Théorie des Nombres - TD9
Unités d'un corps de nombres

Exercice 1 :

a) Soit $d \in \mathbb{N}$ sans facteur carré. On pose $K := \mathbb{Q}(\sqrt{-d})$. Montrer (sans utiliser le théorème des unités) que $\mathbb{Z}_K^*$ est égal à
- $\mathbb{Z}/4\mathbb{Z}$ si $d = 1$.
- $\mathbb{Z}/6\mathbb{Z}$ si $d = 3$.
- $\mathbb{Z}/2\mathbb{Z}$ sinon.

b) Soit K un corps de nombres. Montrer que $\mathbb{Z}_K^*$ est fini si et seulement si $K = \mathbb{Q}$ ou K est un corps quadratique imaginaire.

Solution de l'exercice 1.

a) On sait que l'anneau des entiers de K est $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-d}]$ si $d \equiv 1, 2\ [4]$, et $\mathbb{Z}_K = \mathbb{Z}\left[\frac{1+\sqrt{-d}}{2}\right]$ si $d \equiv 3\ [4]$.

On traite d'abord le cas $d \equiv 1, 2\ [4]$. Un entier $\alpha = a + b\sqrt{-d}$ (avec $a, b \in \mathbb{Z}$) est une unité si et seulement si sa norme est ± 1 si et seulement si $a^2 + db^2 = \pm 1$ si et seulement si $(a, b) = (\pm 1, 0)$ ou ($d = 1$ et $(a, b) = (0, \pm 1)$). Par conséquent, on a $\mathbb{Z}_K^* = \{\pm 1\} \cong \mathbb{Z}/2\mathbb{Z}$ si $d \neq 1$ et $\mathbb{Z}_K^* = \{\pm 1, \pm i\} \cong \mathbb{Z}/4\mathbb{Z}$ si $d = 1$.

Supposons maintenant $d \equiv 3\ [4]$. Alors un entier $\alpha = \frac{a+b\sqrt{-d}}{2}$ (avec $a, b \in \mathbb{Z}$) est une unité si et seulement si $a^2 + db^2 = \pm 4$ si et seulement si $(a, b) = (\pm 1, 0)$ ou ($d = 3$ et $(a, b) = (\pm 1, \pm 1)$, avec les deux signes $\pm$ indépendants). Donc on a $\mathbb{Z}_K^* = \{\pm 1\} \cong \mathbb{Z}/2$ si $d \neq 3$ et $\mathbb{Z}_K^* = \{\pm 1, \pm j, \pm j^2\} \cong \mathbb{Z}/6\mathbb{Z}$ si $d = 3$ (où j est une racine primitive 3-ième de l'unité).

b) Le théorème des unités assure que le groupe $\mathbb{Z}_K^*$ est le produit d'un groupe abélien fini par un groupe abélien libre de type fini de rang $r = r_1 + r_2 - 1$. Par conséquent, le groupe $\mathbb{Z}_K^*$ est fini si et seulement si $r = 0$ si et seulement si $(r_1, r_2) = (1, 0)$ ou $(0, 1)$. Or on a $[K : \mathbb{Q}] = r_1 + 2r_2$, donc le cas $(r_1, r_2) = (1, 0)$ correspond exactement à $K = \mathbb{Q}$, et le cas $(r_1, r_2) = (0, 1)$ correspond à un corps quadratique qui admet un plongement complexe, c'est-à-dire un corps quadratique imaginaire.

Exercice 2 : Soit p un nombre premier impair. On note $K := \mathbb{Q}(\zeta_p)$ et $L := \mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

a) Montrer que K est une extension quadratique de L, et que K est totalement imaginaire (i.e. $r_1 = 0$).

b) Montrer que L est totalement réel (i.e. $r_2 = 0$).

c) Calculer les rangs de $\mathbb{Z}_L^*$ et $\mathbb{Z}_K^*$.

d) On définit $\phi : \mathbb{Z}_K^* \to K^*$ par $\phi(a) := a/\overline{a}$, où $\overline{(.)}$ désigne la conjugaison complexe.

i) Montrer que ϕ est à valeurs dans le groupe des racines de l'unité de K, noté $\mu(K)$, et que c'est un morphisme de groupes.

ii) On note $\varphi : \mathbb{Z}_K^* \to \mu(K)/\mu(K)^2$ le morphisme induit par ϕ. Montrer que $\mathrm{Ker}(\varphi) = \mu(K).\mathbb{Z}_L^*$.

