Université de Paris-Sud
2006-2007

Feuille 1

1. Extensions quadratiques

Soit K une extension quadratique de $\mathbb{Q}$. On note $\mathcal{O}$ la clôture intégrale de $\mathbb{Z}$ dans K :

$$\mathcal{O} = \{x \in K, x \text{ solution d'un polynôme unitaire à coefficients dans } \mathbb{Z}\}.$$

1.0 Montrer que K est de la forme $\mathbb{Q}(\sqrt{\Delta})$ avec $\Delta \in \mathbb{Z} - \{0, 1\}$ sans facteur carré.
1.1 Pour $z = x + y\sqrt{\Delta} \in \mathbb{Q}(\sqrt{\Delta})$, $\bar{z} = x - y\sqrt{\Delta}$. Montrer que

$$z \in \mathcal{O} \text{ si et seulement si } \begin{cases} N_{K/\mathbb{Q}}(z) = N(z) := z\bar{z} \in \mathbb{Z} \\ \mathrm{T}_{K/\mathbb{Q}}(z) = T(z) := z + \bar{z} \in \mathbb{Z} \end{cases}$$

1.2 En déduire $\mathcal{O}$.

2. Norme et Trace

Soient $A \subset B$ des anneaux intègres avec B un A-module libre de rang n. L'élément $\beta \in B$ définit par multiplication une application linéaire $B \to B$, $x \mapsto \beta x$. Le déterminant (resp. la trace) de cette application linéaire est noté $\mathrm{Nm}_{B/A}\beta$ (resp. $\mathrm{Tr}_{B/A}\beta$).

1. Observer que $\mathrm{Nm}_{B/A}\beta\beta' = \mathrm{Nm}_{B/A}\beta \mathrm{Nm}_{B/A}\beta'$.
2. Soient L/K une extension galoisienne de corps de degré n et $y \in L$. Soient $f(X)$ le polynôme minimal de y sur K et $y_1 = y, y_2, \ldots, y_m$ les racines de $f(X)$. Montrer que

$$\mathrm{Tr}_{L/K}\, y = r(y_1 + \cdots + y_m), \quad \mathrm{Nm}_{L/K}\, y = (y_1 \cdots y_m)^r$$

   où $r = [L : K[y]] = n/m$ (on pourra commencer par traiter le cas $r = 1$).
3. En déduire que si L/K est séparable de degré n et si $\{\sigma_1, \ldots, \sigma_n\}$ sont les différents K-plongements de L dans une clôture algébrique de L/K, alors, on a

$$\forall y \in L, \quad \mathrm{Tr}_{L/K}\, y = \sum_{i=1}^{n} \sigma_i(y) \quad \text{et} \quad \mathrm{Nm}_{L/K}(y) = \prod_{i=1}^{n} \sigma_i(y).$$

3. Discriminant

Soient $A \subset B$ des anneaux avec B libre de rang m comme A-module. Soit $\{\beta_1, \ldots, \beta_m\}$ des éléments de B. Le *discriminant de la famille* $\{\beta_1, \ldots, \beta_m\}$ est

$$\mathrm{disc}(\{\beta_1, \ldots, \beta_m\}) := \det(\mathrm{Tr}_{B/A}(\beta_i\beta_j)).$$

1. Montrer que si l'on pose $\mathrm{disc}(B/A) := \mathrm{disc}(\{\text{base de } B/A\})$ on obtient un élément bien défini de $A/(A^\times)^2$.

   Dans le cas particulier où $A = \mathbb{Z}$ et B l'anneau d'entiers $\mathcal{O}_K$ d'un corps de nombres K, le discriminant $\mathrm{disc}(B/\mathbb{Z})$ est un élément bien défini de $\mathbb{Z}$, que l'on appelle *discriminant absolu de* $K/\mathbb{Q}$ et que l'on note $d_{K/\mathbb{Q}}$ ou $d_{\mathcal{O}_K/\mathbb{Z}}$ ou même d_K.

