

Correction des exercices de Théorie de Galois

1. Polynômes, extensions de corps

1) On a l'égalité

$$a_0 t^n + a_1 s t^{n-1} \cdots + a_{n-1} s^{n-1} t + a_n s^n = 0.$$

On en déduit que t divise $a_n s^n$. Puisque s et t sont premiers entre eux, cela entraîne que t divise a_n . De même, s divise $a_0 t^n$, donc s divise a_0 . D'où le résultat.

2) Soient α , β et γ les racines de F dans une extension convenable de K . On a $F = (X - \alpha)(X - \beta)(X - \gamma)$. Soient $F' \in K[X]$ le polynôme dérivé de F et Δ le discriminant de F . Vérifions que l'on a l'égalité

$$(1) \quad \Delta = -F'(\alpha)F'(\beta)F'(\gamma).$$

On a

$$F' = (X - \alpha)(X - \beta) + (X - \alpha)(X - \gamma) + (X - \beta)(X - \gamma).$$

On en déduit les égalités

$$F'(\alpha) = (\alpha - \beta)(\alpha - \gamma), \quad F'(\beta) = (\beta - \alpha)(\beta - \gamma), \quad F'(\gamma) = (\gamma - \alpha)(\gamma - \beta),$$

ce qui entraîne (1). Par suite, on a

$$\Delta = -(3\alpha^2 + p)(3\beta^2 + p)(3\gamma^2 + p).$$

On obtient ainsi

$$\Delta = -\left(27(\alpha\beta\gamma)^2 + 9p(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3p^2(\alpha^2 + \beta^2 + \gamma^2) + p^3\right).$$

Par ailleurs, on a

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 = (\alpha\beta + \alpha\gamma + \beta\gamma)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma),$$

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma).$$

D'après les relations entre les coefficients et les racines d'un polynôme, on a

$$\alpha + \beta + \gamma = 0, \quad \alpha\beta + \alpha\gamma + \beta\gamma = p, \quad \alpha\beta\gamma = -q.$$

Il en résulte l'égalité

$$\Delta = -(4p^3 + 27q^2).$$

3) 1. D'après l'hypothèse faite, F a une racine α dans K . Soient β et γ les autres racines de F dans une extension de K . Si $\beta = \alpha$ ou bien si $\gamma = \alpha$, notre assertion est vérifiée car alors $(X - \alpha)^2$ divise F dans $K[X]$. On peut donc supposer que α est distinct de β et γ . On a

$$F = (X - \alpha)(X^2 - (\gamma + \beta)X + \beta\gamma),$$

de sorte que

$$(1) \quad \beta + \gamma \in K \quad \text{et} \quad \beta\gamma \in K.$$

Par ailleurs, on a

$$(\beta - \gamma)^2 = \frac{\Delta}{(\alpha - \beta)^2(\gamma - \alpha)^2}.$$

On déduit de (1) que $(\alpha - \beta)(\gamma - \alpha)$ est dans K . Puisque Δ est un carré dans K , il en résulte que $\beta - \gamma$ appartient à K . Cela entraîne que 2β et 2γ sont dans K . Le corps K étant de caractéristique différente de 2, les éléments β et γ sont donc aussi dans K .

2. Supposons $K = \mathbb{F}_2$ et $F = X^3 - 1$. Le discriminant de F vaut 1, qui est un carré dans \mathbb{F}_2 et l'on a $F = (X - 1)(X^2 + X + 1)$. Le polynôme $X^2 + X + 1 \in \mathbb{F}_2[X]$ étant irréductible, F a une seule racine dans \mathbb{F}_2 .

3. On a dans ce cas $\Delta = -(4p^3 + 27q^2)$. Par ailleurs, un polynôme de degré 3 à coefficients dans \mathbb{R} possède au moins une racine réelle. Si Δ est positif, Δ est un carré dans \mathbb{R} , et d'après l'assertion 1 les racines de F sont réelles. Inversement, si les racines α , β et γ sont dans \mathbb{R} , on a $\Delta = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2 \geq 0$. D'où le résultat.

4) Le discriminant de F est -23 . Rappelons plus généralement la détermination des racines d'un polynôme $F = X^3 + pX + q \in \mathbb{R}[X]$ si l'on a $\Delta = -(4p^3 + 27q^2) < 0$. Dans ce cas, il existe une unique racine réelle t_1 . Notons t_2 et t_3 les deux autres racines de F conjuguées dans \mathbb{C} . Soit j une racine cubique de 1 autre que 1. Posons

$$\theta_1 = (t_1 + jt_2 + j^2t_3)^3 \quad \text{et} \quad \theta_2 = (t_1 + j^2t_2 + jt_3)^3.$$

On a

$$t_1 + jt_2 + j^2t_3 \in \mathbb{R} \quad \text{et} \quad t_1 + j^2t_2 + jt_3 \in \mathbb{R}.$$

On vérifie que

$$\theta_1\theta_2 = -27p^3, \quad \theta_1 + \theta_2 = -27q.$$

On en déduit que θ_1 et θ_2 sont les racines du polynôme $Y^2 + 27qY - 27p^3$. Par suite, il existe une racine carrée δ de -3Δ telle que l'on ait

$$\theta_1 = -\frac{27}{2}q + \frac{3\delta}{2} \in \mathbb{R} \quad \text{et} \quad \theta_2 = -\frac{27}{2}q - \frac{3\delta}{2} \in \mathbb{R}.$$

Soient μ_1 et μ_2 les racines cubiques réelles de θ_1 et θ_2 . On a

$$\mu_1 = t_1 + jt_2 + j^2t_3 \quad \text{et} \quad \mu_2 = t_1 + j^2t_2 + jt_3.$$

Compte tenu de l'égalité $t_1 + t_2 + t_3 = 0$, on obtient alors

$$t_1 = \frac{1}{3}(\mu_1 + \mu_2), \quad t_2 = \frac{1}{3}(j^2\mu_1 + j\mu_2), \quad t_3 = \frac{1}{3}(j\mu_1 + j^2\mu_2).$$

Avec le polynôme F considéré, on obtient (par exemple)

$$\theta_1 = -\frac{27}{2} + \frac{3\sqrt{69}}{2} \quad \text{et} \quad \theta_2 = -\frac{27}{2} - \frac{3\sqrt{69}}{2},$$

puis les t_i par les formules ci-dessus.

5) 1. Les transpositions de \mathbb{S}_3 laissent fixe F . Par suite, F est un polynôme symétrique. Il existe donc un polynôme G à coefficients dans K en trois indéterminées tel que l'on ait $F = G(\sigma_1, \sigma_2, \sigma_3)$. Afin d'expliciter G , on procède comme suit : parmi les monômes $X_1^{k_1}X_2^{k_2}X_3^{k_3}$ qui interviennent dans F , on détermine celui pour lequel le triplet (k_1, k_2, k_3) est le plus grand pour l'ordre lexicographique de \mathbb{N}^3 . On a nécessairement $k_1 \geq k_2 \geq k_3$. Il s'agit ici du triplet $(2, 1, 0)$. On considère ensuite le polynôme $P = F - \sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\sigma_3^{k_3}$, autrement dit,

$$P = F - \sigma_1\sigma_2.$$

On vérifie alors que l'on a $P = -3\sigma_3$, ce qui conduit à $F = \sigma_1\sigma_2 - 3\sigma_3$.

2. De nouveau on constate que les transpositions de \mathbb{S}_3 laissent fixe F . Le monôme $X_1^{k_1}X_2^{k_2}X_3^{k_3}$ pour lequel le triplet (k_1, k_2, k_3) est le plus grand pour l'ordre lexicographique de \mathbb{N}^3 est $X_1^3X_2$. On considère ainsi le polynôme $F - \sigma_1^2\sigma_2$. On vérifie que l'on a

$$F - \sigma_1^2\sigma_2 = -5(X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2) - 2(X_1^2X_2^2 + X_2^2X_3^2 + X_3^2X_1^2).$$

On a

$$X_1^2X_2X_3 + X_1X_2^2X_3 + X_1X_2X_3^2 = \sigma_1\sigma_3.$$

Par ailleurs, on a

$$X_1^2X_2^2 + X_2^2X_3^2 + X_3^2X_1^2 - \sigma_2^2 = -2\sigma_1\sigma_3.$$

On obtient ainsi

$$F = \sigma_1^2 \sigma_2 - \sigma_1 \sigma_3 - 2\sigma_2^2.$$

6) 1. Le polynôme $F = X^3 - 2$ est irréductible sur \mathbb{Q} (cf. l'exercice 1), donc le degré de K sur \mathbb{Q} est 3.

