Théorie algébrique des nombres (UM4MA234)

Exercice 1.

(1) Soit $\alpha := \frac{2}{3+\sqrt{13}}$. Alors

$$(2/\alpha - 3)^2 = 13$$

et donc

$$\alpha^2 + 3\alpha - 1 = 0$$

Il en suit que α est un entier algébrique de degré $\leqslant 2$ car α annule un polynôme unitaire à coefficients entiers de degré 2. Comme 13 n'est pas un carré, α n'est pas rationnel et donc α est de degré 2.

(2) Soit $\alpha := \frac{-2+\sqrt{2}+i\sqrt{2}}{2}$. De même on trouve que

$$\alpha^4 + 4\alpha^3 + 6\alpha^2 + 4\alpha + 2 = 0$$

et donc que α est entier algébrique de degré $\leqslant 4$. Reste à montrer que α est de degré 4. Si α est de degré < 4 alors $\mathbb{Q}(\alpha)$ est de dimension < 4, or $\sqrt{2}$ et $i \in \mathbb{Q}(\alpha)$ et $(1, \sqrt{2}, i, i\sqrt{2})$ est une famille $\mathbb{Q}$–libre, en effet si $a + b\sqrt{2} + ci + di\sqrt{2} = 0$ alors en séparant partie imaginaire et partie réelle on a

$$a + b\sqrt{2} = 0 = c + d\sqrt{2}$$

et comme $\sqrt{2}$ est irrationnel on a $a = b = c = d = 0$.

(3) Soit $\alpha := \frac{\sqrt{a}+\sqrt{b}}{n}$, où a, b sont des entiers distincts sans facteur carré. On trouve comme polynôme annulateur

$$P = X^4 + \frac{2(a+b)}{n^2}X^2 + \frac{(a-b)^2}{n^4}$$

Montrons que α est de degré 4. En effet les calculs donnent que $\sqrt{a}, \sqrt{b} \in \mathbb{Q}(\alpha)$, comme précédemment supposons que $x+y\sqrt{a}+z\sqrt{b}+w\sqrt{ab} = 0$. Alors $z+w\sqrt{a} \neq 0$ implique que

$$\sqrt{b} = \frac{x + y\sqrt{a}}{z + w\sqrt{a}} \in \mathbb{Q}(\sqrt{a})$$

ce qui est absurde car $\mathbb{Q}(\sqrt{a}) \cap \mathbb{Q}(\sqrt{b}) = \mathbb{Q}$ puisque a, b sont sans facteur carré et distincts. Donc $z + w\sqrt{a} = 0$, c'est-à-dire $z = 0$ et $w = 0$ car $\sqrt{a}$ est irrationnel. Et de même $x + y\sqrt{a} = 0$ implique que $x = y = 0$.

Par conséquent $\mathbb{Q}(\alpha)$ est au moins de dimenison 4 et donc exactement de dimension 4. Donc P est le polynôme minimal de α qui est donc un entier algébrique si et seulement si $n^2|2(a+b)$ et $n|a-b$. Or si c'est le cas alors $n^2|4a$ et donc si p est un nombre premier divisant n alors $p^2|4a$ et donc $p = 2$, il en suit que $n = 2$ ou 1. Finalement α est un entier algébrique si et seulement si $n = 1$ ou ($n = 2$ et $2|a-b$ et $2|a+b$) (l'une des deux divisibilités est superflue).

(Pour déterminer le degré d'un nombre algébrique α on peut également utiliser le résultat suivant : si $\beta \in \mathbb{Q}(\alpha)$ alors $\deg\beta | \deg\alpha$.)

Exercice 2.

(1) L'égalité $v^n P(u/v) = 0$ se réécrit

$$a_n u^n + a_{n-1} v u^{n-1} + \cdots + a_1 v^{n-1} u + a_0 v^n = 0$$

et donc $v | a_n u^n$ et $u | a_0 v^n$. Comme $u \wedge v = 1$, $v | a_n$ et $u | a_0$.

(2) Je pose $x = a/b$, où $a, b \in \mathbb{Z}$. Alors $(\mathrm{e}^{\pm i\pi x})^{2b} = 1$ et donc

$$2\cos(\pi x) = \mathrm{e}^{i\pi x} + \mathrm{e}^{-i\pi x}$$

est entier algébrique comme somme de deux racines de l'unité.

(3) Supposons que $\cos(\pi x) \in \mathbb{Q}$. Alors $2\cos(\pi x) \in \mathbb{Z}$ car les entiers algébriques rationnels sont les entiers. Donc $\cos(\pi x) \in \{0, \pm 1, \pm 1/2\}$, et donc $x \in \{0, 1/3, 1/2, 2/3, 1\}$.

Exercice 3.

(1) $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$ et $\Phi_p(X) = X^{p-1} + \ldots + 1$. D'après l'identité de Bézout, $\{a \mid a \wedge n = 1\}$ est en bijection avec $(\mathbb{Z}/n\mathbb{Z})^\times$ et donc $\deg \Phi = \varphi(n)$.

[μ_n (resp. μ_n^*) désigne l'ensemble des racines (primitives) n–ièmes de l'unité.]

(2) Comme le degré d'un produit est la somme des degrés, des deux égalités la première implique la deuxième. La première égalité a pour membres des polynômes unitaires à racines simples, il suffit donc de montrer que

$$\mu_n = \coprod_{d|n} \mu_d^*$$

Si $z^d = 1$ et d divise n alors $z^n = 1$, c'est-à-dire que $\mu_d \subset \mu_n$. Si $z \in \mu_n$ alors $z = \exp(2i\pi a/n)$ et en notant m le pgcd de a avec n on a que $a = ma'$ et $n = md$, où $a' \wedge d = 1$, et donc $z = \exp(2i\pi a'/d) \in \mu_d^*$. Enfin si $d \neq d'$ divisent n et $z \in \mu_d^*$, $z' \in \mu_{d'}^*$ alors z génère μ_d et z' génère μ_d' qui sont deux groupes distincts, donc $\mu_d^* \cap \mu_{d'}^* = \varnothing$.

(3) Démontrons-le par récurrence. Soit Ψ_n le polynôme produit des Φ_d pour $d|n$ et $d < n$, qui est unitaire comme produit de polynômes unitaires. Par hypothèse de récurrence $\Psi_n(X) \in \mathbb{Z}[X]$, or $X^n - 1 = \Psi_n(X)\Phi_n(X) + 0$ donc par unicité de la division euclidienne (voir corollaire 1) de $X^n - 1$ par $\Psi_n(X)$ on obtient que $\Phi_n(X) \in \mathbb{Z}[X]$.

(4) Soient p un nombre premier et $k \geqslant 1$. $\Phi_{p^k}(X)$ et $\Phi_p(X^{p^{k-1}})$ sont unitaires, il suffit donc de montrer qu'ils ont les mêmes racines comptées avec multiplicité, et comme $\Phi_{p^k}(X)$ est à racines simples il suffit de montrer qu'ils ont les mêmes racines et même degrés. On a une suite exacte

$$1 \to \mu_{p^{k-1}} \to \mu_{p^k} \to \mu_p \to 1$$

où $\mu_{p^k} \to \mu_p$ est la mise à la puissance p^{k-1}, qui car elle est bien définie assure que $\Phi_{p^k}(X)$ divise $\Phi_p(X^{p^{k-1}})$. On a toujours la bijection (entre ensembles ! !) qui découle de la suite exacte

$$\mu_{p^k} \simeq \mu_{p^{k-1}} \times \mu_p$$

mais ici on a de plus une bijection $\mu_{p^k}^* \simeq \mu_{p^{k-1}} \times \mu_p^*$ en raisonnant en termes de générateurs de groupes. D'où $\varphi(p^k) = \varphi(p)p^{k-1}$, c'est-à-dire

$$\deg \Phi_p(X^{p^{k-1}}) = \deg \Phi_p(X) \deg X^{p^{k-1}} = \varphi(p)p^{k-1} = \varphi(p^k) = \deg \Phi_{p^k}(X)$$

[On peut également démontrer le résultat par récurrence sur k et à l'aide de la première égalité du (2).]

(5) L'ensemble des racines n–ièmes de l'unité est stable par $z \mapsto 1/z$, et il en va de même pour l'ensemble de celles primitives car $a \wedge n = 1$ si et seulement si $(-a) \wedge n = 1$. Le terme constant de Φ_n vaut $(-1)^{\varphi(n)}$ sauf si $n = 2$ ou il vaut -1. Donc pour $n > 2$, $\Phi_n(X) = (-1)^{\varphi(n)} X^{\varphi(n)} \Phi_n(1/X)$ puisqu'ils sont unitaires et partagent les même racines. Or $\varphi(n)$ est pair quand $n > 2$, d'où le résultat.

(6) Si $a \wedge n = 1$ alors $ap \wedge n = 1$ et donc ω^p est une racine primitive n–ième de l'unité, et donc $\Phi_n(\omega^p) = 0$.

(7) $Q(X^p)$ est un polynôme annulateur de ω donc $Q(X^p)$ divise $P(X)$.

(8) Je note par $\overline{\cdot}$ la réduction modulo p. $\overline{Q(X^p)} = \overline{Q(X)}^p$ donc $P(X)$ et $Q(X)$ partage au moins un polynôme dans leur factorisation en irréductibles, et par conséquent cela donne un facteur carré dans le polynôme produit $\overline{P(X)Q(X)} = \overline{\Phi_n(X)}$. Mais

$$(\overline{X^n - 1})' = \overline{nX^{n-1}}$$

premier avec $\overline{X^n - 1}$ (propriété de ***séparabilité***) car $n \wedge p = 1$, en contradiction avec le fait qu'un facteur carré divise $\overline{X^n - 1}$. C'est donc que $Q(\omega^p) \neq 0$ et donc $P(\omega^p) = 0$.

