Université Bordeaux 1 — Année 2006–2007 — Session janvier 2007

Scolarité Licence

Étape : MAP5

UE : MAP501 ; Épreuve d'Algèbre 4

Date : 6 janvier 2007, 8h30-11h30

Durée : 3 heures

Documents interdits

Épreuve de M. Qing Liu

Exercice 1 Répondre aux questions suivantes par OUI, NON, ou, si vous n'êtes pas sûr(e) de la réponse, ne rien inscrire.

Attention : toute réponse incorrecte sera comptée négativement ! Il est inutile de recopier l'énoncé, reportez juste le numéro de la question (1.a, 1.b, 3.a etc) avec vos réponses.

1. Soit $F(X) \in \mathbb{Z}[X]$.
   (a) Si $F(X)$ est primitif, alors il est irréductible ;
   NON : $X^2 - 1 \in \mathbb{Z}[X]$ est primitif mais non irréductible.
   (b) Si $F(X)$ est irréductible, alors il est primitif ;
   OUI : le pgcd des coefficients de $F(X)$ divise $F(X)$, et est donc égal à 1.
   (c) Si $F(X)$ est unitaire, irréductible dans $\mathbb{Q}[X]$, alors il est irréductible dans $\mathbb{Z}[X]$.
   OUI : car $F(X)$ est alors primitif et on applique le théorème 4.2.10(1) du cours.
2. L'anneau $\mathbb{Z}[X]$ est :
   (a) principal ;
   NON : Remarque 4.2.12. Plus concrètement, l'idéal $(2, X)$ engendré par 2 et X n'est pas principal.
   (b) factoriel ;
   OUI : Théorème 4.2.10(2).
   (c) noethérien.
   OUI : Théorème 2.2.5.
3. Soient $P(X,Y), Q(X,Y) \in \mathbb{Q}[X,Y] \setminus \{0\}$ premiers entre eux.
   (a) Il existe $R(X,Y), S(X,Y) \in \mathbb{Q}[X,Y]$ tels que
   $$R(X,Y)P(X,Y) + S(X,Y)Q(X,Y) = 1;$$
   NON : il suffit de considérer le cas $P(X,Y) = X$ et $Q(X,Y) = Y$.
   (b) Si $P(X,Y)$ divise $Q(X,Y)F(X,Y)$ avec $F(X,Y) \in \mathbb{Q}[X,Y]$, alors $P(X,Y)$ divise $F(X,Y)$;
   OUI : Proposition 4.1.26(1).

(c) Si $P(X,r)=0$ pour tout $r\in\mathbb{Q}$, alors $P(X,Y)=0$.
OUI : On considère $P(X,Y)$ comme un élément de $A[Y]$ avec $A=\mathbb{Q}[X]$. Comme il a une infinité de zéros et que A est intègre, on a $P(X,Y)=0$ (contraposé du Corollaire 3.2.5).

4. Soient L/K une extension, L_1, L_2 des sous-extensions finies de L/K.
   (a) L_1L_2 est une extension finie de K ;
   OUI : Proposition 5.3.21.
   (b) $[L_1L_2 : K] = [L_1 : K][L_2 : K]$;
   NON en général : Remarque 5.3.23.
   (c) $L_1\cup L_2$ est une extension finie de K.
   NON : ce n'est même pas un corps en général.

Exercice 2 Quels sont parmi les polynômes suivants ceux qui sont irréductibles ? Justifiez vos affirmations.

$$X^4+30X+20\in\mathbb{R}[X], \quad X^4+30X+20\in\mathbb{Q}[X], \tag{1}$$

$$X^2Y^4+Y^2Z^4+X^5Z\in\mathbb{Z}[X,Y,Z]. \tag{2}$$

Solution : (1) $X^4+30X+20$ n'est pas irréductible dans $\mathbb{R}[X]$ car les polynômes irréductibles de $\mathbb{R}[X]$ sont de degré 1 ou 2 (corollaire 5.3.47). Par contre il est irréductible dans $\mathbb{Q}[X]$ par le critère d'Eisenstein avec $A=\mathbb{Z}$ et $f=5$.

