

Correction des exercices des chapitres I et III

Exercice 1

Soit n le degré de f i.e. le degré de K sur \mathbb{Q} . On a

$$(1) \quad D(f) = D(1, \alpha, \dots, \alpha^{n-1}),$$

où $D(1, \alpha, \dots, \alpha^{n-1})$ est le discriminant de K sur \mathbb{Q} du système $(1, \alpha, \dots, \alpha^{n-1})$. Vérifions cet assertion. Soient $\alpha_0 = \alpha, \alpha_1, \dots, \alpha_{n-1}$ les n conjugués de α sur \mathbb{Q} . On a (cf. mon polycopié sur les corps locaux p. 49) :

$$(2) \quad D(1, \alpha, \dots, \alpha^{n-1}) = \left[\det(\alpha_i^j)_{0 \leq i, j \leq n-1} \right]^2.$$

C'est donc un déterminant de Vandermonde au carré. Il en résulte que

$$D(1, \alpha, \dots, \alpha^{n-1}) = \prod_{1 \leq i < j \leq n-1} (\alpha_j - \alpha_i)^2,$$

qui n'est autre que $D(f)$ (par définition du discriminant d'un polynôme unitaire). On considère alors une base (e_0, \dots, e_{n-1}) une base de O_K sur \mathbb{Z} . Pour tout $i = 0, \dots, n-1$, il existe des entiers $a_{i,j} \in \mathbb{Z}$ tels que l'on ait

$$\alpha^i = \sum_{j=0}^{n-1} a_{i,j} e_j.$$

Il en résulte que l'on a

$$D(1, \alpha, \dots, \alpha^{n-1}) = (\det(a_{i,j}))^2 D(e_0, \dots, e_{n-1}).$$

On a $D_K = D(e_0, \dots, e_{n-1})$. Par suite, on a l'égalité

$$D(f) = (\det(a_{i,j}))^2 D_K.$$

Par ailleurs, d'après la théorie des modules de libres type fini sur \mathbb{Z} (en fait sur un anneau principal), on a

$$(3) \quad |\det(a_{i,j})| = [O_K : \mathbb{Z}[\alpha]],$$

d'où l'exercice.

L'égalité (3) provient du résultat suivant : soit M un \mathbb{Z} -module libre de rang n et N un sous- \mathbb{Z} -module de M de même rang. Il existe une base (e_1, \dots, e_n) de M sur \mathbb{Z} et des entiers relatifs a_1, \dots, a_n tels que $(a_1 e_1, \dots, a_n e_n)$ soit une base de N sur \mathbb{Z} (et que a_i divise a_{i+1}). Le module quotient M/N est isomorphe au produit de $\mathbb{Z}/a_i \mathbb{Z}$ et l'indice de N dans M est le produit d des a_i , en valeur absolue. Par ailleurs, d est le déterminant du morphisme d'inclusion de N dans M qui ne dépend pas des bases choisies. D'où l'assertion.

Exercice 2

1) f est irréductible modulo 2 : utiliser le fait que le seul polynôme irréductible de degré 2 sur \mathbb{F}_2 est $X^2 + X + 1$ et on a modulo 2, $f = (X^2 + X)(X^2 + X + 1) + 1$.

2) On a $D(f) = -283$: (cf. le calcul du discriminant du trinôme $X^2 + aX + b$). Puisque $D(f)$ est sans facteurs carrés, on a le résultat d'après l'exercice 1.

3) D'après le théorème 1 du chapitre I, $2O_K$ est un idéal premier de O_K . On a

$$f \bmod 7 = (X + 4)(X^3 + 3X^2 + 2X + 5),$$

d'où $7O_K = \mathfrak{p}_1 \mathfrak{p}_2$, où \mathfrak{p}_1 est de degré résiduel 1 et \mathfrak{p}_2 est de degré résiduel 3.

En fait, on a $\mathfrak{p}_1 = bO_K$, où $b = \alpha - \alpha^2 + \alpha^3$. D'après le théorème 1, on sait que $\mathfrak{p}_1 = (7, \alpha + 4)$. Par ailleurs, la norme de K sur \mathbb{Q} de b est -7 , donc $7 \in bO_K$, et

$$\alpha + 4 = b(2\alpha^3 - \alpha^2 + \alpha),$$

de sorte que \mathfrak{p}_1 est contenu dans bO_K . Puisque b n'est pas inversible dans O_K (car sa norme n'est pas ± 1) et que \mathfrak{p}_1 est maximal, on a le résultat.

