Université Bordeaux 1
UFR Mathématiques et Informatique 19 décembre 2007

Licence de Mathématiques

MHT511, Algèbre 4

Durée 3 heures. Documents interdits.

Exercice 1 (*Irréductibilité de polynômes*) Déterminer si les polynômes suivants sont irréductibles dans les anneaux indiqués :

1. $X^5Y + Y^5Z + Z^5X$ dans $\mathbb{Q}[X, Y, Z]$;
2. $X^3 + 3X + 2$ dans $\mathbb{F}_5[X]$;
3. $X^4 + X^3 + X^2 + X + 1$ dans $\mathbb{Z}[X]$.

Solution: (1) On applique le critère d'Eisenstein avec $A = \mathbb{Q}[Y, Z]$ et l'élément irréductible $f = Z$ de A. On en déduit que $X^5Y + Y^5Z + Z^5X$, qui est de contenu 1, est irréductible dans $\mathbb{Q}[X, Y, Z]$ (Cours, théorème 4.2.13).

(2) Ce polynôme n'a pas de zéro dans $\mathbb{F}_5$ (on calcule ses valeurs en tous les éléments de $\mathbb{F}_5$. Par exemple, en $x = 2 \bmod 5$, on trouve la classe mod 5 de $2^3 + 3 \times 2 + 2 \equiv 1[5]$). Comme il est de degré 3, il est irréductible dans $\mathbb{F}_5[X]$ (Proposition 4.2.11).

(3) C'est le polynôme cyclotomique $\Phi_5(X)$ (exemple 4.2.19). Il est donc irréductible dans $\mathbb{Z}[X]$ (Théorème 4.2.20)

Exercice 2 (*Valeurs spéciales des polynômes cyclotomiques*) Soit $n \geq 2$ un entier naturel. On note $\Phi_n(X) \in \mathbb{Z}[X]$ le polynôme cyclotomique qui s'annule sur les racines n-ièmes de l'unité dans $\mathbb{C}$.

1. Rappeler l'expression de $\Phi_{p^r m}(X)$ lorsque p est un nombre premier ne divisant pas m et r est un entier naturel.
2. Supposons que n a au moins deux facteurs premiers. Montrer que $\Phi_n(0)$ et $\Phi_n(1)$ valent 1. Montrer également que $\Phi_{p^r}(0) = 1$ si $r \geq 1$ et p premier.
3. Supposons que n est le produit de k nombres premiers deux à deux distincts. Montrer que $\Phi'_n(0) = (-1)^{k-1}$. Dans le cas contraire (donc si n a un facteur carré), montrer que $\Phi'_n(0) = 0$.

Solution: (1) On a

$$\Phi_{p^r m}(X) = \frac{\Phi_m(X^{p^r})}{\Phi_m(X^{p^{r-1}})}$$

si p ne divise pas m (Proposition 5.2.18).

(2) Soit p un premier divisant n. Alors $n = p^r m$ avec p ne divisant pas m et $m \geq 2$. Il suit que $\Phi_m(0), \Phi_m(1) \neq 0$ (car $0, 1$ ne sont pas des racines primitives m-ièmes de l'unité si $m \geq 2$). En remplaçant dans la formule ci-dessus X par 0 ou 1, on voit que $\Phi_n(a) = \Phi_{p^r m}(a) = 1$ si $a = 0$ ou 1.

Notons que si n n'a qu'un diviseur premier p, alors $n = p^r$. On a vu en cours (exemple 4.2.19) l'expression explicite de $\Phi_{p^r}(X)$ qui donne

$$\Phi_{p^r}(0) = 1, \quad \Phi_{p^r}(1) = p.$$

En fin, $\Phi_1(X) = X - 1$, donc $\Phi_1(0) = -1$ et $\Phi_1(1) = 0$.

(3) On a $n = p_1 p_2 ... p_k$ avec les p_i premiers et deux à deux distincts. On écrit $n = p_k m$ avec $m = p_1 ... p_{k-1}$. Si $k = 1$, alors

$$\Phi_n(X) = X^{p_1 - 1} + ... + X + 1,$$

donc $\Phi'_n(0) = 1$. Supposons $k \geq 2$. La formule rappelée dans (1) implique que

$$\Phi_n(X) = \frac{\Phi_m(X^{p_k})}{\Phi_m(X)}.$$

En dérivant, on obtient

$$\Phi'_n(0) = \frac{-\Phi_m(0)\Phi'_m(0)}{\Phi_m(0)^2} = -\Phi'_m(0)$$

car la dérivée de $\Phi_m(X^{p_k})$ s'annule en 0. Une récurrence immédiate sur k donne $\Phi'_n(0) = (-1)^{k-1}$.