(9) On a démontré précédemment que si p ne divise pas n alors $P(\omega^p) = 0$, et donc le polynôme minimal de ω^p est aussi P. On peut comme ça démontrer que si $m \wedge n = 1$ alors ω^m a pour polynôme minimal P, mais ce faisant on parcourt toutes les racines primitives n–ièmes de l'unité et donc $\Phi_n | P$, finalement $\Phi_n = P$.

Exercice 4.

Soit α une racine de P.

(1) α^n est un entier algébrique car les entiers algébriques forment un anneau, et $|\alpha^n| = |\alpha|^n \leqslant 1$.

(2) Soit $K = \mathbb{Q}(\alpha)$. Alors

$$P(X) = \prod_{\sigma : K \to \mathbb{C}} (X - \sigma(\alpha))$$

Considérons maintenant les polynômes P_n définis par

$$P_n(X) = \prod_{\sigma : K \to \mathbb{C}} (X - \sigma(\alpha)^n) = \prod_{\sigma : K \to \mathbb{C}} (X - \sigma(\alpha^n))$$

Ils sont tous dans $\mathbb{Z}[X]$ car

$$P_n(X) = (P_{\min, \alpha^n}(X))^{[K : \mathbb{Q}(\alpha^n)]}$$

et leurs coefficients sont bornés car leurs racines sont toutes de module $\leqslant 1$. L'ensemble $\{\alpha^n, n > 0\}$ est donc fini (car inclus dans l'ensemble des zéros

d'un nombre fini de polynômes). Il en suit qu'il existe $n > m$ tels que $\alpha^n = \alpha^m$.

(3) Ou $\alpha = 0$ et dans ce cas-là $P(X) = X - 0 = X$, ou $\alpha \neq 0$ et donc d'après la réponse à la question (2) il existe $n > m$ tels que $\alpha^{n-m} = 1$, c'est-à-dire α est une racine de l'unité dont le polynôme minimal est un polynôme cyclotomique.

Exercice 5.

(1) Je note G_d le groupe des unités de $\mathcal{O}_{\mathbb{Q}(\sqrt{-d})}$. Soit $x = a + b\sqrt{-d}$. x est une unité si et seulement si x est entier et $a^2 + db^2 = 1$, comme a, b sont en toute généralité dans $\frac{1}{2}\mathbb{Z}$. On en déduit que $a' := 2a, b' := 2b$ vérifient $(a')^2 + d(b')^2 = 4$. Il en suit que si $G_d \neq \{\pm 1\}$ alors $d \in \{1, 2, 3\}$, $a' \in \{\pm 1, \pm 2\}$ et $b' \in \{\pm 2, \pm 1\}$. En exhaustant tous les cas on obtient que $G_d = \{\pm 1\}$ sauf pour

$$G_1 = \{\pm 1, \pm\sqrt{-1}\} \quad G_3 = \{\pm 1, \pm(1 + \sqrt{-3})/2, \pm(1 - \sqrt{-3})/2\}$$

Exercice 6.

(1) K est au plus de degré 4 et contient deux sous-extensions de degré 2, donc $\dim_{\mathbb{Q}} K = 4$. C'est une base car libre (voir exercice 1) et de taille 4.

(2) Je note par M_α la matrice dans cette base de la multiplication par α, où $\alpha \in K$. Alors

$$M_{\sqrt{2}} = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad M_{\sqrt{3}} = \begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad M_{\sqrt{6}} = \begin{pmatrix} 0 & 0 & 0 & 6 \\ 0 & 0 & 3 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

(3) $K|\mathbb{Q}$ est de degré 4, il y a donc 4 plongements à énumérer. On connaît les deux plongements d'un corps quadratique dans $\mathbb{C}$ et comme K est engendré en tant que $\mathbb{Q}$–algèbre par $\sqrt{2}, \sqrt{3}$ on a que

$$\{K \hookrightarrow \mathbb{C}\} = \{\mathrm{id}, (\sqrt{2} \mapsto -\sqrt{2}; \sqrt{3} \mapsto \sqrt{3}), (\sqrt{2} \mapsto \sqrt{2}; \sqrt{3} \mapsto -\sqrt{3}), (\sqrt{2} \mapsto -\sqrt{2}; \sqrt{3} \mapsto -\sqrt{3})\}$$

(4) $K \to M_\alpha$ est un morphisme d'anneaux, en particulier si $a, b, c, d \in \mathbb{Q}$ et $\alpha := a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ alors

$$M_\alpha = I_4 + bM_{\sqrt{2}} + cM_{\sqrt{3}} + dM_{\sqrt{6}}$$

Or

$$\det M_\alpha = \prod_{\sigma : K \hookrightarrow \mathbb{C}} \sigma(\alpha)$$

D'où finalement

$$\begin{vmatrix} a & 2b & 3c & 6d \\ b & a & 3d & 3c \\ c & 2d & a & 2b \\ d & c & b & a \end{vmatrix} = (a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})(a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6})(a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6})(a-b\sqrt{2}-c\sqrt{3}-d\sqrt{6})$$

Exercice 7.

(1) Si P n'était pas irréductible alors il possèderait une racine dans $\mathbb{Q}$ et donc dans $\mathbb{Z}$.

Soit n une telle racine. Alors $n \neq 1, -1 \mod 3$ car $(-1)^3 - 1 + 3 = 1 \mod 3$ et $(1)^3 + 1 + 3 = 2 \mod 3$, et donc $n = 3k$ mais c'est absurde car on obtient $3(3k^2 + 1) = 1$.

[On pouvait aussi déjà regarder modulo 2, ou alors encore plus simplement écrire que $P(n) = 0$ si et seulement si $\alpha(\alpha^2 + 1) = 3$ qui n'a manifestement pas de solution dans $\mathbb{Z}$.]

P est irréductible de degré 3 et α en est une racine, donc $K = \mathbb{Q}(\alpha)$ est de degré 3 sur $\mathbb{Q}$.

(2) Je prends $(1, \alpha, \alpha^2)$ pour base de K. Dans cette base la multiplication par α^2 est la matrice

$$M_{\alpha^2} = \begin{pmatrix} 0 & 3 & 0 \\ 0 & -1 & 3 \\ 1 & 0 & -1 \end{pmatrix}$$

et donc $\mathrm{Tr}_{K|\mathbb{Q}}(\alpha^2) = -2$. Par ailleurs sur le polynôme minimal on peut lire puis déduire par multiplicativité de la norme les trois égalités

$$N_{K|\mathbb{Q}}(\alpha) = 3 \quad \mathrm{Tr}_{K|\mathbb{Q}}(\alpha) = 0 \quad N_{K|\mathbb{Q}}(\alpha^2) = 9$$

(3) Soit $Q(X) := \det(XI_3 - M_\alpha) \in \mathbb{Q}[X]$, le polynôme caractéristique de M_α. Alors pour tout $x \in K$, $N_{K|\mathbb{Q}}(x) = Q(x)$. Par ailleurs si $r = [K : \mathbb{Q}(\alpha)]$ alors $Q = P^r$, mais ici $r = 1$ donc $Q = P$.

Exercice 8.

(1) Supposons que $p = 1 \mod n$. Je pose $K := \mathbb{Q}(\zeta_n)$ le n–ième corps cyclotomique et $k = n/(p-1)$. Soit $\mathfrak{p}$ un idéal premier au-dessus de p. Alors l'image de ζ_n^k dans $\mathcal{O}_K/\mathfrak{p}$ est une racine $(p-1)$–ième de l'unité donc est un élément de $\mathbb{F}_p$, et d'autre part $\Phi_n(\zeta_n^k) = 0$. [...]

(2) $\Phi_n(N) | N^n - 1$ et $(N^n - 1) \wedge N^n = 1$ donc $\Phi_n(N) \wedge N^n = 1$, donc $\Phi_n(N) \wedge N = 1$.

(3) Supposons qu'ils forment un ensemble fini A. Soit N un multiple de leur produit. Comme $\Phi_n(N) \wedge N = 1$, si $\Phi_n(N) \neq 0, 1, -1$ alors il existe au moins un nombre premier p qui le divise et qui ne divise pas N, or $N \in \mathbb{F}_p$ est une racine de $\Phi_n(X)$ et donc $p = 1 \mod n$ mais p divise $\Phi_n(N)$ donc $p \notin A$: ce qui est absurde. Il reste donc à montrer qu'on peut écarter les cas où $\Phi_n(N) \in \{0, 1, -1\}$, comme il y a au plus $3 \deg \Phi_n$ tels N il suffit de prendre un N assez grand.

Exercice 9.

(1) $P'(X) = \sum_i \prod_{j \neq i} (X - \alpha_j)$. Par conséquent,

$$P'(\alpha_i) = \prod_{j \neq i} (\alpha_i - \alpha_j)$$

et donc

$$\prod_{i=1}^{n} P'(\alpha_i) = \prod_{i<j} (\alpha_i - \alpha_j)(\alpha_j - \alpha_i) = (-1)^{n(n-1)/2} \prod_{i<j} (\alpha_i - \alpha_j)^2$$

(2) Supposons $a, b \neq 0$ (raisonner par densité pour les autres valeurs de a et b, en usant du fait que le discriminant est une fonction polynomiale des coefficients du polynôme). Soit α une racine de P qui est donc non nulle. Alors

$$P'(\alpha) = n\alpha^{n-1} + a = (nb/\alpha - a(n-1)) = a(n-1)\alpha^{-1}(-nb/(n-1)a - \alpha)$$

Et donc en faisant le produit sur toutes les racines on obtient

$$\mathrm{disc}(P) = (-1)^{\frac{n(n-1)}{2}} a^n (n-1)^n \underbrace{(-1)^n b^{-1}}_{\text{produit des racines}} P(-nb/(n-1)a)$$

c'est-à-dire

$$\mathrm{disc}(P) = (-1)^{\frac{n(n-1)}{2}} (n^n b^{n-1} - (-1)^n (n-1)^{n-1} a^n)$$

(3) Appliquer la formule de Vandermonde.

