

## Correction du premier devoir

### Exercice 1

1) Supposons que  $K$  soit un corps fini. Dans ce cas,  $L/K$  étant une extension finie,  $L$  est aussi un corps fini et l'ensemble de ses sous-corps qui contiennent  $K$  est fini. Par ailleurs, le groupe multiplicatif  $L^*$  est cyclique (cf. le cours). Si  $\alpha$  est un générateur de ce groupe, on a donc  $L = K(\alpha)$ . Il en résulte que la proposition est vraie si  $K$  est fini.

2.1) On considère l'ensemble des sous-corps de  $L$  de la forme  $K(\alpha_1 + u\alpha_2)$  où  $u \in K$ . Ils contiennent  $K$ . Le corps  $K$  étant infini, on déduit de l'hypothèse faite l'existence de deux éléments distincts  $c$  et  $d$  de  $K$  tels que l'on ait  $K(\alpha_1 + c\alpha_2) = K(\alpha_1 + d\alpha_2)$ . Vérifions que l'on a

$$(1) \quad K(\alpha_1, \alpha_2) = K(\alpha_1 + c\alpha_2).$$

En utilisant le fait que  $\alpha_1 + c\alpha_2$  et  $\alpha_1 + d\alpha_2$  sont dans  $K(\alpha_1 + c\alpha_2)$ , on déduit qu'il en est de même de  $\alpha_2$ . L'égalité  $\alpha_1 = (\alpha_1 + c\alpha_2) - c\alpha_2$  entraîne alors que  $\alpha_1 \in K(\alpha_1 + c\alpha_2)$ . Par suite,  $K(\alpha_1, \alpha_2)$  est contenu dans  $K(\alpha_1 + c\alpha_2)$ . Inversement,  $\alpha_1 + c\alpha_2$  appartient à  $K(\alpha_1, \alpha_2)$ , d'où l'égalité (1) et le résultat.

2.2) Considérons pour tout entier  $n \geq 1$  la propriété  $P(n)$  suivante : pour toute famille  $(x_i)_{1 \leq i \leq n}$  d'éléments de  $L$ , l'extension  $K(x_1, \dots, x_n)/K$  possède un élément primitif. Démontrons que  $P(n)$  est vraie pour tout  $n \geq 1$ . Par définition,  $P(1)$  est vraie. Soient  $n$  un entier  $\geq 2$  tel que  $P(n-1)$  soit vraie et  $(x_i)_{1 \leq i \leq n}$  une famille d'éléments de  $L$ . On a  $K(x_1, \dots, x_n) = K(x_1, \dots, x_{n-1})(x_n)$  et d'après l'hypothèse de récurrence, il existe  $y \in L$  tel que  $K(x_1, \dots, x_{n-1}) = K(y)$ . On a donc  $K(x_1, \dots, x_n) = K(y, x_n)$ . D'après la question 2.1, l'extension  $K(y, x_n)/K$  a un élément primitif. On en déduit que la propriété  $P(n)$  est vraie et notre assertion. Par ailleurs, si  $(\alpha_i)_{1 \leq i \leq N}$  est une base de  $L$  sur  $K$ , on a  $L = K(\alpha_1, \dots, \alpha_N)$ , d'où le résultat.

3.1) Soit  $g \in E[X]$  le polynôme minimal de  $\alpha$  sur  $E$ . Puisque  $f$  appartient à  $E[X]$  et que  $f(\alpha) = 0$ ,  $g$  divise  $f$  dans  $E[X]$ . Notons  $K_g$  le sous-corps de  $L$  engendré par  $K$  et les coefficients de  $g$ . Vérifions que l'on a  $E = K_g$ . D'abord  $K_g$  est un sous-corps de  $E$  et l'on a  $K_g(\alpha) = E(\alpha) = L$ . On en déduit les égalités

$$[K_g(\alpha) : K_g] = [E(\alpha) : K_g] = [E(\alpha) : E][E : K_g].$$

Par ailleurs, le fait que  $g$  appartienne à  $K_g[X]$  entraîne que  $[K_g(\alpha) : K_g] \leq [E(\alpha) : E]$ . Il en résulte que  $[E : K_g] = 1$  et notre assertion.