Supposons maintenant que n a un facteur carré d^2. Alors $n = p^r m$ pour un certain premier p (diviseur de d) avec $r \geq 2$ et p ne divise pas m. On dérive de nouveau l'expression donnée en (1) et on voit que $\Phi'_n(0) = 0$.

Exercice 3 (*Extensions quadratiques*) Soit K un corps de caractéristique $\neq 2$.

1. Soit F/K une extension quadratique (c'est-à-dire que $[F : K] = 2$). Montrer qu'il existe $\alpha \in F^*$, $\alpha \notin K$, tel que $\alpha^2 \in K$ et que $F = K[\alpha]$. Montrer que $\{1, \alpha\}$ est une base de F en tant que K-espace vectoriel.
2. Montrer que $\beta \in F$ satisfait les propriétés de α ci-dessus si et seulement si $\beta = b\alpha$ pour un certain $b \in K^*$.
3. Prenons $K = \mathbb{F}_p$ un corps premier à $p \geq 3$ éléments. Soit $\bar{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$. Soient $\alpha, \beta \in \bar{\mathbb{F}}_p^*$ avec $\alpha, \beta \notin \mathbb{F}_p$ et $\alpha^2, \beta^2 \in \mathbb{F}_p$. Montrer que $\alpha/\beta \in \mathbb{F}_p$.

Solution: (1) Soit $\gamma \in F \setminus K$. Alors $\{1, \gamma\}$ est une famille libre sur K, de cardinal $2 = \dim_K F$, c'est donc une base. Par suite

$$F = K + K\gamma \subseteq K[\gamma] \subseteq F.$$

Donc $F = K[\gamma]$. Le polynôme minimal de γ sur K est de degré $[K[\gamma] : K] = 2$. On a donc une relation

$$\gamma^2 + a\gamma + b = 0$$

pour certains $a, b \in K$. Comme K est de caractéristique différente de 2, on peut écrire la relation comme suit

$$\left(\gamma + \frac{a}{2}\right)^2 + \left(b - \frac{a^2}{4}\right) = 0.$$

Si on pose $\alpha = \gamma + \frac{a}{2}$, on a bien $\alpha^2 \in K$, $\alpha \notin K$. Le même raisonnement que ci-dessus montre que $\{1, \alpha\}$ est une base de F sur K et que $F = K[\alpha]$.

(2) On a $\beta = a + b\alpha$ pour certains $a, b \in K$. Donc

$$(a^2 + b^2\alpha^2) + 2ab\alpha = \beta^2 \in K$$

avec $a^2 + b^2\alpha^2 \in K$. Comme $\{1, \alpha\}$ est libre sur K, on a $2ab = 0$. Mais $b \in K^*$ car sinon $\beta \in K$, et 2 est inversible dans K puisque K est de caractéristique différente de 2, donc $a = 0$ et $\beta = b\alpha$.

(3) Les corps $\mathbb{F}_p[\alpha]$ et $\mathbb{F}_p[\beta]$ sont des sous-extensions de $\bar{\mathbb{F}}_p$ de même degré ($= 2$) sur $\mathbb{F}_p$, elles sont donc égales (théorème 5.4.2(a)). Par (2), on a $\alpha/\beta \in \mathbb{F}_p$ (prendre $K = \mathbb{F}_p$ et $F = \mathbb{F}_p[\alpha] = \mathbb{F}_p[\beta]$).

Exercice 4 (*Sous-extensions quadratiques*) Soit K un corps de caractéristique $\neq 2$. Soit L/K une extension. Notons

$$R = \{\alpha \in L^* \mid \alpha^2 \in K, \alpha \notin K\}.$$

Soient $\alpha_1, ..., \alpha_n \in R$ tels que pour tout $k \leq n$, on ait $\alpha_k \notin K[\alpha_1, ..., \alpha_{k-1}]$.