(4) On écrit

$$N_{K|\mathbb{Q}}(P'(\alpha)) = \prod_{\sigma: K \to \mathbb{C}} \sigma(P'(\alpha)) = \prod_{\sigma: K \to \mathbb{C}} P'(\sigma(\alpha)) = (-1)^{\frac{n(n-1)}{2}} \mathrm{disc}(P)$$

Exercice 10.

(1) La matrice M_α de l'endomorphisme de multiplication par α dans la base $(1, \alpha, \ldots, \alpha^{n-1})$ est égale modulo p à

$$\begin{pmatrix} 0 & & & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}$$

c'est-à-dire est triangulaire inférieure stricte modulo p. Il en va de même avec ses puissances. Donc si $u_0, \ldots, u_{n-1} \in \mathbb{Z}$ alors

$$\begin{aligned} N_{K|\mathbb{Q}}(u_0 + u_1\alpha + \ldots + u_{n-1}\alpha^{n-1}) &= \det(u_0 \mathrm{I}_n + u_1 M_\alpha + \ldots + u_{n-1} M_\alpha^{n-1}) \\ &= \underbrace{\det(u_0 \mathrm{I}_n)}_{=u_0^n} \mod p \end{aligned}$$

(2) On le démontre par récurrence sur i. Supposons que $u_0, \ldots, u_{i-1}$ soient divisibles par p. Alors

$$\sum_{i \geqslant j} u_j \alpha^j = \omega - \sum_{i<j} u_j \alpha^j \in p\mathcal{O}_K$$

c'est-à-dire qu'il existe $\gamma \in \mathcal{O}_K$ tel que

$$p\gamma = u_i \alpha^i + \ldots + u_{n-1}\alpha^{n-1}$$

Il en suit que

$$p^n N_{K|\mathbb{Q}}(\gamma) = N_{K|\mathbb{Q}}(\alpha)^i N_{K|\mathbb{Q}}(u_i + \ldots + u_{n-1}\alpha^{n-1-i})$$

La valuation p–adique de $N_{K|\mathbb{Q}}(u_i + \ldots + u_{n-1}\alpha^{n-1-i})$ est donc $\geqslant n-i > 0$, c'est-à-dire par le résultat de la question (1) $p | u_i^n$, d'où $p | u_i$.

(3) Supposons que $p|\#(\mathcal{O}_K/\mathbb{Z}[\alpha])$. Alors ce dernier possède un élément d'ordre p, c'est-à-dire qu'il existe $\omega \notin \mathbb{Z}[\alpha]$ tel que $p\omega \in \mathbb{Z}[\alpha]$. Par la question précédente on aurait que p divise tous les u_i, et donc que $\omega = (p\omega)/p \in \mathbb{Z}[\alpha]$: ***absurde***.

(4) On trouve $\mathrm{disc}(1, \alpha, \alpha^2) = -5^2 \cdot 11$. Or d'après ce qui précède

$$\#(\mathcal{O}_K/\mathbb{Z}[\alpha]) \wedge 5 = 1 \quad \text{et} \quad \#(\mathcal{O}_K/\mathbb{Z}[\alpha])^2 | 5^2 \cdot 11$$

donc $\#(\mathcal{O}_K/\mathbb{Z}[\alpha]) = 1$.

(5) Je pose $P(X) := \Phi_p(X+1)$ qui est un polynôme p–Eisenstein. En effet, on a l'égalité

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X+1-1} = \underbrace{\frac{X^p + 1^p - 1}{X}}_{=X^{p-1}} \mod p$$

et le coefficient constant de P est $\Phi_p(0+1) = p$. Maintenant $K_p = \mathbb{Q}(\zeta - 1)$ où ζ est une racine de Φ_p. Comme $\zeta - 1$ est racine de $P(X)$, d'après (3) p ne divise pas $\#(\mathcal{O}_{K_p}/\mathbb{Z}[\zeta - 1])$. Or on vérifie que $\mathbb{Z}[\zeta - 1] = \mathbb{Z}[\zeta]$ et donc $\mathrm{disc}(K_p) = \mathrm{disc}(1, \zeta, \ldots, \zeta^{p-2}) = \mathrm{disc}(\Phi_p)$. Or ce dernier discriminant est $\pm$ une puissance de p et donc $\#(\mathcal{O}_{K_p}/\mathbb{Z}[\zeta - 1]) = 1$, c'est-à-dire $\mathcal{O}_{K_p} = \mathbb{Z}[\zeta]$.

(6) Soit $p > 2$. Premièrement on peut choisir ζ de telle sorte à ce que

$$\omega_p = \zeta + \zeta^{-1}$$

qui est un entier algébrique donc $\mathbb{Z}[\omega_p] \subset \mathcal{O}_{K_p^+}$. Soit $x \in \mathcal{O}_{K_p^+}$. Alors $x \in \mathcal{O}_K = \mathbb{Z}[\zeta]$. Il existe donc $a_0, \ldots, a_{p-1}$ des entiers tels que

$$x = a_0 + a_1\zeta + \ldots + a_{p-1}\zeta^{p-1}$$

Or x est réel et $\overline{\zeta} = \zeta^{-1}$ donc $x = \overline{x}$ implique que si $i \in \{1, \ldots, p-1\}$ alors $a_i = a_{p-i}$, c'est-à-dire

$$x = a_0 + a_1(\zeta + \zeta^{-1}) + a_2(\zeta^2 + \zeta^{-2}) + \ldots + a_{\frac{p-1}{2}}(\zeta^{\frac{p-1}{2}} + \zeta^{-\frac{p-1}{2}})$$

Comme $\zeta^k + \zeta^{-k} = 2\cos(2k\pi/p)$ on a que

$$\begin{aligned} x &= a_0 + a_1 2\cos(2\pi/p) + a_2 2\cos(4\pi/p) + \ldots + a_{\frac{p-1}{2}} 2\cos((p-1)\pi/p) \\ &= a_0 + a_1 T_1(\omega_p) + a_2 T_2(\omega_p) + \ldots + a_{\frac{p-1}{2}} T_{\frac{p-1}{2}}(\omega_p) \in \mathbb{Z}[\omega_p] \end{aligned}$$

D'où le résultat.

(7) On fait comme en (4).

Exercice 11.

(1) Il s'agit de montrer que le $\mathbb{Z}$–module $M := \mathcal{O}_K/\mathbb{Z}[\alpha, \beta]$ est trivial. L'idée est la suivante : en calculant le discriminant de $\mathbb{Z}[\alpha, \beta]$ on sait que $\#M$ est impair et donc que 2 y est inversible. Par conséquent pour montrer que M est trivial il suffit de montrer que $M[\frac{1}{2}]$ est trivial c'est-à-dire que $\mathcal{O}_K[\frac{1}{2}] = \mathbb{Z}[\frac{1}{2}][\alpha][\beta]$.

Je commence par le calcul du discriminant. On vérifie que $(1, \alpha, \beta, \alpha\beta)$ est une base de $\mathbb{Z}[\alpha, \beta]$ (pour cela on vérifie essentiellement la liberté de la famille

puisque $\alpha^2\beta$ et $\alpha\beta^2$ sont combinaisons $\mathbb{Z}$–linéaires de la famille). Les relations centrales sont $\mathrm{Tr}(1) = 4$ et $\mathrm{Tr}(\sqrt{m}) = \mathrm{Tr}(\sqrt{n}) = \mathrm{Tr}(\sqrt{mn}) = 0$ (obtenues en sommant les images par les plongements de K dans $\mathbb{C}$). S'en suivent les relations

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(\beta) = 2 \quad \mathrm{Tr}(\alpha\beta) = 1$$

Les équations minimales $\alpha^2 - \alpha = \frac{m-1}{4}$ et $\beta^2 - \beta = \frac{n-1}{4}$ impliquent que

$$\mathrm{Tr}(\alpha^2) = m + 1 \quad \mathrm{Tr}(\beta^2) = n + 1$$

Je peux calculer $\mathrm{Tr}(\alpha^2\beta)$ et $\mathrm{Tr}(\alpha\beta^2)$ à partir du système

$$\begin{aligned} \mathrm{Tr}(\alpha^2\beta) + \mathrm{Tr}(\beta^2\alpha) &= \mathrm{Tr}(\alpha\beta(\alpha+\beta)) = \frac{m+n}{2} + 1 \\ \mathrm{Tr}(\alpha^2\beta) - \mathrm{Tr}(\beta^2\alpha) &= \mathrm{Tr}(\alpha\beta(\alpha-\beta)) = \frac{m-n}{2} \end{aligned}$$

et par ailleurs

$$\mathrm{Tr}(\alpha^2\beta^2) = \mathrm{Tr}\left(\alpha\beta + \frac{\beta(m-1)}{4} + \frac{\alpha(n-1)}{4} + \frac{(m-1)(n-1)}{16}\right) = 1 + \frac{m-1}{2} + \frac{n-1}{2} + \frac{(m-1)(n-1)}{4}$$

Finalement le discriminant est le déterminant de la matrice

$$\begin{pmatrix} 4 & 2 & 2 & 1 \\ 2 & m+1 & 1 & \frac{m+1}{2} \\ 2 & 1 & n+1 & \frac{n+1}{2} \\ 1 & \frac{m+1}{2} & \frac{n+1}{2} & \mathrm{Tr}(\alpha^2\beta^2) \end{pmatrix}$$

Un petit calcul montre qu'on obtient ainsi

$$\mathrm{disc}(1, \alpha, \beta, \alpha\beta) = (mn)^2$$

D'où le fait que $(\#M)^2 | (mn)^2$ qui est impair par hypothèse. (Reste à faire)

(2) Soit $B := \mathcal{O}_K/2\mathcal{O}_K$. C'est une $\mathbb{F}_2$–algèbre on peut donc définir un morphisme $\mathbb{F}_2[X,Y] \longrightarrow B$ de telle sorte à ce que X (resp. Y) s'envoie sur l'image de α (resp. de β) par la projection $\mathcal{O}_K \to B$. Comme

$$\alpha^2 - \alpha = \frac{m-1}{4} \in 2\mathcal{O}_K \quad \beta^2 - \beta = \frac{n-1}{4} \in 2\mathcal{O}_K$$

le morphisme passe au quotient par l'idéal (X^2-X, Y^2-Y) et il est surjectif car $\mathcal{O}_K = \mathbb{Z}[\alpha, \beta]$. C'est un isomorphisme car d'une part A est de dimension 4 et V aussi (se rappeler que $\mathcal{O}_K \simeq \mathbb{Z}^4$ en tant que $\mathbb{Z}$–module et donc $B \simeq (\mathbb{Z}/2\mathbb{Z})^4$).

