UNIVERSITÉ DE RENNES 1

Théorie des nombres

Examen — Première session — corrigé

Exercice 1

Soit p un nombre premier impair.

Question 1

Montrer que $\mathbb{F}_{p^2}^\times$ contient un élément α d'ordre exactement 8.

Le groupe $\mathbb{F}_{p^2}^\times$ est cyclique d'ordre p^2-1. Il suffit donc de montrer que $\mathbb{Z}/(p^2-1)\mathbb{Z}$ contient un élément d'ordre exactement 8.

On a $p \equiv \pm 1 \text{ ou } \pm 3 \pmod 8$, or $(\pm 1)^2 \equiv (\pm 3)^2 \equiv 1 \pmod 8$, donc $p^2 \equiv 1 \pmod 8$. Comme $8\frac{p^2-1}{8} = p^2-1$, et si $k \in \{1, \dots, 7\}$, $0 < k\frac{p^2-1}{8} < p^2-1$ donc $(p^2-1) \nmid \frac{p^2-1}{8}$, la classe de $\frac{p^2-1}{8}$ est d'ordre exactement 8 dans $\mathbb{Z}/(p^2-1)\mathbb{Z}$.

Question 2

Soit $Q \in \mathbb{F}_p[X]$ le polynôme minimal de α sur $\mathbb{F}_p$. Montrer que Q est de degré 1 ou 2. (Indication : on pourra considérer le degré de l'extension $\mathbb{F}_p(\alpha)/\mathbb{F}_p$).

Comme $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^2}$ et $[\mathbb{F}_{p^2} : \mathbb{F}_p] = 2$, on a $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] \in \{1, 2\}$. Or $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg(Q)$ (puisque $1, \alpha, \dots, \alpha^{\deg(Q)-1}$ est une base de $\mathbb{F}_p(\alpha)$), donc $\deg(Q) \in \{1, 2\}$.

Question 3

En déduire que le polynôme $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.

Comme α est d'ordre exactement 8, on a $\alpha^8 = 1$ et $\alpha^4 \neq 1$ dans $\mathbb{F}_{p^2}$. En considérant la factorisation $X^8-1 = (X^4-1)(X^4+1)$, on trouve donc $\alpha^4+1 = 0$, donc α est racine de X^4+1 dans $\mathbb{F}_{p^2}$, donc $Q \mid (X^4+1)$ dans $\mathbb{F}_p[X]$. Comme $\deg(X^4+1) = 4$ et $\deg(Q) \in \{1, 2\}$, le polynôme Q est un facteur non trivial de X^4+1, donc X^4+1 n'est pas irréductible dans $\mathbb{F}_p[X]$.

Question 4

Quelle est la décomposition en produit d'irréductibles de $X^4 + 1$ dans $\mathbb{F}_2[X]$?

Comme $\mathbb{F}_2[X]$ est de caractéristique 2, on a :

$$(X+1)^4 = \left((X+1)^2\right)^2 = \left(X^2+1\right)^2 = X^4 + 1.$$

Question 5

Montrer que $X^4 + 1$ est irréductible dans $\mathbb{Z}[X]$.

Par translation, il est équivalement de montrer que $(X+1)^4 + 1$ est irréductible. Or $(X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$ est un polynôme d'Eisenstein (pour le nombre premier 2) unitaire donc il est irréductible dans $\mathbb{Z}[X]$.

Exercice 2

Soit p un nombre premier qui s'écrit comme somme de deux carrés. Combien y a-t-il de couples $(x, y) \in \mathbb{Z}^2$ tels que $p = x^2 + y^2$? (On pourra être amené à distinguer le cas $p = 2$. Indication : chercher les diviseurs de p dans $\mathbb{Z}[\sqrt{-1}]$.)