1. Montrer que pour tout $k \leq n$, on a $[K[\alpha_1, ..., \alpha_k] : K[\alpha_1, ..., \alpha_{k-1}]] = 2$ et
$$[K[\alpha_1, ..., \alpha_k] : K] = 2^k$$
2. Soit $I = \{k_1, ..., k_s\}$ une partie de $\{1, ..., n\}$ à s éléments. Montrer que
$$\alpha_I := \alpha_{k_1} \cdots \alpha_{k_s} \in R.$$
3. Soit $k \leq n$ et soit $\alpha \in K[\alpha_1, ..., \alpha_k] \cap R$. En écrivant $\alpha = \lambda\alpha_k + \mu$ avec $\lambda, \mu \in K[\alpha_1, ..., \alpha_{k-1}]$, montrer que $\lambda\mu = 0$.
   (a) Si $\mu = 0$, montrer que $\lambda \in K^*$ ou $\lambda \in K[\alpha_1, ..., \alpha_{k-1}] \cap R$.
   (b) Si $\lambda = 0$, montrer que $\alpha \in K[\alpha_1, ..., \alpha_{k-1}] \cap R$.

   En déduire par récurrence sur k qu'il existe $b \in K^*$ et I une partie de $\{1, 2, ..., n\}$ telle que $\alpha = b\alpha_I$.
4. Calculer les degrés sur $\mathbb{Q}$ des sous-extensions
$$\mathbb{Q}[\sqrt{2}, \sqrt{3}], \quad \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}], \quad \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}]$$
   de $\mathbb{R}$.
5. Montrer que $K[\alpha_1, ..., \alpha_n]$ admet exactement $2^n - 1$ sous-K-extensions quadratiques qui sont les $K[\alpha_I]$, I parcourant les parties non-vides de $\{1, ..., n\}$. En déduire que si L/K est finie, alors L n'a qu'un nombre fini de sous-extensions quadratiques, ce nombre étant majoré par $[L : K] - 1$.

Solution: Notons $F_k = K[\alpha_1, ..., \alpha_k]$.

(1) On a $F_k = F_{k-1}[\alpha_k]$. Le polynôme minimal de α_k sur F_{k-1} est de degré au plus 2 car il divise

$$X^2 - \alpha_k^2 \in K[X] \subseteq F_{k-1}[X],$$

et au moins 2 puisque $\alpha_k \notin F_{k-1}$. Donc ce polynôme minimal est de degré 2, il suit que $[F_k : F_{k-1}] = 2$. Ce qui donne

$$[F_k : K] = [F_k : F_{k-1}][F_{k-1} : F_{k-2}]...[F_1 : F] = 2^k.$$

(2) On peut supposer que $k_s > k_j$ pour tout $j < s$. Il est clair que $\alpha_I^2 \in K$ et $\alpha_I \in L^*$. Si $\alpha_I \in K$, alors

$$\alpha_{k_s} = \alpha_I(\alpha_{k_1}...\alpha_{k_{s-1}})^{-1} \in F_{k_s-1},$$

ce qui est contraire à l'hypothèse.

(3) On sait que $\{1, \alpha_k\}$ est une base de F_k sur F_{k-1}, donc on peut bien écrire

$$\alpha = \lambda\alpha_k + \mu, \quad \lambda, \mu \in F_{k-1}.$$

On a

$$(\lambda^2\alpha_k^2 + \mu^2) + 2\lambda\mu\alpha_k = \alpha^2 \in K \subseteq F_{k-1}.$$

Donc comme dans l'exercice 3.2 ci-dessus, on conclut que $\lambda\mu = 0$.

(3.a) Si $\mu = 0$, alors $\alpha = \lambda\alpha_k$ et $\lambda \neq 0$. Cela implique que $\lambda^2 \in K$. Alors ou bien $\lambda \in K^*$, ou bien $\lambda \notin K$, auquel cas on a $\lambda \in R \cap F_{k-1}$ par définition de R.

(3.b) Si $\lambda = 0$, alors $\alpha \in F_{k-1}$, donc $\alpha \in F_{k-1} \cap R$.