Exercice 3

Supposons qu'il existe un nombre premier p inerte dans K . Soit \mathfrak{P} l'idéal premier de O_K au-dessus de p . Le degré de l'extension O_K/\mathfrak{P} sur \mathbb{F}_p est le degré n de l'extension K/\mathbb{Q} (car $e = g = 1$ et $n = efg$). Le sous-groupe de décomposition $D_{\mathfrak{P}}$ en \mathfrak{P} de $\text{Gal}(K/\mathbb{Q})$ est isomorphe au groupe de Galois de O_K/\mathfrak{P} sur \mathbb{F}_p (qui est cyclique). Par suite, $\text{Gal}(K/\mathbb{Q})$ et $D_{\mathfrak{P}}$ sont égaux, d'où une contradiction.

Un exemple d'une telle situation est la suivante : soient a et b deux entiers relatifs tels que le polynôme $f = X^3 + aX + b \in \mathbb{Z}[X]$ soit irréductible sur \mathbb{Q} et que $-(4a^3 + 27b^2)$ ne soit pas un carré dans \mathbb{Z} . Soit K le corps de décomposition de f dans $\overline{\mathbb{Q}}$. Alors $\text{Gal}(K/\mathbb{Q})$ est isomorphe à S_3 qui n'est pas cyclique. [Si α est une racine de f dans \mathbb{C} , on a l'égalité $K = \mathbb{Q}(\alpha, \sqrt{-(4a^3 + 27b^2)})$. D'après les hypothèses faites, on a donc $[K : \mathbb{Q}] = 6$ et $\text{Gal}(K/\mathbb{Q})$ est isomorphe à S_3].

Exercice 4

Posons $f = X^4 - 2$. Il est irréductible sur K : f est irréductible modulo 5 et 5 est décomposé dans K , donc f est irréductible modulo un idéal premier au-dessus de 5. Par suite, f est irréductible sur $\mathbb{Z}[i]$, donc aussi sur K (vrai pour les anneaux intégralement clos). Ainsi, L/K est une extension de degré 4, galoisienne car μ_4 est contenu dans K . [On peut aussi dire que L est le corps de décomposition de $X^4 - 2$ sur \mathbb{Q}]. Par ailleurs, on a les inclusions,

$$K \subseteq M := K(\sqrt{2}) \subseteq L = M(\sqrt{u}) \quad \text{avec} \quad u = \sqrt{2}.$$

Soit \mathfrak{p} un idéal premier de $\mathbb{Z}[i]$ distinct de $(1+i)$ (l'idéal au-dessus de 2). D'après le corollaire, M/K est non ramifiée en \mathfrak{p} . De même, si \mathfrak{P} est un idéal de O_M au-dessus de \mathfrak{p} , alors $\sqrt{2}$ n'est pas dans \mathfrak{P} (sinon $2 = (\sqrt{2})^2$ serait dans \mathfrak{P}), et l'assertion 1 du corollaire entraîne de nouveau le fait que \mathfrak{P} soit non ramifié dans L . D'où l'exercice.

Exercice 5

Posons $f = X^3 - X - 1$. Le discriminant $D(f)$ est -23 , qui est sans facteurs carrés, donc $O_K = \mathbb{Z}[\alpha]$. Cela entraîne que $\mathfrak{D}_{K/\mathbb{Q}} = (3\alpha^2 - 1)O_K$. Par ailleurs, la norme sur \mathbb{Q} de $3\alpha^2 - 1$ est 23. On en déduit que l'idéal $(3\alpha^2 - 1)O_K$ est premier et que c'est un idéal au-dessus de 23.