2. Supposons $A = \mathbb{Z}$. Soit N le sous-A-module de B engendré par $\{\gamma_1, \ldots, \gamma_m\}$. Montrer que si le module N est d'indice fini dans B alors

$$\operatorname{disc}(\{\gamma_1, \ldots, \gamma_m\}) = (B : N)^2 \operatorname{disc}(B/\mathbb{Z})$$

3. Soit$K = \mathbb{Q}[x]$ un corps de nombres de degré n avec α un entier algébrique (justifier...). Montrer que si $d = \operatorname{disc}(1, x, \ldots, x^{n-1})$ on a

$$\mathbb{Z}[x] \subset \mathcal{O}_K \subset \frac{1}{d}\mathbb{Z}[x].$$

4. Soit $K = \mathbb{Q}[\alpha]$ un corps de nombres de degré n avec α un entier algébrique. Montrer que si $\operatorname{disc}(\{1, \alpha, \ldots, \alpha^{n-1}\})$ est sans facteur carré, alors

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \quad \text{et} \quad d_K = \operatorname{disc}(\{1, \alpha, \ldots, \alpha^{n-1}\}).$$

5. Soit L/K une extension finie séparable de degré n. Soit $\sigma_1, \ldots, \sigma_n$ les K-homomorphismes distincts de L dans une clôture algébrique de L. Alors pour toute base $\beta_1, \ldots, \beta_n$ de L sur K, montrer que

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \det(\sigma_i \beta_j)^2.$$

6. Soit $L = K[\beta]$ et $f(X)$ le polynôme minimal de β sur K. Supposons que $f(X)$ se factorise sous la forme $f(X) = \Pi(X - \beta_i)$ sur une clotûre algébrique de L. Montrer que

$$\operatorname{disc}(1, \beta, \ldots, \beta^{n-1}) = \prod_{i<j} (\beta_i - \beta_j)^2 = (-1)^{n(n-1)/2} \operatorname{Nm}_{L/K}(f'(\beta)).$$

   Ce nombre est appelé le *discriminant de* f et noté $\operatorname{disc}(f)$. On pourrait également le définir comme le résultant de f et f'.

4. Application

Soient k un corps, $a, b \in k$, $n \in \mathbb{N}\backslash\{0, 1\}$ et $P = X^n + aX + b$. On suppose que P est irréductible et **séparable**.

1. Montrer que

$$\operatorname{disc}(P) = (-1)^{\frac{n(n-1)}{2}} \left(n^n b^{n-1} + (-1)^{n+1}(n-1)^{n-1} a^n\right).$$

2. Cas particulier où $n = 2$ et $n = 3$.
3. On suppose $n = 3$. Soit x une racine de P dans une clôture algébrique $\overline{k}$ de k et K le corps de décomposition de $k(x)$ dans $\overline{k}$. Montrer que le groupe de Galois $\operatorname{Gal}(K/k)$ est soit isomorphe au groupe symétrique S_3 soit au groupe alterné A_3 et que

$$k(x) = K \iff [K : k] = 3 \iff \operatorname{disc}(P) \text{ est un carré dans } k.$$

4. Déterminer l'anneau des entiers de $\mathbb{Q}[x]$ où x est une racine du polynôme $X^3 - X - 1$ et le groupe de Galois de son corps de décomposition.
5. Calculer le discriminant d'une extension quadratique de $\mathbb{Q}$.

5. Extensions cyclotomiques

1. Soient $K/\mathbb{Q}$ un corps de nombres et $\mathcal{O}_K$ la clôture intégrale de $\mathbb{Z}$ dans K, *i.e.* l'anneau des entiers de $\mathcal{O}_K$. C'est un anneau de Dedekind. Soient L une extension finie séparable de degré n d'un corps de nombres K et B la clôture intégrale de $\mathcal{O}_K$ dans L. Soient $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ sa décomposition en idéaux premiers dans B. Soit $f_i = [B/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$, $1 \leq i \leq g$ le degré d'inertie. On rappelle que

$$\sum_{i=1}^{g} e_i f_i = n.$$

   Dans la suite on note $r \geq 1$, p premier, ζ une racine primitive p^r-ième de l'unité, $K = \mathbb{Q}[\zeta]$ et $\mathcal{O}_K$ son anneau d'entiers.