(2) Le polynôme s'écrit $a_4Y^4+a_2Y^2+a_0\in\mathbb{Z}[X,Z]$ avec $a_4=X^2, a_2=Z^4$ et $a_0=X^5Z$. Il est primitif car $\text{pgcd}(a_0,a_2,a_4)=1$. Le critère d'Eisenstein appliqué à $A=\mathbb{Z}[X,Z]$, $f=Z$ implique l'irréductibilité.

Exercice 3 (Polynômes symétriques)

1. En développant $(X+Y)^4$, exprimer $X^4+Y^4\in\mathbb{Z}[X,Y]$ en fonction de $X+Y$ et XY.
2. Exprimer $P(X,Y,Z)=X^2Y^2+X^2Z^2+Y^2Z^2\in\mathbb{Z}[X,Y,Z]$ en fonction des polynômes symétriques élémentaires $s_1,s_2,s_3\in\mathbb{Z}[X,Y,Z]$.

Solution : (1) On a

$$\begin{aligned}(X+Y)^4 &= X^4+4X^3Y+6X^2Y^2+4XY^3+Y^4\\ &= (X^4+Y^4)+2XY(2X^2+3XY+2Y^2)\\ &= (X^4+Y^4)+2XY(2(X+Y)^2-XY)\\ &= (X+Y)^4-2(XY)(2(X+Y)^2-(XY)).\end{aligned}$$

(2) On utilise la remarque 3.3.10. On a $\tilde{P}(X,Y)=X^2Y^2=\tilde{s}_2^2$. Donc $P(X,Y,Z)=s_2^2+s_3F$ avec $\deg F\leq 1$, donc $F=as_1$ avec $a\in\mathbb{Z}$. En prenant $X=Y=Z=1$, on obtient $a=-2$. D'où

$$P(X,Y,Z)=s_2^2-2s_1s_3.$$

On peut aussi trouver directement :

$$P(X,Y,Z)=(XY+XZ+YZ)^2-2(X^2YZ+XY^2Z+XYZ^2)=s_2^2-2s_3s_1.$$

Exercice 4 Soient p un nombre premier et $\bar{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. Rappelons que $\mathbb{F}_{p^d}$ désigne une sous-extension de $\bar{\mathbb{F}}_p$ de degré d sur $\mathbb{F}_p$. Fixons un $a \in \mathbb{F}_p$.

1. Si a n'est pas un carré dans $\mathbb{F}_p$, montrer que $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{a}]$, où $\sqrt{a}$ est une racine carré de a dans $\bar{\mathbb{F}}_p$.
2. Si a n'est pas un cube dans $\mathbb{F}_p$, montrer que $\mathbb{F}_{p^3} = \mathbb{F}_p[\sqrt[3]{a}]$, où $\sqrt[3]{a}$ est une racine cubique de a dans $\bar{\mathbb{F}}_p$.

Solution : (1) Comme $X^2 - a$ est sans racine dans $\mathbb{F}_p$, il est irréductible, donc $\mathbb{F}_p[\sqrt{a}]$ est une sous-extension de $\bar{\mathbb{F}}_p$ de degré 2 sur $\mathbb{F}_p$. Par l'unicité d'une sous-extension de degré donné (théorème 5.4.2(a)), on a $\mathbb{F}_p[\sqrt{a}] = \mathbb{F}_{p^2}$.

(2) Raisonnement similaire à (1).

Exercice 5 Notons $i = \sqrt{-1} \in \mathbb{C}$ et

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

On sait que $\mathbb{Z}[i]$ est un anneau principal. Soit d un entier naturel impair sans facteur carré. Fixons une racine quatrième $\sqrt[4]{-d} \in \mathbb{C}$ de $-d$.

1. Montrer que $\mathrm{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i] \subset \mathbb{C}$.
2. Montrer que $\mathbb{Q}[i, \sqrt[4]{-d}]$ est un corps de décomposition de $X^4 + d \in \mathbb{Q}[X]$.
3. Montrer que $X^4 + d$, considéré comme un polynôme dans $\mathbb{Q}[i][X]$, est irréductible (on pourra utiliser les résultats de l'exercice 6.3 ci-après).
4. Déterminer le degré $\big[\mathbb{Q}[i, \sqrt[4]{-d}] : \mathbb{Q}\big]$.

