

## Correction du premier devoir

### Exercice 1

Soit  $\Delta$  le discriminant de  $F$ . Démontrons que l'on a

$$(1) \quad \Delta = (-1)^{\frac{n(n+1)}{2}} b^{n-2} \left( (-1)^n n^n b - a^n (n-1)^{n-1} \right).$$

Soient  $\alpha_1, \dots, \alpha_n$  les racines de  $F$  dans une clôture algébrique de  $K$ . Si  $F'$  est le polynôme dérivé de  $F$ , on a

$$\Delta = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n F'(\alpha_i),$$

autrement dit,

$$(2) \quad \Delta = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^n \alpha_i^{n-2} (n\alpha_i + a(n-1)).$$

Posons

$$G = F\left(\frac{X - a(n-1)}{n}\right) \in K[X].$$

Les racines de  $G$  sont les éléments  $n\alpha_i + a(n-1)$  pour  $i = 1, \dots, n$ . Si  $c$  désigne le terme constant de  $G$ , on a donc

$$\prod_{i=1}^n (n\alpha_i + a(n-1)) = (-1)^n n^n c.$$

On a l'égalité

$$c = \left( -\frac{a(n-1)}{n} \right)^n + a \left( -\frac{a(n-1)}{n} \right)^{n-1} + b.$$

On en déduit que l'on a

$$(3) \quad \prod_{i=1}^n (n\alpha_i + a(n-1)) = (-1)^n n^n b - a^n (n-1)^{n-1}.$$

Par ailleurs, on a

$$(4) \quad \prod_{i=1}^n \alpha_i^{n-2} = ((-1)^n b)^{n-2}.$$

En remarquant que l'on a

$$\frac{n(n-1)}{2} + n(n-2) \equiv \frac{n(n+1)}{2} \pmod{2},$$

les égalités (2), (3) et (4) entraînent alors la formule (1).

## Exercice 2

1. Démontrons plus généralement l'énoncé suivant :

**Lemme.** Soient  $p$  et  $q$  deux nombres premiers distincts et  $G$  un groupe d'ordre  $pq$ . On suppose que l'on a  $p < q$  et que  $p$  ne divise pas  $q - 1$ . Alors,  $G$  est cyclique.

Démonstration : Pour démontrer cet énoncé on peut utiliser les théorèmes de Sylow. Procédons ici de la façon suivante. D'après le théorème de Cauchy, il existe dans  $G$  un élément  $a$  d'ordre  $p$  et un élément  $b$  d'ordre  $q$ . Notons  $H$  le sous-groupe de  $G$  engendré par  $a$  et  $K$  celui engendré par  $b$ . Puisque l'indice de  $K$  dans  $G$  est  $p$  et que  $p$  est le plus petit nombre premier divisant l'ordre de  $G$ , le sous-groupe  $K$  est distingué dans  $G$ . En particulier, pour tout  $k \in K$ , l'élément  $aka^{-1}$  appartient à  $K$ . Soit  $\varphi : K \rightarrow K$  l'application définie par l'égalité  $\varphi(k) = aka^{-1}$ . C'est un automorphisme de  $K$ . Vérifions que  $\varphi$  est l'identité  $Id_K$  de  $K$ . L'élément  $a$  étant d'ordre  $p$  on a  $\varphi^p = Id_K$ . Par ailleurs, le groupe des automorphismes de  $K$  est d'ordre  $q - 1$  : en effet,  $K$  est isomorphe à  $\mathbb{Z}/q\mathbb{Z}$  donc le groupe des automorphismes de  $K$  est isomorphe à  $\mathbb{Z}/(q - 1)\mathbb{Z}$ . Puisque  $p$  ne divise pas  $q - 1$ , ce groupe ne possède pas d'élément d'ordre  $p$ , par suite  $\varphi = Id_K$ . On en déduit que  $a$  et  $b$  commutent. En utilisant le fait que  $H \cap K$  est le sous-groupe trivial, on constate alors que  $ab$  est un élément de  $G$  d'ordre  $pq$ , donc  $G$  est cyclique d'ordre  $pq$ . D'où le lemme.

Notre assertion se déduit du lemme en prenant  $p = 3$  et  $q = 5$ .

2. Supposons que  $\mathbb{A}_5$  possède un sous-groupe d'ordre 15. D'après l'assertion 1, il est cyclique. Un générateur de ce groupe est donc un élément d'ordre 15 de  $\mathbb{A}_5$ . Tout revient ainsi à vérifier que  $\mathbb{A}_5$  n'a pas d'éléments d'ordre 15. On remarque pour cela que les éléments de  $\mathbb{A}_5$ , qui est d'ordre 60, autres que l'identité sont les doubles transpositions à supports disjoints (il y en a 15), les 3-cycles (il y en a 20) et les 5-cycles (il y en a 24), qui sont respectivement d'ordre 2, 3 et 5. D'où notre assertion.

