Feuille d'exercices 5

1 Corps quadratiques

Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique, de discriminant D égal à d ou $4d$ selon que d est congru ou non à 1 modulo 4. Notons $p_1, \ldots, p_k$ les diviseurs premiers distincts de D, c'est-à-dire les nombres premiers de $\mathbb{Z}$ qui se ramifient dans K et, pour chacun d'eux, notons $\mathfrak{p}_i$ l'unique idéal premier de $\mathcal{O}_K$ qui divise p_i, de sorte que $p_i\mathcal{O}_K = \mathfrak{p}_i^2$. Notons encore $x \mapsto \overline{x}$ l'unique automorphisme non trivial de K, appelé conjugaison, même dans le cas réel ($d > 0$).

Exercice 1. *Trouver un exemple de deux entiers d'un corps quadratique qui ont même norme sans être ni conjugués ni associés.*

Exercice 2. *Montrer que, si $\epsilon \in \mathbb{Q}(\sqrt{d})$ est une unité de norme 1 d'un corps quadratique, il existe un entier γ tel que $\epsilon = \frac{\gamma}{\gamma'}$, où γ' est le conjugué de γ.*

Exercice 3. *On considère le corps $K = \mathbb{Q}(\sqrt{-43})$. On pose $\omega = \frac{-1+\sqrt{-43}}{2}$, et on rappelle que l'anneau des entiers de K admet $\{1, \omega\}$ comme base sur $\mathbb{Z}$.*

(1) Calculer le polynôme minimal de ω sur $\mathbb{Q}$. Montrer que 2 et 3 sont inertes dans K.

(2) Calculer la constante de Minkowski de K. Montrer que $\mathcal{O}$ est principal.

(3) Soit $\alpha \notin \mathbb{Z}$ un élément de $\mathcal{O}$ qui engendre un idéal premier. Montrer que $N_{L/\mathbb{Q}}(\alpha)$ est un nombre premier.

(4) Soit x et $y \neq 0$ deux entiers premiers entre eux tels que $x^2 + xy + 11y^2$ soit strictement inférieur à 121. Montrer que $x^2 + xy + 11y^2$ est un nombre premier.

Exercice 4. *Soit $K = \mathbb{Q}(\sqrt{-23})$ et $\alpha = \frac{1+\sqrt{-23}}{2}$.*

(1) Calculer le polynôme minimal de α, le discriminant D_K de K et la constante de Minkowski M_K de K.

(2) Montrer que les idéaux $\mathfrak{p} = (2, \alpha)$ et $\mathfrak{q} = (3, \alpha)$ sont premiers et non principaux.

(3) Donner la factorisation de $2\mathcal{O}_K$ et $3\mathcal{O}_K$ en produit d'idéaux premiers.

(4) Montrer que $\mathfrak{p}^3$ est principal.

(5) Calculer le nombre de classes h_K. On pourra commencer par montrer que h_K est inférieur ou égal à 5.

Exercice 5. *Soit $K = \mathbb{Q}(\sqrt{-5})$ et $L = K(\sqrt{2})$.*

(1) Montrer que l'idéal $\mathfrak{p} = (2, 1 + \sqrt{-5})$ de $\wr_K$ n'est pas principal, mais que son carré l'est. Calculer le nombre de classes de K.

(2) Montrer que $\beta = \frac{1+\sqrt{-5}}{\sqrt{2}}$ est un entier de L. Montrer que l'idéal $\mathfrak{p}' = \mathfrak{p}\mathcal{O}_L$ de $\mathcal{O}_L$ est principal.

(3) Montrer que pour tout idéal $\mathfrak{a}$ de $\mathcal{O}_K$, $\mathfrak{a}\mathcal{O}_L$ est principal.

