ENS de Lyon
M1 Introduction à la théorie des nombres

Examen partiel du 28 février 2020

Exercice 1 — 1. L'égalité demandée se déduit immédiatement des identités

$$\mathrm{pgcd}(\mathfrak{a},\mathfrak{b}) = \mathfrak{a}+\mathfrak{b}, \quad \mathrm{ppcm}(\mathfrak{a},\mathfrak{b}) = \mathfrak{a}\cap\mathfrak{b} \quad \text{et} \quad \mathfrak{a}\cdot\mathfrak{b} = \mathrm{ppcm}(\mathfrak{a},\mathfrak{b})\cdot\mathrm{pgcd}(\mathfrak{a},\mathfrak{b}),$$

en observant que l'on a $\mathrm{pgcd}(\mathfrak{a},\mathfrak{b}) = (1)$ puisque les idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux.

Remarque. On peut aisément donner une preuve directe de cette égalité en observant l'inclusion évidente $\mathfrak{a}\cdot\mathfrak{b} \subset \mathfrak{a}\cap\mathfrak{b}$ et en utilisant l'hypothèse de coprimalité des idéaux $\mathfrak{a}$ et $\mathfrak{b}$, équivalente à $\mathfrak{a}+\mathfrak{b} = (1)$, pour écrire $1 = a_0 + b_0$ avec $a_0 \in \mathfrak{a}, b_0 \in \mathfrak{b}$ et en déduire $x = xa_0 + xb_0 \in \mathfrak{a}\cdot\mathfrak{b}$ pour tout $x \in \mathfrak{a}\cap\mathfrak{b}$.

2. Soit $L/\mathbf{Q}$ une extension finie galoisienne contenant K. Fixons un diviseur premier $\mathfrak{P}$ de $p\mathcal{O}_L$. Pour tout $\sigma \in \mathrm{Gal}(L|\mathbf{Q})$, l'idéal $\sigma^{-1}(\mathfrak{P})\cap\mathcal{O}_K$ est un diviseur premier de $p\mathcal{O}_K$, donc est égal à l'un des $\mathfrak{p}_i$ et, par suite, contient α. Nous en déduisons que $\mathfrak{P}$ contient tous les conjugués $\sigma(\alpha)$ de α, donc contient

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) = \sum_{\sigma}\sigma(\alpha),$$

la somme portant sur un ensemble de représentants des classes à droite modulo $\mathrm{Gal}(L|K)$. Au final, il vient

$$\mathrm{Tr}_{K/\mathbf{Q}}(\alpha) \in \mathfrak{P}\cap\mathbf{Z} = p\mathbf{Z}.$$

3. Soit $i \in \{1,\dots,r\}$. Les idéaux $\mathfrak{p}_i$ et $\mathfrak{p}_j^{e_j}$, $j \in \{1,\dots,r\}\setminus\{i\}$, étant deux à deux premiers entre eux, le théorème chinois des restes garantit que le morphisme canonique

$$\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}_i \oplus \bigoplus_{j\neq i}\mathcal{O}_K/\mathfrak{p}_j^{e_j}$$

est surjectif. On en déduit immédiatement l'existence, pour tout $i \in \{1,\dots,r\}$, d'une famille $\mathcal{B}_i$ d'éléments de $\mathcal{O}_K$ se projetant sur une $\mathbf{F}_p$-base de $\mathcal{O}_K/\mathfrak{p}_i$ et sur 0 dans chaque facteur $\mathcal{O}_K/\mathfrak{p}_j^{e_j}$ pour j distinct de i.

On a par ailleurs $\mathfrak{p}_i^2 \neq \mathfrak{p}_i$ pour tout $i \in \{1,\dots,r\}$ en invoquant, par exemple, l'existence d'un inverse pour tout idéal fractionnaire de $\mathcal{O}_K$.