(3) Comme $\forall s \in \mathbb{F}_2, s^2 = s$, chaque application $\{X, Y\} \to \{0, 1\}$ induit un morphisme $A \to \mathbb{F}_2$ qui est déterminé par les images de X et de Y par $\mathbb{F}_2[X,Y] \to A \to \mathbb{F}_2$. D'où le résultat.

(4) Si $\mathcal{O}_K$ est monogène alors il existe $\gamma \in \mathcal{O}_K$ tel que $\mathcal{O}_K = \mathbb{Z}[\gamma]$, et donc $B = \mathbb{F}_2[\sigma]$, où σ est l'image de γ dans B, et on dispose donc d'un morphisme surjectif $\mathbb{F}_2[T] \longrightarrow B \simeq A$: ainsi l'application

$$\mathrm{Hom}_{\mathrm{Anneaux}}(A, \mathbb{F}_2) \longrightarrow \mathrm{Hom}_{\mathrm{Anneaux}}(\mathbb{F}_2[T], \mathbb{F}_2) \simeq \mathbb{F}_2$$

est injective ce qui est absurde.

Exercice 12.

(1,a) Soit $A := \mathbb{Z}\alpha_1 \oplus \ldots \oplus \mathbb{Z}\alpha_n$. Alors $\#(\mathcal{O}_K/A)^2$ divise $\mathrm{disc}(\alpha_1, \ldots, \alpha_n)$ qui est sans facteur carré, donc $\#(\mathcal{O}_K/A) = 1$. D'où le résultat.

(1,b) Premièrement le polynôme $P(T) := T^4 - T - 1$ est irréductible. En effet, s'il ne l'était pas alors ou il serait le produit de deux polynômes de degré 2 ou alors il aurait une racine rationnelle : dans le deuxième cas la racine serait ± 1, d'après [Exercice 2, (1)], or c'est manifestement impossible ; dans le premier cas en écrivant ce que l'écriture en produit de polynômes de degré 2 à coefficients entiers implique, on obtient une absurdité. Donc P est irréductible, et K est de degré 4.

Calculons le discriminant de $\mathbb{Z}[\alpha]$ d'après la formule pour le discriminant de P. On obtient $\mathrm{disc}(\mathbb{Z}[\alpha]) = -283$ et 283 est un nombre premier. Donc $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

(2,a) On passe de $(\alpha_1, \ldots, \alpha_n)$ à la famille $(\omega, \alpha_2, \ldots, \alpha_n)$ par une opération sur les colonnes et donc

$$\mathrm{disc}(\omega, \alpha_2, \ldots, \alpha_n) = x_1^2 \mathrm{disc}(\alpha_1, \ldots, \alpha_n)$$

Comme $(\omega, \alpha_2, \ldots, \alpha_n)$ est une $\mathbb{Q}$–base de K formée d'entiers algébriques et que $x_1 \in [0, 1[$ par minimalité on obtient que $x_1 = 0$.

(2,b) Soit $\omega \in \mathcal{O}_K$. Alors en particulier $\omega \in K$ et donc il existe $x_1, \ldots, x_n \in \mathbb{Q}$ tels que $\omega = x_1\alpha_1 + \ldots + x_n\alpha_n$. On peut réécrire ça de la façon suivante

$$\underbrace{\omega - (\lfloor x_1 \rfloor \alpha_1 + \ldots + \lfloor x_n \rfloor \alpha_n)}_{\in \mathcal{O}_K} = \underbrace{(x_1 - \lfloor x_1 \rfloor)}_{\in [0,1[} \alpha_1 + \ldots + \underbrace{(x_n - \lfloor x_n \rfloor)}_{\in [0,1[} \alpha_n$$

D'après ce qui précède, $x_1 = \lfloor x_1 \rfloor$. En fait l'argument précédent montre également que pour tout i, $x_i = \lfloor x_i \rfloor$ (en considérant la famille $(\alpha_1, \ldots, \omega, \ldots, \alpha_n)$ en mettant ω à la place de α_i). Ainsi les x_i sont entiers et donc $\omega \in \mathbb{Z}[\alpha_1, \ldots, \alpha_n]$.

(3,a) Le polynôme $T^3 - T - 4$ est irréductible sur $\mathbb{Q}[X]$ car il est de degré 3 et n'a pas de racine dans $\mathbb{F}_3$: K est donc de degré 3. Le discriminant de $\mathbb{Z}[\alpha]$ est donc celui de P qui est $4 \cdot 107$.

(3,b) $\omega \in \mathcal{O}_K$ car il vérifie l'équation $\omega^3 + 2\omega^2 - 6\omega - 8 = 0$. Calculons maintenant le discriminant de la famille $(1, \alpha, \omega)$:

$$\mathrm{disc}(1, \alpha, \omega) = \left(\frac{1}{2}\right)^2 \mathrm{disc}(1, \alpha, \alpha^2) = 107$$

Comme 107 est premier on en déduit que $(1, \alpha, \omega)$ est une base de $\mathcal{O}_K$ et en particulier que $\mathbb{Z}[\alpha]$ n'a pas le même discriminant que $\mathcal{O}_K$ et donc $\mathcal{O}_K \neq \mathbb{Z}[\alpha]$.

Exercice 13.

(1) Les $\varphi_i(z)$ sont les racines du polynôme caractéristique de la multiplication par z dans K, on a donc

$$(X - z)^n = \Pi_z(X)^{[K:\mathbb{Q}(z)]}$$

Mais comme $\Pi_z(X)$ est à racines simples on en déduit que $[K : \mathbb{Q}(z)] = n$ et donc $z \in \mathbb{Q}$.

(1,bis). La première remarque est qu'un plongement de K s'étend à un plongement de L et donc les plongements de K sont à valeurs dans L. Par conséquent, si ψ est un plongement de L alors $\psi \circ \varphi_i$ est un plongement de K comme composée de morphismes de corps. Maintenant ψ est un automorphisme de L donc on peut considérer ψ^{-1} qui est également un plongement de L, et l'application induite $\varphi_i \mapsto \psi^{-1} \circ \varphi_i$ est l'inverse de $\varphi_i \mapsto \psi \circ \varphi_i$.

(2) On utilise la définition du déterminant d'une matrice comme somme indexée par les permutations de $\{1, \dots, n\}$ et la formule

$$\mathrm{disc}(\alpha_1, \dots, \alpha_n) = (\det(\varphi_i(\alpha_j)))^2$$

(3) Comme a et b sont des entiers algébriques (en tant qu'expression algébrique à coefficients entiers d'entiers algébriques) il reste à montrer que $a+b$ et ab sont dans $\mathbb{Q}$. Pour cela on utilise le résultat de la question 1 appliqué à L. D'après (1,bis) il existe une permutation $\tau \in S_n$ telle que $\psi \circ \varphi_i = \varphi_{\tau(i)}$. Si $\varepsilon(\tau) = 1$ alors $(\psi(a), \psi(b)) = (a, b)$ et si $\varepsilon(\tau) = -1$ alors $(\psi(a), \psi(b)) = (b, a)$. Par conséquent dans tous les cas

$$\psi(a+b) = a+b \qquad \psi(ab) = ab$$

D'où le résultat.

(4) Soient $(\alpha_1, \dots, \alpha_n)$ une base de $\mathcal{O}_K$. Alors

$$\mathrm{disc}(K) = \mathrm{disc}(\alpha_1, \dots, \alpha_n) = (a-b)^2 = (a+b)^2 - 4ab = (a+b)^2 \mod 4$$

Or $a+b$ est un entier donc $\mathrm{disc}(K) = 0, 1 \mod 4$.

Exercice 14.

(1) $(1, j, j^2)$ est un exemple de triangle équilatéral, et les autres sont obtenus à partir de lui en appliquant une similitude qui consiste à composer une translation (additionner par un $\alpha \in \mathbb{C}$) et une rotation + homothétie (multiplier par un $\beta \in \mathbb{C}^\times$), et donc si z_1, z_2, z_3 sont les sommets d'un tel triangle alors

$$z_1 + z_2 j + z_3 j^2 = \alpha + \beta + (\alpha + \beta j)j + (\alpha + \beta j^2)j^2 = \alpha(1 + j + j^2) + \beta(1 + j^2 + j^4) = 0$$

Réciproquement, si $z_1 + z_2 j + z_3 j^2 = 0$ (et $z_1 \neq z_3$ sinon le triangle est trivial...) alors en translatant par $-z_1$ on obtient $(z_2 - z_1)j + (z_3 - z_1)j^2 = 0$, c'est-à-dire

$$\frac{z_3 - z_1}{z_2 - z_1} = -j^2$$

équation qui donne l'angle entre les segments $[z_1, z_2]$ et $[z_1, z_3]$. Finalement l'équation initiale est stable par permutation cyclique des z_i, cela permet de déduire que les trois angles du triangles sont égaux.

(2) D'après ce qui précède, l'existence d'un triangle non trivial donnerait que $-j^2 \in K$, absurde car $-j^2 \notin \mathbb{Q}$. On peut aussi dire que le polynôme minimal de j sur K est $1 + X + X^2$, car ce dernier est le polynôme minimal de j sur $\mathbb{Q}$ et $K \cap \mathbb{Q}(j) = \mathbb{Q}$, ainsi l'existence d'un triangle équilatéral donnerait

que $z_1 + z_2X + z_3X^2$ serait un multiple de $1 + X + X^2$, et donc $z_1 = z_2 = z_3$.