2. Supposons F réductible sur K . Cela signifie que F a une racine dans K , autrement dit que son discriminant, qui est -3 , est un carré dans K . Le corps $\mathbb{Q}(\sqrt{-3})$ est donc contenu dans K , ce qui entraîne que le degré de K sur \mathbb{Q} est pair, d'où une contradiction.

3. Le polynôme minimal de j sur K est F , donc le degré de $K(j) = \mathbb{Q}(\alpha, j)$ sur K est 2. Il en résulte que $\mathbb{Q}(\alpha, j)$ est une extension de degré 6 de \mathbb{Q} .

4. Posons $\theta = \alpha + j$. On a $(\theta - j)^3 - 2 = 0$, d'où, en tenant compte du fait que $j^3 = 1$ et $\theta + \theta^2 \neq 0$,

$$j = \frac{\theta^3 - 3\theta - 3}{3(\theta + \theta^2)}.$$

En particulier, j appartient à $\mathbb{Q}(\theta)$. On en déduit que α est aussi dans $\mathbb{Q}(\theta)$, donc $\mathbb{Q}(\alpha, j)$ est contenu dans $\mathbb{Q}(\theta)$. Par ailleurs, $\mathbb{Q}(\theta)$ est contenu dans $\mathbb{Q}(\alpha, j)$. D'où le résultat.

5. Soit G le polynôme minimal de θ sur \mathbb{Q} . Il est de degré 6, et G est l'unique polynôme unitaire de $\mathbb{Q}[X]$ de degré 6 dont θ est racine. Pour le déterminer, on écrit les égalités $2 = \alpha^3 = (\theta - j)^3$, d'où l'on déduit que θ est racine du polynôme

$$H = X^3 - 3jX^2 + 3j^2X - 3 \in \mathbb{Q}(j)[X].$$

Soit \overline{H} le polynôme conjugué de H sur \mathbb{C} . On a $\overline{H} = X^3 - 3j^2X^2 + 3jX - 3$ et l'on vérifie que l'on a

$$H\overline{H} = X^6 + 3X^5 + 6X^4 + 3X^3 + 9X + 9.$$

Ce polynôme est à coefficients dans \mathbb{Q} unitaire, de degré 6, et il admet θ pour racine. C'est donc le polynôme G cherché.

7) 1. Soit α un élément de K qui ne soit pas dans \mathbb{Q} . Le degré de l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est 2 et $\mathbb{Q}(\alpha)$ est contenu dans K . Par suite $K = \mathbb{Q}(\alpha)$. Soit $F = X^2 + bX + c \in \mathbb{Q}[X]$ le polynôme minimal de α sur \mathbb{Q} . Soit δ une racine carrée de $b^2 - 4c$. On a $2\alpha = -b \pm \delta$, de sorte que $K = \mathbb{Q}(\delta)$. Par ailleurs, il existe u et v dans \mathbb{Z} tels que $b^2 - 4c = u/v$. On a alors $K = \mathbb{Q}(\sqrt{uv})$. Il existe un entier d sans facteurs carrés tel que uv soit dans $d\mathbb{Z}^2$. On obtient ainsi $K = \mathbb{Q}(\sqrt{d})$ et l'assertion.

2. Il existe a et b dans \mathbb{Q} tels que l'on ait $\sqrt{d} = a + b\sqrt{d'}$. Si $b = 0$, l'entier d est un carré dans \mathbb{Z} et il en est de même de d' . Supposons $b \neq 0$. On a $2b\sqrt{d}\sqrt{d'} = d + d'b^2 - a^2$, ce qui entraîne que $\sqrt{d}\sqrt{d'}$ est dans \mathbb{Q} , puis que dd' est un carré dans \mathbb{Q} . D'où le résultat.

8) Le polynôme minimal de α sur $K(\alpha^2)$ divise $X^2 - \alpha^2$, de sorte que le degré n de l'extension $K(\alpha)/K(\alpha^2)$ est 1 ou 2. Puisque α est de degré impair sur K , on a donc $n = 1$.

9) 1. Il résulte de l'exercice 1 que $X^3 - X + 1$ est irréductible sur \mathbb{Q} donc K/\mathbb{Q} est une extension de degré 3.

2. On considère l'application \mathbb{Q} -linéaire $\varphi : K \rightarrow K$ telle que $\varphi(x) = ax$. C'est un isomorphisme. La matrice M de φ dans la base $(1, \alpha, \alpha^2)$ est

$$\begin{pmatrix} 1 & 0 & -1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

On vérifie que

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

On a $M^{-1t}(1, 0, 0) = {}^t(0, 1, -1)$. L'inverse de a est donc $\alpha - \alpha^2$.

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 que l'on a $(2 - \alpha^2)a = 1$ et l'inverse de a est donc $2 - \alpha^2$.

10) 1. On vérifie d'abord de P n'a pas de racine dans \mathbb{F}_2 . Par ailleurs, une égalité de la forme $P = (X^2 + aX + 1)(X^2 + bX + 1)$ entraîne à la fois $a + b = 0$ et $a + b = 1$, d'où une contradiction et le fait que P soit irréductible sur \mathbb{F}_2 .

2. Le \mathbb{F}_2 -espace vectoriel K est de dimension 4, d'où $|K| = 16$.

3. On a $\alpha^4 = \alpha + 1$, d'où $\alpha^5 = \alpha^2 + \alpha$, et en particulier, α^5 est distinct de 1. De même on a $\alpha^3 \neq 1$. Ainsi l'ordre de α dans K^* est 15.

4. Supposons F réductible dans K . Soit β une racine de F dans K . Dans ce cas, β^2 et β^4 sont les deux autres racines de F dans K : en effet, on a $0 = (\beta^3 + \beta + 1)^2 = \beta^6 + \beta^2 + 1$, de même $\beta^{12} + \beta^4 + 1 = 0$, et par ailleurs, on a $\beta \neq \beta^2$, $\beta^2 \neq \beta^4$ et $\beta^4 \neq \beta$. On en déduit que $\beta^7 = 1$. On a $\beta \neq 1$, donc β est d'ordre 7 dans K^* , ce qui conduit à une contradiction car $|K^*| = 15$; d'où le fait que F soit irréductible sur K . Pour le démontrer, on peut aussi utiliser l'exercice 11 qui suit. La dimension sur \mathbb{F}_2 de $K[X]/(F)$ est 12, donc le cardinal de $K[X]/(F)$ est 2^{12} .

Dans les exercices qui suivent, si L/K est une extension finie de corps, on notera $[L : K]$ son degré.

11) Soit Ω un corps algébriquement clos contenant L . Soit α une racine de F dans Ω . Si a_n est le coefficient dominant de F , il s'agit de prouver que $\frac{1}{a_n}F$ est le polynôme minimal de α sur L , autrement dit que l'on a $n = [L(\alpha) : L]$. On a

$$[L(\alpha) : K] = [L(\alpha) : K(\alpha)][K(\alpha) : K] = [L(\alpha) : L]d.$$

On a $n = [K(\alpha) : K]$. Puisque d est premier à n , il en résulte que n divise $[L(\alpha) : L]$. L'inégalité $[L(\alpha) : L] \leq n$ entraîne alors le résultat.

12) 1. Soient $(a_i)_{1 \leq i \leq m}$ une base de K/k et $(b_j)_{1 \leq j \leq n}$ une base de L/k . La famille $(a_i b_j)_{i,j}$ est un système générateur ayant au plus mn éléments du k -espace vectoriel KL . Ainsi, KL est une K -algèbre de dimension finie, qui est intègre. Par suite, KL est un corps, car une algèbre intègre A qui est de dimension finie sur un corps, est un corps : en effet, si x_0 est un élément non nul de A , alors x_0 est inversible dans A , comme on le constate en considérant l'endomorphisme de A qui à x associe xx_0 . Par ailleurs, le sous-corps de Ω engendré par K et L contient les sommes finies $\sum a_i b_i$ où $a_i \in K$ et $b_i \in L$, donc contient KL . D'où le résultat.

2. Cette assertion se déduit du fait que le k -espace vectoriel KL contient un système générateur ayant au plus mn éléments.