4. En vertu du théorème chinois des restes, nous disposons d'un isomorphisme de $\mathbf{F}_p$-algèbres

$$\mathcal{O}_K/p\mathcal{O}_K \xrightarrow{\sim} \bigoplus_{j=1}^{r}\mathcal{O}_K/\mathfrak{p}_j^{e_j}.$$

Pour tout $i \in \{1,\dots,r\}$, la famille $\left(\pi_i^\ell\beta\right)_{0\leqslant\ell\leqslant e_i-1,\beta\in\mathcal{B}_i}$ se projette sur 0 dans chaque facteur $\mathcal{O}_K/\mathfrak{p}_j^{e_j}$ avec $j \neq i$; pour établir que $\mathcal{B}$ est une $\mathbf{F}_p$-base de $\mathcal{O}_K/p\mathcal{O}_K$, il suffit donc de prouver que la famille $\left(\pi_i^\ell\beta\right)_{0\leqslant\ell\leqslant e_i-1,\beta\in\mathcal{B}}$ se projette sur une base du $\mathbf{F}_p$-espace vectoriel $V_i = \mathcal{O}_K/\mathfrak{p}_i^{e_i}$.

Ce dernier est filtré par les sous-espaces vectoriels $\mathfrak{p}_i^\ell/\mathfrak{p}_i^{\ell+1}$, $0 \leqslant \ell \leqslant e_i - 1$. Pour pour tout ℓ, l'application

$$\mathcal{O}_K/\mathfrak{p}_i \to \mathfrak{p}_i^\ell/\mathfrak{p}_i^{\ell+1}, x \mapsto \pi_i^\ell x$$

est un isomorphisme de $\mathbf{F}_p$-espaces vectoriels : en effet, elle est non nulle de par le choix de π_i et le membre de droite est un $\mathcal{O}_K/\mathfrak{p}_i$ espace vectoriel de dimension 1 (ce qui se prouve en reproduisant le raisonnement

de la fin de la proposition 2.10 des notes de cours). Il en découle que chaque famille $\left(\pi^\ell\beta\right)_{\beta\in\mathcal{B}_i}$ induit une $\mathbf{F}_p$-base de $\mathfrak{p}_i^\ell/\mathfrak{p}_i^{\ell+1}$, puis que la famille $\left(\pi_i^\ell\beta\right)_{0\leqslant\ell\leqslant e_i-1,\beta\in\mathcal{B}}$ se projette sur une base de V_i.

5. Soit M le sous-$\mathbf{Z}$-module de $\mathcal{O}_K$ engendré par $\mathcal{B}$. C'est un $\mathbf{Z}$-module libre, de rang

$$\mathrm{rg}(M)=\dim_{\mathbf{F}_p}M/pM=\dim_{\mathbf{F}_p}\mathcal{O}_K/p\mathcal{O}_K=\mathrm{rg}(\mathcal{O}_K)$$

et tel que $p\nmid(\mathcal{O}_K:M)$ en vertu de la question précédente.

Dans ces conditions, on déduit de l'identité

$$\mathrm{disc}(\mathcal{B})=(\mathcal{O}_K:M)^2D_K$$

que les entiers $\mathrm{disc}(\mathcal{B})$ et D_K ont la même valuation p-adique.

Écrivons

$$\mathrm{disc}(\mathcal{B})=\det(A)\quad\text{avec}\quad A=\left(\mathrm{Tr}_{K/\mathbf{Q}}(\beta\beta')\right)_{\beta,\beta'\in\mathcal{B}}.$$