Exercice 6. *Montrer que, si $\mathfrak{a}$ est un idéal entier de K stable par conjugaison, c'est-à-dire si $\mathfrak{a} = \overline{\mathfrak{a}}$, alors il existe une partie H de $\{1 \ldots k\}$ et un entier naturel m tel que*

$$\mathfrak{a} = m \prod_{i \in H} \mathfrak{p}_i.$$

Exercice 7. *Démontrer un cas très particulier du théorème 90 de Hilbert: si x est un élément de norme 1 dans K, il existe un élément y de K^* tel que $x = y/\overline{y}$. On pourra chercher y sous la forme $z + x\overline{z}$.*

On notera $Cl_K[2]$ le groupe des classes d'idéaux de carré trivial de K. C'est un $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel.

Exercice 8. *Soit $\mathfrak{a}$ un idéal représentant d'un élément de $Cl_K[2]$, c'est-à-dire un idéal dont le carré est principal. Montrer qu'il existe un élément α de K^* tel que $\overline{\mathfrak{a}} = \alpha\mathfrak{a}$. Montrer que α ou α^2 est de norme 1 et en déduire l'existence d'un élément β de K^* tel que $\beta\mathfrak{a}$ soit stable par conjugaison. En déduire que $Cl_K[2]$ est engendré par les classes des idéaux $\mathfrak{p}_i$. Montrer que son ordre est un diviseur de 2^{k-1}.*

Exercice 9. *Achever la démonstration du théorème 1 du cours: montrer que si $D < 0$, l'ordre de $Cl_K[2]$ vaut exactement 2^{k-1}, et que dans tous les cas, les groupes $Cl_K[2]$ et $Cl_K/2Cl_K$ sont isomorphes.*

Exercice 10. *Soit $K = \mathbb{Q}(\sqrt{(}d))$ un corps quadratique réel, et $\epsilon = \frac{x+y\sqrt{d}}{2}$ son unité fondamentale. Montrer que x et y sont positifs. Montrer que y est le plus petit entier naturel tel que dy^2 diffère d'un carré par ± 4. Calculer les unités fondamentales de $\mathbb{Q}(\sqrt{d})$ pour $d \in \{2, 3, 5, 6, 7, 10\}$.*

Exercice 11. *On considère le corps quadratique imaginaire $K = \mathbf{Q}(\sqrt{-13})$, et on note σ son automorphisme non trivial.*

(1) Démontrer les assertions suivantes:

- *(a) L'anneau des entiers de K est $\mathcal{O} = \mathbf{Z} \oplus \mathbf{Z}\sqrt{-13}$ et son discriminant vaut -52.*
- *(b) $2\mathcal{O} = \mathfrak{p}^2$, où $\mathfrak{p} = \sigma(\mathfrak{p})$ est un idéal premier de $\mathcal{O}$ qui n'est pas principal.*
- *(c) $13\mathcal{O} = \mathfrak{q}^2$, où $\mathfrak{q} = \sigma(\mathfrak{q})$ est l'idéal premier engendré par $\sqrt{-13}$.*
- *(d) $3\mathcal{O}$ est un idéal premier de $\mathcal{O}$.*
- *(e) Les seules unités de $\mathcal{O}$ sont 1 et -1.*

(2) Montrer que toute classe d'idéaux de K admet parmi ses représentants un idéal entier de norme inférieure à 5. Déduire de ce qui précède que le nombre de classes de K vaut 2.

(3) Montrer que pour tout entier rationnel y, l'idéal $\mathfrak{d}$ de $\mathcal{O}$ engendré par $y + \sqrt{-13}$ et $y - \sqrt{-13}$ admet au plus $\mathfrak{p}$ et $\mathfrak{q}$ comme diviseurs premiers — autrement dit, $\mathfrak{p}$ et $\mathfrak{q}$ sont les seuls idéaux premiers pouvant contenir $\mathfrak{d}$.