3. On a

$$[KL : k] = [KL : K]m = [KL : L]n.$$

Les entiers m et n étant premiers entre eux, m divise $[KL : L]$ et n divise $[KL : K]$. Les degrés $[KL : L]$ et $[KL : K]$ divisent $[KL : k]$, les entiers m et n divisent donc $[KL : k]$. Puisque m et n sont premiers entre eux, mn divise $[KL : k]$. D'après l'assertion 1, on a donc $mn = [KL : k]$.

4. On prend $k = \mathbb{Q}$, $K = \mathbb{Q}(\alpha)$ où $\alpha^3 = 2$ et $L = \mathbb{Q}(j\alpha)$ où $j^3 = 1$, $j \neq 1$. On a $[K : \mathbb{Q}] = [L : \mathbb{Q}] = 3$. Vérifions que $[KL : \mathbb{Q}] = 6$. On a

$$\mathbb{Q} \subseteq K \subseteq KL \subseteq \mathbb{Q}(\alpha)\mathbb{Q}(j).$$

Compte tenu de la question 2, on a $[\mathbb{Q}(\alpha)\mathbb{Q}(j) : \mathbb{Q}] = 6$. Ainsi $[KL : \mathbb{Q}] = 3$ ou 6. Si $[KL : \mathbb{Q}] = 3$, on a $KL = K$ et j est dans K , ce qui n'est pas. D'où l'assertion.

5. D'après l'assertion 3, on a $[L(\alpha) : K] = nd$, d'où $[L(\alpha) : L] = n$ et le résultat.

13) 1. Soit $\varphi : K^* \rightarrow K^*$ l'application qui à x associe x^2 . Elle est injective si $p = 2$, donc bijective car K est fini, d'où l'assertion.

2. L'application φ est un morphisme de groupes. Si $p \neq 2$, son noyau, qui est ± 1 , est d'ordre 2. En factorisant φ , on constate ainsi que $|K^{*2}| = (q-1)/2$, puis $|K^2| = (q+1)/2$.

3. Si $p = 2$, cela résulte de l'assertion 1. Supposons $p \geq 3$. D'après 2, Si a est un élément de K , l'ensemble $S = \{a - x^2/x \in K\}$ est de cardinal $(q+1)/2$. On en déduit que $S \cap K^2$ n'est pas vide (principe des tiroirs), d'où le résultat.

4. L'ensemble K^{*2} est un sous-groupe de K^* d'ordre $(q-1)/2$. Si a est dans K^{*2} , on a donc $a^{\frac{q-1}{2}} = 1$. On en déduit que K^{*2} est l'ensemble des racines du polynôme $X^{\frac{q-1}{2}} - 1 \in K[X]$. Par conséquent, si a un élément de K^* tel que $a^{\frac{q-1}{2}} = 1$, alors a est un carré dans K . Inversement, pour tout $x \in K^*$, on a $(x^2)^{\frac{q-1}{2}} = x^{q-1} = 1$. D'où le résultat.

14) Soit p un nombre impair. D'après l'exercice 13, -1 est un carré dans \mathbb{F}_p si et seulement si $(-1)^{\frac{p-1}{2}} = 1$, autrement dit, si et seulement si on a $p \equiv 1 \pmod{4}$. Si 4 divise $p - 3$, le polynôme $X^2 + 1$ est donc irréductible sur \mathbb{F}_p , et K est un corps qui est un \mathbb{F}_p -espace vectoriel de dimension 2. D'où l'assertion.

15) 1. Puisque a et b sont des indéterminées, le polynôme F est irréductible sur K et c'est le polynôme minimal de α sur K . Soient $\alpha_1 = \alpha, \dots, \alpha_n$ les racines de F dans une clôture algébrique de K . On a l'égalité

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

Il en résulte que l'on a

$$\Delta = (-1)^{\frac{n(n-1)}{2}} N_{K(\alpha)/K}(F'(\alpha)),$$

où $N_{K(\alpha)/K}(F'(\alpha))$ désigne la norme de $K(\alpha)$ sur K de $F'(\alpha)$. Par ailleurs, le déterminant du K -endomorphisme φ de $K(\alpha)$ de multiplication par $F'(\alpha)$ est égal à $N_{K(\alpha)/K}(F'(\alpha))$. On vérifie que le coefficient a_{ij} de la i -ème ligne et de la j -ième colonne de la matrice de φ dans la base $(1, \alpha, \dots, \alpha^{n-1})$ du K -espace vectoriel $K(\alpha)$ est donné par les égalités suivantes :

$$a_{11} = a, \quad a_{n1} = n, \quad a_{ij} = (1 - n)a \quad \text{si } 2 \leq j \leq n \text{ et } i = j,$$

$$a_{ij} = -nb \quad \text{si } 2 \leq j \leq n \text{ et } i = j - 1, \quad a_{ij} = 0 \quad \text{sinon.}$$

En développant le déterminant de cette matrice suivant la première colonne on obtient alors le résultat annoncé.

2. Pour tout entier $n \geq 1$, il existe un unique polynôme $\Delta(A, B)$ dans l'anneau des polynômes $\mathbb{Z}[A, B]$ ayant la propriété suivante : pour tout corps K et tout polynôme unitaire $f = X^n + aX + b \in K[X]$, le discriminant de f est $\Delta(a, b)$. En prenant pour K le corps $\mathbb{Q}(A, B)$, on constate que $\Delta(A, B)$ est le discriminant du polynôme $X^n + AX + B$ de $K[X]$, qui a été déterminé dans la question 1. D'où le résultat.

16) 1. On peut supposer que F est unitaire. Supposons que $\gamma := \alpha - \beta \in K$ et posons

$$F = X^n + \sum_{i=0}^{n-1} a_i X^i \quad \text{avec } n \geq 1.$$

Notons G le polynôme $F(X + \gamma)$. On a $G(\beta) = 0$ et G est un polynôme unitaire de degré n à coefficients dans K car γ est dans K . Puisque F est le polynôme minimal de β , on en déduit que F divise G , puis que $F = G$. En égalant les coefficients de F et G de degré

$n - 1$, on obtient que $a_{n-1} = n\gamma + a_{n-1}$, d'où $n\gamma = 0$. Le corps K étant de caractéristique 0, cela entraîne $\gamma = 0$, d'où une contradiction et le résultat.

2. Supposons par exemple $p = 2$, $K = \mathbb{F}_2$ et considérons le polynôme $F = X^2 + X + 1$. On constate alors que l'assertion précédente est fausse : si α est une racine de F dans une clôture algébrique de \mathbb{F}_2 , l'autre racine de F est $\alpha + 1$. Pour tout nombre premier p , le polynôme $X^p - X + 1 \in \mathbb{F}_p[X]$ fournit en fait un contre exemple à l'assertion 1 (cf. l'exercice 20).

17) On a $(\overline{\mathbb{Q}} \cap \mathbb{R})(i) \subseteq \overline{\mathbb{Q}}$. Inversement, soit z un élément de $\overline{\mathbb{Q}}$. Il existe x et y réels tels que $z = x + iy$. Il s'agit de montrer que x et y sont algébriques. Le conjugué \bar{z} de z est dans $\overline{\mathbb{Q}}$; en effet, la conjugaison complexe fixe les éléments de \mathbb{Q} , par suite, z étant racine d'un polynôme à coefficients dans \mathbb{Q} , il en est de même de \bar{z} . On a donc

$$x = \frac{z + \bar{z}}{2} \in \overline{\mathbb{Q}} \quad \text{et} \quad y = \frac{z - \bar{z}}{2i} \in \overline{\mathbb{Q}},$$

d'où le résultat.

18) 1. On suppose F réductible sur K . Soit g un polynôme unitaire non constant de $K[X]$ de degré $k < p$ qui divise F . Soit c le terme constant de g . Soit u une racine de F dans une clôture algébrique Ω de K . Les racines de F dans Ω sont les ζu , où ζ parcourt les racines p -ièmes de l'unité de Ω . L'élément $\pm c$ est le produit de k de ces racines, d'où

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

Par ailleurs, puisque l'on a $1 \leq k < p$, il existe des entiers r et s tels que l'on ait $rk + sp = 1$. On a ainsi

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

Il en résulte que $u\eta^r$ appartient à K , d'où $u^p \in K^p$ i.e. a est K^p . Cela conduit à une contradiction, d'où le résultat.

[Si K est fini de caractéristique p , tout élément de K est une puissance p -ième dans K , comme on le constate en considérant le morphisme de $K^* \rightarrow K^*$ qui à x associe x^p . Si a est dans K , il existe donc $b \in K$ tel que $a = b^p$, de sorte que $X^p - a = (X - b)^p$].