Puisque, par construction,

$$\pi_i^\ell\beta_i\beta'\in\mathfrak{p}_1\cdots\mathfrak{p}_r$$

pour tous $\ell\geqslant 1$, $\beta_i\in\mathcal{B}_i$ et $\beta'\in\mathcal{B}$, on déduit que la question 2 que

$$\sum_{i=1}^r(e_i-1)f_i$$

colonnes de A sont divisibles par p ; il vient donc

$$v_p(D_K)=v_p(\mathrm{disc}(\mathcal{B}))\geqslant\sum_{i=1}^r(e_i-1)f_i.$$

Exercice 2 — 1. Par définition de l'élément de Frobenius $(\mathfrak{p},L/\mathbf{Q})$, on a

$$(\mathfrak{p},L/\mathbf{Q})(x)-x^p\in\mathfrak{p}$$

pour tout $x\in\mathcal{O}_L$. En particulier, si $x\in\mathcal{O}_{L'}$, il vient

$$(\mathfrak{p},L/\mathbf{Q})\,(x)-x^p\in\mathfrak{p}\cap\mathcal{O}_{L'}=\mathfrak{p}',$$

c'est-à-dire que $(\mathfrak{p},L/\mathbf{Q})$ est envoyé sur $(\mathfrak{p}',K/\mathbf{Q})$ par la projection canonique $\mathrm{Gal}(L|\mathbf{Q})\to\mathrm{Gal}(K|\mathbf{Q})$.

2. Le corps K est de degré au plus 4 sur $\mathbf{Q}$, et en fait de degré précisément 4 puisque $\mathbf{Q}(\sqrt{7})$ ne contient pas de racine carrée de 10 (l'équation diophantienne $(x+y\sqrt{7})^2=10$ n'a pas de solution dans $\mathbf{Z}$).

Tout plongement σ de K dans $\mathbf{C}$ envoie $\sqrt{7}$ sur $\pm\sqrt{7}$ et $\sqrt{10}$ sur $\pm\sqrt{10}$, donc stabilise K. Puisqu'il y a exactement 4 plongements distincts de K dans $\mathbf{C}$, ceci nous fournit 4 automorphismes de K et l'extension $K/\mathbf{Q}$ est donc galoisienne.

Tout automorphisme de K étant uniquement défini par la donnée des images de $\sqrt{7}$ et $\sqrt{10}$, nous pouvons décrire les éléments de $\mathrm{Gal}(K|\mathbf{Q})$: outre l'identité, ce groupe contient un élément s tel que $s(\sqrt{7})=\sqrt{7}$ et $s(\sqrt{10})=-\sqrt{10}$, un élément t tel que $t(\sqrt{7})=-\sqrt{7}$ et $t(\sqrt{10})=\sqrt{10}$ et l'élément $st=ts=-\mathrm{id}$. Ces trois derniers automorphismes sont d'ordre 2 et donc

$$\mathrm{Gal}(L|\mathbf{Q})=\langle s\rangle\times\langle t\rangle\simeq\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}.$$

3. L'anneau des entiers du corps quadratique $\mathbf{Q}(\sqrt{7})$ est $\mathbf{Z}[\sqrt{7}]$ puisque $7\equiv 3\pmod 4$. Le critère de Dedekind s'applique et la factorisation de $3\mathcal{O}_K$ reflète donc celle de T^2-7 modulo 3 ; puisque $T^2-7=T^2-1=(T-1)(T+1)$ dans $\mathbf{F}_3[T]$, il vient

$$3\mathcal{O}_{\mathbf{Q}(\sqrt{7})}=\mathfrak{p}\cdot\mathfrak{p}',\quad\text{avec}\quad\mathfrak{p}=(3,1+\sqrt{7})\text{ et }\mathfrak{p}'=(3,1-\sqrt{7}).$$

On raisonne de même avec le corps quadratique $\mathbf{Q}(\sqrt{10})$, d'anneau des entiers $\mathbf{Z}[\sqrt{10}]$ puisque $10 \equiv 2 \pmod 4$. Comme $T^2 - 10 = T^2 - 1 = (T-1)(T+1)$ dans $\mathbf{F}_3[T]$, il vient

$$3\mathcal{O}_{\mathbf{Q}[\sqrt{10}]} = \mathfrak{q} \cdot \mathfrak{q}', \quad \text{avec } \mathfrak{q} = (3, 1+\sqrt{10}) \text{ et } \mathfrak{q}' = (3, 1-\sqrt{10}).$$