Soient $a, b \in \mathbb{Z}$ tels que $p = a^2 + b^2$. On a alors

$$p = \mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(a + b\sqrt{-1}) = \mathrm{N}_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(a - b\sqrt{-1}) = (a + b\sqrt{-1})(a - b\sqrt{-1}).$$

Comme $a + b\sqrt{-1}$ et $a - b\sqrt{-1}$ ont pour norme un nombre premier, ils sont irréductibles. L'égalité $p = (a+b\sqrt{-1})(a-b\sqrt{-1})$ est donc la factorisation de p en produit d'irréductibles dans l'anneau factoriel $\mathbb{Z}[\sqrt{-1}]$. Comme $\mathbb{Z}[\sqrt{-1}]^\times = \{\pm 1, \pm\sqrt{-1}\}$, par unicité de la factorisation en produit d'irréductibles, on en déduit que les diviseurs de p dans $\mathbb{Z}[\sqrt{-1}]$ sont :

$$\underbrace{\pm 1, \pm\sqrt{-1},}_{\text{norme } 1}\ \underbrace{\pm a \pm b\sqrt{-1}, \pm b \pm a\sqrt{-1},}_{\text{norme } p}\ \underbrace{\pm p, \pm p\sqrt{-1}}_{\text{norme } p^2}.$$

Notons que les diviseurs de norme p donnent des couples d'entiers dont la somme des carrés est p.

Réciproquement, si $(x, y) \in \mathbb{Z}^2$ vérifient $p = x^2 + y^2$, alors on a $p = (x + y\sqrt{-1})(x - y\sqrt{-1})$ dans $\mathbb{Z}[\sqrt{-1}]$, donc $x + y\sqrt{-1}$ est un diviseur de p de norme p. On a donc

$$\left\{(x, y) \in \mathbb{Z}^2 / x^2 + y^2 = p\right\} = \{(\pm a, \pm b), (\pm b, \pm a)\}.$$

Il reste à compter le nombre d'éléments de cet ensemble.

Si $a = 0$, on aurait $p = b^2$, ce qui est impossible puisque p est premier. Donc $a \neq 0$ et $a \neq -a$. De même on a $b \neq -b$.

Si $a = \pm b$, alors on a $p = 2a^2$. Comme p est premier, ce n'est possible que si $a = \pm 1$, et donc $p = 2$.

Si $p \neq 2$, il y a donc 8 couples d'entiers dont la somme des carrés est p.

Si $p = 2$, alors on peut prendre $a = b = 1$, et il y a 4 couples d'entiers dont la somme des carrés est 2.

Exercice 3

Soit $P(X) = X^3 + X + 1 \in \mathbb{Q}[X]$.

Question 1

Montrer que P est irréductible dans $\mathbb{Q}[X]$.

Comme $\deg(P) < 4$, il suffit de montrer que P n'est pas de racine dans $\mathbb{Q}$. Si $\frac{a}{b} \in \mathbb{Q}$ (avec a et b premiers entre eux) était une racine de P, on aurait $a \mid 1$ (le cœfficient constant) et $b \mid 1$ (le cœfficient dominant), donc $\frac{a}{b} \in \{\pm 1\}$. Or $P(1) = 3 \neq 0$ et $P(-1) = -1 \neq 0$, donc P n'a pas de racine dans $\mathbb{Q}$, donc il est irréductible dans $\mathbb{Q}[X]$.

Question 2

Soit $K = \mathbb{Q}[X]/(P)$. Notons $\alpha \in K$ la classe de X. Calculer la trace $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^m)$ pour $m \in \{0, 1, 2, 3, 4\}$.

On a :

$$\begin{aligned}
\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^0) &= \mathrm{Tr}_{K/\mathbb{Q}}(1) = [K : \mathbb{Q}] = \deg(P) \\
&= 3 \\
\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^1) &= 0 \quad \text{car le cœfficient de } X^2 \text{ dans } P \text{ est } 0. \\
\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2) &= 0^2 - 2 \cdot 1 \quad \text{à l'aide des relations cœfficients-racines pour } X \text{ et } X^2 \\
&= -2 \\
\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^3) &= \mathrm{Tr}_{K/\mathbb{Q}}(-\alpha - 1) \quad \text{car } P(\alpha) = 0 \\
&= 0 - 3 \quad \text{par linéarité} \\
&= -3 \\
\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^4) &= \mathrm{Tr}_{K/\mathbb{Q}}(-\alpha^2 - \alpha) = 2 - 0 \\
&= 2.
\end{aligned}$$

Question 3

Déterminer une $\mathbb{Z}$-base de l'anneau $\mathscr{O}_K$ des entiers de K.