iii) En déduire que l'indice de $\mu(K).\mathbb{Z}_L^*$ dans $\mathbb{Z}_K^*$ vaut 1 ou 2.

e) On veut montrer que $\mathbb{Z}_K^* = (\zeta_p).\mathbb{Z}_L^*$. On raisonne par l'absurde et on suppose $(\zeta_p).\mathbb{Z}_L^* \subsetneq \mathbb{Z}_K^*$.

i) Montrer que φ est surjective.

ii) Montrer qu'il existe $u \in \mathbb{Z}_K^*$ et $m \in \mathbb{Z}$ tels que $\overline{u} = -\zeta_p^m u$.

iii) En décomposant u dans la base $(1, \zeta_p, \ldots, \zeta_p^{p-2})$, montrer que $2u \in \mathfrak{p}$, où $\mathfrak{p}$ est l'idéal premier $(1-\zeta_p)$ de $\mathbb{Z}_K$.

iv) Conclure.

f) En déduire que pour $p=5$, $\mathbb{Z}_K^* = \left\{\pm\zeta_5^k \left(\frac{1+\sqrt{5}}{2}\right)^n ; 0 \leq k \leq 4, n \in \mathbb{Z}\right\}$.

Solution de l'exercice 2.

a) On note $u := \zeta_p + \zeta_p^{-1}$. On a $u = \frac{\zeta_p^2+1}{\zeta_p}$, donc $\zeta_p^2 - u\zeta_p + 1 = 0$. Donc ζ_p est racine du polynôme $X^2 - uX + 1 \in L[X]$, donc l'extension K/L est de degré au plus 2. Or $L \neq K$ puisque L est un sous-corps de $\mathbb{R}$ alors que $\zeta_p \in K$ n'est pas un nombre réel, donc K/L est bien une extension quadratique.

L'extension $K/\mathbb{Q}$ est galoisienne de degré $p-1$. Les conjugués de ζ_p sont exactement les ζ_p^i, avec $1 \leq i \leq p-1$. Donc aucun conjugué de ζ_p n'est un réel, donc $r_1 = 0$. Donc K est un corps totalement imaginaire.

b) Les conjugués de $u = \zeta_p + \zeta_p^{-1}$ sont obtenus via les conjugués de ζ_p. Les conjugués de u sont les $\zeta_p^i + \zeta_p^{-i}$, avec $1 \leq i \leq \frac{p-1}{2}$. Or pour chaque i, on a $\zeta_p^i + \zeta_p^{-i} = \zeta_p^i + \overline{\zeta_p^i} \in \mathbb{R}$, donc tous les conjugués de u sont réels, donc $r_2 = 0$, i.e. L est un corps totalement réel.

c) Le théorème des unités assure que le rang de $\mathbb{Z}_L^*$ vaut $r_1 + r_2 - 1 = \frac{p-1}{2} + 0 - 1 = \frac{p-3}{2}$. De même, le rang de $\mathbb{Z}_K^*$ vaut $r_1 + r_2 - 1 = 0 + \frac{p-1}{2} - 1 = \frac{p-3}{2}$. En particulier, les rangs de $\mathbb{Z}_L^*$ et $\mathbb{Z}_K^*$ sont égaux, donc $\mathbb{Z}_L^*$ est un sous-groupe d'indice fini de $\mathbb{Z}_K^*$.

d) i) Tout d'abord, il est clair que ϕ est à valeurs dans $\mathbb{Z}_K^*$. Soit $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$. Alors pour $a \in \mathbb{Z}_K^*$, on a $\sigma(\phi(a)) = \frac{\sigma(a)}{\sigma(\overline{a})}$. Or le groupe $\mathrm{Gal}(K|\mathbb{Q})$ est abélien, donc σ commute à la conjugaison complexe, donc $\sigma(\phi(a)) = \sigma(a)/\overline{\sigma(a)}$. En particulier, le nombre complexe $\sigma(\phi(a))$ est de module 1. Donc tous les conjugués de $\phi(a)$ sont de module 1. Donc l'entier $\phi(a)$ est une racine de l'unité (voir exercice 7 de la feuille 6). Donc ϕ est à valeurs dans $\mu(K)$. Il est évident que ϕ est un morphisme de groupes.

