EXAMEN DE THÉORIE ALGÉBRIQUE DES NOMBRES – MAT552 – 19/12/2018

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.

Problème 1. *On pose* $\alpha = \frac{1+\sqrt{-155}}{2}$ *et* $A = \mathbb{Z}[\alpha]$.

(i) Déterminer des représentants de $\mathrm{Cl}(-155)$ *et ses classes ambiguës.*

(ii) En déduire la structure du groupe $\mathrm{P}(-155)$*.*

(iii) En utilisant le théorème de Dedekind, déterminer la structure du groupe $\mathrm{Pic}(A)$*.*

On se propose de redémontrer le (iii) sans utiliser le théorème de Dedekind.

(iv) Montrer que tout idéal non nul de A *est équivalent à un idéal contenant un entier* N *avec* $1 \leq N \leq 7$*.*

(v) Montrer que $\mathrm{Cl}(A)$ *est un groupe, et qu'il est engendré par les classes des idéaux premiers de* A *contenant* $2, 3, 5$ *ou* 7*.*

(vi) Montrer qu'il existe exactement deux idéaux premiers de A *contenant* 3*, à savoir* $T = (3, \alpha)$ *et* $T' = (3, \alpha - 1)$*, et que l'on a* $(3) = TT'$*.*

(vii) Montrer que les idéaux (2) *et* (7) *sont premiers, et que l'on a* $(5) = C^2$ *avec* C *l'unique idéal premier de* A *contenant* 5*.*

(viii) Montrer $(\alpha - 3) = CT^2$ *et que* C *n'est pas principal.*

(ix) En déduire que $\mathrm{Cl}(A)$ *est engendré par la classe de* T*, et conclure.*

Si K est un corps de nombres, on rappelle que $\Sigma(K)$ désigne l'ensemble de ses plongements. On dira que K est *totalement réel* si pour tout σ dans $\Sigma(K)$ on a $\sigma(K) \subset \mathbb{R}$.

Problème 2. (Un théorème de Hermite) *On fixe un entier* $n \geq 1$*. On se propose de démontrer que pour tout entier* d *il n'existe qu'un nombre fini de corps de nombres totalement réels, de degré* n*, et de discriminant* d*.*

(i) (Question prélimininaire) Soient K *un corps de nombres et* $x \in K$ *avec* $\mathbb{Q}(x) \neq K$*. Montrer que pour tout* σ *dans* $\Sigma(K)$*, il existe* τ *dans* $\Sigma(K) - \{\sigma\}$ *vérifiant* $\tau(x) = \sigma(x)$*.*

Dans les questions suivantes, K est un corps de nombres totalement réel fixé de degré n, et on pose $\Sigma(K) = \{\sigma_1, \ldots, \sigma_n\}$ (justifier) et $d = |\mathrm{disc}\, K|$.

(ii) Montrer qu'il existe un élément $x \in \mathcal{O}_K$ *non nul vérifiant* $|\sigma_1(x)| \leq 2^{n-1}\sqrt{d}$ *et* $|\sigma_i(x)| \leq 1/2$ *pour tout* $i \neq 1$*.*

(iii) Montrer $|\sigma_1(x)| \geq 2^{n-1}$*.*

(iv) En déduire $K = \mathbb{Q}(x)$*.*

(v) Conclure en examinant le polynôme caractéristique de x *dans l'extension* $K/\mathbb{Q}$*.*

Problème 3. (Un anneau d'entiers non monogène)

Partie I. Soit p un nombre premier. Pour tout anneau A on note $\mathrm{Hom}(A, \mathbb{Z}/p\mathbb{Z})$ l'ensemble des morphismes d'anneaux de A dans $\mathbb{Z}/p\mathbb{Z}$.

(i) Montrer que si x est dans $\overline{\mathbb{Z}}$, et si R est le polynôme minimal de x sur $\mathbb{Q}$, alors $\mathrm{Hom}(\mathbb{Z}[x], \mathbb{Z}/p\mathbb{Z})$ est en bijection avec l'ensemble des racines dans $\mathbb{Z}/p\mathbb{Z}$ de la réduction modulo p de R.