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

19) D'abord F n'est pas inversible dans $\mathbb{Z}[X]$ car $n \geq 1$. Supposons qu'il existe deux polynômes g et h dans $\mathbb{Z}[X]$ tels que $F = gh$. Il s'agit alors de prouver que g ou h vaut ± 1 . Notons $s : \mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ la surjection canonique. Soit

$$\varphi : \mathbb{Z}[X] \rightarrow (\mathbb{Z}/p\mathbb{Z})[X]$$

l'application définie par

$$\varphi\left(\sum u_i X^i\right) = \sum_i s(u_i) X^i.$$

C'est un homomorphisme d'anneaux. Il résulte des hypothèses faites que l'on a

$$\varphi(F) = \varphi(g)\varphi(h) = s(a_n)X^n.$$

On en déduit qu'il existe des entiers λ, μ et $k \geq 0$ tels que l'on ait

$$\varphi(g) = s(\lambda)X^k \quad \text{et} \quad \varphi(h) = s(\mu)X^{n-k}.$$

Démontrons que l'on a

$$(1) \quad k = 0 \quad \text{ou} \quad k = n.$$

Supposons pour cela que l'on ait $0 < k < n$. Le polynôme $g - \lambda X^k$ appartient à $p\mathbb{Z}[X]$. Puisque $k > 0$, le terme constant de g est divisible par p . De même, puisque $k < n$ le terme constant de h est aussi divisible par p . Cela contredit le fait que p^2 ne divise pas a_0 , d'où la condition (1).

Supposons $k = 0$. On a $\varphi(g) = s(\lambda)$. Si le degré de g est ≥ 1 , le coefficient dominant de g est donc divisible par p , ce qui entraîne que p divise a_n , d'où une contradiction. Par suite, le degré de g est nul, autrement dit, g est un entier. Puisque g divise F et que les a_i sont premiers entre eux, on a donc $g = \pm 1$. De même si $k = n$, on montre que l'on a $h = \pm 1$. D'où l'exercice.

20) 1. Posons $F = X^p - X + u$. Soit α une racine de F dans une clôture algébrique Ω de \mathbb{F}_p . Les racines de F dans Ω sont les $a + \alpha$ où a parcourt \mathbb{F}_p . Supposons qu'il existe un polynôme $G \in \mathbb{F}_p[X]$ qui divise F dont le degré n est tel que $1 \leq n < p$. Il existe des éléments $a_{i_1}, \dots, a_{i_n} \in \mathbb{F}_p$ tels que les racines de G soient les $\alpha + a_{i_k}$ pour k entre 1 et n . On a

$$\sum_{k=1}^n \alpha + a_{i_k} \in \mathbb{F}_p,$$

par suite $n\alpha$ est dans \mathbb{F}_p . Puisque n est non nul modulo p , il en résulte que α est dans \mathbb{F}_p , ce qui conduit à une contradiction, car α^p est distinct de α . D'où le résultat.

2) Posons $P = X^p - X + a$ et supposons P réductible sur \mathbb{Q} . Dans ce cas, P est réductible dans $\mathbb{Z}[X]$, autrement dit il existe un polynôme unitaire non constant H dans $\mathbb{Z}[X]$ de degré $n < p$ qui divise P . Notons \overline{P} et \overline{H} les polynômes de $\mathbb{F}_p[X]$ déduit respectivement de P et H en réduisant leurs coefficients modulo p . Le polynôme \overline{H} , qui est de degré n , divise ainsi \overline{P} dans $\mathbb{F}_p[X]$. On obtient une contradiction car d'après l'assertion 1 et l'hypothèse faite sur a , \overline{P} est irréductible sur \mathbb{F}_p .

21) Soit Ω une clôture algébrique de K . Supposons F irréductible sur K . Si α est une racine de F dans Ω , le degré de $K(\alpha)$ sur K est n . Inversement, supposons que F soit réductible sur K . Il existe deux polynômes non constants G et H de $K[X]$ de degré $< n$ tels que $F = GH$. Nécessairement G ou H est de degré $\leq n/2$. Si tel est le cas de G et si β est une racine de G dans Ω , on a $[K(\beta) : K] \leq n/2$. D'où le résultat.

22) 1. Soit G le polynôme $F(X+1)$. On a

$$G = X^4 + 4X^3 + 6X^2 + 4X + 2.$$

D'après le critère d'Eisenstein, G est irréductible dans $\mathbb{Z}[X]$ et il en est de même de F .

2. Notons encore F le polynôme de $\mathbb{F}_p[X]$ que l'on obtient par réduction modulo p . Si $p = 2$, on a $F = (X+1)^4$, d'où l'assertion dans ce cas. Supposons $p \geq 3$. Soient Ω une clôture algébrique de \mathbb{F}_p et K l'extension de degré 2 de \mathbb{F}_p contenue dans Ω . Le groupe K^* est cyclique d'ordre $p^2 - 1$. Puisque 8 divise $p^2 - 1$, le groupe K^* possède donc un sous-groupe H d'ordre 8 (cf. l'exercice 44). Soit α un générateur de H . On a $\alpha^8 = 1$ et $\alpha^4 \neq 1$. On déduit de l'égalité $\alpha^8 - 1 = (\alpha^4 - 1)(\alpha^4 + 1)$ que $\alpha^4 + 1 = 0$ i.e. que α est une racine de F dans K . Puisque K est une extension de degré 2 de \mathbb{F}_p , il résulte alors de l'exercice 21 que F est réductible sur \mathbb{F}_p . D'où le résultat.

3. Posons $P = (X^2 - a)(X^2 - b)(X^2 - ab)$. Si p divise ab , 0 est une racine de P modulo p . Par ailleurs, suivant la parité de a , 0 ou 1 est une racine de P modulo 2. On peut donc supposer que l'on a $p \geq 3$ et que p ne divise pas ab . Tout revient à vérifier que l'un des entiers a , b et ab est un carré dans \mathbb{F}_p . Supposons que ni a ni b ne soient des carrés dans \mathbb{F}_p . Puisque ab n'est pas nul modulo p , on a $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$. Il résulte alors de l'assertion 4 de l'exercice 13, que l'on a

$$a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

On en déduit la congruence

$$(ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

ce qui prouve que ab est un carré modulo p . D'où le résultat.

23) 1. On a $X^p - 1 = (X - 1)\Phi_p(X)$. Posons $Y = X - 1$. On a

$$\Phi_p(Y+1) = \sum_{k=1}^p C_p^k Y^{k-1}.$$

Par ailleurs, pour tout k compris entre 1 et $p-1$, p divise C_p^k et l'on a $C_p^1 = p$, $C_p^p = 1$. D'après le critère d'Eisenstein, $\Phi_p(Y+1)$ est irréductible sur \mathbb{Q} et il en est de même de $\Phi_p(X)$. Par ailleurs, on a $\Phi_p(\zeta) = 0$. Il en résulte que $\Phi_p(X)$ est le polynôme minimal de ζ sur \mathbb{Q} , d'où $[K : \mathbb{Q}] = p - 1$.

2. On a

$$\cos \frac{2\pi}{p} = \frac{\zeta + \zeta^{-1}}{2},$$

d'où l'assertion.

3. Posons $K^+ = \mathbb{Q}(\cos \frac{2\pi}{p})$. Si $p = 2$, on a $K^+ = \mathbb{Q}$. Supposons $p \geq 3$. L'élément ζ n'est pas dans K^+ car K^+ est contenu dans \mathbb{R} et ζ n'est pas réel. Par ailleurs, ζ est racine d'un polynôme de degré 2 à coefficients dans K^+ , à savoir $X^2 - (\zeta + \zeta^{-1})X + 1$, qui est donc le polynôme minimal de ζ sur K^+ . L'extension K/K^+ est donc de degré 2. Par suite, le degré de K^+/\mathbb{Q} est $\frac{p-1}{2}$.

4. On suppose $p = 5$. Posons

$$Y = X + \frac{1}{X}.$$

On vérifie que l'on a

$$\Phi_5(X) = X^2(Y^2 + Y - 1).$$

Ainsi $\zeta + \zeta^{-1}$ est racine du polynôme $Y^2 + Y - 1 \in \mathbb{Z}[Y]$. Puisque $\cos \frac{2\pi}{5}$ est positif, on en déduit que (en notant $\sqrt{5}$ la racine carrée positive de 5)

$$\cos \frac{2\pi}{5} = \frac{-1 + \sqrt{5}}{4},$$

et le résultat.