ii) Remarquons d'abord que $\mu(K) = \{\pm\zeta_p^k, 0 \leq k \leq p-1\}$, et que $\mu(K)^2 = \{\zeta_p^k, 0 \leq k \leq p-1\}$. Soit $a \in \mathbb{Z}_K^*$. On a $a \in \mathrm{Ker}(\varphi)$ si et seulement si $a/\overline{a} \in \mu(K)^2$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $a/\overline{a} = \zeta_p^{2k}$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $a\zeta_p^{-k} = \overline{a\zeta_p^{-k}}$ si et seulement si il existe $k \in \mathbb{Z}$ tel que $a\zeta_p^{-k} \in \mathbb{Z}_K^* \cap \mathbb{R} = \mathbb{Z}_L^*$ si et seulement si $a \in \mu(K).\mathbb{Z}_L^*$. D'où l'égalité $\mathbb{Z}_K^* = \mu(K)\mathbb{Z}_L^*$.

iii) Par théorème de factorisation, le morphisme φ induit un morphisme injectif $\overline{\varphi} : \mathbb{Z}_K^*/\mathrm{Ker}(\varphi) \to \mu(K)/\mu(K)^2$, d'où un morphisme injectif $\overline{\varphi} : \mathbb{Z}_K^*/\mu(K).\mathbb{Z}_L^* \to \mathbb{Z}/2\mathbb{Z}$. Donc le cardinal du groupe $\mathbb{Z}_K^*/\mu(K).\mathbb{Z}_L^*$ vaut au plus 2, donc l'indice de $\mu(K).\mathbb{Z}_L^*$ dans $\mathbb{Z}_K^*$ vaut 1 ou 2.

e) i) Par hypothèse, l'indice de $\mathrm{Ker}(\varphi)$ dans $\mathbb{Z}_K^*$ vaut 2, donc φ n'est pas le morphisme nul. Or un morphisme non nul à valeur dans $\mathbb{Z}/2\mathbb{Z}$ est surjectif, donc φ est surjectif.

ii) Par la question précédente, il existe $u \in \mathbb{Z}_K^*$ tel que $\varphi(u) \neq 1$. Donc $\phi(u) \in \mu(K) \setminus \mu(K)^2$, i.e. il existe $m \in \mathbb{Z}$ tel que $\phi(u) = -\zeta_p^m$. D'où le résultat.

iii) Il existe des entiers $a_0, \ldots, a_{p-2}$ tels que $u = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ (on rappelle que $\mathbb{Z}_K = \mathbb{Z}[\zeta_p]$, voir exercice 11 de la feuille 6). Alors modulo $\mathfrak{p}$, on trouve $u \equiv a_0 + \cdots + a_{p-2}$ et $\overline{u} \equiv a_0 + \cdots + a_{p-2}$. Or l'égalité $\overline{u} = -\zeta_p^m u$ se réduit modulo $\mathfrak{p}$ en $\overline{u} \equiv -u$. Donc finalement, on a $u \equiv -u$ modulo $\mathfrak{p}$, i.e. $2u \in \mathfrak{p}$.

iv) L'entier u est une unité, donc $u \notin \mathfrak{p}$ (sinon $\mathfrak{p} = \mathbb{Z}_K$). Si $2 \in \mathfrak{p}$, alors la norme de 2 est divisible par la norme de $1-\zeta_p$, qui vaut p. Donc p divise 2, ce qui n'est pas. Donc $2 \notin \mathfrak{p}$. Mais $\mathfrak{p}$ est un idéal premier (car $\mathbb{Z}_K/\mathfrak{p} = \mathbb{Z}[1-\zeta_p]/(p, 1-\zeta_p) \cong \mathbb{Z}/p\mathbb{Z}$), donc les conditions $2 \notin \mathfrak{p}$, $u \notin \mathfrak{p}$ et $2u \in \mathfrak{p}$ sont contradictoires. Donc finalement on a bien $Z_K^* = \mu(K)\mathbb{Z}_L^*$.

f) Pour $p=5$, on a $L = \mathbb{Q}(\sqrt{5})$ car $\zeta_5 + \zeta_5^{-1}$ est racine du polynôme $X^2 + X - 1$, de discriminant $\Delta = 5$. Or on sait que $Z_L = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$, et il suffit de déterminer une unité fondamentale de cet

anneau. On vérifie que $\frac{1+\sqrt{5}}{2}$ est une unité fondamentale de $\mathbb{Z}_L$, donc les questions précédentes assurent que

$$\mathbb{Z}_K^* = \left\{ \pm\zeta_5^k \left(\frac{1+\sqrt{5}}{2}\right)^n ; 0 \leq k \leq 4, n \in \mathbb{Z} \right\} .$$

