

Corrigé du DS du lundi 02 mars 2008.

Exercice

Dans ce qui suit, A désigne un anneau de Dedekind de corps des fractions $K = Fr(A)$. L'objet de l'exercice est d'établir la propriété suivante :

(★) Si I est un idéal fractionnaire de A , il existe $(\alpha, \beta) \in K^2$ tels qu'on ait : $I = \alpha A + \beta A$.

On rappelle que tout idéal fractionnaire non nul I de A s'écrit de façon unique comme un produit fini :

$$I = \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{\nu_{\mathfrak{p}}(I)}$$

où $\mathfrak{p}$ parcourt l'ensemble des idéaux $\mathcal{P}$ premiers non nuls de A et où les entiers relatifs $\nu_{\mathfrak{p}}(I)$ sont presque tous nuls. En particulier, si $I = \alpha A$ est principal (avec $\alpha \in K^\times$), on pose $\nu_{\mathfrak{p}}(\alpha) = \nu_{\mathfrak{p}}(\alpha A)$.

1. Si I et J sont deux idéaux fractionnaires non nuls de A , vérifier qu'on a pour tout $\mathfrak{p} \in \mathcal{P}$:

$$\nu_{\mathfrak{p}}(I + J) = \min \{ \nu_{\mathfrak{p}}(I), \nu_{\mathfrak{p}}(J) \} .$$

Rappelons que si I et J sont deux idéaux fractionnaires non nuls de A , on a l'équivalence

$$I \subset J \Leftrightarrow \forall \mathfrak{p} \in \mathcal{P}, \nu_{\mathfrak{p}}(I) \geq \nu_{\mathfrak{p}}(J), \quad (1)$$

ceci découlant du fait que $I \subset J$ si et seulement si $IJ^{-1} \subset A$. Comme $I + J$ est le plus petit idéal contenant I et J , la propriété que $\nu_{\mathfrak{p}}(I + J) = \min \{ \nu_{\mathfrak{p}}(I), \nu_{\mathfrak{p}}(J) \}$ pour tout $\mathfrak{p} \in \mathcal{P}$ découle immédiatement de (1).

2. Soit maintenant I un idéal entier non nul (i.e. $0 \neq I \subset A$), et α un élément non nul de I .
 - (a) Montrer qu'il existe un entier naturel r et, pour $1 \leq i \leq r$, des idéaux premiers $\mathfrak{p}_i$ ainsi que des entiers $n_i \geq m_i \geq 0$ tels qu'on ait :

$$I = \prod_{i=1}^r \mathfrak{p}_i^{m_i} \quad \text{et} \quad \alpha A = \prod_{i=1}^r \mathfrak{p}_i^{n_i} .$$

L'inclusion $\alpha A \subset I$ se traduit, en utilisant à nouveau (1), par la propriété

$$\forall \mathfrak{p} \in \mathcal{P}, \nu_{\mathfrak{p}}(\alpha A) \geq \nu_{\mathfrak{p}}(I). \quad (2)$$

Par ailleurs, les idéaux αA et I étant entiers, leurs valuations $\mathfrak{p}$ -adiques sont des entiers naturels presque tous nuls. En baptisant $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ les idéaux maximaux $\mathfrak{p}$ pour lesquels $\nu_{\mathfrak{p}}(I)$ est non nul, et m_i (resp. n_i) la valuation $\mathfrak{p}_i$ -adique de I (resp. αA), on obtient le résultat demandé.

- (b) Pour chaque $1 \leq i \leq r$, on fait choix d'un élément $b_i \in \mathfrak{p}_i^{m_i} \setminus \mathfrak{p}_i^{m_i+1}$. Prouver qu'il existe alors un $\beta \in I$ qui vérifie les r congruences :

$$\beta \equiv b_i \pmod{\mathfrak{p}_i^{m_i+1}}, \text{ pour } 1 \leq i \leq r.$$

C'est le lemme chinois : les idéaux $\mathfrak{p}_i^{m_i+1}$ étant deux à deux premiers entre eux, il existe $\beta \in A$ tel que $\beta \equiv b_i \pmod{\mathfrak{p}_i^{m_i+1}}$, pour $1 \leq i \leq r$. De plus, puisque $b_i \in \mathfrak{p}_i^{m_i}$ pour tout i , on conclut que $\beta \in \bigcap_{i=1}^r \mathfrak{p}_i^{m_i} = \prod_{i=1}^r \mathfrak{p}_i^{m_i} = I$.

