université de BORDEAUX Collège S & T	**Année universitaire 2017/2018** **Session 1 d'automne** **Parcours : 4TMF5** **Code UE : 4TMF502U** **Épreuve : Structure algébrique 2** **Date : 22/10/2017** **Heure : 14h00–17h00** Documents non autorisés. Calculette homologuée autorisée. Épreuve de M. Qing LIU

Exercice 1 *Soit A un anneau intègre qui n'est pas un corps. Montrer que $A[X]$ n'est jamais principal (considérer l'idéal (a, X) de $A[X]$ engendré par un élément $a \in A$ non nul et non inversible et X).*

Solution Si (a, X) est engendré par un seul élément $P(X) \in A[X]$, alors il existe $Q(X), R(X) \in A[X]$ tels que $X = P(X)Q(X)$ et $a = P(X)R(X)$. La deuxième égalité implique que $P(X) = b$ est constante dans A, et la première égalité implique (en comparant les coefficients dominants) que b est inversible dans A (donc inversible dans $A[X]$). Ce qui implique que $(a, X) = A[X]$.

En écrivant $1 = aF(X) + XG(X)$, et en considérant les termes constants, on trouve $1 = aF(0)$ et que a est inversible dans A, contrairement à l'hypothèse de départ.

Exercice 2 *Quels sont parmi les polynômes suivants ceux qui sont irréductibles (justifier la réponse) ?*

1. $X^4 + 30X^2 + 20 \in \mathbb{R}[X]$;
2. $X^4 + 30X^2 + 20 \in \mathbb{Q}[X]$;
3. $XY^4 + YZ^4 + ZX^4 \in \mathbb{Q}[X, Y, Z]$.
4. $X^3 - 3X - 1 \in \mathbb{Q}[X]$.

Solution

1. Les polynômes irréductibles dans $\mathbb{R}[X]$ sont de degré ≤ 2. Donc $X^4 + 30X^2 + 20$ n'est pas irréductible dans $\mathbb{R}[X]$.

2. Par le critère d'Eisenstein avec l'élément irréductible $5 \in \mathbb{Z}$, on obtient que $X^4 + 30X^2 + 20$ est irréductible dans $\mathbb{Q}[X]$.

3. On applique Eisenstein à $XY^4 + Z^4Y + ZX^4 \in \mathbb{Q}[X, Z][Y]$ avec l'élément irréductible Z. Ce qui prouve l'irréductibilité du polynôme.

4. On pose $X = Y + 1$, le polynôme devient alors $Y^3 + 3Y^2 - 3 \in \mathbb{Z}[Y]$. Une application évident d'Eisenstein implique son irréductibilité.

Exercice 3 *Soit $z \in \mathbb{C}$ un nombre complexe.*

1. *Montrer que z est algébrique (sur $\mathbb{Q}$) si et seulement si son conjugué $\bar{z}$ l'est.*

2. *Montrer que z est algébrique si et seulement si sa partie réelle et sa partie imaginaire sont algébriques.*

Solution

1. Si z est zéro d'un polynôme $P(X) \in \mathbb{Q}[X]$, en appliquant la conjugaison complexe à l'égalité $P(z) = 0$, on obtient $P(\bar{z}) = 0$. Donc $\bar{z}$ est algébrique. Inversement si $\bar{z}$ est algébrique, alors $z = \bar{\bar{z}}$ est algébrique.

2. Si z est algébrique, sa partie réelle $(z + \bar{z})/2$ et sa partie imaginaire $(z - \bar{z})/2i$ sont algébriques par (1) (noter que $i = \sqrt{-1}$ est algébrique). Inversement si les parties réelle et imaginaire de z sont algébrique, alors z est algébrique puisqu'il s'exprime polynômialement en fonction de celles-ci et de i.

Exercice 4 *Soient $\sqrt{2}, \sqrt{3}, \sqrt{5} \in \mathbb{R}$ les racines carrées positives de $2, 3, 5$. Nous avons vu en TD que $K := \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ est une extension de $\mathbb{Q}$ de degré 4. Nous allons calculer le degré de $L := \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ sur $\mathbb{Q}$.*

1. *Montrer que 1 et $\sqrt{3}$ forment une base de K en tant que $\mathbb{Q}[\sqrt{2}]$-espace vectoriel.*
2. *Montrer qu'un nombre rationnel $r \in \mathbb{Q}$ est un carré dans $\mathbb{Q}[\sqrt{2}]$ si et seulement si r ou $2r$ est un carré dans $\mathbb{Q}$. En particulier, 5 et $5/3$ ne sont pas des carrés dans $\mathbb{Q}[\sqrt{2}]$.*
3. *En utilisant la question 4.1, montrer que 5 n'est pas un carré dans K.*
4. *Montrer que $[L : K] = 2$ et que $[L : \mathbb{Q}] = 8$.*

Solution

1. Puisque $K = \mathbb{Q}[\sqrt{2}][\sqrt{3}]$ et que $[K : \mathbb{Q}[\sqrt{2}]] = [K : \mathbb{Q}]/[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, $\sqrt{3}$ est de degré 2 sur $\mathbb{Q}[\sqrt{2}]$, donc $\{1, \sqrt{3}\}$ est une base de K sur $\mathbb{Q}[\sqrt{2}]$.