(ii) Montrer que si K est un corps de nombres, et si $P_1, \ldots, P_r$ désignent les idéaux premiers distincts de $\mathcal{O}_K$ de norme p, alors $\mathrm{Hom}(\mathcal{O}_K, \mathbb{Z}/p\mathbb{Z})$ a au moins r éléments.

(iii) (suite) En déduire que si $\mathcal{O}_K$ est de la forme $\mathbb{Z}[x]$ avec x dans $\mathcal{O}_K$, on a $r \leq p$.

Partie II. Soient α dans $\overline{\mathbb{Q}}$, $K = \mathbb{Q}(\alpha)$ et R le polynôme minimal de α sur $\mathbb{Q}$.

(iv) Montrer que pour tout $t \in \mathbb{Q}$ on a $\mathrm{N}_{K/\mathbb{Q}}(t - \alpha) = R(t)$.

(v) On suppose $\alpha \neq 1$. Montrer $\mathrm{Tr}_{K/\mathbb{Q}} \frac{1}{1-\alpha} = \frac{R'(1)}{R(1)}$.

Partie III. Soient $\alpha \in \mathbb{C}$ vérifiant $\alpha^3 - \alpha - 8 = 0$ et $K = \mathbb{Q}(\alpha)$. On se propose de démontrer que $\mathcal{O}_K$ n'est pas de la forme $\mathbb{Z}[x]$ avec $x \in \mathcal{O}_K$.

(vi) Montrer que $t^3 - t - 8$ est irréductible dans $\mathbb{Q}[t]$. En déduire $[K : \mathbb{Q}]$.

(vii) En contemplant l'égalité $8 = \alpha(\alpha - 1)(\alpha + 1)$, montrer que tout idéal premier de $\mathcal{O}_K$ contenant 2 contient soit α, soit $\alpha + 1$ (exclusivement).

(viii) Montrer que l'idéal principal $P = (\alpha - 2)\mathcal{O}_K$ est de norme 2.

(ix) En déduire que P est l'unique idéal premier de $\mathcal{O}_K$ contenant 2 et α.

(x) On suppose qu'il existe un unique idéal premier Q de $\mathcal{O}_K$ contenant 2 et $\alpha + 1$. Montrer qu'il existe un entier $m \geq 1$ vérifiant $(\alpha - 1)\mathcal{O}_K = Q^m = (\alpha + 1)\mathcal{O}_K$.
Indication : on pourra observer $\mathrm{N}_{K/\mathbb{Q}}(\alpha \pm 1) = 8$.

(xi) (suite) En déduire que l'élément $\beta = \frac{1+\alpha}{1-\alpha}$ est dans $\mathcal{O}_K$.

(xii) Montrer $\mathrm{Tr}_{K/\mathbb{Q}} \beta = -7/2$.

(xiii) En déduire qu'il existe au moins 2 idéaux premiers de $\mathcal{O}_K$ contenant 2 et $\alpha + 1$, disons Q_1 et Q_2.

(xiv) Montrer $2\mathcal{O}_K = PQ_1Q_2$ et $\mathrm{N}(Q_1) = \mathrm{N}(Q_2) = 2$.

(xv) Conclure.

Partie IV. (Bonus)

(xvi) Montrer $(\alpha) = P^3$.

(xvii) Quitte à échanger les rôles de Q_1 et Q_2, montrer $(\alpha + 1)\mathcal{O}_K = Q_1^2 Q_2$ et $(\alpha - 1)\mathcal{O}_K = Q_1 Q_2^2$.

(xviii) En déduire $\frac{\alpha(\alpha+1)}{2} \in \mathcal{O}_K$.

(xix) Montrer $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\frac{\alpha(\alpha+1)}{2}$. (Observer que le discriminant de $t^3 - t - 8$ est $-4 \cdot 431$.)

(xx) Retrouver que l'anneau $\mathcal{O}_K / 2\mathcal{O}_K$ est isomorphe à l'anneau produit $(\mathbb{Z}/2\mathbb{Z})^3$.