta_\alpha\,.$$

En effet, un élément de Δ est combinaison linéaire finie, à coefficients dans A, de discriminants de bases de L/K à éléments dans B: c'est donc un élément d'un Δ_α.

Inversement, puisque $[L_\alpha : K_\alpha] = [L : K]$, toute base de L_α/K_α à coefficients dans B_α est une base de L/K à coefficients dans B, et Δ contient $\bigcup_{\alpha\in I} \Delta_\alpha$.

2. *Ramification.*

Remarquons que dans l'anneau A, tout idéal premier $\mathscr{P}$ est maximal. Le localisé $A_{\mathscr{P}}$ est un anneau de valuation, donc, à $\mathscr{P}$, on peut associer une valuation v sur K, de groupe des valeurs Γ_v. Comme l'extension L/K est finie, il n'existe dans B qu'un nombre fini d'idéaux premiers au-dessus de $\mathscr{P}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$ (cf. Bourbaki [3] § 8). A chaque $\mathfrak{p}_i$ est associée une valuation v_i de L qui prolonge v; le groupe Γ_{v_i} des valeurs de v_i admet Γ comme sous-groupe.

Définition 2.

Soit $\mathscr{P}$ un idéal premier de A. Nous dirons que $\mathscr{P}$ se ramifie dans l'extension L/K si l'un des indices $e_i = (\Gamma_{v_i}:\Gamma_v)$ est strictement supérieur à 1.

Remarque: si $f_i = [B/\mathfrak{p}_i:A/\mathscr{P}]$, l'inégalité $\sum_{i=1}^{l} e_i f_i \leqq n$ est encore vraie. (cf. Bourbaki [3]).

Proposition 2.

Pour qu'un idéal premier $\mathscr{P}$ de A se ramifie dans l'extension L/K, il faut et il suffit qu'il contienne l'idéal discriminant Δ.

La démonstration de cette proposition repose sur le principe bien connu de la propagation de la non-ramification vers le haut. On peut énoncer ce principe de la manière suivante:

soient k le corps des quotients d'un anneau de Dedekind, M et N deux extensions algébriques finies séparables de k, linéairement disjointes sur k. Si $\mathscr{P}$ est un idéal premier de k non ramifié dans l'extension M/k, tout idéal premier $\mathfrak{p}$ de N qui divise $\mathscr{P}$ est non ramifié dans l'extension $M\,.\,N/N$.

Posons $\mathscr{P}_\alpha = \mathscr{P} \cap A_\alpha$, et notons v^α (resp v_i^α) la restriction de v (resp v_i) à K_α (resp L_α).

Supposons $\mathscr{P}$ ramifié dans L/K: il existe un indice $i \in [1, l]$ tel que $(\Gamma_{v_i}:\Gamma_v) > 1$. On ne peut trouver $\alpha_0 \in I$ tel que $(\Gamma_{v_i^{\alpha_0}}:\Gamma_{v^{\alpha_0}}) = 1$; sinon, la « propagation de la non-ramification vers le haut », et l'égalité $K = \bigcup_{\substack{\beta \in I \\ \beta \geqq \alpha_0}} K_\beta$ permettraient de conclure que $(\Gamma_{v_i}:\Gamma_v) = 1$. Donc pour tout $\alpha \in I$, $\mathscr{P}_\alpha$ est ramifié dans L_α/K_α : $\mathscr{P}_\alpha$ contient le discriminant Δ_α de L_α/K_α, et $\mathscr{P}$ contient $\Delta = \cup\, \Delta_\alpha$.

Inversement, si $\mathscr{P}$ contient Δ, pour tout $\alpha \in I$, on a les inclusions:

$$\mathscr{P}_\alpha \supset \Delta \cap A_\alpha \supset \Delta_\alpha \,.$$

Donc $\mathscr{P}_\alpha$ se ramifie dans L_α/K_α. Par « propagation de la non-ramification vers le haut », il existe au moins un indice i tel que pour tout α, $(\Gamma_{v_i}\alpha : \Gamma_v\alpha) > 1$. Pour cette valeur de i, $(\Gamma_{v_i} : \Gamma_v) > 1$, et $\mathscr{P}$ est ramifié dans L/K.

II. Bases entières.

1. *Exemple*

$$\begin{tikzcd}[arrows=dash]
 & & & L = K(\sqrt[3]{3}) \arrow[d] \\
 & & \mathbf{Q}(j, \zeta_n, \sqrt[3]{3}) \arrow[ur] \arrow[d] & K \\
 & \mathbf{Q}(j, \sqrt[3]{3}) \arrow[ur] \arrow[d] & \mathbf{Q}(j, \zeta_n) \arrow[ur] & \\
 & \mathbf{Q}(j) \arrow[ur] & & \\
 \mathbf{Q} \arrow[ur] \arrow[uur] & & &
\end{tikzcd}$$

Soit K le corps obtenu en adjoignant à $\mathbf{Q}$, j et toutes les racines 5^n-ièmes de l'unité; soit ζ_n une racine primitive 5^n-ième de l'unité. Le corps K, extension cyclotomique de $\mathbf{Q}$, est une extension abélienne de $\mathbf{Q}$. Mais $\mathbf{Q}(j, \sqrt[3]{3})/\mathbf{Q}$ n'est pas abélienne; donc $L = K(\sqrt[3]{3})$ est une extension de degré 3 de K.

Les extensions $\mathbf{Q}(j, \sqrt[3]{3}, \zeta_n)/\mathbf{Q}(j, \zeta_n)$ sont des extensions de Kummer. Les seuls idéaux qui peuvent se ramifier sont ceux qui divisent 3. La théorie de Kummer (cf. Hecke [6]) permet de calculer leur participation au discriminant de L_n/K_n; on obtient: $\Delta_n = 3^4 A_n$. Mais comme $Z[j]$ est principal, $\mathbf{Q}(j, \sqrt[3]{3})/\mathbf{Q}(j)$ admet une base entière, $\{\lambda, \mu, \nu\}$, de discriminant 3^4. Donc L/K admet $\{\lambda, \mu, \nu\}$ comme base entière.

2. *Caractérisation des A-modules B de type fini.*

Proposition 3.

A et B étant définis au paragraphe précédent, les propositions suivantes sont équivalentes :

a — B est un A-module de type fini.