Exercice 3 : Soit $K/\mathbb{Q}$ un corps cubique (de degré 3) de discriminant négatif.

a) Montrer que $r_1 = r_2 = 1$. Dans toute la suite, on considère K comme un sous-corps de $\mathbb{R}$ via son unique plongement réel.

b) Soit $\epsilon > 1$ une unité fondamentale de $\mathbb{Z}_K$. Montrer que ϵ est de norme 1.

c) On pose $u := \sqrt{\epsilon}$. Montrer que les conjugués de ϵ sont de la forme ϵ, $u^{-1}e^{i\theta}$, $u^{-1}e^{-i\theta}$.

d) Montrer que le discriminant d_ϵ de la base $(1, \epsilon, \epsilon^2)$ vaut $d_\epsilon = -4\sin^2(\theta)(u^3 + u^{-3} - 2\cos(\theta))^2$.

e) On pose $y := \cos(\theta)$ et $a := u^3 + u^{-3}$.

i) Montrer que $a > 2$.

ii) On note y_0 la racine négative du polynôme $4y^2 - ay - 2$. Montrer que $|d_\epsilon| \leq 4(1-y_0^2)(a-2y_0)^2$.

iii) Montrer que $y_0 < -\frac{1}{2u^3}$. En déduire que $u^{-6} - 4y_0^2 - 4y_0^4 < 0$.

iv) Montrer que $|d_\epsilon| < 4\epsilon^3 + 24$.
[Indication : on pourra utiliser successivement les deux égalités $ay_0 = 4y_0^2 - 2$ et $a^2y_0^2 = 16y_0^4 - 16y_0^2 + 4$, puis appliquer la question e) iii).]

f) En déduire que $|D_K| < 4\epsilon^3 + 24$.

g) Montrer que pour toute unité $\eta > 1$ dans $\mathbb{Z}_K^*$, si $4\eta^{\frac{3}{2}} + 24 < |D_K|$, alors η est une unité fondamentale.

h) Applications :

i) Si $K = \mathbb{Q}(\sqrt[3]{2})$, calculer D_K et montrer que $\sqrt[3]{2} - 1$ est une unité fondamentale (on admet que $\mathbb{Z}_K = \mathbb{Z}[\sqrt[3]{2}]$: cf feuille de TD8, exercice 11).

ii) Si $K = \mathbb{Q}(\alpha)$, où α est la racine réelle de $X^3 + 2X + 1$, calculer D_K et montrer que $\frac{-1}{\alpha}$ est une unité fondamentale.

iii) Si $K = \mathbb{Q}(\alpha)$, où α est la racine réelle de $X^3 + 10X + 1$, calculer D_K et montrer que $\frac{-1}{\alpha}$ est une unité fondamentale.

Solution de l'exercice 3.

a) Un théorème du cours assure que le signe du discriminant est donné par $(-1)^{r_2}$, donc r_2 doit être impair. Or $r_1 + 2r_2 = 3$, donc nécessairement $r_2 = 1$ et donc $r_1 = 1$.
Dans toute la suite, on verra donc K comme un sous-corps de $\mathbb{R}$ via son unique plongement réel.

b) On note $\sigma : K \to \mathbb{C}$ un plongement complexe de K. Alors les conjugués de ϵ sont $\epsilon, \sigma(\epsilon), \overline{\sigma(\epsilon)}$, où $\overline{(.)}$ désigne la conjugaison complexe. Donc en particulier on a $N_{K/\mathbb{Q}}(\epsilon) = \epsilon\sigma(\epsilon)\overline{\sigma(\epsilon)} = \epsilon|\sigma(\epsilon)|^2 > 0$. Or ϵ est une unité, donc sa norme vaut ± 1, donc puisqu'elle est positive, elle vaut 1.

c) Il existe $\rho > 0$ et $\theta \in \mathbb{R}$ tels que $\sigma(\epsilon) = \rho e^{i\theta}$. Alors la question précédente assure que $1 = N_{K/\mathbb{Q}}(\epsilon) = \epsilon|\sigma(\epsilon)|^2 = u^2\rho^2$. Donc $\rho = u^{-1}$, donc les conjugués de ϵ sont bien ϵ, $u^{-1}e^{i\theta}$ et $u^{-1}e^{-i\theta}$.