Exercice 15.

(1) L'application linéaire $\mathbb{R}^2 \to \mathbb{R}^2$ donnée par la matrice

$$M := \begin{pmatrix} p & u \\ 0 & 1 \end{pmatrix}$$

induit une bijection entre réseaux $\mathbb{Z}^2 \to L$. Donc

$$\mathrm{covol}(L) = |\det M| \mathrm{covol}(\mathbb{Z}^2) = p$$

(2) $C_d(r)$ est une ellipse centrée en $(0,0)$ et de demi-axes de longueur $\sqrt{r}$, $\sqrt{r/d}$, donc

$$\mathrm{vol}(C_d(r)) = \frac{\pi r}{\sqrt{d}}$$

Elle est bien compacte, symétrique et convexe donc d'après le lemme du corps convexe si $2^{-2}\mathrm{vol}(C_d(r)) \geqslant \mathrm{covol}(L)$ alors $L \cap C_d(r) \neq \varnothing$. D'où le résultat avec

$$r = \frac{4p\sqrt{d}}{\pi}$$

(3) Soit (a,b) l'élément dans cette intersection. Alors $a = ub[p]$ et donc comme $a = ub[p]$ et $u^2 = -d[p]$ on a que $a^2 + db^2 = 0[p]$. Soit k l'entier tel que $a^2 + db^2 = kp$ alors $0 \leqslant kp = a^2 + db^2 \leqslant \frac{4p\sqrt{d}}{\pi}$, d'où le résultat en simplifiant par p.

(4,5) Premièrement si p est de la forme a^2+db^2 alors p ne peut pas diviser a et b car sinon p^2 diviserait p, et si b est divisible par p alors a aussi car $a^2 = -db^2[p]$. Donc b est inversible modulo p et on conclut sur le fait que $-d$ est un carré modulo p. On démontre ainsi un sens à chaque fois des deux équivalences à démontrer.

Supposons que $p = 1, 3[8]$ et $p \neq 2$, et $d = 2$. Alors -2 est un carré modulo p et la constante h associée vaut 1, donc d'après (3) p est de la forme $a^2 + 2b^2$.

Supposons que $p = 1[3]$ et $p \neq 3$, et $d = 3$. Alors -3 est un carré modulo p et la constante h associée vaut 2, donc d'après (3) p ou $2p$ est de la forme $a^2 + 3b^2$. Si $2p = a^2 + 3b^2$ alors modulo 3 on obtient $-1 = a^2$: ***absurde***. Donc p est de la forme $a^2 + 3b^2$.

Exercice 16.

(1,2) I est maximal si et seulement si $\mathcal{O}_K/I$ est un corps. Par conséquent, si $N(I)$ est premier alors $\mathcal{O}_K/I$ est un anneau de cardinal p : il est donc isomorphe à $\mathbb{F}_p$ qui est bien un corps ; si I est maximal alors $\mathcal{O}_K/I$ est un corps fini qui est de cardinal une puissance d'un nombre premier et $N(I) = |\mathcal{O}_K/I|$.

Exercice 17.

(1,a) $\mathfrak{P}$ est un idéal premier de $\mathcal{O}_K$ donc $\mathfrak{P} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. Il existe donc p un nombre premier tel que $p\mathbb{Z} = \mathfrak{P} \cap \mathbb{Z}$ et il n'y a qu'un seul

nombre premier dans $p\mathbb{Z}$, d'où le résultat. Enfin l'inclusion d'idéaux implique que $N|N(p\mathcal{O}_K) = |N_{K|\mathbb{Q}}(p)| = p^2$ et $N \neq 1$ car $\mathfrak{P} \neq \mathcal{O}_K$. Donc $N \in \{p, p^2\}$.

(1,b) Si $N = p^2$ alors $|(p\mathcal{O}_K)/\mathfrak{P}| = \frac{N_K(p\mathcal{O}_K)}{N} = 1$, c'est-à-dire $\mathfrak{P} = p\mathcal{O}_K$.

(1,c) Supposons $N = p$. Écrivons la décomposition de $p\mathcal{O}_K$ en produits d'idéaux premiers, comme $\mathfrak{P} \subset p\mathcal{O}_K$ alors il existe un idéal $\mathfrak{P}'$ tel que

$$p\mathcal{O}_K = \mathfrak{P}\mathfrak{P}'$$

La multiplicativité de la norme donne que $p^2 = pN_K(\mathfrak{P}')$ et donc que $N_K(\mathfrak{P}') = p$. Il en suit que $\mathfrak{P}'$ est maximal, c'est-à-dire premier, d'après (1, Ex.16) et donc que $p\mathcal{O}_K = \mathfrak{P}\mathfrak{P}'$ est bien une décomposition en produit d'idéaux premiers. Comme $\mathcal{O}_K$ est monogène généré par ω on en conclut que P modulo p se décompose en $(T-a)(T-b)$, où $a, b \in \mathbb{F}_p$, et que $\mathfrak{P} = (p, \omega - c)$, où c est un entier. Finalement si $\mathfrak{P}$ n'est pas principal alors pour tout $\alpha \in P$, $\alpha\mathcal{O}_K \neq \mathfrak{P}$, c'est-à-dire $|N_{K|\mathbb{Q}}(\alpha)| = N_K(\alpha\mathcal{O}_K)$ est divisible par p et $> p$. Donc $|N_{K|\mathbb{Q}}(\alpha)| \geqslant 2p$. On conclut en remarquant que si $n \in \mathbb{Z}$ alors $\omega - (c + np) \in \mathfrak{P}$.

(2) $d = 101 = 1[4]$, donc le discriminant vaut 101 et la borne de Minkowski vaut un peu plus que 10. Par conséquent, $\mathrm{Cl}(\mathcal{O}_K)$ est généré par des idéaux premiers contenant un nombre premier $p \in \{2, 3, 5, 7\}$. Soit $\mathfrak{P}$ un tel idéal. Montrons qu'il est nécessairement principal. S'il est de norme p^2 alors d'après (1,b) il est principal. S'il est de norme $p = 2, 3$ ou 7 alors $P(T) = T^2 - T - 25$ est, d'après (1,c), réductible modulo p mais c'est absurde car P est de degré 2 et n'a pas de racine modulo $2, 3$ ou 7. Supposons qu'il est de norme 5. Comme

$$T^2 - T - 25 = T(T-1)[5]$$

d'après (1,c) $\mathfrak{P} = (5, \omega)$ ou $(5, \omega - 1)$ mais comme leur produit vaut $5\mathcal{O}_K$, montrer que l'un est principal revient à montrer que $(5, \omega)$ est principal. Eh bien, si $(5, \omega)$ n'est pas principal alors toujours d'après (1,c) pour $n = 1$ on obtient que $5 = |N_{K|\mathbb{Q}}(\omega - 5)| \geqslant 2 \cdot 5 = 10$, absurde. Donc $\mathfrak{P}$ est principal.

Exercice 18.

(1) $T^3 - 2$ est 2–Eisenstein donc K est degré 3. Calcul classique du discriminant de $(1, \alpha, \alpha^2)$. L'indice i de A dans $\mathcal{O}_K$ a donc au plus 2 ou 3 dans sa décomposition en facteurs premiers. Or $T^3 - 2$ est 2–Eisenstein donc d'après un exercice précédent 2 ne divise pas i et $(T-1)^3 - 2$ est 3–Eisenstein donc 3 ne divise pas i (car $A = \mathbb{Z}[\alpha] = \mathbb{Z}[\alpha + 1]$) ; $i = 1$ et donc $A = \mathcal{O}_K$.

(2) La borne de Minkoswki est < 3. $\mathrm{Cl}(\mathcal{O}_K)$ est généré par les $I_2(Q)$ où Q est un facteur irréductible de $T^3 - 2 \in \mathbb{F}_2[T]$, or il n'y a que T comme tel facteur. Donc $\mathrm{Cl}(\mathcal{O}_K)$ est généré par $I_2(T) = (2, \alpha) = I$ et comme $I^3 = 2\mathcal{O}_K$, on obtient que $\mathrm{Cl}(\mathcal{O}_K) = \{[\mathcal{O}_K], [I], [I^2]\}$. D'où le résultat.

(3) *(Démonstration rapide)* I possède α et $2 = \alpha^3 \in \alpha\mathcal{O}_K$, donc $I = \alpha\mathcal{O}_K$. *(Démonstration qui se généralise même si $N_{K|\mathbb{Q}}(\alpha)$ n'est pas un nombre premier)* $I^3 = 2\mathcal{O}_K$ *implique que* $N(I) = 2$, *or par ailleurs*

$$|I/\alpha\mathcal{O}_K| = N(\alpha\mathcal{O}_K)/N(I) = 1$$

d'où le résultat.

Exercice 19.

(1) On applique la méthode et on trouve à chaque fois que la famille génératrice du groupe des classes est composée d'idéaux principaux.

(2) $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ et la borne de Minkowski est < 3. Le polynôme minimal de $\sqrt{-5}$ est T^2+5 et il se décompose en $(T+1)^2$ modulo 2. Donc $\mathrm{Cl}(\mathcal{O}_K)$ est généré par la classe de $\mathfrak{p} = (2, 1+\sqrt{-5})$ qui est d'ordre 2 car $2\mathcal{O}_K = \mathfrak{p}^2$. Cette égalité donne également $N(\mathfrak{p}) = 2$: $\mathfrak{p}$ n'est donc pas principal car 2 ne s'écrit par comme la norme d'un $a = x + y\sqrt{-5} \in \mathcal{O}_K$ qui vaut $x^2 + 5y^2$.