3. Le fait que  $f$  soit irréductible de degré 5 entraîne que 5 divise l'ordre de  $\text{Gal}(f)$ . On utilise ensuite la condition c) : puisque  $\ell$  ne divise pas  $D(f)$ , le polynôme  $\bar{f}$  de  $\mathbb{F}_\ell[X]$  déduit de  $f$  par réduction modulo  $\ell$  est séparable. Par hypothèse, on a  $\bar{f} = (X - a)(X - b)g$ , où  $a$  et  $b$  sont deux éléments distincts de  $\mathbb{F}_\ell$  et où  $g$  est irréductible sur  $\mathbb{F}_\ell$  de degré 3. Il en résulte l'existence dans  $\text{Gal}(f)$  d'un élément d'ordre 3 (cf. par exemple le rappel 3 de la feuille d'exercices). Par suite, 15 divise l'ordre de  $\text{Gal}(f)$ .

4. En choisissant une numérotation des racines de  $f$ , on dispose d'un morphisme de groupes injectif de  $\text{Gal}(f)$  dans  $\mathbb{S}_5$ . Puisque  $D(f)$  est un carré dans  $\mathbb{Z}$ , l'image de  $\text{Gal}(f)$

dans  $\mathbb{S}_5$  est un sous-groupe de  $\mathbb{A}_5$ . Tout revient ainsi à démontrer que  $\text{Gal}(f)$  est d'ordre 60. On déduit de l'assertion 3 que l'on a  $|\text{Gal}(f)| \in \{15, 30, 60\}$ . D'après l'assertion 2, on a  $|\text{Gal}(f)| \neq 15$ . Vérifions que l'on a  $|\text{Gal}(f)| \neq 30$ . Supposons le contraire. Dans ce cas,  $\mathbb{A}_5$  doit posséder un sous-groupe  $H$  d'indice 2. Ce sous-groupe est distingué dans  $\mathbb{A}_5$  et le groupe quotient  $\mathbb{A}_5/H$  est d'ordre 2 isomorphe à  $\mathbb{Z}/2\mathbb{Z}$ . On en déduit l'existence d'un morphisme de groupes surjectif  $s$  de  $\mathbb{A}_5$  sur  $\mathbb{Z}/2\mathbb{Z}$ . Par ailleurs,  $\mathbb{A}_5$  est engendré par les 3-cycles  $(*)$ , et un 3-cycle étant d'ordre 3, son image par  $s$  est 0. Il en résulte que  $s$  est le morphisme trivial, qui n'est pas surjectif. D'où une contradiction et la proposition. [Pour démontrer que  $|\text{Gal}(f)| \neq 30$ , on peut aussi utiliser le fait que  $\mathbb{A}_5$  est un groupe simple i.e. que  $\mathbb{A}_5$  ne possède pas de sous-groupes distingués autres que  $\mathbb{A}_5$  et le sous-groupe trivial].

(\*) Vérifions que pour tout  $n \geq 3$ , le groupe alterné  $\mathbb{A}_n$  est engendré par les 3-cycles. On peut supposer  $n \geq 4$ . Soit  $\sigma$  un élément de  $\mathbb{A}_n$ . Le groupe  $\mathbb{S}_n$  étant engendré par les transpositions,  $\sigma$  s'écrit comme un produit pair de transpositions (car sa signature est 1). Par ailleurs, si  $a, b, c$  et  $d$  sont des éléments distincts de  $\{1, \dots, n\}$ , on a les égalités

$$(a, b)(b, c) = (a, b, c) \quad \text{et} \quad (a, b)(c, d) = (a, b)(b, c)(b, c)(c, d) = (a, b, c)(b, c, d),$$

ce qui entraîne le résultat.

5. Le critère d'Eisenstein, utilisé avec le nombre premier 5, entraîne que  $f$  est irréductible sur  $\mathbb{Z}$  et par suite sur  $\mathbb{Q}$ .

6. On déduit de la formule (1) de l'exercice 1 que l'on a  $D(f) = 2^{24} \cdot 3^6 \cdot 5^8 \cdot 7^2$ .

7. Soit  $\bar{f}$  le polynôme de  $\mathbb{F}_{11}[X]$  déduit de  $F$  par réduction modulo 11. On vérifie que l'on a

$$\bar{f} = (X + 9)(X + 6)(X^3 + X^2 + 8X + 2).$$

Le polynôme  $X^3 + X^2 + 8X + 2$  n'a pas de racines dans  $\mathbb{F}_{11}$  et 11 ne divise pas  $D(f)$ , d'où l'assertion. Compte tenu de ce qui précède et de la proposition,  $\text{Gal}(f)$  est donc isomorphe à  $\mathbb{A}_5$ .