- (c) Conclure de ce qui précède à l'égalité $\nu_{\mathfrak{p}}(\alpha A + \beta A) = \nu_{\mathfrak{p}}(I)$ pour tout $\mathfrak{p} \in \mathcal{P}$.

La question précédente montre en particulier que $\nu_{\mathfrak{p}_i}(\beta A) = m_i$ pour $1 \leq i \leq r$. On a alors $\nu_{\mathfrak{p}}(\alpha A + \beta A) = \min \{\nu_{\mathfrak{p}}(\alpha A), \nu_{\mathfrak{p}}(\beta A)\}$ pour tout $\mathfrak{p} \in \mathcal{P}$, d'où $\nu_{\mathfrak{p}_i}(\alpha A + \beta A) = \min \{n_i, m_i\} = m_i$ pour $1 \leq i \leq r$, soit $\nu_{\mathfrak{p}_i}(\alpha A + \beta A) = \nu_{\mathfrak{p}_i}(I)$, pour $1 \leq i \leq r$, ce qui établit bien le résultat demandé (on a $\nu_{\mathfrak{p}}(\alpha A + \beta A) = \nu_{\mathfrak{p}}(I) = 0$ pour $\mathfrak{p} \notin \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$).

3. Prouver la propriété $(\star)$ pour tout idéal entier puis tout idéal fractionnaire de l'anneau A .

Remarquons tout d'abord que la propriété $(\star)$ est évidente si $I = 0$ (en prenant $\alpha = \beta = 0$), ce qui permet de supposer désormais que I est *non nul*. Les résultats de la question précédente prouvent que, si I un idéal *entier* non nul et α un élément non nul de A , alors il existe $\beta \in I$ tel que $\alpha A + \beta A = I$, ce qui établit en particulier la propriété $(\star)$ dans ce cas. Dans le cas général, *i.e.* si I est un idéal fractionnaire non nul quelconque, il existe $0 \neq \lambda \in K$ tel que $I' = \lambda I$ soit un idéal entier. Si α est un élément non nul de I , $\alpha' = \lambda \alpha$ est un élément non nul de I' , et il existe, en vertu de ce qui précède, un élément $\beta' \in I'$ tel que $\alpha' A + \beta' A = I'$. L'élément $\beta = \lambda^{-1} \beta'$ appartient à I , et on a bien $\alpha A + \beta A = I$.

Problème

Le but du problème est d'étudier l'anneau des entiers $A = \mathcal{O}_L$ du corps $L = \mathbb{Q}(\sqrt{-1}, \sqrt{3})$.

1. On s'intéresse d'abord aux propriétés galoisiennes de l'extension $L/\mathbb{Q}$.

- (a) Observer que $K_3 = \mathbb{Q}[\sqrt{3}]$ ne contient pas $i = \sqrt{-1}$; conclure que $[L : \mathbb{Q}]$ vaut 4.

On observe que K_3 est contenu dans $\mathbb{R}$, et ne peut par conséquent pas contenir i .

- (b) Montrer que L est une extension galoisienne de $\mathbb{Q}$. Quel est l'ordre de $G = \text{Gal}(L/\mathbb{Q})$?

L'extension $L/\mathbb{Q}$ est engendrée par les deux éléments $\theta_1 = \sqrt{-1}$ et $\theta_2 = \sqrt{3}$. Elle contient leurs conjugués $\theta'_1 = -\sqrt{-1}$ et $\theta'_2 = -\sqrt{3}$. Elle est donc normale et par conséquent galoisienne, $\mathbb{Q}$ étant parfait. En particulier, $G = \text{Gal}(L/\mathbb{Q})$ est d'ordre 4.

- (c) On note $K_1 = \mathbb{Q}[\sqrt{-1}]$ puis σ l'unique élément non trivial de $G_1 = \text{Gal}(L/K_1)$ et $\tau \in G$ la conjugaison complexe. Quel est le sous-corps de L fixé par τ ?

La sous-extension $L^{<\tau>}$ fixée par τ contient $\sqrt{3}$. La théorie de Galois indique par ailleurs que $[L : L^{<\tau>}] = 2$. On en déduit que $L^{<\tau>} = \mathbb{Q}[\sqrt{3}] = K_3$.