(3) $\mathcal{O}_K = \mathbb{Z}[\sqrt{-14}]$ et la borne de Minkowski est < 5. Le polynôme minimal de $\sqrt{-14}$ est $T^2 + 14$ et il se décompose en T^2 modulo 2 et $(T-1)(T+1)$ modulo 3. Je note

$$\mathfrak{p}_2 := (2, \sqrt{-14}), \quad \mathfrak{p}_{3,-} := (3, \sqrt{-14} - 1), \quad \mathfrak{p}_{3,+} := (3, \sqrt{-14} + 1)$$

ils vérifient les relations

$$\mathfrak{p}_2^2 = 2\mathcal{O}_K \qquad \mathfrak{p}_{3,-}\mathfrak{p}_{3,+} = 3\mathcal{O}_K \qquad N(\mathfrak{p}_2) = 2 \qquad N(\mathfrak{p}_{3,+}) = N(\mathfrak{p}_{3,-}) = 3$$

On cherche un élément dont la décomposition en nombres premiers de sa norme ne comporte que des 2 et 3 : par exemple $a_\pm := 2 \pm \sqrt{-14}$. L'idéal $\mathfrak{a}_\pm := a^\pm \mathcal{O}_K$ est de norme $18 = 2 \cdot 3^2$. Par conséquent sa décomposition comprend une occurence de $\mathfrak{p}_2$. Par ailleurs elle comporte deux occurences de $\mathfrak{p}_{3,+}$, ou deux de $\mathfrak{p}_{3,-}$, ou une occurence de $\mathfrak{p}_{3,+}$ et une de $\mathfrak{p}_{3,-}$: mais la troisième situation est impossible car on aurait $2 \pm \sqrt{-14} \in \mathfrak{a}_\pm \subset \mathfrak{p}_{3,+}\mathfrak{p}_{3,-} = 3\mathcal{O}_K$. Finalement le fait que $a_+a_- = 2$ implique que $\mathfrak{a}_- \neq \mathfrak{a}_+$ (sinon $2 \in \mathfrak{a}_+$ et donc $\mathfrak{p}_2^2$ divise $\mathfrak{a}_+$: absurde) et donc que quitte à échanger $+$ et $-$ dans la notation des idéaux on a

$$\mathfrak{a}_\pm = \mathfrak{p}_2(\mathfrak{p}_{3,\pm})^2$$

Le groupe des classes de $\mathcal{O}_K$ est donc engendré par un élément d'ordre 4 car $\mathfrak{p}_2$ n'est pas principal (2 n'est pas de la forme x^2+14y^2 avec $x, y \in \mathbb{Z}$), donc $\mathrm{Cl}(\mathcal{O}_K) \simeq \mathbb{Z}/4\mathbb{Z}$.

Exercice 20.

(1) La borne de Minkowski est < 7, et modulo $2, 3, 5$ le polynôme minimal de $\sqrt{-30}$ vaut T^2, on pose donc $\mathfrak{p}_p = (p, \sqrt{-30})$.

(2) La normde $\sqrt{-30}$ vaut $30 = 2 \cdot 3 \cdot 5$ donc $\sqrt{-30}\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$.

Exercice 21.

(1) $\Pi_{\alpha,K}(T) = T^n$ modulo p est une écriture en produits d'irréductibles de $\mathbb{F}_p[T]$, et donc $p\mathcal{O}_K = \mathfrak{p}^n$, où $\mathfrak{p} = I_p(T) = (p, \alpha)$.

(1,bis) Je note $\Pi_{\alpha,K}(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1T + a_0$. Soit $\mathfrak{p}$ un idéal divisant $p\mathcal{O}_K$ et $e \geqslant 1$ l'entier tel que $p\mathcal{O}_K = \mathfrak{p}^e\mathfrak{a}$ et $\mathfrak{p}$ ne divise pas $\mathfrak{a}$. Il suffit de montrer que $e \geqslant n$, car en appliquant les normes on a déjà que $e \leqslant n$. L'équation $\Pi_{\alpha,K}(\alpha) = 0$ donne que $\alpha^n \in p\mathcal{O}_K \subset \mathfrak{p}$, comme $\mathfrak{p}$ est premier on en déduit que $\alpha \in \mathfrak{p}$. Il en suit que $a_i\alpha^i \in \mathfrak{p}^{e+1}$ donc $\alpha^n + a_0 \in \mathfrak{p}^{e+1}$. Or a_0 n'est pas divisible par p^2, donc $a_0 \notin \mathfrak{p}^{e+1}$, d'où $\alpha^n \notin \mathfrak{p}^{e+1}$. On conclut avec $\alpha^n \in \mathfrak{p}^n$, qui donne $n < e + 1$.

(2,a) Si $\mathfrak{p} = \mathfrak{p}^2$ alors $N(\mathfrak{p}) = N(\mathfrak{p})^2$ et donc $N(\mathfrak{p}) = 1$, ce qui est absurde car $\mathfrak{p} \neq \mathcal{O}_K$.

(2,b) $\beta\mathcal{O}_K \subset \mathfrak{p}$, il existe donc un idéal $\mathfrak{b}$ de $\mathcal{O}_K$ tel que $\beta\mathcal{O}_K = \mathfrak{p}\mathfrak{b}$. Si $\mathfrak{p}$ divise $\mathfrak{b}$ alors $\beta \in \mathfrak{p}^2$: absurde. Donc $\mathfrak{p}$ ne divise pas $\mathfrak{b}$, mais comme il est premier cela veut dire que $\mathfrak{b}$ et $\mathfrak{p}$ sont premiers entre eux, c'est-à-dire $\mathfrak{b}+\mathfrak{p} = \mathcal{O}_K$.

(2,c) $\mathfrak{p}$ est totalement ramifié donc $N(\mathfrak{p}) = p$, il en suit que

$$N(\beta\mathcal{O}_K) = N(\mathfrak{p})N(\mathfrak{b}) = pN(\mathfrak{b})$$

et $N(\beta\mathcal{O}_K) = |N_{K|\mathbb{Q}}(\beta)| = |b_0|$. D'où $p|b_0$. Si $p^2|b_0$ alors $p|N(\mathfrak{b})$, donc $p\mathcal{O}_K \subset \mathfrak{b}$ et $\mathfrak{b} \subset \mathfrak{p}$: absurde.

(2,d) Démontrons par récurrence sur j que $p|b_i$ pour $\forall i < j$, ($j \in \{0, \ldots, n-1\}$). L'égalité $\beta^n + b_{n-1}\beta^{n-1} + \ldots + b_1\beta + b_0 = 0$ implique que

$$\beta^n + b_{n-1}\beta^{n-1} + \ldots + b_j\beta^j = 0 \mod p\mathcal{O}_K$$

et comme $(\beta\mathcal{O}_K)^n = \mathfrak{p}^n\mathfrak{b}^n$, en particulier $\beta^n\mathcal{O}_K \subset p\mathcal{O}_K$, en multipliant par β^{n-1-j} on obtient

$$b_j\beta^{n-1} = 0 \mod p\mathcal{O}_K$$

En prenant les normes on obtient que p^n divise $b_j^n b_0^{n-1}$. Comme b_0 est de valuation p–adique 1, b_j est divisible par p.

(2,e) Le polynôme caractéristique de β est donc un polynôme p–Eisenstein, en particulier il est irréductible et donc $K = \mathbb{Q}(\beta)$.

Exercice 22.

(1) Le discriminant de $T^4 - 2$ est -2^{11} et comme $T^4 - 2$ est 2–Eisenstein, il en suit que $|\mathcal{O}_K/\mathbb{Z}[2^{\frac{1}{4}}]|^2$ divise 2^11 et est premier avec 2, d'où le résultat.

La borne de Minkowski de $\mathbb{Q}(2^{\frac{1}{4}})$ est < 7.

Pour 2 on a un idéal premier $\mathfrak{p}_2$ tel que $\mathfrak{p}_2^4 = 2\mathcal{O}_K$.

Pour 3 on a

$$T^4 - 2 = (T^2 - T - 1)(T^2 + T - 1)$$

et donc deux idéaux premiers $\mathfrak{p}_{3,+}, \mathfrak{p}_{3,-}$ tels que

$$\mathfrak{p}_{3,+}\mathfrak{p}_{3,-} = 3\mathcal{O}_K$$

Pour 5 le polynôme T^4-2 est irréductible modulo 5 donc $5\mathcal{O}_K$ est premier et principal.

Finalement, $\mathrm{Cl}(\mathcal{O}_K)$ est généré par $[\mathfrak{p}_2]$ (d'ordre 4) et $[\mathfrak{p}_{3,+}]$.

Exercice 23.

(1,a) Si x, y ont un diviseur commun a alors a^2 divise d et donc $a = \pm 1$. Si x et d sont divisibles par un nombre premier p alors p divise y^2 et donc p divise y, finalement p^2 divise d : absurde. De même pour y et d.

(1,b) $\mathfrak{a}+\overline{\mathfrak{a}}$ possède $y \pm \sqrt{-d}$ donc $2y$ et $2\sqrt{-d}$, et donc $2y$ et $2d$. Finalement, y et d étant premiers entre eux on obtient que $2 \in \mathfrak{a} + \overline{\mathfrak{a}}$.

$2\mathcal{O}_K = \mathfrak{p}^2$, où $\mathfrak{p} = (2, \sqrt{-d}+1)$ ou $(2, \sqrt{-d})$ en fonction de la parité de d. Par conséquent, $\mathfrak{a} + \overline{\mathfrak{a}}$ possédant 2 on obtient que

$$\mathfrak{a} + \overline{\mathfrak{a}} = 2\mathcal{O}_K \text{ ou } \mathfrak{p} \text{ ou } \mathcal{O}_K$$

Mais comme $2 \notin \mathfrak{a}+\overline{\mathfrak{a}}$, il reste $\mathcal{O}_K$ ou $\mathfrak{p}$. Dans ce dernier cas, on aurait $\mathfrak{p}$ divise $\mathfrak{a}$ et $\overline{\mathfrak{a}}$, et une seule fois car $y \pm \sqrt{-d} \notin 2\mathcal{O}_K = \mathfrak{p}^2$. Or on sait par ailleurs que $\mathfrak{a}\overline{\mathfrak{a}} = (x\mathcal{O}_K)^3$: absurde. D'où $\mathfrak{a} + \overline{\mathfrak{a}} = \mathcal{O}_K$.