d) Le discriminant d_ϵ vaut

$$d_\epsilon = \left((\epsilon - \sigma(\epsilon))(\epsilon - \overline{\sigma(\epsilon)})(\sigma(\epsilon) - \overline{\sigma(\epsilon)})\right)^2 ,$$

donc on a

$$d_\epsilon = \left((u^2 - u^{-1}e^{i\theta})(u^2 - u^{-1}e^{-i\theta})(2iu^{-1}\sin(\theta))\right)^2 = -4\sin^2(\theta)\left(u^3 + u^{-3} - 2\cos(\theta)\right)^2 ,$$

d'où le résultat.

e) i) On remarque que $0 < \left(u^{\frac{3}{2}} - u^{-\frac{3}{2}}\right)^2 = u^3 + u^{-3} - 2 = a - 2$, d'où $a > 2$.

ii) On a $d_\epsilon = -4(1-y^2)(a-2y)^2$. On définit donc la fonction $f(y) := -4(1-y^2)(a-2y)^2$. C'est un polynôme, et on a $f'(y) = -8(a-2y)(4y^2 - ay - 2)$. Donc $f'(y) = 0$ si et seulement si $y = \frac{a}{2}$ ou $y = y_0$ ou $y = -\frac{1}{2y_0}$. En étudiant le tableau de variations de f, on note que la fonction f est négative sur l'intervalle $[-1, 1]$ et qu'elle atteint son minimum sur cet intervalle en $y = y_0$ (il est clair que $-1 \leq y_0 \leq 0$ car en $y = -1$, le polynôme de degré 2 dont y_0 est racine prend une valeur positive : voir question e) i)). Par conséquent, puisque le cosinus prend ses valeurs dans $[-1, 1]$, on en déduit que $|d_\epsilon| \leq |f(y_0)|$, d'où le résultat.

iii) Il suffit de vérifier que $4(-\frac{1}{2u^3})^2 - a(-\frac{1}{2u^3}) - 2 < 0$, ce qui revient à montrer que $u > 1$, ce qui est vrai par définition de u (puisque $\epsilon = u^2 > 1$).
On a donc $y_0 < -\frac{1}{2u^3}$, donc en élevant au carré, on a $u^{-6} - 4y_0^2 < 0$, donc a fortiori $u^{-6} - 4y_0^2 - 4y_0^4 < 0$.

iv) On a montré (voir e) ii)) que $|d_\epsilon| \leq 4(1-y_0^2)(a-2y_0)^2$. Or on a

$$4(1-y_0^2)(a-2y_0)^2 = 4(1-y_0^2)(a^2-4ay_0+4y_0^2) = 4(1-y_0^2)(a^2-16y_0^2+8+4y_0^2) = 4(1-y_0^2)(a^2+8-12y_0^2)\,.$$

Or

$$4(1-y_0^2)(a^2+8-12y_0^2) = 4(a^2+8-10y_0^2-a^2y_0^2+2y_0^4)\,,$$

donc en utilisant $a^2y_0^2 = 16y_0^4 - 16y_0^2 + 4$, on obtient

$$4(1-y_0^2)(a-2y_0)^2 = 4(a^2+4-4y_0^2-4y_0^4) = 4(u^6+6+u^{-6}-4y_0^2-4y_0^4)\,.$$

Or la question e) iii) assure que $u^{-6} - 4y_0^2 - 4y_0^4 < 0$, donc les calculs précédents assurent que

$$|d_\epsilon| < 4(u^6+6) = 4\epsilon^3 + 24\,.$$

f) On sait que $f^2 D_K = d_\epsilon$, où f est l'indice de $\mathbb{Z}[\epsilon]$ dans $\mathbb{Z}_K$, donc en particulier $|D_K| \leq |d_\epsilon|$, d'où le résultat.

g) Puisque ϵ est l'unité fondamentale et puisque $\eta > 1$, il existe $n \geq 1$ tel que $\eta = \epsilon^n$. Alors l'hypothèse $4\eta^{\frac{3}{2}} + 24 < |D_K|$ implique que $4\epsilon^{\frac{3n}{2}} + 24 < |D_K|$. Or la question f) assure que $|D_K| < 4\epsilon^3 + 24$. Donc on en déduit que $\epsilon^{\frac{3n}{2}} < \epsilon^3$, donc $\frac{3n}{2} < 3$, donc $n = 1$, donc $\eta = \epsilon$.