(4) Soient α, β des entiers naturels tels que $(y + \sqrt{-13})\mathcal{O} = \mathfrak{c}\mathfrak{p}^\alpha\mathfrak{q}^\beta$, où $\mathfrak{c}$ est un idéal de $\mathcal{O}$ qui n'est divisible ni par $\mathfrak{p}$ ni par $\mathfrak{q}$. Montrer que $\mathfrak{c}$ et $\sigma(\mathfrak{c})$ n'ont pas de diviseur premier commun.

On désigne désormais par $(x, y) \in \mathbb{Z}^2$ une solution en entiers rationnels de l'équation

$$Y^2 = X^3 - 13 \qquad (*).$$

(5) Déduire de la relation $(x)^3 = (y+\sqrt{-13})(y-\sqrt{-13})$ l'existence d'un idéal $\mathfrak{c}$ de $\mathcal{O}$ et de deux entiers naturels a et b tels que

$$(y + \sqrt{-13})\mathcal{O} = (\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b)^3.$$

(6) Montrer que $\mathfrak{c}\mathfrak{p}^a\mathfrak{q}^b$ est un idéal principal.

(7) En déduire qu'il existe des entiers rationnels u, v tels que

$$y = u^3 - 39uv^2 \quad , \quad 1 = v(3u^2 - 13v^2).$$

(8) Dans le taxi qui l'amène à la mairie-préfecture où il doit épouser Alice, Bernard s'aperçoit qu'en soustrayant le carré du dernier nombre de la plaque minéralogique de la voiture au cube de l'âge de sa fiancée, il pourrait se croire à Marseille. Alice est-elle en âge de se marier, et si oui, dans quelle ville sera célébré l'heureux événement ?

2 Corps de nombres

Exercice 1. *Dans $K = \mathbb{Q}(\theta = \sqrt[4]{5})$, calculer les discriminants*

$$\Delta(1, \theta, \theta^2, \theta^3),$$

$$\Delta(1+\theta, 1+\theta^2, 1+\theta^3, 1+\theta^4)$$

$$\Delta(1, \theta, \frac{1+\theta^2}{2}, \frac{\theta+\theta^3}{2}).$$

Exercice 2. *Montrer qu'un entier algébrique dont tous les conjugués (dans $\mathbb{C}$) sont de module strictement inférieur à 1 est forcément nul.*

Exercice 3. *Montrer qu'un entier algébrique dont tous les conjugués (dans $\mathbb{C}$) sont de module inférieur ou égal à 1 est une racine de l'unité ou est nul.*

Exercice 4. *Montrer que, dans un corps de nombres K de degré n, tout idéal (entier) non nul contient une infinité d'entiers naturels mais que, si b est un entier naturel non nul, il n'est pas contenu dans plus de b^n idéaux entiers.*

Exercice 5. *Dans tout le problème, K désigne le corps $\mathbb{Q}(\alpha)$, avec $\alpha^3 = 17$, et A désigne l'anneau des entiers de K*

(1) Donner la décomposition en idéaux premiers de $17A$.

(2) Donner la forme de la décomposition en idéaux premiers de $7A$, $5A$ et $2A$. Dans chaque cas, on calculera le nombre de diviseurs premiers distincts, leur indice de ramification et leur degré résiduel.

(3) On pose $\beta = \frac{1-\alpha+\alpha^2}{3}$. Calculer $(\alpha+1)\beta$. En déduire que β est racine du polynôme $P = X^3 - X^2 + 6X - 12$. Calculer les discriminants des bases $\{1, \alpha, \alpha^2\}$ et $\{1, \alpha, \beta\}$ de $K/\mathbb{Q}$. En déduire que cette dernière est une base de A comme $\mathbb{Z}$-module.

(4) Montrer que $\beta - 1$ n'appartient à aucun idéal premier de degré résiduel 2. Ë l'aide des idéaux premiers énumérés au b), trouver la décomposition en produit d'idéaux premiers de $(\beta-2)A$ et $(\alpha-3)A$. En déduire que les idéaux premiers en question sont tous principaux.