3.2) Puisque  $L[X]$  est un anneau factoriel, il n'existe qu'un nombre fini de polynômes unitaires de  $L[X]$  qui divisent  $f$ . La question 3.1 entraîne alors le résultat.

## Exercice 2

1) Les corps de caractéristique 2 sont pythagoriciens, car pour tous les éléments  $x$  et  $y$  dans un tel corps, on a  $x^2 + y^2 = (x + y)^2$ . Les corps algébriquement clos sont aussi pythagoriciens.

2) Soit  $K$  un corps pythagorien. Démontrons que toute somme de carrés dans  $K$  est un carré dans  $K$ . Pour tout  $n \geq 1$ , on considère la propriété  $P(n)$  suivante : pour tout  $(x_1, \dots, x_n) \in K^n$ , l'élément  $x_1^2 + \dots + x_n^2$  est un carré dans  $K$ . La propriété  $P(1)$  est vraie. Soit  $n$  un entier  $\geq 1$  tel que  $P(n)$  soit vraie. Considérons un  $n + 1$ -uplet  $(x_1, \dots, x_{n+1})$  d'éléments de  $K$ . Par hypothèse, il existe  $x \in K$  tel que l'on ait  $x_1^2 + \dots + x_n^2 = x^2$ . On a donc  $x_1^2 + \dots + x_{n+1}^2 = x^2 + x_{n+1}^2$  qui est carré dans  $K$  d'après l'hypothèse faite sur  $K$ . D'où le résultat. L'implication inverse résulte de la définition d'un corps pythagorien.

3) Supposons que  $K$  soit une extension finie de  $\mathbb{Q}$ . Dans ce cas, l'extension  $K/\mathbb{Q}$  a un élément primitif et d'après l'exercice 1,  $K$  ne possède qu'un nombre fini de sous-corps. Par ailleurs, si  $p$  et  $q$  sont des nombre premiers distincts on a  $\mathbb{Q}(\sqrt{p}) \neq \mathbb{Q}(\sqrt{q})$  (cf. l'exercice 7 de la feuille d'exercices). Il en résulte que  $K$  a une infinité de sous-corps, ce qui conduit à une contradiction.

4) Soit  $K$  une extension finie de  $\mathbb{Q}$ . Puisque  $K$  n'a qu'un nombre fini de sous-corps, il existe un nombre premier  $p$  tel que  $\sqrt{p}$  ne soit pas dans  $K$ . Par suite,  $p \cdot 1 = 1 + \dots + 1$  n'est pas un carré dans  $K$  et d'après la question 2,  $K$  n'est pas pythagorien.

## Exercice 3

1.1) Supposons que  $G$  opère deux fois transitivement sur  $X$ . Soient  $a$  un élément de  $X$  et  $x, y$  deux éléments de  $X - \{a\}$ . D'après l'hypothèse faite, il existe  $\sigma \in G$  tel que l'on ait  $\sigma(a) = a$  et  $\sigma(x) = y$ . Puisque  $\sigma$  fixe  $a$ , on en déduit l'assertion (ii). L'implication (ii)  $\implies$  (iii) est immédiate. Supposons maintenant que l'assertion (iii) soit réalisée. Soient  $(x_1, x_2)$  et  $(y_1, y_2)$  deux couples d'éléments distincts de  $X$ . Puisque  $G$  opère transitivement sur  $X$ , il existe  $\alpha$  et  $\beta$  dans  $G$  tel que l'on ait  $\alpha(x_1) = a$  et  $\beta(y_1) = a$ . Posons  $\alpha(x_2) = x'_2$  et  $\beta(y_2) = y'_2$ . On a  $x_1 \neq x_2$  et  $y_1 \neq y_2$ , par suite  $x'_2$  et  $y'_2$  sont distincts de  $a$ . Par hypothèse, il existe donc un élément  $g$  de  $\text{stab}(a)$  tel que l'on ait  $g(x'_2) = y'_2$ . On vérifie alors que l'on a l'égalité

$$\beta^{-1}g\alpha(x_i) = y_i \quad \text{pour } i = 1 \text{ et } i = 2.$$

D'où l'assertion (i) et le résultat.