En réduisant f modulo 23 (cf. Pari), on constate que (théorème 1)

$$23O_K = \mathfrak{P}_1\mathfrak{P}_2^2,$$

où \mathfrak{P}_i est de degré résiduel 1. Puisque \mathfrak{P}_1 est non ramifié dans K/\mathbb{Q} et que $\mathfrak{D}_{K/\mathbb{Q}}$ n'est divisible que par des idéaux premiers ramifiés, on en déduit que \mathfrak{P}_2 est le seul diviseur premier de $\mathfrak{D}_{K/\mathbb{Q}}$. On a donc

$$\mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{P}_2 = (3\alpha^2 - 1)O_K.$$

[En fait, on peut aussi justifier que $v_{\mathfrak{P}_2}(\mathfrak{D}_{K/\mathbb{Q}}) = 1$ en remarquant que la norme de $\mathfrak{D}_{K/\mathbb{Q}}$ est $|D_K| = 23$, ou bien que 2 est premier à la caractéristique résiduelle 23].

Exercice 6

On a $L = K(\sqrt{-1})$. D'après le corollaire, L/K est non ramifiée en dehors de l'idéal premier \mathfrak{p} de O_K au-dessus de 2. Par ailleurs, $-1 = (\sqrt{3})^2 - 4 \times 1$, donc L/K est aussi non ramifiée en \mathfrak{p} (assertion 2 du corollaire). D'où l'exercice [un plongement σ de L dans \mathbb{C} vérifie $\sigma(i)^2 = -1$, donc n'est pas réel, de sorte que L est un corps totalement imaginaire].

Exercice 7

L'extension K_1K_2/K est non ramifiée aux places à l'infini : si $\sigma : K \rightarrow \mathbb{R}$ est un plongement de K dans \mathbb{R} , tous ses prolongements à K_1 et K_2 sont aussi réels par hypothèse.

Si $\tau : K_1 K_2 \rightarrow \mathbb{C}$ est un prolongement de σ à $K_1 K_2$, τ est déterminé par ses restrictions à K_1 et à K_2 qui sont réelles, donc $\tau(K_1 K_2)$ est contenu dans \mathbb{R} [τ restreint à K_1 ou à K_2 sont des prolongements de σ à K_1 ou à K_2].

En ce qui concerne les places finies : posons $L = K_1 K_2$. Il s'agit de vérifier que L/K_1 et L/K_2 sont non ramifiées (ce qui prouvera l'assertion). On utilise pour cela le fait que le groupe de Galois $\text{Gal}(L/K_1)$ est isomorphe par l'application de restriction r à $\text{Gal}(K_2/K_1 \cap K_2)$. Soient \mathfrak{P} un idéal premier de O_L et $I_{\mathfrak{P}}(L/K_1)$ le sous-groupe d'inertie en \mathfrak{P} de $\text{Gal}(L/K_1)$. On pose $\mathfrak{p} = \mathfrak{P} \cap O_{K_2}$. Par définition, $I_{\mathfrak{P}}(L/K_1)$ est le sous-ensemble de $\text{Gal}(L/K_1)$ formé des éléments σ tels que $\sigma(x) - x \in \mathfrak{P}$ pour tout $x \in O_L$. Pour tout $y \in O_{K_2}$, en notant $\tau = r(\sigma)$, on a donc $\tau(y) - y \in \mathfrak{p}$, de sorte que τ appartient au sous-groupe d'inertie en \mathfrak{p} de $\text{Gal}(K_2/K_1 \cap K_2)$. On a donc une injection de $I_{\mathfrak{P}}(L/K_1)$ dans $I_{\mathfrak{p}}(K_2/K_1 \cap K_2)$. Puisque $I_{\mathfrak{p}}(K_2/K_1 \cap K_2)$ est trivial, il en est de même de $I_{\mathfrak{P}}(L/K_1)$, donc \mathfrak{P} est non ramifié dans L/K_1 . D'où le résultat.

Exercice 8

L'extension L/K est non ramifiée aux places à l'infini car K est totalement imaginaire. On a $L = K(\sqrt{-1})$ et le corollaire entraîne l'assertion : on a $-1 = (\sqrt{-5})^2 - 4 \times (-1)$.