Solution : (1) Comme $\mathbb{Q}[i]$ est un corps, on a $\mathrm{Frac}(\mathbb{Z}[i]) \subseteq \mathbb{Q}[i]$. Mais l'inclusion inverse est évidente.

(2) Les racines complexes du polynôme $X^4 + d$ sont $i^k \sqrt[4]{-d}$, $k = 0, 1, 2, 3$. Elles appartiennent toutes à $\mathbb{Q}[i, \sqrt[4]{-d}]$. Inversement, $i = (i\sqrt[4]{-d})/\sqrt[4]{-d}$. D'où l'égalité

$$\mathbb{Q}[i^k \sqrt[4]{-d}]_{k=0,1,2,3} = \mathbb{Q}[i, \sqrt[4]{-d}].$$

(3) Fixons un nombre premier p qui divise d. Alors $p \geq 3$. Soit f un élément irréductible de $\mathbb{Z}[i]$ qui divise p. D'après l'exercice 6.3 ci-dessous, f^2 ne divise pas p. De plus, pour tout autre facteur premier $\ell \neq p$ de d, f ne divise pas ℓ car on a $1 = ap + b\ell$ pour certains $a, b \in \mathbb{Z}$, ce qui implique que p, ℓ sont premiers entre eux dans $\mathbb{Z}[i]$. Par suite f^2 ne divise pas d. Comme f divise les autres coefficients de $X^4 + d$, sauf le coefficient dominant, le critère d'Eisenstein implique alors que $X^4 + d$ est irréductible dans $\mathbb{Z}[i][X]$.

(4) On a

$$\big[\mathbb{Q}[i, \sqrt[4]{-d}] : \mathbb{Q}\big] = \big[\mathbb{Q}[i][\sqrt[4]{-d}] : \mathbb{Q}[i]\big]\,\big[\mathbb{Q}[i] : \mathbb{Q}\big] = 4 \times 2 = 8.$$

Exercice 6 Soit $p \in \mathbb{N}$ un nombre premier. On souhaite connaître la décomposition de p en produit d'éléments irréductibles de $\mathbb{Z}[i]$.

1. Pour tout $z \in \mathbb{Z}[i]$, on note $\bar{z} \in \mathbb{Z}[i]$ son conjugué (complexe) et $N(z) = z\bar{z}$.

(a) Montrer que pour tous $z_1, z_2 \in \mathbb{Z}[i]$, on a $N(z_1) \in \mathbb{N}$ et $N(z_1 z_2) = N(z_1)N(z_2)$.

(b) Soit $z \in \mathbb{Z}[i]$. Montrer que $z \in \mathbb{Z}[i]^*$ (ensemble des éléments inversibles de $\mathbb{Z}[i]$) si et seulement si $N(z) = 1$. En déduire que $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

2. Décomposition de p dans $\mathbb{Z}[i]$.

(a) Soient $z_1, z_2 \in \mathbb{Z}[i]$ non-inversibles tels que $p = z_1 z_2$. Montrer que $p = N(z_1) = N(z_2)$, que z_1, z_2 sont irréductibles dans $\mathbb{Z}[i]$, et que $z_2 = \bar{z}_1$.

(b) Montrer que si p n'est pas une somme de carrés $a^2 + b^2$ avec $a, b \in \mathbb{Z}$, alors p est irréductible dans $\mathbb{Z}[i]$.

(c) Montrer que dans le cas contraire, on a $p = N(f) = f\bar{f}$ avec $f, \bar{f} \in \mathbb{Z}[i]$ irréductibles.

(d) Dire si les nombres premiers $2, 3, 5, 7, 11$ sont irréductibles dans $\mathbb{Z}[i]$.

3. Supposons que p est divisible par f^2 avec $f \in \mathbb{Z}[i]$ irréductible.

(a) Montrer que $p = N(f)$ et que $\bar{f}$ est associé à f, i.e. $\bar{f} = uf$ avec $u \in \mathbb{Z}[i]^*$.

(b) Montrer que si $u = \pm 1$, alors $f \in \mathbb{Z} \cup \mathbb{Z}i$.

