Examen de Théorie algébrique des nombres – MAT552 – 14/12/2016

Documents autorisés : polycopié du cours, notes de cours et PC, calculatrice. Les corrigés des exercices du polycopié, ainsi que les corrigés des examens antérieurs, ne sont pas autorisés. Il n'est pas nécessaire de traiter toutes les questions pour avoir la note maximale.

Problème 1. (*Formes de discriminant* -95) *On pose* $\alpha = \frac{1+\sqrt{-95}}{2}$ *et* $A = \mathbb{Z}[\alpha]$ $(= \mathrm{A}_{-95})$.

(i) Déterminer des représentants de $\mathrm{Cl}(-95)$*, ainsi que ses classes primitives.*

(ii) Déterminer l'ensemble des éléments d'ordre 2 *du groupe* $\mathrm{P}(-95)$.

(iii) Justifier que A *est un anneau de Dedekind et donner* $\Pi_{\alpha,\mathbb{Q}}$.

On considère les idéaux $D = 2A + \alpha A$, $\overline{D} = 2A + (\alpha - 1)A$ *et* $C = 5A + (\alpha + 2)A$.

(iv) Montrer que ces idéaux sont premiers et déterminer leur norme.

(v) Montrer que C *n'est pas principal, ainsi que les relations* $(5) = C^2$ *et* $(2) = D\overline{D}$.

(vi) En déduire la classe $\mathrm{q}_C \in \mathrm{P}(-95)$ *associée à* C *par la bijection de Dedekind.*

(vii) En déduire aussi l'égalité $(7 + \alpha) = \overline{D}^4 C$.

(viii) Montrer que $\mathrm{Cl}(A)$ *est un groupe cyclique d'ordre* 8*, engendré par la classe de* D.

(ix) Montrer que $2, \alpha$ *est une* $\mathbb{Z}$*-base de* D*, puis déterminer la classe* $\mathrm{q}_D \in \mathrm{P}(-95)$.

(x) Déterminer le carré et le cube de la classe de $(2, 1, 12)$ *dans* $\mathrm{P}(-95)$.

(xi) En déduire la table de multiplication du groupe $\mathrm{P}(-95)$.

(xii) (Application) Supposons que l'entier n *est représenté par la forme* $(2, 1, 12)$*. Montrer que* n^2, n^3 *et* n^4 *sont respectivement représentés par les formes* $(4, 1, 6)$, $(3, 1, 8)$ *et* $(5, 5, 6)$.

Problème 2. *Soient* K *un corps de nombres et* A *un ordre de* K*. On se propose d'abord de démontrer l'équivalence des propriétés suivantes :*

(a) $A = \mathcal{O}_K$,

(b) tout idéal maximal de A *est inversible,*

(c) tout idéal non nul de A *est inversible.*

Si $x \in K$ *et* $E \subset K$*, on pose* $xE = \{xe,\ e \in E\}$ *et* $A[x] = \{P(x),\ P \in A[X]\}$.

(i) Soient $a, b \in A$ *avec* $b \neq 0$*, et soit* I *un idéal inversible de* A*, tels que* $aI \subset bI$*. Montrer que* b *divise* a *dans* A.

(ii) Montrer que tout élément de K *s'écrit sous la forme* a/m *avec* $a \in A$ *et* $m \in \mathbb{Z}$ *non nul. En déduire que pour tout sous-ensemble fini* E *de* K *il existe* $m \in \mathbb{Z}$ *non nul tel que* $mE \subset A$.

(iii) Soit $x \in \mathcal{O}_K$*. Montrer qu'il existe* $m \in \mathbb{Z}$ *non nul tel que* $mA[x] \subset A$.

(iv) (suite) En déduire qu'il existe un idéal I *non nul de* A *vérifiant* $xI \subset I$.

(v) Montrer (c) $\Rightarrow$ *(a).*

(vi) Soient I, J des idéaux non nuls de A avec $IJ = I$. Montrer $J = A$. (On pourra se contenter de pointer l'endroit du cours où cet énoncé est démontré !)

(vii) Montrer (b) $\Rightarrow$ (c). Conclure.

On s'intéresse maintenant au cas $A = \mathbb{Z}[\alpha]$ avec $\alpha \in \overline{\mathbb{Z}}$. Soient $\Pi_{\alpha,\mathbb{Q}} \in \mathbb{Z}[X]$ le polynôme minimal de α sur $\mathbb{Q}$, p un nombre premier fixé et $P \in (\mathbb{Z}/p\mathbb{Z})[X]$ la réduction modulo p de $\Pi_{\alpha,\mathbb{Q}}$. On rappelle que pour tout diviseur Q de P dans $(\mathbb{Z}/p\mathbb{Z})[X]$, on dispose de l'idéal de A noté $\mathrm{I}(Q)$ dans le cours.