Exercice 9

La formule (4) donne directement que $h_K = 2$. Avec le corollaire de [Sa] : on a

$$D_K = -20, \quad n = 2, \quad r_2 = 1.$$

Par suite la constante de Minkowski est

$$C = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_K|^{1/2} \simeq 2,847.$$

Toute classe d'idéaux contient donc un idéal entier de norme ≤ 2 . Les idéaux de O_K de norme ≤ 2 sont O_K et l'idéal premier \mathfrak{p} de O_K au-dessus de 2 (2 est ramifié dans K). Cet idéal n'est pas principal : sinon il existe $a, b \in \mathbb{Z}$ tels que $\mathfrak{p} = (a + b\sqrt{-5})O_K$. Puisque $2O_K = \mathfrak{p}^2$, on obtient alors une contradiction (les unités de O_K sont ± 1). Il en résulte que la classe de \mathfrak{p} est d'ordre 2 dans $Cl(K)$ (le groupe des classes de K). Toute classe d'idéaux fractionnaires de K non triviale étant la classe de \mathfrak{p} , on a donc $h_K = 2$.

Exercice 10

Si $u \in s_1^{-1}(\mathfrak{P})$, on a $s_1(u) \in \mathfrak{P}$ et la congruence $s_1(u) \equiv s_2(u) \pmod{\mathfrak{P}}$ entraîne que $u \in s_2^{-1}(\mathfrak{P})$. Par conséquent, $s_2 s_1^{-1}$ appartient à $D_{\mathfrak{P}}(L/K)$. Pour tout $x \in O_L$, $s_1^{-1}(x)$ est aussi dans O_L , et l'on a

$$s_2 s_1^{-1}(x) = s_2(s_1^{-1}(x)) \equiv s_1(s_1^{-1}(x)) \equiv x \pmod{\mathfrak{P}}.$$

Cela entraîne que $s_1 = s_2$ (car $D_{\mathfrak{P}}(L/K)$ est isomorphe à $\text{Gal}(\ell/k)$).

Exercice 11

On a $\left(\frac{2}{q}\right) = (2, F/\mathbb{Q})$ (comme dans la démonstration du théorème, en identifiant $\text{Gal}(F/\mathbb{Q})$ à ± 1). Par ailleurs, 2 est décomposé dans F si et seulement si $q^* \equiv 1 \pmod{8}$ et 2 est inerte dans F si et seulement si $q^* \equiv 5 \pmod{8}$. On a

$$(-1)^{(q^2-1)/8} = (-1)^{(q^{*2}-1)/8},$$

qui vaut 1 si $q^* \equiv 1 \pmod{8}$ et -1 si $q^* \equiv 5 \pmod{8}$. On en déduit que

$$(2, F/\mathbb{Q}) = (-1)^{(q^2-1)/8}.$$

D'où l'exercice.

Exercice 12

1) On vérifie avec la constante de Minkowski que $h_K = 2$.

2) On a $H = K(\sqrt{2})$. Si $L = K(\sqrt{2})$, on a $[L : K] = 2$ et H/K est non ramifiée à l'infini. Soit \mathfrak{p} un idéal premier de K . Si 2 n'est pas dans \mathfrak{p} , H/K est non ramifiée en \mathfrak{p} (cf. le corollaire). Si $2 \in \mathfrak{p}$, on écrit que $L = K(\sqrt{5})$ et que $5 = 3^2 - 4$, ce qui entraîne le résultat.

Pour la justification de l'assertion p. 16 : considérer les Frobenius en p : la restriction de $(p, K_1 K_2 / K)$ à K_1 est $(p, K_1 / K)$ et idem pour K_2 . [ici K_i est une extension abélienne finie d'un corps K]. De plus p est totalement décomposé dans K_i si et seulement si $(p, K_i / K)$ est trivial. Par ailleurs, $(p, K_1 K_2 / K)$ est déterminé par ses restrictions à K_1 et à K_2 . D'où l'assertion.

Voir à ce sujet, en toute généralité, Cox. p. 178, ex. 8.14.

Exercice 13

On trouve

$$p \equiv 1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45 \pmod{56}.$$

En fait, on a

$$\begin{aligned} \left(\frac{-14}{p}\right) &= \left(\frac{-1}{p}\right) \left(\frac{14}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{2}{p}\right) \left(\frac{7}{p}\right). \\ \left(\frac{7}{p}\right) \left(\frac{p}{7}\right) &= (-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right). \end{aligned}$$

Il en résulte que

$$\left(\frac{-14}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{p}{7}\right) = (-1)^{\frac{p^2-1}{8}} \left(\frac{p}{7}\right).$$

Cela entraîne le résultat compte tenu du fait que $(-1)^{\frac{p^2-1}{8}} = 1$ si $p \equiv \pm 1 \pmod{8}$ et $\left(\frac{p}{7}\right) = 1$ si $p \equiv 1, 2, 4 \pmod{7}$.