Si $k = 1$, on a $\alpha = b\alpha_I$ avec $I = \{1\}$ et pour un certain $b \in K^*$ (exercice 3.2). Supposons la propriété vraie en $k-1$. Dans le cas (a), on a ou bien $\lambda \in K^*$, alors $\alpha = \lambda\alpha_I$ avec $I = \{k\}$; ou bien $\lambda \in R \cap F_{k-1}$. Dans ce dernier cas, par hypothèse de récurrence, il existe une partie J de $\{1, ..., k-1\}$ telle que $\lambda = b\alpha_J$ avec un $b \in K^*$. Il suit que $\alpha = b\alpha_{J\cup\{k\}}$.

Dans le cas (b), on applique directement l'hypothèse de récurrence. On conclut donc que α est toujours de la forme désirée.

(4) On va appliquer (1) avec $K = \mathbb{Q}$, $L = \mathbb{R}$ et $\alpha_1 = \sqrt{2}, \alpha_2 = \sqrt{3}, \alpha_3 = \sqrt{5}$ et $\alpha_4 = \sqrt{7}$. Le point essentiel est de vérifier la propriété que $\alpha_k \notin \mathbb{Q}[\alpha_1, ..., \alpha_{k-1}]$ pour tout $k \leq 4$.

Une remarque préliminaire. Soit p un nombre premier. On note que si $\sqrt{p} = b\sqrt{n}$ pour certains $b \in \mathbb{Q}^*$ et n entier naturel, alors p divise n. En effet, on a $p = b^2n$. On écrit $b = t/s$ avec t, s entiers naturels premiers entre eux. Donc $s^2p = t^2n$. Si p ne divise pas n, alors p divise t, donc $t = pt_1$ et $s^2 = pt_1n$. Ce qui implique que p divise aussi s. Contradiction avec l'hypothèse t, s premiers entre eux.

On a $\alpha_1 = \sqrt{2} \in R$. Comme $\sqrt{3} \notin \mathbb{Q}^*\sqrt{2}$, on a $\alpha_2 := \sqrt{3} \notin \mathbb{Q}[\alpha_1]$. Les éléments de $R \cap \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ sont des multiples par un élément de $\mathbb{Q}^*$ de $\sqrt{2}, \sqrt{3}$ ou de $\sqrt{6}$. Comme $\sqrt{5}$ n'est pas de cette forme, on voit que $\alpha_3 := \sqrt{5} \notin \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. De la même façon, les éléments de $R \cap \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$ sont des multiples rationnels de $\sqrt{n}$ avec n divisible uniquement par $2, 3$ ou 5. On en déduit que

$\alpha_4 := \sqrt{7} \notin \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{5}]$. On conclut que les extensions de l'énoncé sont de degrés respectifs $4, 8$ et 16 sur $\mathbb{Q}$.

(5) D'après l'exercice 3.1 et (3), les sous-extensions quadratiques de L/K sont de la forme $K[\alpha_I]$ (noter que $K[b\alpha_I] = K[\alpha_I]$ pour tout $b \in K^*$). De plus, si $K[\alpha_I] = K[\alpha_J]$, alors $I = J$. En effet, sinon, on peut supposer qu'il existe $k \in I$ qui est strictement supérieur à tout élément de J et tout élément de I différent de k. Comme on a $\alpha_I = b\alpha_J$ avec un $b \in K^*$, on obtient $\alpha_k \in K[\alpha_1, ..., \alpha_{k-1}]$. Contradiction. Il y a donc autant des sous-extensions quadratiques de L/K que de parties non-vides I de $\{1, ..., n\}$. Or il y a exactement $2^n - 1$ parties de cette forme.

Enfin, supposons L/K finie de degré $d = [L : K]$. Soient $A = \{\alpha_1, ..., \alpha_n\}$ un sous-ensemble de R vérifiant $\alpha_k \notin K[\alpha_1, ..., \alpha_{k-1}]$ pour tout $k \leq n$. D'après (1), $2^n \leq d$. On peut prendre un A de cardinalité maximale. Toute sous-extension quadratique F de L/K est engendrée par un $\alpha \in R$. Par maximalité de A, on a $\alpha \in K[\alpha_1, ..., \alpha_n]$. Il suit de la forme $F = K[\alpha_I]$ pour une partie non-vide I de $\{1, ..., n\}$. Par conséquent, il y a au plus $2^n - 1 \leq d - 1$ sous-extensions quadratiques de L/K.