(viii) Que vaut $\mathrm{I}(P)$?

(ix) Soient $Q, Q' \in (\mathbb{Z}/p\mathbb{Z})[X]$. On suppose que Q et Q' sont des diviseurs de P dans $(\mathbb{Z}/p\mathbb{Z})[X]$, et qu'ils sont premiers entre eux. Soient $\widetilde{Q}, \widetilde{Q'} \in \mathbb{Z}[X]$ vérifiant $\widetilde{Q} \equiv Q \bmod p$ et $\widetilde{Q'} \equiv Q' \bmod p$. Montrer qu'il existe $U, U' \in \mathbb{Z}[X]$ tels que $U(\alpha)\widetilde{Q}(\alpha) + U'(\alpha)\widetilde{Q'}(\alpha) \in 1 + pA$.

(x) (suite) En déduire $\mathrm{I}(QQ') = \mathrm{I}(Q)\mathrm{I}(Q')$.

(xi) Montrer que si P est sans facteur carré, tout idéal premier de A contenant p est inversible.

Problème 3. *Soit ℓ un nombre premier impair, on considère l'anneau $A = \mathbb{Z}[\zeta]$ avec $\zeta = e^{2i\pi/\ell}$. On se propose d'abord de redémontrer que A est l'anneau des entiers du corps de nombres $K = \mathbb{Q}(\zeta)$. On pose $\Phi_\ell(X) = \frac{X^\ell - 1}{X - 1} = 1 + X + \cdots + X^{\ell-1}$; on rappelle que $\Phi_\ell(X)$ est irréductible dans $\mathbb{Q}[X]$.*

(i) Donner les entiers $[K : \mathbb{Q}]$, r_1 et r_2 associés au corps de nombres K. Montrer que l'application $\sigma \mapsto \sigma(\zeta)$ induit une bijection entre $\Sigma(K)$ et $\{\zeta^i,\ \ i = 1, \ldots, \ell - 1\}$.

(ii) Montrer $\mathrm{N}_{K/\mathbb{Q}}(1 - \zeta) = \ell$.

(iii) En déduire que $(1 - \zeta)$ est un idéal maximal de A contenant ℓ.

(iv) En déduire également $|\mathrm{disc}\, \mathbb{Z}[\zeta]| = \ell^{\ell-2}$.

(v) Montrer que $(1 - \zeta)$ est l'unique idéal premier de A contenant ℓ.

(vi) Montrer que si p est un nombre premier $\neq \ell$, alors la réduction modulo p de $\Phi_\ell(X)$ est sans facteur carré dans $(\mathbb{Z}/p\mathbb{Z})[X]$.

(vii) Conclure (on utilisera les résultats du problème 2).

On considère désormais le cas particulier $\ell = 7$. On se propose de démontrer que l'anneau $A = \mathbb{Z}[e^{2i\pi/7}]$ est principal. On utilisera librement les données et informations situées plus bas.

(viii) Montrer que tout idéal non nul de A est équivalent à un idéal de A contenant un entier N avec $1 \leq N \leq 4$.

(ix) Montrer que le groupe $\mathrm{Cl}(A)$ est engendré par la classe de l'idéal $(2, \zeta^3 + \zeta + 1)$.

(x) Montrer $\mathrm{N}_{K/\mathbb{Q}}(\zeta^3 + \zeta + 1) = 8$, puis conclure.

Données : (a) on a $\frac{\sqrt{7}}{\pi^3} \cdot 2^4 \cdot 3^{-4} \cdot 5 \cdot 7^2 = 4.13$ à 10^{-2} près, (b) la réduction modulo 3 de $\Phi_7(X)$ est irréductible dans $(\mathbb{Z}/3\mathbb{Z})[X]$, (c) on a $\Phi_7(X) \equiv (X^3 + X + 1)(X^3 + X^2 + 1) \bmod 2$, (d) on a l'égalité

$$\det \begin{bmatrix} 1 & 0 & 0 & -1 & 1 & -1 \\ 1 & 1 & 0 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 & -1 \\ 1 & 0 & 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & -1 & 1 & 0 \end{bmatrix} = 8.$$