

## Correction des exercices - Chapitre V

### Exercice 1

On vérifie que l'on a dans  $(\mathbb{Z}/2\mathbb{Z})[X]$  l'égalité

$$X^3 + X^2 + 1 = X(X^2 + X + 1) + (X + 1).$$

Le quotient est donc  $X$  et le reste est  $X + 1$ .

### Exercice 2

En utilisant l'algorithme d'Euclide, on obtient le tableau suivant :

	1	$-\frac{1}{2} + \frac{X}{6}$	$\frac{9X}{4}$	$\frac{4X}{3}$	
$(X + 1)^3$	$(X - 1)^3$	$6X^2 + 2$	$\frac{8X}{3}$	2	0
1	0	1	$\frac{1}{2} - \frac{X}{6}$	$\frac{3}{8}X^2 - \frac{9}{8}X + 1$	
0	1	-1	$\frac{1}{2} + \frac{X}{6}$	$-\frac{3}{8}X^2 - \frac{9}{8}X - 1$	

On en déduit la relation de Bézout

$$\left(\frac{3}{8}X^2 - \frac{9}{8}X + 1\right)(X + 1)^3 - \left(\frac{3}{8}X^2 + \frac{9}{8}X + 1\right)(X - 1)^3 = 2.$$

### Exercice 3

Le polynôme  $X^2 + X + 1$  est irréductible dans  $(\mathbb{Z}/2\mathbb{Z})[X]$ , car il est de degré 2 et n'a pas de racines dans  $\mathbb{Z}/2\mathbb{Z}$ . C'est le seul, car les autres polynômes de degré 2 dans  $(\mathbb{Z}/2\mathbb{Z})[X]$  sont  $X^2$ ,  $X^2 + X$  et  $X^2 + 1$  et ils ont une racine dans  $\mathbb{Z}/2\mathbb{Z}$ .

### Exercice 4

Pour tout corps commutatif  $K$ , on a l'égalité dans  $K[X]$ ,

$$(1) \quad X^4 + 1 = (X^2 + 1)^2 - 2X^2.$$

Dans  $\mathbb{R}[X]$ , on a donc

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1).$$

Les polynômes  $X^2 - \sqrt{2}X + 1$  et  $X^2 + \sqrt{2}X + 1$  sont irréductibles sur  $\mathbb{R}$  car leur discriminant, qui vaut  $-2$ , est négatif. C'est donc la décomposition cherchée dans  $\mathbb{R}[X]$ . On en déduit celle dans  $\mathbb{C}[X]$

$$X^4 + 1 = \left(X - \frac{1+i}{\sqrt{2}}\right) \left(X - \frac{1-i}{\sqrt{2}}\right) \left(X - \frac{-1+i}{\sqrt{2}}\right) \left(X + \frac{1+i}{\sqrt{2}}\right).$$

Par ailleurs, on a dans  $(\mathbb{Z}/2\mathbb{Z})[X]$  l'égalité  $X^2 + 1 = (X + 1)^2$ . D'après (1), on obtient ainsi la décomposition

$$X^4 + 1 = (X + 1)^4.$$

Dans  $(\mathbb{Z}/3\mathbb{Z})[X]$ , on a les égalités

$$X^4 + 1 = (X^2 - 1)^2 + 2X^2 = (X^2 - 1)^2 - X^2 = (X^2 - X - 1)(X^2 + X - 1).$$

Les polynômes  $X^2 - X - 1$  et  $X^2 + X - 1$  sont irréductibles dans  $(\mathbb{Z}/3\mathbb{Z})[X]$  car ils sont de degré 2 et sans racines dans  $\mathbb{Z}/3\mathbb{Z}$ , d'où la décomposition cherchée.

### Exercice 5

Soit  $f \in \mathbb{Q}[X]$  un polynôme irréductible sur  $\mathbb{Q}$ . L'hypothèse faite sur  $f$  entraîne que  $f$  est premier avec son polynôme dérivé  $f'$  dans  $\mathbb{Q}[X]$ . Il existe donc  $U$  et  $V$  dans  $\mathbb{Q}[X]$  tels que l'on ait  $Uf + Vf' = 1$  (égalité de Bézout). Par suite,  $f$  et  $f'$  sont aussi premiers entre eux dans  $\mathbb{C}[X]$ , donc toutes les racines de  $f$  dans  $\mathbb{C}$  sont simples.