Justifications dans la proposition 2 p. 25

Le fait que $\text{Gal}(HL/L)$ soit isomorphe à $\text{Gal}(H/E)$ se justifie dans Lang, Algebra p. 196. La surjectivité utilise le théorème d'Artin p. 194. Soit $\sigma : L \rightarrow \mathbb{R}$ un plongement. On peut prolonger σ à HL en considérant la restriction de σ à E puis un prolongement de cette restriction à H . On obtient de cette façon $[H : E] = [HL : L]$ prolongements de σ à HL qui est le nombre total de prolongements de σ à HL . D'où l'assertion. En ce qui concerne les places finies, on procède comme dans l'exercice 7 en considérant les groupes d'inerties.

Exercice 1 du chapitre III

Il s'agit de déterminer l'unité fondamentale de $\mathbb{Q}(\sqrt{5})$ (cf. [Sa], p. 76 pour un exposé général). C'est la plus petite unité de l'anneau d'entiers de $\mathbb{Q}(\sqrt{5})$ qui soit > 1 [Les unités positives d'un corps quadratique réel K forment un groupe isomorphe à \mathbb{Z} . Ce groupe admet un unique générateur > 1 , c'est l'unité fondamentale de K : si $uv = 1$ et $u \neq 1$, alors un seul des nombres $\pm u$ ou $\pm v$ est > 1 et c'est le plus grand des quatre (*). Les éléments de O_K si $K = \mathbb{Q}(\sqrt{5})$ sont de la forme

$$(1) \quad \frac{a + b\sqrt{5}}{2},$$

où a et b sont des entiers de même parité. Soit

$$u = \frac{a_1 + b_1\sqrt{5}}{2},$$

l'unité fondamentale. Sa norme sur \mathbb{Q} est ± 1 . En l'écrivant sous la forme ci-dessus, on obtient

$$a_1^2 - 5b_1^2 = \pm 4.$$

D'après (*), les unités > 1 de O_K sont de la forme (1) avec $a, b > 0$. On a donc $a_1, b_1 > 0$. On détermine le plus petit entier $b > 0$ tel que $-5b^2$ diffère de ± 4 par un carré. On trouve $b = 1$, d'où $b_1 = 1$ puis $a_1 = 1$ (cela est expliqué dans Samuel).

Le régulateur est donc

$$R = \log\left(\frac{1 + \sqrt{5}}{2}\right) \sim 1,618.$$

Remarque.

Le fait que les v_s (p. 27) soient distincts de ± 1 et distincts deux à deux est démontré dans [Ribén] p. 177. En ce qui concerne le fait qu'elles soient indépendantes : voir [Ribén] p. 609 chapitre 27).

Exercice supplémentaire

Calcul du discriminant de K^+ : le discriminant relatif de K/K^+ est la norme de la différentielle relative. Cette différentielle est \mathfrak{P} [K/K^+ est non ramifiée en dehors de p , il y a un unique idéal premier au-dessus de p et l'exposant est $e - 1 = 1$ (2 est premier à p)]. Par suite, on a

$$|D_K| = N_{K^+/\mathbb{Q}}(\Delta_{K/K^+})D_{K^+}^2,$$

où Δ_{K/K^+} est le discriminant relatif de K/K^+ (formule 8 de Samuel p. 112). D'où

$$p^{p-2} = pD_{K^+}^2.$$

Cela conduit à

$$D_{K^+} = p^{\frac{p-3}{2}}.$$

Exercice 3 du chapitre III

Soit g le plus petit entier ≥ 1 tel que $g \bmod p$ engendre \mathbb{F}_p^* . On a

$$\sum_{j=1}^{p-1} j^m \equiv \sum_{r=0}^{p-2} (g^r)^m = \frac{(g^m)^{p-1} - 1}{g^m - 1} \equiv 0 \bmod p,$$

compte tenu du fait que $g^{p-1} \equiv 1 \bmod p$ et que $g^m \not\equiv 1 \bmod p$ car $p-1$ ne divise pas m . D'où l'exercice.