2. Supposons qur $r = (a+b\sqrt{2})^2$ avec $a, b \in \mathbb{Q}$. Alors $r = (a^2+2b^2)+2ab\sqrt{2}$, donc $r = a^2 + 2b^2$ et $ab = 0$. Si $b = 0$, alors $r = a^2$, sinon $a = 0$ et $2r = (2b)^2$.

Inversement si r est un carré dans $\mathbb{Q}$ c'est un carré dans K ; si $2r = q^2$ est un carré dans $\mathbb{Q}$, alors $r = ((q/2)\sqrt{2})^2$ est un carré dans K.

3. Si 5 est un carré dans K, il existe $\lambda_0, \lambda_1 \in \mathbb{Q}[\sqrt{2}]$ tels que $5 = (\lambda_0+\lambda_1\sqrt{3})^2$. Il suit que $(\lambda_0^2+3\lambda_1^2-5)+2\lambda_0\lambda_1\sqrt{3} = 0$. D'après (1), on a $\lambda_0\lambda_1 = 0$. Donc $\lambda_0 = 0$ ou $\lambda_1 =$ à, ce qui implique que $5/3$ ou 5 est un carré dans $\mathbb{Q}[\sqrt{2}]$, impossible d'après (2).

4. Comme $\sqrt{5}$ est de degré au plus 2 sur K, et qu'il n'appartient pas à K, on a $[L : K] = 2$. D'où $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}] = 8$.

Exercice 5 *Soit $\sqrt[3]{2} \in \mathbb{R}$ la racine cubique réelle de 2. Soit*

$$\alpha = \sqrt{3 + \sqrt[3]{2}} \in \mathbb{R}_{>0}$$

la racine carrée positive de $3 + \sqrt[3]{2}$. On souhaite trouver le polynôme minimal de α sur $\mathbb{Q}$.

1. *Trouver un polynôme unitaire $P(X) \in \mathbb{Q}[X]$ de degré 6 qui s'annule en α.*

2. *Soit* $K = \mathbb{Q}[\sqrt[3]{2}]$. *Montrer que* $[K : \mathbb{Q}] = 3$, *que* $K \subseteq \mathbb{Q}[\alpha]$ *et que l'extension* $\mathbb{Q}[\alpha]/K$ *est de degré* 1 *ou* 2. *En déduire que* $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ *ou* 6.

3. *On va montrer que* $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 6$. *Supposons* $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$.

   (a) *Montrer qu'il existe* $a_0, a_1, a_2 \in \mathbb{Q}$ *tels que*

   $$(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2)^2 = 3 + \sqrt[3]{2}.$$

   (b) *Montrer que l'on a les égalités suivantes*

   $$\begin{cases} a_1^2 + 2a_0a_2 &= 0 \quad (A) \\ 2a_2^2 + 2a_0a_1 &= 1 \quad (B) \\ a_0^2 + 4a_1a_2 &= 3 \quad (C) \end{cases}$$

   (c) *Montrer que* $a_0 \neq 0$, $a_1 \neq 0$ *et* $a_2 \neq 0$.

   (d) *Soit* $N \in \mathbb{N}^*$ *le plus petit dénominateur commun des* a_i. *Écrivons* $a_i = b_i/N$ *avec* $b_i \in \mathbb{Z}$ *non nuls et* $\text{pgcd}(b_0, b_1, b_2, N) = 1$. *Montrer en utilisant la relation* (B) *ci-dessus que* N *est pair.*

   (e) *Montrer que* b_1 *et* b_0 *sont pairs.*

   (f) *Montrer que* b_2 *est aussi pair. Conclure.*

4. *En déduire que le polynôme* $P(X)$ *de 5.1 ci-dessus est le polynôme minimal de* α *sur* $\mathbb{Q}$.

Solution

1. On a $(\alpha^2 - 3)^3 - 2 = 0$. Donc

$$P(X) := (X^2 - 3)^3 - 2 = X^6 - 9X^4 + 27X^2 - 29$$

convient.

2. Le polynôme $X^3 - 2 \in \mathbb{Q}[X]$ est irréductible par le critère d'Eisenstein (ou bien parce qu'il est de degré ≤ 3 et n'a pas de racine rationnelle). Donc c'est le polynôme minimal de $\sqrt[3]{2}$ sur $\mathbb{Q}$ et $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$. On a $\sqrt[3]{2} = \alpha^2 - 3 \in \mathbb{Q}[\alpha]$, donc $K = \mathbb{Q}[\sqrt[3]{2}] \subseteq \mathbb{Q}[\alpha]$. Comme $\alpha^2 \in K$, $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt[3]{2}, \alpha] = K[\alpha]$ est de degré 1 ou 2 sur K.