### Exercice 6

Soit  $f \in \mathbb{R}[X]$  un polynôme irréductible sur  $\mathbb{R}$  de degré au moins égal à 2. Il possède une racine  $a$  dans  $\mathbb{C} \setminus \mathbb{R}$ . Le nombre complexe conjugué  $\bar{a}$  est aussi une racine de  $f$ , car  $f$  est à coefficients réels. On a  $a \neq \bar{a}$ . Il en résulte que  $(X - a)(X - \bar{a})$  divise  $f$ . Par ailleurs, on a

$$(X - a)(X - \bar{a}) = X^2 - (a + \bar{a})X + |a|^2 \in \mathbb{R}[X].$$

Parce que  $f$  est irréductible, ce polynôme de degré 2 est associé à  $f$ , autrement dit il existe  $\lambda \in \mathbb{R}$  tel que l'on ait

$$f = \lambda(X^2 - (a + \bar{a})X + |a|^2).$$

Ainsi,  $f$  est un polynôme de degré 2, ayant un discriminant négatif vu qu'il n'a pas de racines réelles. Inversement, les polynômes de  $\mathbb{R}[X]$  ayant cette propriété, ou ceux de degré 1, sont irréductibles sur  $\mathbb{R}$ , d'où le résultat.

### Exercice 7

- 1) Un polynôme unitaire de degré 2 dans  $(\mathbb{Z}/p\mathbb{Z})[X]$  est la forme  $X^2 + aX + b$ , avec  $a, b \in \mathbb{Z}/p\mathbb{Z}$ . Il y en a donc  $p^2$ .

- 2) Les polynômes réductibles sur  $\mathbb{Z}/p\mathbb{Z}$  sont de la forme  $(X - a)(X - b)$ , avec  $a$  et  $b$  dans  $\mathbb{Z}/p\mathbb{Z}$ . Il y en a  $p$  pour lesquels  $a = b$  et  $p(p - 1)/2$  pour lesquels  $a \neq b$ . On en déduit qu'il existe

$$p^2 - p - \frac{p(p - 1)}{2} = \frac{p(p - 1)}{2}$$

polynômes irréductibles unitaires de degré 2 dans  $(\mathbb{Z}/p\mathbb{Z})[X]$ .

### Exercice 8

- 1) Si on a  $n \geq 2$ , la multiplicité de la racine  $a$  de  $f$  est au moins 2, donc le plus grand diviseur commun de  $f$  et de son polynôme dérivé est de degré  $\geq 1$ . En particulier,  $f$  est réductible sur  $\mathbb{Q}$ .
- 2) L'assertion est vérifiée si on a  $n \leq 1$ . Supposons  $n \geq 2$  et le résultat vrai pour tous les polynômes de degré au plus  $n - 1$ . D'après la question 1, Il existe  $P$  et  $Q$  dans  $\mathbb{Q}[X]$ , de degré au plus  $n - 1$ , tels que  $f = PQ$ . Notons  $\nu_f(a)$ ,  $\nu_P(a)$  et  $\nu_Q(a)$  les multiplicités de  $a$  dans  $f$ ,  $P$  et  $Q$ . On a  $\nu_f(a) = \nu_P(a) + \nu_Q(a)$  et par hypothèse on a  $\nu_f(a) > n/2$ . L'égalité  $n = \deg(P) + \deg(Q)$  entraîne ainsi  $\nu_P(a) > \deg(P)/2$  ou bien  $\nu_Q(a) > \deg(Q)/2$ . L'hypothèse de récurrence entraîne alors le résultat.