(5) Ecrire la décomposition en produit d'idéaux premiers des idéaux βA et $(\beta-1)A$, et trouver des générateurs de deux idéaux premiers divisant $3A$. Calculer $\frac{(\beta-1)\beta^2}{2(\beta-2)}$ et en déduire la décomposition en produit d'idéaux premiers de $3A$.

(6) Montrer que les idéaux fractionnaires de A sont tous principaux.

(7) On pose $\gamma = \frac{3}{\alpha-2}$. Décomposer en produit d'idéaux premiers l'idéal $(\alpha+1)A$, puis γA. Calculer le polynôme minimal Q de γ sur $\mathbb{Q}$ et montrer que $\{1, \gamma, \gamma^2\}$ est une base du $\mathbb{Z}-$module A. Trouver la décomposition en produit d'idéaux premiers de $Q'(\gamma)A$ et calculer $|N_{K/\mathbb{Q}}(Q'(\gamma))|$.

Exercice 6. *Soit θ une racine d'un polynôme F de $\mathbb{Z}[X]$ unitaire de degré n irréductible sur $\mathbb{Q}$, $K = \mathbb{Q}(\theta)$, $\mathcal{O}$ l'anneau des entiers de K, et D le discriminant de K. On note k l'indice $[\mathcal{O} : R]$ de l'anneau $R = \mathbb{Z}[\theta]$ dans $\mathcal{O}$, et D_θ le discriminant de la base $\{1, \theta, \ldots, \theta^{n-1}\}$ de K sur $\mathbb{Q}$.*

(1) Exprimer D_θ en fonction de D et de k. Montrer que, si un nombre premier q ne divise pas D_θ, il ne divise pas non plus k.

(2) Soit p un nombre premier. On suppose que F est un polynôme d'Eisenstein relativement à p (p divise tous les coefficients sauf le coefficient dominant, et p^2 ne divise pas le coefficient constant). On note $\mathfrak{p}$ l'idéal de $\mathcal{O}$ engendré par p et θ. Montrer que la norme $N\mathfrak{p}$ de $\mathfrak{p}$ divise p^n et $N_{K/\mathbb{Q}}(\theta)$. En déduire que $N\mathfrak{p} = p$, que $\mathfrak{p}$ est un idéal premier de degré résiduel 1 et que $p\mathcal{O} = \mathfrak{p}^n$.

(3) *Montrer que θ^{n-1} n'appartient pas à $\mathfrak{p}^n$. En déduire que pour tout entier i compris entre 1 et n, θ^i n'appartient pas à $\mathfrak{p}^{i+1}$, et que tout élément de $\mathcal{O}$ est congru modulo le sous-groupe $p\mathcal{O}$ à un élément de R.*

(4) *Montrer que p ne divise pas l'indice k de R dans $\mathcal{O}$.*

(5) *On considère désormais le cas $\theta = \sqrt[5]{2}$. Montrer que l'indice k de R dans $\mathcal{O}$ n'est pas divisible pas 2.*

(6) *Calculer le polynôme minimal de $\theta - 2$. Montrer que 5 ne divise pas k.*

(7) *Montrer que dans ce cas $\mathcal{O}$ est égal à R.*

Exercice 7. *On note $\zeta = e^{\frac{2i\pi}{23}}$ et $L = \mathbb{Q}(\zeta)$. On rappelle que le degré de L sur $\mathbb{Q}$ est 22. Le but de ce problème est de montrer que l'anneau $\mathcal{O}$ des entiers de L n'est pas principal.*

(1) *Montrer que $2^{23} - 1$ est divisible par 47 mais pas pas 47^2. Calculer $N_{L/\mathbb{Q}}(\zeta - 2)$.*

(2) *Notons $\mathfrak{a}$ l'idéal de $\mathcal{O}$ engendré par 47 et $\zeta - 2$. Montrer que, pour tout élément β de $\mathfrak{a}$, 47 divise $N_{L/\mathbb{Q}}(\beta)$.*