- (d) Préciser l'action de τ , σ et $\sigma\tau$ sur $\sqrt{-1}$ et $\sqrt{3}$; conclure que $\sigma\tau$ est d'ordre 2 et en déduire la structure de G .

Comme $L = K_1[\sqrt{3}]$, on a $\sigma(\sqrt{3}) = -\sqrt{3}$ et $\sigma(\sqrt{-1}) = \sqrt{-1}$. Par ailleurs, $\tau(\sqrt{-1}) = -\sqrt{-1}$ et $\tau(\sqrt{3}) = \sqrt{3}$, d'où $\sigma\tau(\sqrt{-1}) = -\sqrt{-1}$ et $\sigma\tau(\sqrt{3}) = -\sqrt{3}$. Donc $\sigma\tau$ est d'ordre 2 ($\sigma\tau \neq \text{Id}_L$ et $(\sigma\tau)^2 = \text{Id}_L$). Ainsi, G , qui est d'ordre 4 et contient trois éléments d'ordre 2 est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- (e) Conclure que L contient un troisième sous-corps non trivial K_2 que l'on précisera.

Par conséquent, L contient $K_2 := L^{<\sigma\tau>} = \mathbb{Q}[i\sqrt{3}]$, qui est une sous-extension de degré 2 ($[L : L^{<\sigma\tau>}] = 2$ par la correspondance de Galois), qui est bien distincte de K_1 et K_3 (toujours par la théorie de Galois : K_1 , K_2 et K_3 sont les trois sous-corps de L correspondant aux trois sous-groupes non triviaux de G , à savoir $<\sigma>$, $<\sigma\tau>$ et $<\tau>$).

2. On va maintenant préciser le discriminant $d_L = \text{Disc}(\mathcal{O}_L)$ de L .

- (a) On note B le $\mathbb{Z}$ -module libre engendré par $(1, i, \sqrt{3}, i\sqrt{3})$. Vérifier que B est un sous-anneau de A et aussi un sous-module d'indice fini.

Les polynômes minimaux de i , $\sqrt{3}$ et $i\sqrt{3}$ sont respectivement X^2+1 , X^2-3 et X^2+3 , donc ces 3 éléments sont entiers sur $\mathbb{Z}$. Le $\mathbb{Z}$ -module B est donc contenu dans A . Que B soit un sous-anneau de A est clair (il suffit de vérifier que les sommes et produits deux à deux des générateurs $1, i, \sqrt{3}$ et $i\sqrt{3}$ sont dans B , ce qui est clair). Un théorème du cours affirme que A est un $\mathbb{Z}$ -module libre de rang 4. Comme B est un sous- $\mathbb{Z}$ -module libre de même rang, on conclut, en utilisant le théorème de la base adaptée que le quotient A/B est un groupe abélien fini (détails vus en TD). En particulier, l'indice de B dans A est fini.

- (b) Montrer que pour tout élément $x = \alpha + \beta i + \gamma\sqrt{3} + \delta i\sqrt{3}$ de L , avec $(\alpha, \beta, \gamma, \delta) \in \mathbb{Q}^4$, on a $\text{Tr}_{L/\mathbb{Q}}(x) = 4\alpha$.

On a

$$\begin{aligned} \text{Tr}_{L/\mathbb{Q}}(x) &= x + \sigma(x) + \tau(x) + \sigma\tau(x) \\ &= \alpha + \beta i + \gamma\sqrt{3} + \delta i\sqrt{3} \\ &\quad + \alpha + \beta i - \gamma\sqrt{3} - \delta i\sqrt{3} \\ &\quad + \alpha - \beta i + \gamma\sqrt{3} - \delta i\sqrt{3} \\ &\quad + \alpha - \beta i - \gamma\sqrt{3} + \delta i\sqrt{3} \\ &= 4\alpha \end{aligned}$$

- (c) Calculer le discriminant d_B de B . Quels sont les facteurs premiers possibles de d_L ?