### Exercice 9

- 1) Supposons  $f$  réductible sur  $K$ . Il existe  $g \in K[X]$ , unitaire non constant de degré  $k < p$ , qui divise  $f$ . Soit  $c$  le terme constant de  $g$ . Soit  $u$  une racine de  $f$  dans  $\mathbb{C}$ . Les racines de  $f$  dans  $\mathbb{C}$  sont les  $\zeta u$ , où  $\zeta$  parcourt l'ensemble des racines  $p$ -ièmes de l'unité de  $\mathbb{C}^*$ . L'élément  $\pm c$  est le produit de  $k$  de ces racines, d'où

$$\pm c = \eta u^k \quad \text{avec} \quad \eta^p = 1.$$

Parce que l'on a  $1 \leq k < p$ , il existe des entiers  $r$  et  $s$  tels que l'on ait  $rk + sp = 1$  (égalité de Bézout). On a ainsi

$$u = u^{rk} u^{sp} = \pm \left( \frac{c}{\eta} \right)^r a^s.$$

Par suite,  $u\eta^r$  appartient à  $K$ , donc  $u^p$  est dans  $K^p$  i.e.  $a$  est dans  $K^p$ , d'où le résultat.

- 2) On a l'égalité  $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ .

### Exercice 10

- 1) Soit  $\alpha$  la classe de  $X$  modulo l'idéal  $(f)$ . Le système  $(1, \alpha)$  est une base du  $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel  $A$  (th. 5.9). Tout élément de  $A$  s'écrit donc de manière unique sous la forme  $a + b\alpha$ , avec  $a, b \in \mathbb{Z}/2\mathbb{Z}$ . Il en résulte que  $A$  est fini de cardinal 4.

2) Le groupe des éléments inversibles de  $A$  est (th. 5.10)

$$\left\{1 + (X^2), 1 + X + (X^2)\right\}.$$

3) L'anneau  $A$  n'est pas intègre, car on a  $\alpha^2 = 0$  et  $\alpha$  n'est pas nul.

### Exercice 11

- 1) Le polynôme  $X^3 - X + 1$  n'a pas de racines dans  $\mathbb{Q}$  (cf. le lemme 5.6) et il est de degré 3. Il est donc irréductible sur  $\mathbb{Q}$ . Ainsi  $K$  est un corps (cor. 5.5).
- 2) On considère l'application  $\mathbb{Q}$ -linéaire  $\varphi : K \rightarrow K$  telle que  $\varphi(x) = ax$ . C'est un isomorphisme. La matrice de  $\varphi$  dans la base  $(1, \alpha, \alpha^2)$  est

$$M = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

On vérifie que l'on a

$$M^{-1} = \begin{pmatrix} 0 & 1 & -1 \\ 1 & -1 & 2 \\ -1 & 1 & -1 \end{pmatrix}.$$

On a

$$M^{-1} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix},$$

donc l'inverse de  $a$  est  $\alpha - \alpha^2$ .

3) En utilisant l'algorithme d'Euclide on obtient la relation de Bezout

$$(X - 1)(X^3 - X + 1) + (2 - X^2)(X^2 - X + 1) = 1.$$

On en déduit l'égalité  $(2 - \alpha^2)a = 1$ . L'inverse de  $a$  est donc  $2 - \alpha^2$ .

### Exercice 12

1) On a l'égalité

$$f = (1 + X + X^2)^2$$

et le polynôme  $1 + X + X^2$  est irréductible sur  $\mathbb{Z}/2\mathbb{Z}$ .

- 2) En notant  $\alpha$  la classe de  $X$  modulo  $(f)$ , le système  $(1, \alpha, \alpha^2, \alpha^3)$  est une base du  $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel  $A$ . Il en résulte que  $A$  est fini de cardinal 16 (cf. l'exercice 10).
- 3) L'anneau  $A$  n'est pas intègre car  $f$  est réductible (cor. 5.5).
- 4) L'élément  $\xi = 1 + \alpha + \alpha^2$  convient (question 1).