h) i) On sait que $D_K = -27.2^2 = -108$ (voir feuille de TD8, exercice 11 par exemple). On considère $\eta := 1 + \sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{Z}_K$. Alors $\eta = \frac{1}{\sqrt[3]{2}-1}$. Le polynôme minimal de $\sqrt[3]{2} - 1$ est $(X+1)^3 - 2 = X^3 + 3X^2 + 3X - 1$, donc $\sqrt[3]{2} - 1$ est une unité, donc η est une unité et $\eta > 1$.
On applique alors le critère de la question g) pour montrer que η est une unité fondamentale. On a $\eta \approx 3,847 < 4$ et donc $4\eta^{\frac{3}{2}} + 24 < 4.8 + 24 = 56 < 108 = |D_K|$. Donc la question g) assure que η est une unité fondamentale, donc $\sqrt[3]{2} - 1$ aussi.

ii) Au vu du polynôme minimal, α est une unité, et $-1 < \alpha < 0$. Donc $\eta := \frac{-1}{\alpha}$ est une unité > 1. On a $\mathrm{disc}(1, \alpha, \alpha^2) = -59$ sans facteur carré, donc $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ et $D_K = -59$. Un calcul approché donne $\eta \approx 2,205 < 4$, donc $4\eta^{\frac{3}{2}} + 24 < 4.8 + 24 = 56 < 59 = |D_K|$, donc la question g) assure que η est une unité fondamentale.

iii) Au vu du polynôme minimal, α est une unité, et $-1 < \alpha < 0$. Donc $\eta := \frac{-1}{\alpha}$ est une unité > 1. On a $\mathrm{disc}(1, \alpha, \alpha^2) = -4027$ et 4027 est un nombre premier, donc $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ et $D_K = -4027$. Un calcul approché donne $\eta \approx 10,01 < 16$, donc $4\eta^{\frac{3}{2}} + 24 < 4.64 + 24 = 280 < 4027 = |D_K|$, donc la question g) assure que η est une unité fondamentale.

Exercice 4 : On pourra utiliser les résultats de l'exercice 3.

a) Soit α un entier algébrique, de polynôme minimal $P \in \mathbb{Z}[X]$. Soit $r \in \mathbb{Z}$ tel que $P(r) = \pm 1$. Montrer que $\alpha - r$ est une unité de $\mathbb{Z}_{\mathbb{Q}(\alpha)}$.

b) Montrer que $\frac{1}{2-\sqrt[3]{7}}$ est une unité fondamentale dans $K = \mathbb{Q}(\sqrt[3]{7})$.

c) On note β la racine réelle de $X^3 + X - 3$. Montrer que $\frac{1}{\beta-1}$ est une unité fondamentale de $\mathbb{Q}(\beta)$.

Solution de l'exercice 4.

a) On définit le polynôme $Q(X) := P(X + r) \in \mathbb{Z}[X]$. Alors $Q(\alpha - r) = P(\alpha) = 0$, donc Q est un polynôme annulateur unitaire de $\alpha - r$ à coefficients entiers. En écrivant $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, on voit que le coefficient constant de Q vaut exactement $P(r) = \pm 1$, donc $\alpha - r$ est un entier de norme ± 1, donc c'est une unité.

b) On applique la question précédente à $\alpha := \sqrt[3]{7}$, $P(X) = X^3 - 7$ et $r = 2$. Puisque $P(2) = 1$, $\sqrt[3]{7} - 2$ est une unité de $\mathbb{Z}_K$, donc $\eta := \frac{1}{2-\sqrt[3]{7}}$ est une unité de K. Or $D_K = -27.7^2 = -1323$ (voir feuille de TD8, exercice 11) et $\eta \approx 11,48 < 16$, donc $4\eta^{\frac{3}{2}} + 24 < 280 < 1323 = |D_K|$. Donc la question g) de l'exercice 3 assure que η est une unité fondamentale de K.

c) On a $\mathrm{disc}(\mathbb{Z}[\alpha]) = -247 = -13.19$ sans facteur carré, donc $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ et $D_K = -247$. Puisque le polynôme $X^3 + X - 3$ évalué en 1 vaut -1, la question a) assure que $\beta - 1$ est une unité de $\mathbb{Z}_K$. Donc $\eta := \frac{1}{\beta-1}$ est une unité de $\mathbb{Z}_K$. Un calcul approché assure que $1 < \eta < 10$, donc $4\eta^{\frac{3}{2}} + 24 < 40\sqrt{10} + 24 < 40.4 + 24 = 184 < 247 = |D_K|$. Donc la question g) de l'exercice 3 assure que η est une unité fondamentale de K.