### Exercice 3

1. Pour tout  $\tau \in G$  il existe un unique élément  $k$  tel que  $1 \leq k \leq 12$  et que  $\tau(\zeta) = \zeta^k$ . L'application  $\varphi : G \rightarrow (\mathbb{Z}/13\mathbb{Z})^*$  définie par

$$\varphi(\tau) = k \text{ mod. } 13,$$

est un isomorphisme de groupes. Par ailleurs,  $(\mathbb{Z}/13\mathbb{Z})^*$  est un groupe cyclique d'ordre 12 qui est engendré par la classe de 2. L'élément  $\varphi^{-1}(2 \text{ mod. } 13)$  i.e.  $\sigma$  est donc un générateur de  $G$ .

Autre démonstration : on peut aussi calculer directement l'ordre de  $\sigma$  dans  $G$ . On a

$$\sigma^2(\zeta) = \zeta^4, \quad \sigma^3(\zeta) = \zeta^8, \quad \sigma^4(\zeta) = \zeta^3 \quad \text{et} \quad \sigma^6(\zeta) = \zeta^{-1},$$

ce qui entraîne que  $\sigma$  est d'ordre 12 i.e. que  $\sigma$  est un générateur de  $G$ .

2. Notons  $1_K$  l'élément neutre de  $G$  i.e. l'application identité de  $K$ . On a

$$H_1 = \{1_K\}, \quad H_2 = \{1_K, \sigma^6\}, \quad H_3 = \{1_K, \sigma^4, \sigma^8\},$$

$$H_4 = \{1_K, \sigma^3, \sigma^6, \sigma^9\}, \quad H_6 = \{1_K, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}\}, \quad H_{12} = G.$$

3. L'extension  $K/K_d$  est galoisienne de groupe de Galois  $H_d$ . Le degré de  $K$  sur  $K_d$  est donc égal à  $d$ , et celui de  $K_d$  sur  $\mathbb{Q}$  est  $12/d$ .

4. Soit  $\gamma$  un élément de  $H_d$ . L'application de  $f : H_d \rightarrow H_d$  définie pour tout  $\tau \in H_d$  par  $f(\tau) = \gamma\tau$  est une bijection de  $H_d$  sur  $H_d$ . Il en résulte que l'on a

$$\gamma(\alpha_d) = \sum_{\tau \in H_d} \gamma\tau(\zeta) = \alpha_d.$$

Par suite,  $\alpha_d$  est laissé fixe par les éléments de  $H_d$ , donc  $\alpha_d$  appartient à  $K_d$ .

5. Il s'agit de prouver l'égalité  $K_d = \mathbb{Q}(\alpha_d)$ . On vérifie que l'on a

$$\alpha_1 = \zeta, \quad \alpha_2 = \zeta + \zeta^{-1}, \quad \alpha_3 = \zeta + \zeta^3 + \zeta^9, \quad \alpha_4 = \zeta + \zeta^{-1} + \zeta^5 + \zeta^{-5},$$

$$\alpha_6 = \zeta + \zeta^{-1} + \zeta^3 + \zeta^{-3} + \zeta^4 + \zeta^{-4}, \quad \alpha_{12} = -1.$$

On en déduit l'assertion si  $d = 1$  ou  $d = 12$ .

Si  $d = 2$  : le corps  $\mathbb{Q}(\alpha_2)$  est contenu dans  $K_2$ . Par ailleurs, les extensions  $K_2/\mathbb{Q}$  et  $\mathbb{Q}(\alpha_2)/\mathbb{Q}$  sont de degré 6 (cf. l'exercice 23)), d'où  $K_2 = \mathbb{Q}(\alpha_2)$ .

Si  $d = 3$  : l'extension  $K_3/\mathbb{Q}$  est de degré 4 et  $\mathbb{Q}(\alpha_3)$  est contenu dans  $K_3$ . Supposons que l'on ait  $K_3 \neq \mathbb{Q}(\alpha_3)$ . Dans ce cas,  $\mathbb{Q}(\alpha_3)$  est une extension de degré au plus 2 de  $\mathbb{Q}$ . Par ailleurs, d'après le théorème de correspondance de Galois,  $K_6$  est l'unique extension quadratique de  $\mathbb{Q}$  contenue dans  $K$ . Il en résulte que  $\alpha_3$  appartient à  $K_6$ . En particulier,  $\alpha_3$  est fixé par les éléments de  $H_6$ . Or  $\sigma^2(\alpha_3) = \zeta^{-1} + \zeta^{-3} + \zeta^4$ , qui est distinct de  $\alpha_3$ , car sinon  $\zeta$  serait racine d'un polynôme unitaire à coefficients dans  $\mathbb{Q}$  de degré  $< 12$ , ce qui n'est pas. On obtient ainsi une contradiction et l'égalité  $K_3 = \mathbb{Q}(\alpha_3)$ .