1.2) Puisque  $G$  contient un  $n - 1$ -cycle il existe un élément  $a \in X$  tel que  $\text{stab}(a)$  opère transitivement sur  $X - \{a\}$ . D'après la question 1.1,  $G$  opère donc deux fois transitivement

sur  $X$ . Par ailleurs, il existe  $b$  et  $c$  dans  $X$  tels que la transposition  $(b, c)$  soit dans  $G$ . On en déduit que si  $(u, v)$  est une transposition de  $\mathbb{S}_n$ , il existe  $\sigma \in G$  tel que l'on ait  $\sigma(b) = u$  et  $\sigma(c) = v$ . On a  $\sigma(b, c)\sigma^{-1} = (u, v)$ , ce qui prouve que  $(u, v)$  appartient à  $G$ . Le fait que les transpositions engendrent  $\mathbb{S}_n$  entraîne alors le résultat.

2.1) On vérifie que l'on a

$$(1) \quad s_2(f) = (X^2 + X + 1)(X^3 + X^2 + 1) \in \mathbb{F}_2[X].$$

Les polynômes  $X^2 + X + 1$  et  $X^3 + X^2 + 1$  n'ayant pas de racines dans  $\mathbb{F}_2$  (et étant de degré 2 et 3) ils sont donc irréductibles dans  $\mathbb{F}_2[X]$ . Par ailleurs, on a

$$(2) \quad s_3(f) = (X + 1)(X^4 + 2X^3 + X^2 + 2X + 1) \in \mathbb{F}_3[X].$$

Vérifions que  $P := X^4 + 2X^3 + X^2 + 2X + 1$  est irréductible dans  $\mathbb{F}_3[X]$ . On constate d'abord que  $P$  n'a pas de racines dans  $\mathbb{F}_3$ . Supposons par ailleurs qu'il existe  $a, b, c, d$  dans  $\mathbb{F}_3$  tels que l'on ait

$$P = (X^2 + aX + b)(X^2 + cX + d).$$

Cela conduit aux égalités  $b = d = 1$ ,  $ac = 2$  et  $a + c = 2$  et à une contradiction. D'où notre assertion. Les égalités (1) et (2) sont donc les décompositions cherchées.

2.2) Le polynôme  $s_2(f) \in \mathbb{F}_2[X]$  est séparable. En particulier,  $f$  est aussi un polynôme séparable, autrement dit,  $f$  a cinq racines distinctes dans  $\mathbb{C}$ . Choisissons une numérotation de ces racines  $x_1, \dots, x_5$  et identifions le groupe de Galois  $\text{Gal}(f)$  de  $f$  à un sous-groupe de  $\mathbb{S}_5$  comme dans le rappel 3 de la feuille d'exercices.

Supposons que  $f$  soit réductible sur  $\mathbb{Q}$ . On déduit alors de l'égalité (2) qu'il existe exactement deux orbites de  $\{x_1, \dots, x_5\}$  sous l'action de  $\text{Gal}(f)$  dont une est réduite à un élément. Cela entraîne que l'une des racines de  $f$  appartient à  $\mathbb{Q}$ . Puisque  $f$  est unitaire à coefficients dans  $\mathbb{Z}$  cette racine est  $\pm 1$  (cf. l'exercice 1 de la feuille d'exercices), d'où une contradiction et le fait que  $f$  soit irréductible sur  $\mathbb{Q}$ . Ainsi  $\text{Gal}(f)$  est un sous-groupe transitif de  $\mathbb{S}_5$ . Par ailleurs, on déduit de l'égalité (2) l'existence d'un 4-cycle dans  $\text{Gal}(f)$ . D'après l'égalité (1), il existe une transposition  $\sigma_1$  et un 3-cycle  $\sigma_2$  dont les supports sont disjoints, tels que  $\sigma_1\sigma_2$  appartienne à  $\text{Gal}(f)$ . L'égalité  $(\sigma_1\sigma_2)^3 = \sigma_1$  entraîne alors que  $\text{Gal}(f)$  contient une transposition. D'après la question 1.2, on a donc  $\text{Gal}(f) = \mathbb{S}_5$ .