Comme α est entier (puisque racine de $X^3 + X + 1$, la base $1, \alpha, \alpha^2$ de K sur $\mathbb{Q}$ est formée d'entiers. Son discriminant est

$$\begin{aligned}\operatorname{disc}_{K/\mathbb{Q}}(1,\alpha,\alpha^2) &= \begin{vmatrix} \operatorname{Tr}_{K/\mathbb{Q}}(1) & \operatorname{Tr}_{K/\mathbb{Q}}(\alpha) & \operatorname{Tr}_{K/\mathbb{Q}}(\alpha^2) \\ \operatorname{Tr}_{K/\mathbb{Q}}(\alpha) & \operatorname{Tr}_{K/\mathbb{Q}}(\alpha^2) & \operatorname{Tr}_{K/\mathbb{Q}}(\alpha^3) \\ \operatorname{Tr}_{K/\mathbb{Q}}(\alpha^2) & \operatorname{Tr}_{K/\mathbb{Q}}(\alpha^3) & \operatorname{Tr}_{K/\mathbb{Q}}(\alpha^4) \end{vmatrix} \\ &= \begin{vmatrix} 3 & 0 & -2 \\ 0 & -2 & -3 \\ -2 & -3 & 2 \end{vmatrix} \\ &= -12 + 0 + 0 - (-8) - 27 - 0 \\ &= -31.\end{aligned}$$

Comme ce discriminant est sans facteur carré, on en déduit que la base $1, \alpha, \alpha^2$ est aussi une $\mathbb{Z}$-base de l'anneau des entiers de K.

Question 4

En déduire que $\mathscr{O}_K = \mathbb{Z}[\alpha]$.

D'après la question précédente, on a $\mathscr{O}_K = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2$. En particulier, on a donc $\mathscr{O}_K \subseteq \mathbb{Z}[\alpha]$. D'autre part, $\alpha \in \mathscr{O}_K$ et $\mathscr{O}_K$ est une $\mathbb{Z}$-algèbre, donc $\mathbb{Z}[\alpha] \subseteq \mathscr{O}_K$, donc on trouve $\mathscr{O}_K = \mathbb{Z}[\alpha]$.

Exercice 4

Quelles sont les unités de l'anneau des entiers de $\mathbb{Q}(\sqrt{51})$? (Le détail des calculs doit être inclus dans la réponse).

Comme $51 = 3 \cdot 17$ est sans facteur carré et $51 \equiv 3 \not\equiv 1 \pmod 4$, l'anneau des entiers de $\mathbb{Q}(\sqrt{51})$ est $\mathbb{Z}[\sqrt{51}]$. Ses unités sont les éléments de norme ± 1 et sont donc données par les solutions de l'équation diophantienne

$$x^2 - 51y^2 = \pm 1.$$

On utilise l'algorithme de résolution vu en cours.

$$\begin{aligned} \left\lfloor \sqrt{51} \right\rfloor &= 7 & \frac{1}{\sqrt{51}-7} &= \frac{\sqrt{51}+7}{2} \\ \left\lfloor \frac{\sqrt{51}+7}{2} \right\rfloor &= 7 & \frac{2}{\sqrt{51}-7} &= \sqrt{51}+7 \\ \left\lfloor \sqrt{51}+7 \right\rfloor &= 14 \end{aligned}$$

Le développement en fraction continue de $\sqrt{51}$ est donc $[7, \overline{7, 14}]$. La période est paire, donc l'équation $x^2 - 51y^2 = -1$ n'a pas de solution (i.e. $\mathbb{Z}[\sqrt{51}]$ ne contient pas d'élément de norme -1).

On a :

$$7 + \frac{1}{7} = \frac{50}{7}$$

donc la solution fondamentale est $50^2 - 51 \cdot 7^2 = 1$, i.e. une unité fondamentale de $\mathbb{Z}[\sqrt{51}]$ est $50 + 7\sqrt{51}$. On a donc :

$$\mathbb{Z}[\sqrt{51}]^\times = \left\{ \pm(50 + 7\sqrt{51})^n ; n \in \mathbb{Z} \right\}.$$

Exercice 5

Soit K un corps de nombres. On note $\mathscr{O}_K$ l'anneau des entiers de K.