Si  $d = 4$  : on a  $\sigma(\alpha_4) = \zeta^2 + \zeta^{-2} + \zeta^3 + \zeta^{-3}$ . On vérifie comme ci-dessus que  $\sigma(\alpha_4)$  est distinct de  $\alpha_4$ , d'où l'on déduit que  $\alpha_4$  n'est pas dans  $\mathbb{Q}$ . Puisque  $\alpha_4$  appartient à  $K_4$ , qui est une extension de degré 3 de  $\mathbb{Q}$ , il en résulte que l'on a  $K_4 = \mathbb{Q}(\alpha_4)$ .

Si  $d = 6$  : on constate de nouveau que  $\alpha_6$  n'est pas dans  $\mathbb{Q}$ . Puisque  $K_6$  est une extension quadratique de  $\mathbb{Q}$  et que  $\alpha_6$  appartient à  $K_6$ , on a ainsi  $K_6 = \mathbb{Q}(\alpha_6)$ .

6. Le groupe  $G$  étant abélien, tous ses sous-groupes sont distingués et l'extension  $K_d/\mathbb{Q}$  est donc galoisienne. Par ailleurs, l'application de restriction

$$G \rightarrow \text{Gal}(K_d/\mathbb{Q}),$$

qui à un élément de  $G$  associe sa restriction à  $K_d$ , est un morphisme surjectif de groupes. En particulier, la restriction  $\sigma_d$  de  $\sigma$  à  $K_d$  est un générateur de  $\text{Gal}(K_d/\mathbb{Q})$ . Puisque ce groupe est d'ordre  $12/d$ , on a donc

$$\text{Gal}(K_d/\mathbb{Q}) = \left\{ 1_{K_d}, \sigma_d, \dots, \sigma_d^{\frac{12}{d}-1} \right\}.$$

7. Notons  $F_d$  le polynôme minimal de  $\alpha_d$  sur  $\mathbb{Q}$ . D'après la question 5, le degré de  $F_d$  est  $12/d$ . Il résulte de la question 6 que les conjugués de  $\alpha_d$  sur  $\mathbb{Q}$ , autrement dit les racines de  $F_d$ , sont les éléments

$$\sigma_d^i(\alpha_d) \quad \text{i.e.} \quad \sigma^i(\alpha_d) \quad \text{pour} \quad i = 0, \dots, \frac{12}{d} - 1.$$

On en déduit l'égalité

$$F_d = \prod_{i=0}^{\frac{12}{d}-1} (X - \sigma^i(\alpha_d)).$$

On a  $F_{12} = X + 1$ . On a par ailleurs,

$$F_1 = \prod_{i=0}^{11} (X - \sigma^i(\zeta)) = \sum_{i=0}^{12} X^i.$$

Pour les autres valeurs de  $d$ , les conjugués de  $\alpha_d$  sur  $\mathbb{Q}$  sont :

$$\begin{aligned} \text{si } d = 2 : & \quad \alpha_2, \quad \zeta^2 + \zeta^{-2}, \quad \zeta^3 + \zeta^{-3}, \quad \zeta^4 + \zeta^{-4}, \quad \zeta^6 + \zeta^{-6}, \quad \zeta^8 + \zeta^{-8}, \\ \text{si } d = 3 : & \quad \alpha_3, \quad \zeta^2 + \zeta^5 + \zeta^6, \quad \zeta^4 + \zeta^{10} + \zeta^{12}, \quad \zeta^7 + \zeta^8 + \zeta^{11}, \\ \text{si } d = 4 : & \quad \alpha_4, \quad \zeta^2 + \zeta^{-2} + \zeta^3 + \zeta^{-3}, \quad \zeta^4 + \zeta^{-4} + \zeta^7 + \zeta^{-7}, \\ \text{si } d = 6 : & \quad \alpha_6, \quad \zeta^2 + \zeta^{-2} + \zeta^6 + \zeta^{-6} + \zeta^8 + \zeta^{-8}. \end{aligned}$$

On constate alors que l'on a

$$F_2 = X^6 + X^5 - 5X^4 - 4X^3 + 6X^2 + 3X - 1, \quad F_3 = X^4 + X^3 + 2X^2 - 4X + 3,$$

$$F_4 = X^3 + X^2 - 4X + 1, \quad F_6 = X^2 + X - 3.$$

On notera que le corps  $K_6$  est  $\mathbb{Q}(\sqrt{13})$ , ce qui était prévisible compte tenu de l'exercice 47).