Justification de $B_{2n+1} = 0$: il suffit d'utiliser la formule

$$\frac{-z}{e^{-z} - 1} = \frac{z}{e^z - 1} + z.$$

Exercice (cf. [Wa], p. 17, ex. 2.4).

Le groupe $(\mathbb{Z}/p^2\mathbb{Z})^*$ est cyclique $(*)$, donc il existe un unique sous-corps K de $\mathbb{Q}(\mu_{p^2})$ de degré p sur \mathbb{Q} . On montre que 2 est totalement décomposé dans K si et seulement si $2^{p-1} \equiv 1 \bmod p^2$. C'est vrai si $p = 2$. Supposons $p \geq 3$. Soient f le degré résiduel de 2 dans $\mathbb{Q}(\mu_{p^2})/\mathbb{Q}$ et g le nombre de places de $\mathbb{Q}(\mu_{p^2})$ au-dessus de 2 . On a $p(p-1) = fg$ (2 est non ramifié). L'entier f est l'ordre de 2 dans $(\mathbb{Z}/p^2\mathbb{Z})^*$.

Supposons 2 totalement décomposé dans K . Dans ce cas, p divise g . Il en résulte que f divise $p-1$. La congruence $2^f \equiv 1 \bmod p^2$ entraîne alors $2^{p-1} \equiv 1 \bmod p^2$. Inversement, supposons cette congruence réalisée. L'entier f divise alors $p-1$ de sorte que p divise g , donc 2 est totalement décomposé dans K (sinon 2 serait inerte dans K et g serait au plus $p-1$). D'où l'exercice. (cf. 1093 et 3511 comme exemple de p tels que $2^{p-1} \equiv 1 \bmod p^2$).

(*) : il s'agit d'expliciter un élément d'ordre $p(p-1)$ dans $(\mathbb{Z}/p^2\mathbb{Z})^*$. On a $(1+p)^p \equiv 1 \pmod{p^2}$, donc $1+p$ est d'ordre p dans $(\mathbb{Z}/p^2\mathbb{Z})^*$. Soit $\psi : (\mathbb{Z}/p^2\mathbb{Z})^* \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$ la surjection canonique. Il existe y tel que $\langle \psi(y) \rangle = (\mathbb{Z}/p\mathbb{Z})^*$. Soit r l'ordre de y . On a $\psi(y^r) = 1 = \psi(y)^r$, d'où $p-1$ divise r . Il existe donc $x \in \langle y \rangle$ d'ordre $p-1$. L'élément $x(1+p)$ est alors d'ordre $p(p-1)$. D'où l'assertion.

On en fait montrer l'assertion suivante (2 ne joue aucun rôle) :

soit ℓ un nombre premier. Alors ℓ est totalement décomposé dans K si et seulement si on a $\ell^{p-1} \equiv 1 \pmod{p^2}$:

Supposons ℓ totalement décomposé dans K . Dans ce cas, p divise g . En effet, g est le nombre de places au-dessus de p dans K multiplié par le nombre de places de $\mathbb{Q}(\mu_{p^2})$ au-dessus d'un idéal de K qui au-dessus de p (qui est le même pour toutes les places de K). Il en résulte que f divise $p-1$. La congruence $\ell^f \equiv 1 \pmod{p^2}$ entraîne alors $\ell^{p-1} \equiv 1 \pmod{p^2}$. Inversement, supposons cette congruence réalisée. L'entier f divise alors $p-1$ de sorte que p divise g , donc ℓ est totalement décomposé dans K (sinon ℓ serait inerte dans K et g serait au plus $p-1$). D'où l'exercice.

On le constate avec $p = 3$ i.e. avec le corps K de degré 3 contenu dans $\mathbb{Q}(\mu_9)$. On a $K = \mathbb{Q}(\alpha)$ où α est racine du polynôme $X^3 - 6X^2 + 9X - 1$: ℓ est totalement décomposé dans K si et seulement si $\ell^2 \equiv 1 \pmod{9}$.