5. On écrit que l'on a

$$\Phi_7(X) = X^3 \left(X^3 + \frac{1}{X^3} + X^2 + \frac{1}{X^2} + X + \frac{1}{X} + 1 \right).$$

Soit ζ une racine primitive 7-ième de l'unité. En posant comme ci-dessus

$$Y = X + \frac{1}{X},$$

on constate que $2 \cos \frac{2\pi}{7} = \zeta + \zeta^{-1}$ est racine du polynôme $Y^3 + Y^2 - 2Y - 1 \in \mathbb{Z}[Y]$. Puisque le degré de $\zeta + \zeta^{-1}$ sur \mathbb{Q} est 3 (assertion 3), c'est donc son polynôme minimal sur \mathbb{Q} .

2. Séparabilité

24) Supposons la caractéristique de K différente de 3. Le polynôme dérivé de F , qui est $3(X^2 - 1)$, est premier avec F , ce qui montre que F est séparable dans ce cas et donc que α est séparable sur K . Si la caractéristique de K vaut 3, on a $F = (X - 1)^3$, d'où $\alpha = 1$ puis $K(\alpha) = K$ et l'exercice.

25) Si f est de la forme $g(X^p)$, le polynôme dérivé de f est nul, donc f est inséparable. Inversement, supposons f inséparable. Posons $f = \sum_{i=0}^n a_i X^i$. On a

$$f' = \sum_{i=1}^n i a_i X^{i-1}.$$

D'après l'hypothèse faite, on a $f' = 0$, d'où $i a_i = 0$ pour $i = 1, \dots, n$. Si a_i n'est pas nul, i est donc divisible par p , ce qui entraîne le résultat.

26) Soient α un élément de L et F son polynôme minimal sur K . Il s'agit de montrer que F est séparable. Dans le cas contraire, F étant irréductible, il existe $G \in K[X]$ tel que $F(X) = G(X^p)$ (exercice 25). Il en résulte que le degré de F est multiple de p , par suite p divise le degré de L sur K . D'où une contradiction et le résultat.

27) Posons $L = K(\alpha, \beta)$. Soit Ω une clôture algébrique de K contenant L . Soit d le degré de L sur K . Le corps K étant de caractéristique 0, l'extension L/K est séparable. Par suite, il existe d plongements $\sigma_1, \dots, \sigma_d$ de L dans Ω égaux à l'identité sur K . Vérifions qu'il existe un entier n tel que pour tous i et j compris entre 1 et d tels que $i \neq j$, on ait

$$(1) \quad \sigma_i(\alpha + n\beta) \neq \sigma_j(\alpha + n\beta).$$

Supposons le contraire. Pour tout entier $r \in \mathbb{Z}$ il existe alors deux indices i et j distincts tels que $\sigma_i(\alpha + r\beta) = \sigma_j(\alpha + r\beta)$. Par ailleurs, \mathbb{Z} est infini et l'ensemble des couples (i, j) considérés est fini. On en déduit l'existence de deux entiers r et s distincts et d'un couple (i, j) tels que $i \neq j$ et que $\sigma_i(\alpha + r\beta) = \sigma_j(\alpha + r\beta)$ et $\sigma_i(\alpha + s\beta) = \sigma_j(\alpha + s\beta)$. Il en résulte que $\sigma_i(\alpha) = \sigma_j(\alpha)$ et $\sigma_i(\beta) = \sigma_j(\beta)$, d'où $\sigma_i = \sigma_j$ et une contradiction. Cela prouve la condition (1). L'élément $\alpha + n\beta$ appartient à L et d'après (1) son polynôme minimal sur K a au moins d racines. Le degré de $\alpha + n\beta$ sur K est donc égal à d . On en déduit que $K(\alpha + n\beta) = L$ et le résultat.

28) 1. L'élément X est algébrique sur K de degré p . En effet, considérons le polynôme $F = T^p - X^p \in K[T]$. On a $F = (T - X)^p$, de sorte que X est la seule racine de F dans une clôture algébrique de K . Puisque X n'appartient pas à K , l'élément X^p n'est pas une puissance p -ième dans K . D'après l'exercice 18, F est donc irréductible sur K , et est

ainsi le polynôme minimal de X sur K . De même, Y est algébrique sur $K(X)$ de degré p , comme on le constate en considérant le polynôme $T^p - Y^p \in K(X)[T]$ qui est irréductible sur $K(X)$. Compte tenu du fait que l'on a $L = K(X, Y)$, on en déduit le résultat.

2. Supposons qu'il existe $\theta \in L$ tel que $L = K(\theta)$. Il existe des éléments F et G dans $\mathbb{F}_p[X, Y]$ tels que l'on ait

$$\theta = \frac{F(X, Y)}{G(X, Y)}.$$

Puisque L est de caractéristique p , on a

$$\theta^p = \frac{F(X^p, Y^p)}{G(X^p, Y^p)},$$

et donc θ^p appartient à K . On en déduit que le degré de θ sur K est au plus p , ce qui contredit le fait que L/K soit de degré p^2 . D'où le résultat.

3. Extensions galoisiennes, groupe de Galois d'un polynôme

29) Soit f un automorphisme de \mathbb{R} . Supposons f différent de l'identité. Prouvons que f est strictement croissant. Il suffit pour cela de vérifier que pour tout $a > 0$ on a $f(a) > 0$. Si a est un réel > 0 , il existe $x \in \mathbb{R}^*$ tel que $a = x^2$, d'où $f(a) = f(x)^2$. On a donc $f(a) \geq 0$ et f étant injective, on a $f(a) > 0$; d'où l'assertion. Par hypothèse, il existe $y \in \mathbb{R}$ tel que $f(y) \neq y$. Supposons par exemple $y < f(y)$. Puisque \mathbb{Q} est dense dans \mathbb{R} , il existe $r \in \mathbb{Q}$ tel que l'on ait $y < r < f(y)$. Par ailleurs, f fixe les éléments de \mathbb{Q} car f fixe les entiers. On obtient ainsi $f(y) < f(r) = r$ et une contradiction. D'où l'exercice.

30) On vérifie que $F = X^4 - 2X^2 - 1$ est irréductible sur \mathbb{Q} . Il suffit pour cela de prouver qu'il est irréductible dans $\mathbb{Z}[X]$: d'abord F n'a pas de racines dans \mathbb{Z} et une égalité de la forme $F = (X^2 + aX + 1)(X^2 + bX - 1)$ entraîne $a = b = 0$, d'où une contradiction et l'assertion. Le degré de K sur \mathbb{Q} est donc 4. Par ailleurs, F possède deux racines réelles, à savoir $\pm\sqrt{1+\sqrt{2}}$ et deux racines non réelles. Il en résulte que toutes les racines de F ne sont pas dans $\mathbb{Q}(\alpha)$, ce qui entraîne le résultat.

31) 1. Posons $L = \mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt{3})$. Vérifions que l'on a $K = L$. Puisque $\sqrt{2}$ et $\sqrt{3}$ sont dans L , le corps K est contenu dans L . Inversement, posons $\alpha = \sqrt{2} + \sqrt{3}$. On a $\alpha^2 - 2\alpha\sqrt{2} - 1 = 0$, d'où l'on déduit que $\sqrt{2}$ appartient à K et qu'il en est de même de $\sqrt{3}$. On en déduit que L est contenu dans K , d'où $L = K$. Par ailleurs, le composé de deux extensions galoisiennes de \mathbb{Q} est aussi galoisienne. D'où le résultat.

2. Le polynôme minimal de $\sqrt{2}$ sur \mathbb{Q} est $X^2 - 2$ et celui de $\sqrt{3}$ sur $\mathbb{Q}(\sqrt{2})$ est $X^2 - 3$. Le degré de K sur \mathbb{Q} est donc 4 et le groupe $\text{Gal}(K/\mathbb{Q})$ est d'ordre 4. On vérifie que le polynôme minimal de α sur \mathbb{Q} est $F = X^4 - 10X^2 + 1$ et que l'on a

$$F = (X^2 - \alpha^2) \left(X^2 - \frac{1}{\alpha^2} \right).$$

Les éléments de $\text{Gal}(K/\mathbb{Q})$ sont donc $\sigma_1, \dots, \sigma_4$, où σ_1 est l'identité de K , et où σ_2, σ_3 et σ_4 sont définis par les égalités

$$\sigma_2(\alpha) = -\alpha, \quad \sigma_3(\alpha) = \frac{1}{\alpha}, \quad \sigma_4(\alpha) = -\frac{1}{\alpha}.$$

Les automorphismes σ_i pour $i \neq 1$ sont d'ordre 2, par suite $\text{Gal}(K/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

32) 1. On vérifie d'abord que α est une racine du polynôme

$$F = X^4 - 2aX^2 + a^2 - b.$$

Supposons $b(a^2 - b) = 0$. Si $b = 0$, on a $F = (X^2 - a)^2$ puis $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{a})$. Si $a^2 - b = 0$, on a $\mathbb{Q}(\alpha) = \mathbb{Q}$ ou bien $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2a})$. Sous l'hypothèse faite, $\mathbb{Q}(\alpha)$ est donc une extension galoisienne de \mathbb{Q} .