2. Montrer que K est une extension normale et que l'on a un morphsime injectif du groupe de Galois G_K vers le groupe $(\mathbb{Z}/p^r\mathbb{Z})^\times$ des inversibles de $\mathbb{Z}/p^r$. Montrer également que $\mathbb{Z}[\zeta] \subset \mathcal{O}_K$ et que $[\mathbb{Q}[\zeta] : \mathbb{Q}] \leq \varphi(p^r) = p^{r-1}(p-1)$.
3. On appelle *polynôme cyclotomique* Φ_{p^r} le polynôme $\prod_{\zeta \in \mu_{p^r} \text{primitive}} (X - \zeta)$. Montrer que

$$\Phi_{p^r} = \prod_{[i] \in (\mathbb{Z}/p^r\mathbb{Z})^\times} (X - \zeta^i) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}.$$

4. Soit ξ une autre racine primitive p^r-ième de l'unité. Montrer que $\frac{1-\zeta}{1-\xi}$ est une unité de $\mathcal{O}_K$ (*i.e.* est inversible dans $\mathcal{O}_K$).
5. Soit $\pi = 1 - \zeta$. En calculant $\Phi_{p^r}(1)$, montrer l'égalité d'idéaux dans $\mathcal{O}_K$, $(p) = (\pi)^{\varphi(p^r)}$. En déduire que le corps $\mathbb{Q}[\zeta]$ est de degré $\varphi(p^r)$ sur $\mathbb{Q}$ et que l'élément π est premier dans $\mathcal{O}_K$.
6. Calculer la valeur absolue du discriminant $|\operatorname{disc}(\mathbb{Z}[\zeta] : \mathbb{Z})| = \operatorname{Nm}(\Phi'_{p^r}(\zeta))$ (on pourra commencer par $r = 1$ avant de traiter le cas général). En déduire que $\operatorname{disc}(\mathcal{O}_k/\mathbb{Z})$ est une puissance de p et que $p^M \mathcal{O}_K \subset \mathbb{Z}[\zeta]$ pour tout entier M suffisamment divisible.
7. Montrer que $\mathbb{Z}[\zeta] + \pi^m \mathcal{O}_K = \mathcal{O}_K$ pour $m \geq 1$. En déduire que l'anneau des entiers de $\mathbb{Q}[\zeta]$ est $\mathbb{Z}[\zeta]$ et que le discriminant de $\mathcal{O}_K$ sur $\mathbb{Z}$ est de valeur absolue $p^{p^{r-1}(pr-r-1)}$.
8. Soient K, L des extensions finies de $\mathbb{Q}$ vérifiant

$$[KL : \mathbb{Q}] = [K : \mathbb{Q}][L : \mathbb{Q}].$$

   Soit $d = pgcd(d_{K/\mathbb{Z}}, d_{L/\mathbb{Z}})$. Montrer que

$$\mathcal{O}_{KL} \subset d^{-1} \mathcal{O}_K \cdot \mathcal{O}_L$$

   (Considérer $\{\alpha_1, \ldots, \alpha_m\}$ (resp. $\{\beta_1, \ldots, \beta_n\}$) une base intégrale de K sur $\mathbb{Q}$ (resp. de L sur $\mathbb{Q}$). Soit $\gamma \in \mathcal{O}_{KL}$. On pourra écrire $\gamma = \sum \frac{a_{i,j}}{r} \alpha_i \beta_j$ avec r minimal et montrer que r divise d).
9. sous les hypothèses précédentes et si $d = 1$, montrer que

$$d_{KL/\mathbb{Z}} = d_{K/\mathbb{Z}}^{[L:\mathbb{Q}]} d_{L/\mathbb{Z}}^{[K:\mathbb{Q}]}.$$

   En déduire que

$$|\operatorname{disc}(\mathbb{Z}[\zeta_n]/\mathbb{Z})| = \frac{n^{\varphi(n)}}{\Pi_{p|n} p^{\varphi(n)/(p-1)}}.$$

10. Soit $p \neq 2$. On définit le symbole quadratique pour $n \in \mathbb{Z}$, par 0 si $(n,p) \neq 1$; et si $(n,p) = 1$ on pose

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ est un carré} \quad \mod p \\ -1 & \text{sinon} \end{cases}$$

Soit ζ une racine primitive p-ième de l'unité et $S = \sum_{v=0}^{p-1} \left(\frac{v}{p}\right)\zeta^v$. Montrer que $S^2 = \left(\frac{-1}{p}\right)p$. En déduire que toute extension quadratique de $\mathbb{Q}$ est contenue dans une extension cyclotomique.