(3) *On suppose que $\mathfrak{a}$ est principal, engendré par α. Montrer que la norme $N(\alpha)$ divise 47^{22} et $N(\zeta-2)$. Calculer $N(\alpha)$.*

(4) *Montrer que L contient un corps K quadratique sur $\mathbb{Q}$ et un seul.*

(5) *Posons $\omega = N_{L/K}(\alpha)$. Montrer que ω est un entier de K et que sa norme est 47.*

(6) *On sait, grâce à une formule de Gauß(cf. feuille d'exercices), que $K = \mathbb{Q}(\sqrt{-23})$. Montrer que K ne contient pas d'entier de norme 47, et conclure.*

Exercice 8. *Dans le corps $K = \mathbb{Q}(\sqrt{-47}$, on note $\omega = (1 + \sqrt{-47})/2$ et $\mathfrak{O} = \mathbb{Z}[\omega]$ l'anneau des entiers. On se propose d'étudier le groupe C des classes d'idéaux fractionnaires de K.*

(1) *Montrer que si $\mathfrak{p}$ est l'idéal engendré par 2 et ω, $\mathfrak{p}$ est un idéal de norme 2 distinct de son conjugué $\overline{\mathfrak{p}}$ et que l'on a $2\mathfrak{O} = \mathfrak{p}\overline{\mathfrak{p}}$.*

(2) *Montrer que si A est la norme d'un idéal entier principal $\mathfrak{a}$, alors l'équation*

$$x^2 + 47y^2 = 4A$$

admet une solution (x, y) dans $\mathbb{Z}^2$. Montrer que $\mathfrak{p}$, $\mathfrak{p}^2$, $\mathfrak{p}^3$ et $\mathfrak{p}^4$ ne sont pas principaux.

(3) *Montrer qu'il existe deux idéaux principaux de norme 32. Donner la liste des idéaux entiers de norme 32 et montrer que $\mathfrak{p}^5$ est principal.*

(4) *Montrer qu'il y a au plus huit idéaux entiers de norme inférieure ou égale à 4. Ë l'aide du théorème de Minkowski, montrer que C est cyclique d'ordre 5.*

(5) *Montrer que l'idéal $\mathfrak{q}$ engendré par 3 et ω est de norme 3. Pour quelles valeurs de n l'idéal $\mathfrak{p}^n\mathfrak{q}$ est-il principal ?*

3 Loi de réciprocité supérieure

Soit L/K une extension finie; on note $\mathcal{O}_K$ et $\mathcal{O}_L$ les anneaux d'entiers. Pour $\mathfrak{p}$ un idéal premier non nul de $\mathcal{O}_K$. On écrit

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{b}_1^{e_1} \cdots \mathfrak{b}_r^{e_r}$$

où les $\mathfrak{b}_i$ sont des idéaux premiers distincts non nuls de $\mathcal{O}_L$ et les e_i des entiers ≥ 1. On note en outre f_i le degré de l'extension de corps résiduel $\kappa(\mathfrak{b}_i)/\kappa(\mathfrak{p})$. On rappelle que $\sum_i e_i f_i = [L : K] = n$. En outre si l'extension L/K est galoisienne, $e_i = e$ et $f_i = f$ sont constants. Quand $r = 1$ (resp. $r = n$), on dit que $\mathfrak{p}$ est inerte (resp. totalement décomposé). Quand tous les $e_i = 1$, on dit que $\mathfrak{p}$ est non ramifié. On note $\mathrm{Spl}(L/K)$ l'ensemble des idéaux premiers de K totalement décomposés dans L.

Exercice 1. *Soit K un corps quadratique et $a \in \mathbb{Z}$ un entier sans carré tel que $K = \mathbb{Q}[\sqrt{a}]$.*

(1) Montrer que pour tout premier p, $\mathcal{O}_K/p\mathcal{O}_K \simeq \mathbb{F}_p[X]/(X^2 - a)$.