Supposons $b(a^2 - b) \neq 0$. Dans ce cas, on vérifie que F est séparable. Les racines de F sont $\pm\alpha$ et $\pm\beta$, où β est un élément de \mathbb{C} . On a $(\alpha\beta)^2 = a^2 - b$. Puisque $a^2 - b$ est un carré non nul, on a $\alpha \neq 0$ et β est donc dans $\mathbb{Q}(\alpha)$. Par suite, les racines de F appartiennent à $\mathbb{Q}(\alpha)$. En particulier, les conjugués de α sur \mathbb{Q} sont dans $\mathbb{Q}(\alpha)$, ce qui signifie que $\mathbb{Q}(\alpha)/\mathbb{Q}$ est une extension normale. D'où le résultat.

2. On a dans ce cas $F = (X^2 - 11)(X^2 - 3)$, de sorte que $\mathbb{Q}(\alpha)$ est le corps $\mathbb{Q}(\sqrt{3})$ ou bien $\mathbb{Q}(\sqrt{11})$, qui est donc une extension galoisienne de \mathbb{Q} .

3. Posons $K = \mathbb{Q}(\alpha)$. On vérifie que le polynôme de $\mathbb{F}_5[X]$ déduit de F par réduction modulo 5 est irréductible sur \mathbb{F}_5 (le vérifier en exercice). Il en résulte que F est irréductible sur \mathbb{Q} et que l'extension K/\mathbb{Q} est de degré 4. Supposons qu'elle soit galoisienne. Dans ce cas, K est le corps de décomposition de F et l'on déduit du rappel 3 que le groupe $\text{Gal}(K/\mathbb{Q})$ possède un élément d'ordre 4. Par suite, le groupe $\text{Gal}(K/\mathbb{Q})$ est cyclique d'ordre 4. Il contient donc un unique sous-groupe d'ordre 2. Par ailleurs, si β est une racine de F distincte de $\pm\alpha$, on a $(\alpha\beta)^2 = 13$, de sorte que le corps $\mathbb{Q}(\sqrt{13})$ est contenu dans K . L'égalité, $\alpha^2 = 4 + \sqrt{3}$ entraîne que $\mathbb{Q}(\sqrt{3})$ est aussi contenu dans K . Les extensions $K/\mathbb{Q}(\sqrt{13})$ et $K/\mathbb{Q}(\sqrt{3})$ sont galoisiennes et leurs groupes de Galois sont des sous-groupes distincts d'ordre 2 de $\text{Gal}(K/\mathbb{Q})$. Cela conduit à une contradiction, ce qui prouve notre assertion.

4. Vérifions que le discriminant Δ de F est

$$(1) \quad \Delta = 2^8 b^2 (a^2 - b).$$

Notons $\pm\alpha$ et $\pm\beta$ les racines de F dans \mathbb{C} . Si F' est le polynôme dérivé de F , on a

$$\Delta = F'(\alpha)F'(-\alpha)F'(\beta)F'(-\beta).$$

Par ailleurs, on a $F' = 4X(X^2 - a)$ et $(\alpha\beta)^2 = a^2 - b$, d'où il résulte que l'on a l'égalité

$$\Delta = 2^8(a^2 - b)(\alpha^2 - a)^2(\beta^2 - a)^2.$$

On a

$$(\alpha^2 - a)(\beta^2 - a) = (\alpha\beta)^2 - a(\alpha^2 + \beta^2) + a^2,$$

et en explicitant la deuxième fonction symétrique des racines de F on obtient

$$\alpha^2 + \beta^2 = 2a,$$

ce qui entraîne (1).

5. Posons $K = \mathbb{Q}(\alpha)$. Puisque F est irréductible sur \mathbb{Q} , il résulte de la question 1 que l'extension K/\mathbb{Q} est galoisienne de degré 4. D'après la formule (1), le discriminant de F est un carré dans \mathbb{Z} . Par suite, le groupe de Galois G de K sur \mathbb{Q} est isomorphe à un sous-groupe d'ordre 4 de \mathbb{A}_4 (cf. par exemple l'exercice 37). Il n'est pas cyclique car les seuls éléments d'ordre 4 de \mathbb{S}_4 sont les 4-cycles et ils ne sont pas dans \mathbb{A}_4 . Ainsi G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.

6. Par hypothèse, il existe $t \in \mathbb{Z}$ tel que l'on ait $a^2 - b = bt^2$. Les racines de F sont $\pm\alpha, \pm\beta$ avec

$$\beta = \frac{\sqrt{bt}}{\alpha}.$$

On a $\alpha^2 = a + \sqrt{b}$, donc \sqrt{b} appartient à $K = \mathbb{Q}(\alpha)$ et β est donc aussi dans K . Ainsi, l'extension K/\mathbb{Q} est galoisienne de degré 4. Soit σ l'élément du groupe de Galois de K sur \mathbb{Q} défini par l'égalité

$$\sigma(\alpha) = \beta.$$

Montrons que σ est d'ordre 4, ce qui prouvera l'assertion. Vérifions pour cela que l'on a

$$(2) \quad \sigma(\sqrt{b}) = -\sqrt{b}.$$

Supposons le contraire. On a alors $\sigma(\sqrt{b}) = \sqrt{b}$. De l'égalité $\alpha^2 = a + \sqrt{b}$ on déduit que l'on a $\sigma(\alpha^2) = a + \sigma(\sqrt{b})$, d'où $\sigma\alpha^2 = \alpha^2$, autrement dit,

$$\left(\frac{\sigma\alpha}{\alpha}\right)^2 = 1,$$

ce qui conduit à $\sigma(\alpha) = \pm\alpha$. On obtient ainsi une contradiction car β est distinct de $\pm\alpha$. Cela démontre l'égalité (2). Par suite, on a

$$\sigma(\beta) = \frac{\sigma(\sqrt{b})t}{\beta} = \left(\frac{\sigma(\sqrt{b})}{\sqrt{b}}\right)\alpha = -\alpha.$$

Il en résulte que σ n'est pas d'ordre 2, ce qui entraîne le résultat.

33) Soient α la racine n -ième positive de 2 et K le corps $\mathbb{Q}(\alpha)$. Le polynôme $X^n - 2$ étant irréductible sur \mathbb{Q} (critère d'Eisenstein), K est une extension de \mathbb{Q} de degré n . Par ailleurs, les racines de F dans \mathbb{C} sont les $\zeta\alpha$, où ζ est une racine n -ième de l'unité. Puisque $n \geq 3$, il existe une racine n -ième de l'unité ζ qui n'est pas dans \mathbb{R} , et $\zeta\alpha$ n'est donc pas dans K . En particulier, K/\mathbb{Q} n'est pas galoisienne.

34) 1. Le polynôme minimal de ζ est le p -ième polynôme cyclotomique Φ_p qui est de degré $p - 1$ (exercice 23). Par suite, $\mathbb{Q}(\zeta)/\mathbb{Q}$ est une extension de degré $p - 1$. Par ailleurs, les racines de Φ_p sont les ζ^k , où k parcourt les entiers compris entre 1 et $p - 1$. Puisqu'elles appartiennent à $\mathbb{Q}(\zeta)$, l'extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ est donc galoisienne.