(c) Supposons $u = \pm i$. En écrivant $f = a + bi$ avec $a, b \in \mathbb{Z}$, montrer que f est associé à $1 + i$.

(d) Conclure que $p = 2$ et que f est associé à $1 + i$.

Solution : (1.a) Si $z_1 = a + bi$, alors $N(z_1) = a^2 + b^2 \in \mathbb{N}$. Comme $N(z) = |z|^2$, il est clair que $N(z_1 z_2) = N(z_1)N(z_2)$.

(1.b) Si $z\bar{z} = N(z) = 1$, comme $\bar{z} \in \mathbb{Z}[i]$, z est inversible dans $\mathbb{Z}[i]$. Inversement, si z est inversible, d'inverse z', on a $N(z)N(z') = N(zz') = 1$. Comme $N(z)$ et $N(z')$ sont des entiers naturels, on a $N(z) = 1$. En écrivant $z = a + bi$, la condition $N(z) = 1$ équivaut à $a^2 + b^2 = 1$, donc ou bien $b = 0$ et $a = \pm 1$, ou bien $a = 0$ et $b = \pm 1$. Ce qui implique que $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

(2.a) Si $p = z_1 z_2$ avec z_1, z_2 non-inversibles, alors $p^2 = N(p) = N(z_1)N(z_2)$ avec $N(z_k) \geq 2$. Donc $N(z_k) = p$ pour $k = 1, 2$. Si on a par exemple $z_1 = w_1 w_2$ avec $w_k \in \mathbb{Z}[i]$ non-inversibles, alors p^2 est le produit de trois entiers $N(w_1), N(w_2), N(z_2) \geq 2$, impossible. Donc z_1, z_2 sont irréductibles. Comme $z_1 \bar{z}_1 = N(z_1) = p = z_1 z_2$, on a $z_2 = \bar{z}_1$.

(2.b) En effet, si p n'est pas irréductible dans $\mathbb{Z}[i]$, on a $p = z_1 z_2$ avec $z_k \in \mathbb{Z}[i]$ non-inversibles. Il suit de (2.a) que $p = N(z_1) = a^2 + b^2$ si $z_1 = a + bi$.

(2.c) Si $p = a^2 + b^2$, alors $p = (a + bi)(a - bi)$ et $N(a \pm bi) = p \neq 1$. Donc $a \pm bi$ n'est pas inversible. Il suit de (2.a) que $f := a + bi$ et $\bar{f}$ sont irréductibles.

(2.d) Les nombres $3, 7, 11$ ne sont pas sommes de deux carrés dans $\mathbb{Z}$, et sont donc irréductibles dans $\mathbb{Z}[i]$, tandis que $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$ sont réductibles dans $\mathbb{Z}[i]$.

(3.a) On a $p = f^2 u = f(fu)$, $u \in \mathbb{Z}[i]$. Il suit de (2.a) que $p = N(f) = N(fu)$ et que $fu = \bar{f}$. Donc $N(u) = 1$ et $\bar{f}$ est associé à f.

(3.b) Si $u = 1$, alors $\bar{f} = f$, donc $f \in \mathbb{Z}$. Si $u = -1$, alors $\overline{fi} = fi$, donc $fi \in \mathbb{Z}$ et $f \in \mathbb{Z}i$.

(3.c) Supposons $u = -i$ avec $f = a + bi$. Alors $a - bi = -ai + b$, donc $b = a$ et $f = a(1 + i)$. Comme f est irréductible et que $1 + i \notin \mathbb{Z}[i]^*$, on a $a \in \mathbb{Z} \cap \mathbb{Z}[i]^* = \{\pm 1\}$. Si $u = i$, on a $\overline{(fi)} = -i(fi)$, donc $fi = \pm(1 + i)$. Dans tous les cas, f est associé à $1 + i$.

(3.d) Le cas (3.b) est exclu car $p = N(f)$ serait divisible par le carré d'un entier ≥ 2. Donc f est associé à $1 + i$. Par conséquent, $p = N(1 + i) = 2$.

Notons que dans $\mathbb{Z}[i]$, 2 est effectivement divisible par un carré $(1 + i)^2$ non-inversible.