En vertu de la question précédente, on a

$$\begin{aligned} d_B &= \begin{vmatrix} \text{Tr}_{L/\mathbb{Q}}(1) & \text{Tr}_{L/\mathbb{Q}}(i) & \text{Tr}_{L/\mathbb{Q}}(\sqrt{3}) & \text{Tr}_{L/\mathbb{Q}}(i\sqrt{3}) \\ \text{Tr}_{L/\mathbb{Q}}(i) & \text{Tr}_{L/\mathbb{Q}}(-1) & \text{Tr}_{L/\mathbb{Q}}(i\sqrt{3}) & \text{Tr}_{L/\mathbb{Q}}(-\sqrt{3}) \\ \text{Tr}_{L/\mathbb{Q}}(\sqrt{3}) & \text{Tr}_{L/\mathbb{Q}}(i\sqrt{3}) & \text{Tr}_{L/\mathbb{Q}}(3) & \text{Tr}_{L/\mathbb{Q}}(3i) \\ \text{Tr}_{L/\mathbb{Q}}(i\sqrt{3}) & \text{Tr}_{L/\mathbb{Q}}(-\sqrt{3}) & \text{Tr}_{L/\mathbb{Q}}(3i) & \text{Tr}_{L/\mathbb{Q}}(-3) \end{vmatrix} \\ &= \begin{vmatrix} 4 & 0 & 0 & 0 \\ 0 & -4 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & -12 \end{vmatrix} \\ &= 2^8 \cdot 3^2. \end{aligned}$$

Les facteurs premiers possibles pour d_L sont donc 2 et 3, en vertu de la relation $d_B = (A : B)^2 d_L$.

- (d) Vérifier que 2 et 3 sont bien ramifiés dans l'extension $L/\mathbb{Q}$ (par exemple en considérant une sous-extension quadratique convenable).

Le discriminant d_{K_3} de $K_3 = \mathbb{Q}[\sqrt{3}]$ est égal à 12 (voir le cours). En particulier, 2 et 3, qui divisent d_{K_3} , sont ramifiés dans K_3 , donc a fortiori dans L .

- (e) Conclure que l'indice $(A : B)$ est une puissance de 2.

De la relation

$$2^8 \cdot 3^2 = d_B = (A : B)^2 d_L \quad (3)$$

on a déduit que les éventuels facteurs premiers de $(A : B)$ étaient 2 et 3. Par ailleurs, le fait que 3 soit ramifié dans L entraîne que 3 divise d_L . Par conséquent, si 3 divisait également $(A : B)$, l'exposant de 3 dans $d_B = (A : B)^2 d_L$ serait au moins égal à 3, en contradiction avec l'équation (3). L'indice $(A : B)$ est donc bien une puissance de 2.

3. On regarde enfin L comme un corps cyclotomique : on note $j = \frac{1}{2}(-1 + i\sqrt{3})$ et $\zeta = ij$.

- (a) Vérifier que ζ est une racine 12^e primitive de l'unité et préciser son polynôme minimal Φ_{12} . Exprimer en particulier i et j en fonction de ζ .

Clairement, j et i sont respectivement racine primitive cubique et quatrième de l'unité. Leur produit ζ est donc une racine 12^e primitive de l'unité. Son polynôme minimal est

$$\Phi_{12}(X) = \frac{X^6 + 1}{X^2 + 1} = X^4 - X^2 - 1.$$

(dire que ζ est une racine 12^e primitive de l'unité équivaut à dire que $\zeta^6 = -1$ et $\zeta^2 \neq -1$)

- (b) Conclure que l'on a $L = \mathbb{Q}[\zeta]$ et $G \simeq (\mathbb{Z}/12\mathbb{Z})^\times$.

Comme $L \supset \mathbb{Q}[\zeta]$ et que $[\mathbb{Q}[\zeta] : \mathbb{Q}] = \varphi(12) = 4 = [L : \mathbb{Q}]$, on conclut que $L = \mathbb{Q}[\zeta]$, et que $G = \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \simeq (\mathbb{Z}/12\mathbb{Z})^\times$, l'isomorphisme étant obtenu en associant à la classe modulo 12 d'un entier k étranger à 12 le $\mathbb{Q}$ -automorphisme σ_k de $\mathbb{Q}[\zeta]$ qui à $P(\zeta)$ associe $P(\zeta^k)$.

- (c) En déduire que tout élément γ de G est de la forme $\sigma_k : P(\zeta) \mapsto P(\zeta^k)$ pour un k étranger à 12. Préciser la valeur de k pour successivement $\gamma = \sigma, \tau$ et $\sigma\tau$.