2. Soit $\varphi : \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \rightarrow (\mathbb{Z}/p\mathbb{Z})^*$ l'application définie comme suit : soit σ un élément de $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Puisque $\sigma(\zeta)$ est une racine de Φ_p , il existe un unique entier k tel que $1 \leq k \leq p - 1$ et que $\sigma(\zeta) = \zeta^k$. On pose

$$\varphi(\sigma) = k \text{ mod. } p.$$

C'est un homomorphisme de groupes. En effet, soient σ et τ deux éléments de $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ et k, k' deux entiers entre 1 et $p - 1$ tels que $\sigma(\zeta) = \zeta^k$ et $\tau(\zeta) = \zeta^{k'}$. On a $(\sigma\tau)(\zeta) = \zeta^{kk'}$, d'où $\varphi(\sigma\tau) = kk' \text{ mod. } p$ puis l'assertion. Par ailleurs, si σ est un élément du noyau de φ , on a $\sigma(\zeta) = \zeta$, de sorte que σ est l'identité de $\mathbb{Q}(\zeta)$, donc σ est injectif. Puisque les groupes $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ et $(\mathbb{Z}/p\mathbb{Z})^*$ sont de même ordre $p - 1$, il en résulte que σ est surjectif. D'où le résultat.

35) Soit α une racine p -ième de 2 dans \mathbb{C} . Le polynôme F est irréductible sur \mathbb{Q} , donc le corps $\mathbb{Q}(\alpha)$ est une extension de \mathbb{Q} de degré p . Les racines de F dans \mathbb{C} sont les $\zeta\alpha$, où ζ est une racine p -ième de l'unité. On en déduit que le corps de décomposition L de F est le composé $\mathbb{Q}(\zeta)\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta, \alpha)$, où ζ est une racine primitive p -ième de l'unité. D'après l'assertion 2 de l'exercice 12, son degré sur \mathbb{Q} est donc $p(p - 1)$.

36) Soient a_n le coefficient dominant de F et $\alpha_1, \dots, \alpha_n$ les racines de F dans Ω . Le discriminant de F est

$$\Delta = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

En particulier, Δ est un carré dans le corps de décomposition de F . D'où l'assertion.

37) Soient $\alpha_1, \dots, \alpha_n$ les racines de f dans \mathbb{C} et Δ le discriminant de f . On a

$$\Delta = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Soit σ un élément de $\text{Gal}(f)$. On a l'égalité

$$\sigma\left(\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)\right) = \prod_{1 \leq i < j \leq n} \frac{\sigma(\alpha_i) - \sigma(\alpha_j)}{\alpha_i - \alpha_j} (\alpha_i - \alpha_j).$$

Notons encore σ l'image de σ dans \mathbb{S}_n et $\varepsilon(\sigma)$ sa signature. On en déduit que l'on a

$$(1) \quad \sigma\left(\prod_{1 \leq i < j \leq n} \alpha_i - \alpha_j\right) = \varepsilon(\sigma) \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

Par ailleurs, l'image de $\text{Gal}(f)$ dans \mathbb{S}_n est contenue dans \mathbb{A}_n si et seulement si pour tout $\sigma \in \text{Gal}(f)$ on a $\varepsilon(\sigma) = 1$. D'après (1) cette condition signifie que

$$\prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$

appartient à \mathbb{Q} , autrement dit que Δ est un carré dans \mathbb{Q} . D'où l'exercice.

38) 1. Soit L le corps de décomposition de F dans \mathbb{C} . Le groupe de Galois $\text{Gal}(L/\mathbb{Q})$ est isomorphe à un sous-groupe de \mathbb{S}_3 , en particulier le degré de L sur \mathbb{Q} divise 6. D'après l'exercice 34, $\mathbb{Q}(\sqrt{\Delta}, \alpha)$ est contenu dans L .

a) Supposons que Δ soit un carré dans \mathbb{Q} . L'image de $\text{Gal}(L/\mathbb{Q})$ dans \mathbb{S}_3 est alors contenue dans \mathbb{A}_3 (exercice 37) et le degré de L sur \mathbb{Q} divise 3. Puisque $\mathbb{Q}(\alpha)/\mathbb{Q}$ est une extension de degré 3, on a donc $L = \mathbb{Q}(\alpha)$. D'où l'assertion, car d'après l'hypothèse faite on a $\mathbb{Q}(\sqrt{\Delta}, \alpha) = \mathbb{Q}(\alpha)$.

b) Supposons que Δ ne soit pas un carré dans \mathbb{Q} . Dans ce cas, le degré de l'extension $\mathbb{Q}(\sqrt{\Delta}, \alpha)/\mathbb{Q}$ est égal à 6, ce qui entraîne le résultat.

2. Supposons l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ galoisienne. Dans ce cas, les racines de F sont dans $\mathbb{Q}(\alpha)$ et l'on a $L = \mathbb{Q}(\alpha)$. Par suite, Δ est un carré dans ce corps. Puisque le degré de $\mathbb{Q}(\alpha)$ sur \mathbb{Q} est 3, il en résulte que Δ est un carré dans \mathbb{Q} . Inversement, si Δ est un carré dans \mathbb{Q} , le corps de décomposition de F est $\mathbb{Q}(\alpha)$ (assertion 1). D'où le résultat.

3. Compte tenu de 2, il suffit de rechercher des polynômes irréductibles sur \mathbb{Q} de degré 3 de la forme $X^3 + pX + q \in \mathbb{Z}[X]$ dont le discriminant $\Delta = -(4p^3 + 27q^2)$ est (resp. n'est pas) un carré dans \mathbb{Q} .

Prenons $p = -3$ et $q = 1$. On a $\Delta = 81$ et le polynôme $X^3 - 3X + 1$ est irréductible sur \mathbb{Q} . Si α est l'une de ses racines, l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est donc galoisienne de degré 3.

En prenant $p = q = 1$, on a $\Delta = -31$, le polynôme $X^3 + X + 1$ est irréductible et si α est l'une de ses racines, l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est non galoisienne de degré 3.

4. Posons $F = X^3 - 2X + 2$. Il est irréductible sur \mathbb{Q} et son discriminant est égal à -4×19 . Le corps $\mathbb{Q}(\sqrt{-19})$ est contenu dans le corps de décomposition L de F . L'extension $L/\mathbb{Q}(\sqrt{-19})$ est galoisienne de degré 3 et son groupe de Galois est cyclique d'ordre 3.

Étant donné un nombre premier p et un polynôme $f \in \mathbb{Z}[X]$, on notera dans ce qui suit $r_p(f)$ le polynôme de $\mathbb{F}_p[X]$ déduit de f en réduisant ses coefficients modulo p .

39) 1. La décomposition $r_5(f)$ en produit de polynômes irréductibles de $\mathbb{F}_5[X]$ est

$$(1) \quad r_5(f) = (X + 1)(X^3 + 4X^2 + X + 2).$$

Le polynôme dérivé de $X^3 + 4X^2 + X + 2 \in \mathbb{F}_5[X]$ n'est pas nul. On en déduit que $r_5(f)$ est séparable et que f l'est aussi. Identifions $\text{Gal}(f)$ à un sous-groupe de \mathbb{S}_4 . Il s'agit de prouver que $\text{Gal}(f)$ est un sous-groupe transitif de \mathbb{S}_4 . L'égalité (1) entraîne l'existence d'un cycle d'ordre 3 dans $\text{Gal}(f)$. Il en résulte que si $\text{Gal}(f)$ n'est pas transitif, il existe un point fixe de $\{1, 2, 3, 4\}$ sous l'action de $\text{Gal}(f)$, autrement dit, que f a une racine dans \mathbb{Q} . On constate que ce n'est pas le cas en utilisant l'exercice 1. D'où l'assertion.

2. Le discriminant de f est $2^{12} \cdot 3^4$ (exercice 15), qui est un carré dans \mathbb{Q} , donc $\text{Gal}(f)$ est contenu dans \mathbb{A}_4 (exercice 37). D'après (1), $\text{Gal}(f)$ possède un élément d'ordre 3. Par ailleurs, f étant irréductible de degré 4, l'ordre de $\text{Gal}(f)$ est divisible par 4. Par suite, 12 divise l'ordre de $\text{Gal}(f)$, d'où $\text{Gal}(f) = \mathbb{A}_4$.

3. Supposons qu'il existe une extension quadratique K de \mathbb{Q} contenue dans L . L'extension L/K est galoisienne de degré 6, de sorte que le groupe de Galois de L sur K est un sous-groupe d'ordre 6 de $\text{Gal}(L/\mathbb{Q})$. Puisque $\text{Gal}(L/\mathbb{Q})$ est isomorphe à \mathbb{A}_4 , il suffit de prouver que \mathbb{A}_4 n'a pas de sous-groupe d'ordre 6. Supposons qu'il existe un tel sous-groupe H de \mathbb{A}_4 . Il est d'indice 2 dans \mathbb{A}_4 , donc distingué dans \mathbb{A}_4 . Le groupe \mathbb{A}_4/H étant d'ordre 2, on en déduit que pour tout α dans \mathbb{A}_4 , l'élément α^2 est dans H . Cela entraîne en particulier que tous les 3-cycles appartiennent à H ; en effet, si α est un 3-cycle, on a $\alpha = \alpha^4 = (\alpha^2)^2$. Or il y a huit 3-cycles dans \mathbb{A}_4 . Cela contredit l'existence de H . D'où le résultat.