3(a) L'hypothèse $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 3$ implique par (2) que $\mathbb{Q}[\alpha] = K$. On sait par le cours que $1, \sqrt[3]{2}, \sqrt[3]{2}^2$ est une base de K sur $\mathbb{Q}$. Donc il existe $a_0, a_1, a_2 \in \mathbb{Q}$ tels que $\alpha = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2$. On a alors l'égalité

$$(a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2)^2 = 3 + \sqrt[3]{2}.$$

3(b) En développant l'égalité ci-dessus et on identifiant les coefficients rationnels dans la base $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$, on obtient les relations (A), (B), (C).

3(c) Si $a_0 = 0$, (A) implique que $a_1 = 0$ et (B) implique que $a_2 = 0$. C'est incompatible avec (C).Si $a_1 = 0$, (B) implique que $1/2$ est un carré dans $\mathbb{Q}$, impossible. Si $a_2 = 0$, (C) impique que 3 est un carré dans $\mathbb{Q}$, impossible.

3(d) En remplaçant a_i par b_i/N, les égalités de (b) deviennent

$$\begin{cases} b_1^2 + 2b_0b_2 &= 0 & (A') \\ 2b_2^2 + 2b_0b_1 &= N^2 & (B') \\ b_0^2 + 4b_1b_2 &= 3N^2 & (C') \end{cases}$$

Donc (B') implique que N est pair.

3(e) Par (A') on a b_1 pair. Par (C') et 3(d), on a b_0 pair.

3(f) Il suit de 3(e) que $4 \mid b_0b_1$. Par 3(d) et (B') on trouve b_2 pair. Donc $\mathrm{pgcd}(b_0, b_1, b_2, N)$ est divisible par 2, contradiction.

Exercice 6 *Soit $p > 2$ un nombre premier impair. On souhaite trouver une condition nécessaire et suffisante pour que 2 soit un carré modulo p (c'est-à-dire qu'il existe $x \in \mathbb{F}_p$ tel que $2 = x^2$).*

On fixe une clôture algébrique $\bar{\mathbb{F}}_p$ de $\mathbb{F}_p$ et on note $\alpha \in \bar{\mathbb{F}}_p$ une racine du polynôme $X^4 + 1 \in \mathbb{F}_p[X]$ (ce dernier n'est pas nécessairement irréductible sur $\mathbb{F}_p$).

1. *Montrer que $\alpha \neq 0$ et que $(\alpha + \alpha^{-1})^2 = 2$.*
2. *Montrer que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $\alpha + \alpha^{-1} \in \mathbb{F}_p$.*
3. *Montrer que l'on peut écrire $p = 8q + r$ avec $q \in \mathbb{Z}$ et $r \in \{1, -1, 3, -3\}$.*
4. *Montrer que $\alpha^p + \alpha^{-p} = \alpha^r + \alpha^{-r}$.*
5. *Montrer que $\alpha^3 + \alpha^{-3} \neq \alpha + \alpha^{-1}$.*
6. *En déduire que $\alpha^p + \alpha^{-p} = \alpha + \alpha^{-1}$ si et seulement si $r = \pm 1$.*
7. *Montrer que 2 est un carré modulo p si et seulement si $p \equiv \pm 1 \bmod 8$.*

Solution

1. On a $\alpha^4 + 1 = 0$, donc $\alpha \neq 0$ et on a $\alpha^2 = -\alpha^{-2}$. Il suit que $(\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2 = 2$.

2. Si 2 est le carré d'un élément $x \in \mathbb{F}_p$, alors $\alpha + \alpha^{-1} = \pm x \in \mathbb{F}_p$. La réciproque est triviale.

3. On effectue la division euclidien usuelle $p = 8q' + r$ avec $0 \leq r \leq 7$. Comme p est impair, on a $r \in \{1, 3, 5, 7\}$. Si $r = 5$, on a $p = 8(q' + 1) - 3$; si $r = 7$, on a $p = 8(q' + 1) - 1$.

4. Comme $\alpha^4 = -1$, on a $\alpha^8 = 1$, donc $\alpha^p = (\alpha^8)^q\alpha^r = \alpha^r$. Cela implique que $\alpha^{-p} = \alpha^{-r}$.

5. On a $\alpha^3 + \alpha^{-3} = (-\alpha^{-1}) + (-\alpha) = -(\alpha + \alpha^{-1}) \neq \alpha + \alpha^{-1}$ car $\alpha + \alpha^{-1} \neq 0$ et $2 \in \mathbb{F}_p^*$.

6. Cela découle de 6.4 et de 6.5.

7. On sait par le cours qu'un élément de $x \in \bar{\mathbb{F}}_p$ appartient à $\mathbb{F}_p$ si et seulement si $x^p = x$. Donc par 6.2, 2 est un carré modulo p si et seulement si $\alpha^p + \alpha^{-p} = (\alpha + \alpha^{-1})^p = \alpha + \alpha^{-1}$. On conclut par 6.6.