La description de G a été rappelée à la question précédente. Un calcul immédiat montre que $\tau = \sigma_{-1}$, $\sigma = \sigma_5$ et $\sigma\tau = \sigma_{-5}$ (il suffit de remarquer que $\sigma(\zeta) = \sigma(i)\sigma(j) = ij^2 = \zeta^5$)

- (d) Déterminer suivant la congruence de p modulo 12 le sous-groupe de décomposition d'un premier $p \nmid 12$ dans l'extension $L/\mathbb{Q}$. Préciser dans chaque cas le sous-corps de décomposition et le degré d'inertie f_p .

Un résultat du cours affirme que le groupe de décomposition D_p d'un premier p non ramifié dans $\mathbb{Q}[\zeta]/\mathbb{Q}$ est le sous-groupe cyclique engendré par σ_p . En particulier $f_p = |D_p|$ est égal à l'ordre de σ_p , lui-même égal au plus petit entier naturel n non nul tel que $p^n \equiv 1 \pmod{12}$. On a donc

$$f_p = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{12} \\ 2 & \text{si } p \equiv -1, 5 \text{ ou } -5 \pmod{12}. \end{cases}$$

Dans le premier cas ($p \equiv 1 \pmod{12}$) on a $L^{D_p} = L$, et dans le second cas, on vérifie aisément que $L^{D_p} = K_3, K_1$ ou K_2 selon que $p \equiv -1, 5$ ou $-5 \pmod{12}$ (c'est une conséquence directe des égalités $\tau = \sigma_{-1}$, $\sigma = \sigma_5$ et $\sigma\tau = \sigma_{-5}$).

- (e) Existe-t-il des nombres premiers qui soient totalement inertes dans l'extension $L/\mathbb{Q}$? Que pouvez-vous en conclure sur l'irréductibilité du polynôme Φ_{12} modulo p ?

Un nombre premier p est totalement inerte dans l'extension $L/\mathbb{Q}$ si et seulement si le nombre g_p d'idéaux premiers au-dessus de p est égal à 1, ainsi que l'indice de ramification e_p . En particulier, p est non ramifié, donc étranger à 6. En vertu de la relation $e_p f_p g_p = [L : \mathbb{Q}] = 4$, ceci entraîne que $f_p = 4$, ce qui est impossible vu les valeurs calculées à la question précédente. Soit p un nombre premier non ramifié dans l'extension $L/\mathbb{Q}$, *i.e.* p étranger à 6. On note S la partie multiplicative $\mathbb{Z} - p\mathbb{Z}$. En localisant en p la relation (3), on constate que l'indice $(S^{-1}A : S^{-1}B)$ est inversible dans $S^{-1}\mathbb{Z}$, et donc que $S^{-1}A = S^{-1}B = S^{-1}\mathbb{Z}[\zeta]$. On a par ailleurs les isomorphismes

$$S^{-1}\mathbb{Z}[\zeta]/pS^{-1}\mathbb{Z}[\zeta] \simeq \mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta] \simeq \mathbb{F}_p[X]/(\overline{\Phi_{12}}(X)),$$

où $\overline{\Phi_{12}}(X)$ désigne la réduction modulo p de $\Phi_{12}(X)$. Si $\overline{\Phi_{12}}(X)$ était irréductible dans $\mathbb{F}_p[X]$, le quotient $\mathbb{Z}[\zeta]/p\mathbb{Z}[\zeta] \simeq S^{-1}A/pS^{-1}A \simeq A/pA$ serait un corps, ce qui signifie que pA serait maximal, ou autrement dit que p serait totalement inerte, ce qui est impossible.

En conclusion, le polynôme $\Phi_{12}(X)$ est réductible modulo tous les premiers p étrangers à 6. Il l'est également modulo 2 et 3, étant donné que $X^4 - X^2 - 1 = (X^2 + X + 1)^2$ dans $\mathbb{F}_2[X]$ et $X^4 - X^2 - 1 = (X^2 + 1)^2$ dans $\mathbb{F}_3[X]$. Ainsi $\Phi_{12}(X)$ est un polynôme *irréductible* dans $\mathbb{Z}[X]$ mais *réductible* modulo p pour tout premier p ! Un autre exemple de ce phénomène est fourni par le polynôme $X^4 + 1 = \Phi_8(X)$ (on l'a montré lors du premier TD par des moyens élémentaires, mais on peut retrouver le résultat grâce à des arguments du même type que ceux utilisés ici).