4. Le nombre premier 3 n'est pas ramifié dans $\mathbf{Q}(\sqrt{7})$ et $\mathbf{Q}(\sqrt{10})$, donc il n'est pas ramifié dans $K = \mathbf{Q}(\sqrt{7})\mathbf{Q}(\sqrt{10})$. Le degré résiduel f d'un diviseur premier $\mathfrak{P}$ de $3\mathcal{O}_K$ est l'ordre de l'élément de Frobenius $(\mathfrak{P}, K/\mathbf{Q})$. D'après la question préliminaire, ce dernier se projette dans $\mathrm{Gal}(\mathbf{Q}(\sqrt{7})|\mathbf{Q})$ sur l'élément de Frobenius $(p, \mathbf{Q}(\sqrt{7})/\mathbf{Q})$, lequel est trivial puisque 3 est totalement décomposé dans $\mathbf{Q}(\sqrt{7})$. Par le même argument, la projection de $(\mathfrak{P}, K/\mathbf{Q})$ dans $\mathrm{Gal}(\mathbf{Q}(\sqrt{10})|\mathbf{Q})$ est également triviale. Vu la structure du groupe $\mathrm{Gal}(K|\mathbf{Q})$ décrite à la question 2, on en déduit $f = 1$ et donc $3\mathcal{O}_K$ est le produit de quatre idéaux premiers distincts de degrés résiduels égaux à 1.

5. Raisonnons par l'absure. Si l'anneau $\mathcal{O}_K$ était monogène, engendré par un élément α racine d'un polynôme unitaire f de degré 4 dans $\mathbf{Z}[T]$, alors la factorisation de $3\mathcal{O}_K$ reflèterait celle de f modulo 3 et donc f serait le produit de quatre facteurs de degré 1 distincts. Ceci est absurde puisqu'il n'existe que trois polynômes distincts de la forme $T - a$ dans $\mathbf{F}_3[T]$!

L'anneau $\mathcal{O}_K$ n'est donc pas monogène.

Exercice 3 — 1. Le polynôme minimal f de γ est le polynôme caractéristique de la multiplication par γ dans K. En utilisant la base $\{1, \alpha, \alpha^2\}$, la matrice de cette dernière est

$$\frac{1}{27}\begin{pmatrix} 1 & m & \varepsilon m \\ \varepsilon & 1 & m \\ 1 & \varepsilon & 1 \end{pmatrix}$$

et donc, tous calculs faits,

$$f = T^3 - T^2 - \frac{m-\varepsilon}{3}T - \frac{(m-\varepsilon)^2}{27}.$$

Si $m \equiv \varepsilon \pmod 3$, alors

$$\frac{m-\varepsilon}{3} \in \mathbf{Z} \quad \text{et} \quad \frac{(m-\varepsilon)^2}{27} \in \mathbf{Z},$$

donc f est à coefficients entiers et γ est un entier algébrique.

2. Soit p un nombre premier distinct de 2 et 3. Le corps $\mathbf{F}_p$ contient une racine cubique primtive de l'unité si et seulement si le polynôme $\Phi_3 = T^2 + T + 1$ a une racine dans $\mathbf{F}_p$, ce qui est le cas si et seulement si son discriminant -3 est un carré modulo p.

3. Observons que l'on a

$$(\mathcal{O}_K : \mathbf{Z}[\alpha])^2 D_K = \mathrm{disc}(1, \alpha, \alpha^2) = -\mathrm{N}_{K/\mathbf{Q}}(3\alpha^2) = -27m^2.$$

(a) Distinguons deux cas.

Premier cas : $p \nmid 3m$. On a alors $p(\mathcal{O}_K : \mathbf{Z})$ et le critère de Dedekind s'applique.