Question 1

Soit $a \in \mathscr{O}_K \setminus \{0\}$. Montrer que $|\mathrm{N}_{K/\mathbb{Q}}(a)| = \mathrm{Card}(\mathscr{O}_K/(a))$.

L'idéal (a) est un sous-$\mathbb{Z}$-module du $\mathbb{Z}$-module libre de type fini $\mathscr{O}_K$ (qui est de rang $n = [K : \mathbb{Q}]$). Il existe donc une base $e_1, \dots, e_n$ de $\mathscr{O}_K$ et des entiers $d_1, \dots, d_n \in \mathbb{Z}$ tels que :

- $d_1 \mid d_2 \mid \dots \mid d_n$,
- $d_1 e_1, \dots, d_k e_k$ est une base du $\mathbb{Z}$-module (a), en notant k le plus grand indice tel que d_k soit non nul.

Comme $a \neq 0$, la multiplication par a est injective. En particulier, comme $e_1, \dots, e_n$ est une base de $\mathscr{O}_K$, $ae_1, \dots, ae_n$ est une base du $\mathbb{Z}$-module (a), et celui-ci est de rang n, donc $k = n$.

Comme $ae_1, \dots, ae_n$ et $d_1 e_1, \dots, d_n e_n$ sont deux bases du $\mathbb{Z}$-module (a), la matrice de passage entre les deux est dans $\mathrm{GL}_n(\mathbb{Z})$, donc son déterminant est ± 1. On a donc

$$\mathrm{N}_{K/\mathbb{Q}}(a) = \det_{(e_1,\dots,e_n)}(ae_1, \dots, ae_n) = \pm \det_{(e_1,\dots,e_n)}(d_1 e_1, \dots, d_n e_n) = \pm d_1 \dots d_n.$$

D'autre part, $e_1, \dots, e_n$ est une base de $\mathscr{O}_K$ et $d_1 e_1, \dots, d_n e_n$ est une base de (a). Le quotient $\mathscr{O}_K/(a)$ est donc isomorphe à $\mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_n\mathbb{Z}$, donc

$$\mathrm{Card}(\mathscr{O}_K/(a)) = |d_1 \dots d_n| = |\mathrm{N}_{K/\mathbb{Q}}(a)|.$$

Question 2

Si I est un idéal non nul de $\mathscr{O}_K$, on définit $\mathrm{N}(I) \overset{\text{déf}}{=} \mathrm{Card}(\mathscr{O}_K/I)$. Montrer que $\mathrm{N}(I)$ est fini. (Indication : on pourra fixer un $a \in I \setminus \{0\}$ et comparer $\mathrm{N}(I)$ et $\mathrm{N}((a))$).

Comme l'idéal I est non nul, il existe un $a \in I \setminus \{0\}$. On a alors $(a) \subseteq I$, donc $\mathscr{O}_K/I$ est un quotient de $\mathscr{O}_K/(a)$ (par l'idéal $I/(a)$), donc $\mathrm{N}(I) \leqslant \mathrm{N}((a))$, i.e. $\mathrm{N}(I) \leqslant |\mathrm{N}_{K/\mathbb{Q}}(a)|$ d'après la question précédente. En particulier, $\mathrm{N}(I)$ est fini.

Question 3

Montrer que $\mathrm{N}(I) \in I$.

Le groupe $\mathscr{O}_K/I$ est d'ordre $\mathrm{N}(I)$, donc $\mathrm{N}(I) \cdot 1 = 0$ dans $\mathscr{O}_K/I$ (par théorème de Lagrange), i.e. $\mathrm{N}(I) \in I$.

Question 4

Montrer que si $\mathfrak{p}$ un idéal premier non nul de $\mathscr{O}_K$, alors $\mathscr{O}_K/\mathfrak{p}$ est un corps fini.