(1,c) $\mathfrak{a}\overline{\mathfrak{a}} = (x\mathcal{O}_K)^3$ et $\mathfrak{a}$ et $\overline{\mathfrak{a}}$ sont premiers entre eux donc $\mathfrak{a}$ est lui-même le cube d'un idéal, disons $\mathfrak{a} = \mathfrak{b}^3$. Par conséquent $[\mathfrak{b}]^3 = 1$ dans $\mathrm{Cl}(\mathcal{O}_K)$ dont le cardinal est premier avec 3 : il en suit que $[\mathfrak{b}] = 1$. Finalement $\mathfrak{a}$ est bien le cube d'un idéal principal.

(2) Existent donc $a, b \in \mathbb{Z}$ tels que $\mathfrak{b} = (a + b\sqrt{-d})\mathcal{O}_K$. En particulier $(a + b\sqrt{-d})^3 = y + \sqrt{-d}$, c'est-à-dire

$$a^3 - 3b^2da = y \qquad (3a^2 - b^2d)b = 1$$

En suivent que $b = \pm 1$, $d = 3a^2 - b$, et $y = a(a^2 - 3d)$.

Finalement, ou d est de la forme $3a^2 \pm 1$ et dans ce cas-là b est déterminé par d modulo 3, et donc $\pm a$ est déterminé. Le choix du signe de a correspond au choix du signe de y. Mais en faisant agir la conjugaison complexe on a également que $\overline{\mathfrak{a}} = ((a - b\sqrt{-d})\mathcal{O}_K)^3$ et donc

$$x = (a + b\sqrt{-d})(a - b\sqrt{-d}) = a^2 + d$$

Il y a donc zéro ou deux solutions $(a^2+d, \pm a(a^2-3d))$, où a est déterminé par $d = 3a^2 \pm 1$.

Exercice 24.

(0) D'une part $x^2-y^2 = (x-y)(x+y)$ et d'autre part $x-y$ et $x+y$ ont la même parité donc les solutions de $\mathscr{E}(1)$ sont les solutions de $x - y = \pm 1, x + y = \pm 1$, c'est-à-dire $(x, y) = (\pm 2, 0)$ ou $(0, \pm 2)$.

(1) Soit $(x, y) \in \mathbb{Z}^2$. Alors $(x, y) \in \mathscr{E}(d)$ si et seulement si $N_{K|\mathbb{Q}}(\frac{x}{2}+\frac{y}{2}\sqrt{d}) = \pm 1$ si et seulement si $\frac{x}{2}+\frac{y}{2}\sqrt{d} \in \mathcal{O}_K^\times$. Dans ces équivalences il y a une subtilité qui est de démontrer que si $(x, y) \in \mathbb{Z}^2$ alors $x+y\sqrt{-d} \in \mathcal{O}_K$: c'est immédiat si $d = 1$ modulo 4 car $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, et si $d = 2, 3$ modulo 4 alors $x^2 = dy^2$ modulo 4 et donc $y^2 = x^2 = 0$ modulo 4 (car $2, 3$ ne sont pas des carrés modulo 4) et donc $\frac{x}{2}, \frac{y}{2} \in \mathbb{Z}$. En fonction de la description de $\mathcal{O}_K$ on obtient $n, m \in \mathbb{Z}$ tels que

$$\frac{x}{2} + \frac{y}{2}\sqrt{d} = n + m\sqrt{d} \qquad \text{ou} \qquad \frac{x}{2} + \frac{y}{2}\sqrt{d} = n + m\frac{1 + \sqrt{d}}{2}$$

d'où le résultat, car définis ainsi m, n sont uniquement déterminés par x, y.

Finalement, le théorème des unités pour K affirme que $\mathcal{O}_K^\times \simeq \{\pm 1\} \times \mathbb{Z}$, car il y a deux plongements réels et aucun plongement complexe, et donc $\mathscr{E}(d)$ est infini.

(2) Soient $a + b\sqrt{d} \in \mathcal{O}_K^\times \cap [1, +\infty[$.

Si $a^2 - db^2 = 1$ alors $(a + b\sqrt{d})^{-1} = a - b\sqrt{d}$ et donc

$$a + b\sqrt{d} \geqslant 1 \geqslant a - b\sqrt{d} > 0$$

ce qui donne par soustraction $2b\sqrt{d} > 0$ et donc $a > b\sqrt{d} > 0$.

Si $a^2 - db^2 = 1$ alors on a

$$a + b\sqrt{d} \geqslant b\sqrt{d} - a > 0$$

et donc $b\sqrt{d} > a > 0$. Cela nous dit que $\varphi(\mathcal{O}_K^\times \cap [1, +\infty[\subset \mathbb{N}\times\mathbb{N}$. Réciproquement, si $x, y \geqslant 0$ et $(x, y) \in \mathscr{E}(d) \cap \mathbb{N} \times \mathbb{N}$ alors $\frac{x+y\sqrt{d}}{2} > 1$ car $x, y \geqslant 1$ ou alors $x = 2$ et $y = 0$.

Soient $(x_1, y_1), (x_2, y_2) \in \mathscr{E}(d) \cap \mathbb{N} \times \mathbb{N}$ telles que $y_1 < y_2$.

Si $x_1^2 - dy_1^2 = x_2^2 - dy_2^2$ alors

$$x_2^2 - x_1^2 = d(y_2^2 - y_1^2) > 0$$

et donc $x_2 > x_1$.

Si $x_1^2 - dy_1^2 = x_2^2 - dy_2^2 - 8$ alors $8 + x_1^2 < x_2^2$ et donc $x_2 > x_1$.

Si $x_1^2 - dy_1^2 = x_2^2 - dy_2^2 + 8$ alors

$$x_2^2 - x_1^2 = \underbrace{d(y_2^2 - y_1^2)}_{\geqslant 2\cdot 3 = 6} - 8 \geqslant -2$$

car la différence stricte de deux carrés postifs est $\geqslant 3$, ce qui donne également $x_1 \leqslant x_2$.

Dans tous les cas on en déduit

$$\frac{x_1 + y_1\sqrt{d}}{2} < \frac{x_2 + y_2\sqrt{d}}{2}$$

(3) Soit $v \in \mathcal{O}_K^\times$, $v \neq 1, -1$. Quitte à considérer $-v$ ou $1/v$ on peut supposer $v > 1$. Alors u est minimal donc $v \geqslant u$. Ainsi ou $v = u$ ou $vu^{-1} \in \mathcal{O}_K^\times \cap]1, +\infty[$, dans le deuxième cas $vu^{-1} \geqslant u$, i.e. $v \geqslant u^2$. Par récurrence, on en déduit que ou v n'est jamais une puissance de u ou $v \geqslant u^k$ pour tout $k \geqslant 1$. Mais ce deuxième cas est absurde car $u > 1$ et donc $u^k \to +\infty$ quand $k \to \infty$. Donc v est une puissance de u. D'où $\mathcal{O}_K^\times = \{\pm u^k, k \in \mathbb{Z}\}$.

On peut donc procéder de la façon suivante pour trouver des unités fondamentales. On fait varier $y \geqslant 1$ de façon croissante, et on regarde si $dy^2 \pm 4$ est un carré d'entier. D'après le résultat de la question (2), le nombre algébrique associé croît également et donc la première fois que $dy^2 \pm 4$ est entier c'est qu'on a trouvé l'unité fondamentale de $\mathbb{Q}(\sqrt{d})$. On trouve ainsi

d	u
2	$1 + \sqrt{2}$
3	$2 + \sqrt{3}$
5	$(1 + \sqrt{5})/2$
6	$5 + 2\sqrt{6}$
7	$8 + 3\sqrt{7}$
10	$3 + \sqrt{10}$

Exercice 25.

Rappelons que les anneaux d'entiers sont respectivement $\mathbb{Z}[\zeta_3], \mathbb{Z}[\zeta_5]$ et $\mathbb{Z}[\zeta_7]$. Pour les deux premiers la borne de Minkowski est < 2, et donc leurs groupes des classes sont triviaux.

Plaçons-nous dans le cas $K = \mathbb{Q}(\zeta_7)$. Je note $\zeta = \zeta_7$ qui a pour polynôme minimal le polynôme cyclotomique

$$\Phi_7(T) = \frac{T^7 - 1}{T - 1} = T^6 + T^5 + T^4 + T^3 + T^2 + T + 1$$

La borne de Minkowski est < 4, reste donc à décomposer les nombres premiers $p = 2$ et 3. $\Phi_7(T)$ n'est pas irréductible modulo p si et seulement s'il possède une racine dans $\mathbb{F}_{p^5}$ (en fait dans $\mathbb{F}_{p^3}$ (car si $\Phi_7(T)$ a un facteur modulo p de degré k alors il en a un de degré $6-k\ldots$). Si elle existe cette racine doit être une racine 7–ième de l'unité $\neq 1$. Or on sait que pour tout q,

$$\mathbb{F}_q^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$$

et donc $\mathbb{F}_q$ possède une racine primitive 7–ième de l'unité si et seulement si $7|q-1$. Il en suit d'une part en listant les puissances de 3 que $\Phi_7(T)$ est irréductible modulo 3, et d'autre part comme 7 ne divise pas 2 ni 4 mais $\mathbb{F}_8^\times \simeq \mathbb{Z}/7\mathbb{Z}$ on a que $\Phi_7(T)$ est un produit de deux facteurs irréductibles de degré 3, qu'on peut aisément déterminer