(2) En déduire que tout p ne divisant pas $2a$, (p) est non ramifié dans K puis que pour $p \nmid 2a$, (p) est complètement décomposé si et seulement si $(\frac{a}{p}) = 1$.

(3) Montrer que $\mathrm{Spl}(\mathbb{Q}[\sqrt{a}]/\mathbb{Q})$ est l'ensemble des premiers contenus dans une certaine réunion de classes non nulles modulo $4a$, auquel il faut éventuellement ajouter des diviseurs premiers de $2a$.

Exercice 2. *Soit ζ_n une racine primitive n-ième de l'unité. Soit $K = \mathbb{Q}[\zeta_n]$ d'anneau des entiers $\mathcal{O}_K = \mathbb{Z}[\zeta_n] \simeq \mathbb{Z}[X]/(\Phi_n(X))$.*

(1) Montrer que pour tout p ne divisant pas n, (p) est non ramifié dans K et se décompose en idéaux premiers de même degré résiduel f égal à l'ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$.

(2) Montrer que $\mathrm{Spl}(K/\mathbb{Q})$ est l'ensemble des premiers congrus à 1 modulo n.

Exercice 3. *Soit $\mathfrak{p}$ un idéal premier non nul de K et soit $\mathfrak{b}$ un idéal de L au dessus de $\mathfrak{p}$.*

(1) Montrer que l'ordre du stabilisateur $G_\mathfrak{b}$ est égal à ef.

(2) Dans le cas où $\mathfrak{p}$ est non ramifié, $e = 1$, montrer que $G_\mathfrak{b}$ s'identifie au groupe de Galois de l'extension de corps finis $\kappa(\mathfrak{b})/\kappa(\mathfrak{p})$.

(3) Dans le cas où G est abélien, construire un élément $(\frac{L/K}{\mathfrak{p}})$ associé au Frobenius de $\kappa(\mathfrak{b})/\kappa(\mathfrak{p})$. C'est le ***symbole d'Artin****.*

(4) Calculer le symbole d'Artin pour $K = \mathbb{Q}$ et $L = \mathbb{Q}[\zeta_n]$ (resp. $L = \mathbb{Q}[\sqrt{m}]$) pour p non ramifié.

(5) Soit $L = \mathbb{Q}[\zeta_l]$ et $H = (\mathbb{F}_l^\times)^2 \subset \mathrm{Gal}(L/\mathbb{Q})$ et $M = L^H$.

(i) Montrer que $M = \mathbb{Q}[\sqrt{l^*}]$ avec $l^* = (-1)^{(l-1)/2}$.

(ii) Montrer que $p \neq l$ est non ramifié dans L et M et que la restriction à M de $(\frac{L/Q}{p})$ est $(\frac{M/\mathbb{Q}}{p}) = (\frac{p}{l})$.

(iii) En déduire une nouvelle preuve de la loi de réciprocité quadratique.

Loi de réciprocité d'Artin: Pour $\mathfrak{m}$ un idéal de K, on note $J_k^\mathfrak{m}$ le groupe des idéaux fractionnaires premiers à $\mathfrak{m}$ et $P_K^\mathfrak{m}$ le sous-groupe des idéaux principaux engendré par les idéaux principaux engendré par les $\alpha \equiv 1 \mod \mathfrak{m}$ qui est d'indice fini.

Pour L/K une extension finie abélienne, il existe un idéal $\mathfrak{m}$ de K tel que le morphisme

$$(\frac{L/K}{\quad}) : J_K^\mathfrak{m} \to \mathrm{Gal}(L_K)$$

est surjectif et son noyau $H^\mathfrak{m}$ contient $P_K^\mathfrak{m}$ que l'on peut exprimer explicitement grâce au morphisme norme $N_{L/K}$.

On peut définir aussi le symbole de Jacobi de puissance n-ième $(\frac{a}{b})_n$ donné par le symbole d'Artin d'une extension de la forme $K(\sqrt[n]{a})/K$ avec $K = \mathbb{Q}[\zeta_n]$.