Comme $\mathfrak{p}$ un idéal premier, le quotient $\mathscr{O}_K/\mathfrak{p}$ est un anneau intègre. De plus, d'après la question 2, il est fini.

Montrons que tout anneau A commutatif intègre fini est un corps. Soit $a \in A \setminus \{0\}$. La multliplication par a est injective car l'anneau A est intègre, et elle est donc bijective puisque A est fini. Il existe donc un $b \in A$ tel que $ab = 1$. Tout élément non nul de A est donc inversible, donc A est un corps.

En particulier, ici, $\mathscr{O}_K/\mathfrak{p}$ est un corps.

Question 5

On suppose désormais que $\mathscr{O}_K$ est factoriel. Soit $\mathfrak{p}$ un idéal premier non nul de $\mathscr{O}_K$. Soit $\mathrm{N}(\mathfrak{p}) = \pi_1 \cdots \pi_m$ la factorisation de $\mathrm{N}(\mathfrak{p})$ dans $\mathscr{O}_K$, avec $\pi_1, \dots, \pi_m$ des irréductibles de $\mathscr{O}_K$ (pas forcément distincts). Montrer qu'il existe un $i \in \{1, \dots, m\}$ tel que $\pi_i \in \mathfrak{p}$.

On a $\pi_1 \cdots \pi_m \in \mathfrak{p}$ d'après la question 3, et l'idéal $\mathfrak{p}$ est premier, donc il existe un indice $i \in \{1, \dots, m\}$ tel que $\pi_i \in \mathfrak{p}$.

Question 6

Montrer que $\mathscr{O}_K/(\pi_i)$ est un corps fini.

D'après la question 4, il suffit de montrer que l'idéal principal (π_i) est premier. (On a $\pi_i \neq 0$ puisque $\mathrm{N}(\mathfrak{p}) \neq 0$ par définition de $\mathrm{N}(\mathfrak{p})$).

Soient $a, b \in \mathscr{O}_K$ tels que $ab \in (\pi_i)$. Comme $\pi_i \mid ab$, l'irréductible π_i apparaît (à adjonction près) dans la décomposition de ab en produit d'irréductibles. Comme l'anneau $\mathscr{O}_K$ est factoriel, on en déduit (par unicité de la décomposition de ab en produit d'irréductibles) que π_i apparaît (à adjonction près) dans la décomposition de a ou b en produit d'irréductibles, i.e. $\pi_i \mid a$ ou $\pi_i \mid b$.

L'idéal (π_i) est donc bien premier, et $\mathscr{O}_K/(\pi_i)$ est un corps fini.

Question 7

Montrer que $\mathfrak{p} = (\pi_i)$. (Indication : quels sont les idéaux de $\mathscr{O}_K/(\pi_i)$?)

Comme $\pi_i \in \mathfrak{p}$, on a $(\pi_i) \subseteq \mathfrak{p}$, donc $\mathfrak{p}/(\pi_i)$ est un idéal de l'anneau $\mathscr{O}_K/(\pi_i)$. Or $\mathscr{O}_K/(\pi_i)$ est un corps d'après la question 6, donc ses idéaux sont l'idéal nul et $\mathscr{O}_K/(\pi_i)$ tout entier. On a donc $\mathfrak{p} = (\pi_i)$ ou $\mathfrak{p} = \mathscr{O}_K$.

Comme $\mathfrak{p}$ est un idéal premier (donc $\mathfrak{p} \neq \mathscr{O}_K$), on a $\mathfrak{p} = (\pi_i)$.

Question 8

On admet que tout idéal I non nul de $\mathscr{O}_K$ s'écrit comme un produit $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ d'idéaux premiers non nuls (pas nécessairement distincts). Montrer que l'anneau $\mathscr{O}_K$ est principal.

D'après les questions 5 à 7, tout idéal premier non nul de $\mathscr{O}_K$ est principal. La propriété admise ci-dessus montre alors que tout idéal non nul de $\mathscr{O}_K$ est principal. L'idéal nul étant lui-aussi principal, on en déduit que tous les idéaux de l'anneau $\mathscr{O}_K$ sont principaux. Comme $\mathscr{O}_K$ est un anneau intègre, c'est un anneau principal.