$$\Phi_7(T) - (T^3 + T^2 + 1)(T^3 + T + 1) = -2T^3 \in 2\mathbb{Z}[T]$$

Par conséquent, pour montrer que $\mathrm{Cl}(\mathcal{O}_K)$ est principal il faut et il suffit de montrer que l'idéal $\mathfrak{p} = (2, 1+\zeta+\zeta^3)$ est principal. Pour cela (soyons optimistes) montrons que $\mathfrak{p}$ est généré par $\alpha := 1 + \zeta + \zeta^3$. Pour montrer cela il faut et il suffit de montrer que $8 = N(\mathfrak{p}) = |N_{K|\mathbb{Q}}(\alpha)|$. Allons-y :

$$\begin{aligned} N_{K|\mathbb{Q}}(\alpha) &= \prod_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(\alpha) \\ &= \prod_{k=1}^{6} (1 + \zeta^k + \zeta^{3k}) \\ &= \prod_{k=1}^{3} (1 + \zeta^k + \zeta^{3k})(1 + \zeta^{-k} + \zeta^{-3k}) \\ &= |\beta|^2 \end{aligned}$$

où j'ai posé

$$\beta = \prod_{k=1}^{3} (1 + \zeta^k + \zeta^{3k})$$

Or on a

$$\begin{aligned} \beta &= (1 + \zeta + \zeta^3)(1 + \zeta^2 + \zeta^6)(1 + \zeta^3 + \zeta^9) \\ &= \underbrace{(1 + \zeta + \zeta^3)(1 + \zeta^2 + \zeta^3)}_{\Phi_7(\zeta) + 2\zeta^3}(1 + \zeta^2 + \zeta^{-1}) \end{aligned}$$

On arrive donc à $|\beta|^2 = 4|\gamma|^2$, où $\gamma = 1 + \zeta^2 + \zeta^{-1}$. Finalement

$$|\gamma|^2 = (1 + \zeta^2 + \zeta^{-1})(1 + \zeta^{-2} + \zeta) = 2 + \underbrace{1 + \zeta + \zeta^{-1} + \zeta^3 + \zeta^{-3} + \zeta^2 + \zeta^{-2}}_{= \Phi_7(\zeta)} = 2$$

D'où le résultat escompté.

Problème II. (Formule du nombre de classes)

(1) Δ est le discriminant de $P(T)$ le polynôme minimal de $\sqrt{-d}$ ou $(1+\sqrt{-d})/2$ en fonction de la congruence de d modulo 4, il en suit que Δ est un carré $\neq 0$ modulo p (resp. n'est pas un carré modulo p ; divisible par p) si et seulement si $P(T)$ se factorise modulo p en produit de deux irréductibles distincts (resp. est irréductible modulo p ; est le carré d'un irréductible modulo p). Il en suit que $N(\mathfrak{p}) = p$ si $\left(\frac{\Delta}{p}\right) = 0$ ou 1, et $N(\mathfrak{p}) = p^2$ si $\left(\frac{\Delta}{p}\right) = -1$.

(2) On a l'égalité

$$\begin{aligned}\zeta_K(s) &= \prod_{\mathfrak{p}}(1-N(\mathfrak{p})^{-s})^{-1} \\ &= \prod_{p}\prod_{p\mathcal{O}_K\subset\mathfrak{p}}(1-N(\mathfrak{p})^{-s})^{-1} \\ &= \prod_{(\frac{\Delta}{p})=0}(1-p^{-s})^{-1}\left(\prod_{(\frac{\Delta}{p})=1}(1-p^{-s})^{-1}\right)^2\prod_{(\frac{\Delta}{p})=-1}(1-p^{-2s})^{-1}\end{aligned}$$

On peut maintenant diviser par $\zeta_{\mathbb{Q}}(s)$ et obtenir

$$\frac{\zeta_K(s)}{\zeta_{\mathbb{Q}}(s)} = \prod_{(\frac{\Delta}{p})=1}(1-p^{-s})^{-1}\prod_{(\frac{\Delta}{p})=-1}(1+p^{-s})^{-1} = \prod_p\left(1-\left(\frac{\Delta}{p}\right)p^{-s}\right)^{-1}$$

(3) Si $n = p_1^{a_1}\cdots p_r^{a_r}$, posons

$$\chi_\Delta(n) := \left(\frac{\Delta}{p_1}\right)^{a_1}\cdots\left(\frac{\Delta}{p_r}\right)^{a_r}$$

Alors $\chi_\Delta(p) = \left(\frac{\Delta}{p}\right)$ si p est premier et par définition χ_Δ est multiplicative. Donc

$$\frac{\zeta_K(s)}{\zeta_{\mathbb{Q}}(s)} = \prod_p(1-\chi_\Delta(p)p^{-s})^{-1} = \sum_{n=0}^{\infty}\frac{\chi_\Delta(n)}{n^s}$$

(4,a) D'une part deux éléments de $\mathcal{O}_K$ engendrent le même idéal si et seulement s'ils diffèrent d'un élément de $\mathcal{O}_K^\times$; d'autre part la norme de $b\mathcal{O}_K$ vaut

$$|N_{K|\mathbb{Q}}(b)| = |b|^2 = |b_1|^2x^2 + (b_1\overline{b_2} + b_2\overline{b_1})xy + |b_2|^2y^2$$

avec $b = xb_1 + yb_2$ et $\mathfrak{b} = \mathbb{Z}b_1 \oplus \mathbb{Z}b_2$.

D'après le théorème des unités, $\mathcal{O}_K^\times$ n'est composé que de racines de l'unité. Par conséquent, le nombre d'idéaux principaux de norme $\leqslant T$ vaut $\frac{1}{\omega_K}$ fois le nombre de $b \in \mathfrak{b}$ tels que $|N_{K|\mathbb{Q}}(b)| \leqslant T$: d'après le lemme il y en a

$$\frac{2\pi T}{\sqrt{|\mathrm{disc}(b_1,b_2)|}} + O(\sqrt{T}) = \frac{2\pi T}{N(\mathfrak{b})\sqrt{-\Delta}} + O(\sqrt{T})$$

(4,b) Soient $\mathfrak{b}_1,\ldots,\mathfrak{b}_{h_K}$ des idéaux représentants les classes de $\mathrm{Cl}(\mathcal{O}_K)$. Un idéal $\mathfrak{a}$ de $\mathcal{O}_K$ est tel que $\mathfrak{a}\mathfrak{b}_i$ est principal pour un unique entier i. Par conséquent

les idéaux de $\mathcal{O}_K$ de classe $[\mathfrak{b}_i]^{-1}$ de norme $\leqslant T$ sont en bijection avec les idéaux principaux de $\mathcal{O}_K$ de norme $\leqslant TN(\mathfrak{b}_i)$ inclus dans $\mathfrak{b}_i$. D'où quand $T \to \infty$

$$\begin{aligned} F(T) &= \sum_{i=1}^{h_K} \left(\frac{2\pi(TN(\mathfrak{b}_i))}{N(\mathfrak{b}_i)\omega_K\sqrt{-\Delta}} + O(\sqrt{TN(\mathfrak{b}_i)}) \right) \\ &= \frac{2\pi h_K T}{\omega_K\sqrt{-\Delta}} + O(\sqrt{T}) \end{aligned}$$

(5) Soit $s > 1$. On commence par écrire

$$\begin{aligned} \zeta_K(s) &= \sum_{n=1}^{\infty} \frac{F(n) - F(n-1)}{n^s} \\ &= \sum_{n=1}^{\infty} F(n) \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \end{aligned}$$

Et ensuite

$$\begin{aligned} \frac{1}{n^s} - \frac{1}{(n+1)^s} &= n^{-s}(1 - (1+n^{-1})^{-s}) \\ &= sn^{-1-s} + \epsilon(s,n) \end{aligned}$$

où il existe $C > 0$ tel que pour $s \leqslant 1$, $|\epsilon(s,n)| \leqslant C\frac{s^2}{n^{s+2}}$

Lemme 1. Soient R un anneau et Q un polynôme unitaire dans $R[X]$. Alors pour tout $P \in R[X]$, il existe un unique couple (T, S) tel que $P = QT + S$, $\deg S < \deg Q$.

Corollaire 1. Supposons que $R \subset R'$ soit une inclusion entre anneaux. Supposons que $T(X), S(X)$ soient des polynômes de $R'[X]$ tels que $P = QT + S$ et $\deg S < \deg Q$. Alors $T(X), S(X) \in R[X]$.

Lemme 2. Soit A un anneau de caractéristique p. Alors $x \mapsto x^p$ est un endomorphisme de l'anneau A.

Lemme.(Cauchy) Soit G un groupe fini dont le cardinal est divisible par un nombre premier p. Alors G possède un élément d'ordre p.

Proposition 1. Soient A un $\mathbb{Z}$–module libre de rang r et B un sous$-\mathbb{Z}$–module. Alors B est libre de rang $r' \leqslant r$, et si $r = r'$ et P est la matrice d'une base de B dans une base de A alors

$$\#B/A = \pm \det P$$

Preuve. Application du théorème des facteurs invariants : cf. **Proposition A.3.7.** dans l'annexe du cours. □

Corollaire 2. Soit K un corps de nombres de degré n et $A \subset B \subset \mathcal{O}_K$ deux sous–$\mathbb{Z}$–modules de rang n (ou de façon équivalente tels que $A \otimes_{\mathbb{Z}} \mathbb{Q} = B \otimes_{\mathbb{Z}} \mathbb{Q} = K$, ou encore tels qu'ils contiennent une base de K). Alors

$$\mathrm{disc}(A) = (\#B/A)^2 \mathrm{disc}(B)$$

Lemme. (du corps convexe)

Soient L un réseau de $\mathbb{R}^n$ et $A \subset \mathbb{R}^n$ un sous-ensemble mesurable (la mesure de Lebesgue est notée λ).

Si $2^{-n}\lambda(A) > \mathrm{covol}(L)$ (resp. A est compact et $2^{-n}\lambda(A) \geqslant \mathrm{covol}(L)$) alors

$$A \cap L \neq \varnothing$$