## Exercice 4

1) Le groupe  $G$  est isomorphe au groupe multiplicatif  $(\mathbb{Z}/11\mathbb{Z})^*$ , via l'application qui à un élément  $s \in G$  associe la classe de l'entier  $k$  modulo 11 telle que  $s(\zeta) = \zeta^k$ . Puisque la classe de 2 modulo 11 est d'ordre 10 dans  $(\mathbb{Z}/11\mathbb{Z})^*$ , l'élément  $\sigma$  de  $G$  défini par  $\sigma(\zeta) = \zeta^2$  est donc un générateur de  $G$ .

2) Puisque  $G$  est cyclique d'ordre 10, pour tout diviseur  $d \geq 1$  de 10, il existe un unique sous-groupe d'ordre  $d$  de  $G$ . D'après le théorème de correspondance de Galois, les

sous-corps de  $K$  sont donc  $\mathbb{Q}$ ,  $K$  ainsi que deux corps  $K_1$  et  $K_2$  dont les degrés sur  $\mathbb{Q}$  sont respectivement 2 et 5.

Le polynôme minimal de  $\zeta$  sur  $\mathbb{Q}$  est le polynôme cyclotomique  $1 + \dots + X^{10}$ . Par ailleurs, 0 est un élément primitif de  $\mathbb{Q}$  de polynôme minimal  $X$ . En utilisant par exemple l'exercice 48 de la feuille d'exercices, on constate que l'on a  $K_1 = \mathbb{Q}(\sqrt{-11})$ , le polynôme minimal sur  $\mathbb{Q}$  de  $\sqrt{-11}$  étant  $X^2 + 11$ . Quant au corps  $K_2$ , c'est nécessairement le sous-corps réel  $\mathbb{Q}(\zeta + \zeta^{-1})$  de  $K$ . Tout revient donc à déterminer le polynôme minimal de  $\zeta + \zeta^{-1}$  sur  $\mathbb{Q}$ . On va expliciter pour cela ses conjugués sur  $\mathbb{Q}$ . Ce sont les éléments  $\sigma^k(\zeta + \zeta^{-1})$  pour  $k = 1, \dots, 10$ , autrement dit,

$$\zeta + \zeta^{-1}, \quad \zeta^2 + \zeta^{-2}, \quad \zeta^4 + \zeta^{-4}, \quad \zeta^3 + \zeta^{-3} \quad \text{et} \quad \zeta^5 + \zeta^{-5}.$$

Il en résulte que le polynôme minimal  $F$  de  $\zeta + \zeta^{-1}$  sur  $\mathbb{Q}$  est

$$F = \prod_{i=1}^5 (X - (\zeta^i + \zeta^{-i})).$$

On vérifie alors que l'on a

$$F = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1.$$

## Exercice 5

1) Le polynôme  $F := X^3 - X + 1 \in \mathbb{F}_3[X]$  est irréductible sur  $\mathbb{F}_3$  car il est de degré 3 et il n'a pas de racines dans  $\mathbb{F}_3$ . Si  $\alpha$  est une racine de  $F$  dans  $\Omega$ , l'extension  $\mathbb{F}_3(\alpha)/\mathbb{F}_3$  est donc de degré 3, d'où  $K = \mathbb{F}_3(\alpha)$ .

2) Le groupe  $K^*$  est cyclique d'ordre 26. Les ordres de ses éléments sont donc 1, 2, 13 ou 26. Puisque  $\alpha$  est une racine de  $F$ , il en est de même de  $\alpha^3$  et de  $\alpha^9$ . On vérifie que ces éléments sont distincts deux à deux, ce sont donc les trois racines de  $F$  dans  $\Omega$ . On en déduit que leur produit vaut  $-1$ , d'où l'égalité  $\alpha^{13} = -1$ . Cela entraîne l'assertion.

3) L'extension  $K/\mathbb{F}_3$  est galoisienne et son groupe de Galois est engendré par l'élément de Frobenius  $\sigma$  défini par l'égalité  $\sigma(\alpha) = \alpha^3$ . On a  $\sigma(\alpha^3) = \alpha^9$  et  $\sigma(\alpha^9) = \alpha^{27} = \alpha$ . Pour tout entier  $k$  les coefficients de  $f_k$  sont donc laissés fixes par  $\sigma$ , par suite, ils sont dans  $\mathbb{F}_3$ .