Il y a trois possibilités :

(i) $p\mathcal{O}_K = \mathfrak{p}$ est premier, de degré résiduel 3, si $T^3 - m$ est irréductible modulo p, c'est-à-dire si m n'est pas un cube modulo p ;

(ii) $p\mathcal{O}_K = \mathfrak{p} \cdot \mathfrak{q}$ avec $\mathfrak{p}$ premier de degré résiduel 2 et $\mathfrak{q}$ premier de degré résiduel 1, si $T^3 - m$ admet une unique racine dans $\mathbf{F}_p$; c'est le cas lorsque m est un cube modulo p mais $\mathbf{F}_p$ ne contient pas de racine cubique primitive de l'unité ;

(iii) $p\mathcal{O}_K = \mathfrak{p} \cdot \mathfrak{p}' \cdot \mathfrak{p}''$, avec $\mathfrak{p}, \mathfrak{p}', \mathfrak{p}''$ premiers de degrés résiduels 1, si $T^3 - m$ est scindé sur $\mathbf{F}_p$.

Second cas : $p \neq 3$, $p|m$ et $p^2 \nmid m$.
Le polynôme $T^3 - m$ est alors d'Eisenstein en p et donc

$$p\mathcal{O}_K = \mathfrak{p}^3,$$

avec $\mathfrak{p} = (p, \alpha)$ de degré résiduel 1.

(b) Si $p^2|m$ et $m = ab^2$ avec a sans facteur carré, alors, en posant $\beta = \alpha^2/b$, il vient

$$\beta^3 = \alpha^6/b^3 = m^2/b^3 = a^2 b,$$

ce qui prouve que β est un entier algébrique. En outre, $K = \mathbf{Q}(\beta)$ car $\beta^2 = m\alpha/b^2 = a\alpha$. L'hypothèse $p^2|m$ implique $p|b$ et $p \nmid a$, $p^2 \nmid b$ puisque m n'a pas de facteur cubique ; on en déduit que $T^3 - a^2 b$, le polynôme minimal de β, est d'Eisenstein en p, d'où

$$p\mathcal{O}_K = \mathfrak{p}^3$$

avec $\mathfrak{p} = (p, \beta)$ de degré résiduel 1.

4. Si $m \not\equiv 1 \pmod 9$, alors le polynôme $(T+1)^3 - m = T^3 + 3T^2 + 3T - (m-1)$ est d'Eisenstein en 3 et donc

$$3\mathcal{O}_K = \mathfrak{p}^3$$

avec $\mathfrak{p} = (3, \alpha - 1)$ de degré résiduel 1. De même, si $m \not\equiv -1 \pmod 9$, alors le polynôme $(T-1)^3 - m = T^3 - 3T^2 + 3T - (m+1)$ est d'Eisenstein en 3 et donc

$$3\mathcal{O}_K = \mathfrak{p}^3$$

avec $\mathfrak{p} = (3, \alpha + 1)$ de degré résiduel 1.

5. Si $m \equiv \pm 1 \pmod 9$, alors la question 1 montre que 3 divise $(\mathcal{O}_K : \mathbf{Z}[\alpha])$. En appliquant la valuation 3-adique à l'identité

$$(\mathcal{O}_K : \mathbf{Z}[\alpha])^2 D_K = 27m^2,$$

on en déduit

$$3 = v_3(27m^2) = 2v_3\left((\mathcal{O}_K : \mathbf{Z}[\alpha])\right) + v_3(D_K) \geqslant 2 + v_3(D_K),$$

donc

$$v_3(D_K) \leqslant 1.$$

Comme $v_3(D_K) \neq 0$ par parité, il vient $v_3(D_K) = 1$. On en déduit que 3 est ramifié dans K, donc se factorise sous la forme $3\mathcal{O}_K = \mathfrak{p}^2 \cdot \mathfrak{q}$ ou $3\mathcal{O}_K = \mathfrak{p}^3$, avec $\mathfrak{p}$ et $\mathfrak{q}$ de degrés résiduels 1. Le second cas de figure est exclu : avec la question 5 de l'exercice 1, il impliquerait $v_3(D_K) \geqslant 2$.