- 5) Les éléments non inversibles de  $A$  sont les classes modulo  $(f)$  des polynômes de  $(\mathbb{Z}/2\mathbb{Z})[X]$ , de degré  $\leq 3$ , qui ne sont pas premiers avec  $f$  (th. 5.10). Compte tenu de la première question, ce sont donc les classes modulo  $(f)$  des polynômes

$$0, \quad 1 + X + X^2, \quad X(1 + X + X^2), \quad (X + 1)(1 + X + X^2).$$

On en déduit que l'ensemble cherché est

$$\{0, 1 + \alpha + \alpha^2, \alpha + \alpha^2 + \alpha^3, 1 + \alpha^3\}.$$

- 6) Parce que  $A$  est de cardinal 16, le groupe  $A^*$  est donc d'ordre 12.  
 7) L'égalité  $\alpha^4 = \alpha^2 + 1$  entraîne  $\alpha^6 = 1$ . On a  $\alpha^2 \neq 1$  et  $\alpha^3 \neq 1$ . Il résulte que  $\alpha$  est d'ordre 6 dans  $A^*$ . Par ailleurs, on a (2 est nul dans  $A$ )

$$(\alpha + \alpha^2)^2 = \alpha^2 + \alpha^4 = 1,$$

donc  $\alpha + \alpha^2$  est d'ordre 2.

- 8) Le sous-groupe de  $A^*$  engendré par  $\alpha$  est

$$H = \{1, \alpha, \alpha^2, \alpha^3, 1 + \alpha^2, \alpha + \alpha^3\}.$$

En particulier,  $\alpha + \alpha^2$  n'est pas dans  $H$ . Par ailleurs, les éléments de la forme  $\alpha^i(\alpha + \alpha^2)^j$  pour  $0 \leq i \leq 5$  et  $0 \leq j \leq 1$ , sont dans  $A^*$ . Ils sont distincts deux à deux. En effet, si l'on a  $\alpha^i(\alpha + \alpha^2)^j = \alpha^{i'}(\alpha + \alpha^2)^{j'}$ , on obtient

$$(\alpha + \alpha^2)^{j-j'} = \alpha^{i'-i} \in H,$$

d'où  $j = j'$ , puis  $i = i'$  car  $\alpha$  est d'ordre 6. Il y a donc douze tels éléments, d'où l'assertion vu que  $A^*$  est d'ordre 12.

- 9) L'application  $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \rightarrow A^*$  qui à  $(i + 6\mathbb{Z}, j + 2\mathbb{Z})$  associe  $\alpha^i(\alpha + \alpha^2)^j$  est bien définie car  $\alpha$  est d'ordre 6 et  $\alpha + \alpha^2$  est d'ordre 2. C'est un homomorphisme de groupes. Il est surjectif (question 8). Les groupes  $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  et  $A^*$  étant de même ordre, c'est donc un isomorphisme.

### Exercice 13

- 1) Si  $f$  a une racine  $n \in \mathbb{Z}$ , on a  $f(n) = 0$ , donc tous les nombres premiers divisent  $f(n)$ .
- 2) Parce que  $f$  est distinct de  $\pm 1$ , les polynômes  $f - 1$  et  $f + 1$  n'ont qu'un nombre fini de racines. Il existe donc  $n \in \mathbb{Z}$  tel que  $f(n)$  soit distinct de  $\pm 1$ . L'entier  $f(n)$  est divisible par un nombre premier qui, par définition, est dans  $P(f)$ .
- 3) C'est une conséquence de la première question et de l'hypothèse faite sur  $P(f)$ .

4) Posons  $f = c + a_1X + \cdots + a_nX^n$ . On a

$$f(rcX) = c + \sum_{i=1}^n a_i(rcX)^i = c \left( 1 + \sum_{i=1}^n a_i c^{i-1} r^i X^i \right),$$

de sorte que pour tout  $i = 1, \dots, n$ , l'entier  $b_i = a_i c^{i-1} r^i$  convient.

5) Posons  $g = 1 + b_1X + \cdots + b_nX^n$ . Puisque  $c$  est non nul, on a  $b_n \neq 0$ , donc  $g$  est de degré  $n$ , et en particulier on a  $g \neq \pm 1$ . D'après la question 2, il existe un nombre premier  $p$  qui divise  $g$ . C'est aussi un diviseur premier de  $f$  (question 4). Par suite,  $p$  divise  $r$ . Les entiers  $b_i$  sont donc divisibles par  $p$ . Cela entraîne que  $p$  divise 1, d'où une contradiction et le résultat.

---