4) L'égalité  $\alpha^{26} = 1$  entraîne que l'ensemble des polynômes  $f_k$  est entièrement décrit en faisant varier  $k$  modulo 26. Par ailleurs, en utilisant les égalités  $f_k = f_{3k} = f_{9k}$ , on constate que l'on a :

$$\begin{aligned} f_1 &= f_3 = f_9, & f_2 &= f_6 = f_{18}, & f_4 &= f_{12} = f_{10}, \\ f_5 &= f_{15} = f_{19}, & f_7 &= f_{21} = f_{11}, & f_8 &= f_{24} = f_{20}, \\ f_{14} &= f_{16} = f_{22}, & f_{17} &= f_{25} = f_{23}. \end{aligned}$$

On obtient ainsi les dix polynômes suivants :

$$f_0, f_1, f_2, f_4, f_5, f_7, f_8, f_{13}, f_{14}, f_{17}.$$

Puisque  $\alpha$  est d'ordre 26 dans  $K^*$ , les éléments  $\alpha^n$  sont deux à deux distincts pour les entiers  $n$  tels que  $0 \leq n \leq 25$ . Il en résulte que les dix polynômes ci-dessus n'ont deux à deux aucune racine commune. Ils sont donc distincts. Mis à part  $f_0$  et  $f_{13}$ , ils sont irréductibles sur  $\mathbb{F}_3$  car ils n'ont pas de racines dans  $\mathbb{F}_3$ . Il n'y a pas d'autres polynômes irréductibles de degré 3 unitaires dans  $\mathbb{F}_3$  car un tel polynôme a une racine de la forme  $\alpha^k$  et a aussi pour racine  $\alpha^{3k}$  et  $\alpha^{9k}$  donc est égal à  $f_k$ .

5) Les racines de  $f_k$  sont inverses de celles de  $f_{26-k}$ . Il existe donc  $c \in \mathbb{F}_3$  tel que l'on ait

$$f_{26-k} = cX^3 f_k\left(\frac{1}{X}\right).$$

Puisque  $f_{26-k}$  est unitaire,  $c$  est l'inverse du terme constant de  $f_k$ . On a donc

$$c = -\alpha^{-13k} = (-1)^{k+1}.$$

On obtient ainsi l'égalité

$$(1) \quad f_{26-k} = (-1)^{k+1} X^3 f_k\left(\frac{1}{X}\right).$$

6) On a les égalités

$$f_0 = (X-1)^3, \quad f_{13} = (X+1)^3,$$

et il résulte de (1) qu'il suffit de calculer  $f_1, f_2, f_4$  et  $f_5$  pour obtenir  $f_7, f_8, f_{14}$  et  $f_{17}$ . Par ailleurs,  $f_k$  est le polynôme minimal de  $\alpha^k$  sur  $\mathbb{F}_3$ . Il suffit donc de trouver une relation linéaire non triviale à coefficients dans  $\mathbb{F}_3$  entre 1,  $\alpha^k$ ,  $\alpha^{2k}$  et  $\alpha^{3k}$ . Par définition de  $\alpha$ , on a

$$f_1 = X^3 - X + 1.$$

Pour calculer  $f_2$ , on remarque que l'on a  $\alpha^4 = \alpha^2 - \alpha$  et  $\alpha^6 = \alpha^2 + \alpha + 1$ , ce qui conduit à l'égalité  $\alpha^6 + \alpha^4 + \alpha^2 - 1 = 0$ . On en déduit que l'on a

$$f_2 = X^3 + X^2 + X - 1.$$

De même, on vérifie que l'on a  $\alpha^{12} + \alpha^8 - 1 = 0$  et  $\alpha^{15} - \alpha^{10} + \alpha^5 + 1 = 0$ . Il en résulte que l'on a

$$f_4 = X^3 + X^2 - 1 \quad \text{et} \quad f_5 = X^3 - X^2 + X + 1.$$

Ces égalités conduisent alors à

$$f_7 = X^3 + X^2 - X + 1, \quad f_8 = X^3 - X^2 - X - 1, \quad f_{14} = X^3 - X - 1, \quad f_{17} = X^3 - X^2 + 1.$$