40) 1. La décomposition $r_3(f)$ en produit de polynômes irréductibles de $\mathbb{F}_3[X]$ est

$$(1) \quad r_3(f) = (X + 2)(X^3 + X^2 + X + 2).$$

On en déduit que $r_3(f)$ est séparable. On identifie $\text{Gal}(f)$ à un sous-groupe de \mathbb{S}_4 . D'après (1), existe un cycle d'ordre 3 dans $\text{Gal}(f)$. Puisque f n'a pas de racine dans \mathbb{Q} , cela entraîne comme ci-dessus que f est irréductible.

2. On déduit de ce qui précède que 12 divise l'ordre de $\text{Gal}(f)$. Le discriminant de f est 229 qui n'est pas un carré dans \mathbb{Q} , donc $\text{Gal}(f)$ n'est pas contenu dans \mathbb{A}_4 . Puisque \mathbb{A}_4 est le seul sous-groupe d'ordre 12 de \mathbb{S}_4 , on a donc $\text{Gal}(f) = \mathbb{S}_4$.

3. Supposons qu'il existe une telle extension quadratique K . Notons L le corps de décomposition de f dans \mathbb{C} et H le groupe de Galois de L sur K . L'ordre de H est 12. Par suite, on a $H = \mathbb{A}_4$. Puisque H contient le groupe de Galois de L sur $\mathbb{Q}(\alpha)$, qui est d'ordre 6, on en déduit que \mathbb{A}_4 contient un sous-groupe d'ordre 6. D'où une contradiction (cf. l'exercice 39) et le résultat.

41) 1. Soit α une racine de F dans une clôture algébrique de \mathbb{F}_ℓ . Posons $K = \mathbb{F}_\ell(\alpha)$. Notons n le degré de F , i.e. le degré K sur \mathbb{F}_ℓ , et δ l'ordre de la classe de ℓ dans $(\mathbb{Z}/p\mathbb{Z})^*$. L'égalité $X^p - 1 = (X - 1)\Phi_p$ entraîne $\alpha^p = 1$. Puisque ℓ et p sont distincts, on a $\alpha \neq 1$ et α est donc d'ordre p dans K^* . Le groupe K^* étant d'ordre $\ell^n - 1$, on a $\alpha^{\ell^n - 1} = 1$, par suite on a $\ell^n \equiv 1 \pmod{p}$ et δ divise n . Par ailleurs, la congruence $\ell^\delta \equiv 1 \pmod{p}$ et l'égalité $\alpha^p = 1$ entraînent $\alpha^{\ell^\delta} = \alpha$. D'après les résultats démontrés en cours sur les corps finis, l'extension K/\mathbb{F}_ℓ est galoisienne de degré n , et son groupe de Galois est cyclique engendré par l'élément de Frobenius σ défini pour tout $x \in K$ par l'égalité $\sigma(x) = x^\ell$. L'élément σ^δ est donc l'identité de K . Puisque σ est d'ordre n , il en résulte que n divise δ . On a donc $n = \delta$ et le résultat.

2. Supposons que Φ_p soit irréductible sur \mathbb{F}_ℓ . La question 1 entraîne que la classe de ℓ est d'ordre $p - 1$ dans $(\mathbb{Z}/p\mathbb{Z})^*$. Inversement, supposons que la classe de ℓ soit un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Soit $F \in \mathbb{F}_\ell[X]$ un facteur irréductible de Φ_p . D'après la question 1, son degré est $p - 1$, d'où $F = \Phi_p$ et Φ_p est irréductible sur \mathbb{F}_ℓ .

3. On déduit de ce qui précède que Φ_5 est irréductible sur \mathbb{F}_ℓ si et seulement si on a $\ell \equiv 2, 3 \pmod{5}$. Notons que dans $\mathbb{F}_5[X]$, on a l'égalité $\Phi_5 = (X - 1)^4$ et Φ_5 est donc réductible sur \mathbb{F}_5 .

42) Posons $G = \text{Gal}(K/\mathbb{Q})$. On peut supposer que p est ≥ 3 , car l'énoncé est vrai si $p = 2$. Soit α une racine de f . Puisque $\mathbb{Q}(\alpha)$ est contenu dans K , et que le degré de $\mathbb{Q}(\alpha)$ sur \mathbb{Q} est p , l'ordre de G est divisible par p . Il en résulte que G a un élément d'ordre p (un groupe dont l'ordre est divisible par un nombre premier p possède un élément d'ordre p). Par ailleurs la conjugaison complexe induit un automorphisme de K , i.e. un élément de G ; en effet, f étant à coefficients dans \mathbb{Q} , si z est racine de f , son conjugué \bar{z} l'est aussi. Puisque f a exactement deux racines non réelles, la conjugaison complexe laisse fixe les $p - 2$ racines réelles de f et échange les deux racines imaginaires. On en déduit que l'image de G dans \mathbb{S}_p contient une transposition. Puisqu'elle contient un cycle d'ordre p , il en résulte que l'image de G dans \mathbb{S}_p est \mathbb{S}_p tout entier (*). D'où le résultat.

(*) Il s'agit de vérifier l'assertion suivante : Soient p un nombre premier et H un sous-groupe de \mathbb{S}_p contenant une transposition et un cycle d'ordre p . Alors, on a $H = \mathbb{S}_p$.

Démonstration : Il suffit de vérifier qu'un sous-groupe conjugué de H est \mathbb{S}_p . Soit (a, b) une transposition de H . Il existe $u \in \mathbb{S}_p$ tel que $u(a) = 1$ et $u(b) = 2$. On a l'égalité $u(a, b)u^{-1} = (u(a), u(b)) = (1, 2)$. Quitte à remplacer H par uHu^{-1} , on peut ainsi supposer que $(1, 2)$ est dans H . Soit $c = (1, x_2, \dots, x_p)$ un cycle d'ordre p de H . En modifiant c par une puissance convenable, on peut supposer que $x_2 = 2$. Par ailleurs, il existe $v \in \mathbb{S}_p$ tel que l'on ait

$$v(1) = 1, \quad v(2) = 2 \quad \text{et} \quad v(x_i) = i \quad \text{pour} \quad i \geq 3.$$

On a les égalités

$$v(1, 2)v^{-1} = (1, 2) \quad \text{et} \quad vcv^{-1} = (v(1), v(2), \dots, v(x_p)) = (1, 2, \dots, p).$$

Par suite, quitte à remplacer de nouveau H par vHv^{-1} on peut supposer que

$$t = (1, 2) \in H \quad \text{et} \quad c = (1, 2, \dots, p) \in H.$$

Pour tout entier i tel que $1 \leq i \leq p-2$, on a

$$c^i(1, 2)c^{-i} = (i+1, i+2) \in H.$$

Pour tout un tel entier i , on a l'égalité

$$(i+1, i+2)(1, i+1)(i+1, i+2) = (1, i+2).$$

On en déduit que pour tout i compris entre 2 et p la transposition $(1, i)$ appartient à H . Pour tout $i \neq j$, l'égalité

$$(1, i)(1, j)(1, i) = (i, j),$$

implique alors que les transpositions sont dans H . Puisque \mathbb{S}_p est engendré par les transpositions, on a donc $H = \mathbb{S}_p$. D'où le résultat.

Application. On vérifie que f a trois racines réelles et deux racines imaginaires : on a $f' = X^2(5X^2 - 12)$, et en notant ξ_1, ξ_2 les deux racines non nulles de f' telles que $\xi_1 < \xi_2$, on constate que $f(\xi_1) > 0$ et $f(\xi_2) < 0$. D'où l'assertion.

43) Posons $G = \text{Gal}(K/\mathbb{Q})$. Soient α une racine de f dans \mathbb{C} et σ un élément de $\text{Gal}(K/\mathbb{Q}(\alpha))$. Soit τ un élément de G . On a $\tau(\alpha) = \tau \circ \sigma(\alpha)$, d'où puisque G est abélien, $\sigma \circ \tau(\alpha) = \tau(\alpha)$. L'extension $K/\mathbb{Q}(\alpha)$ étant galoisienne, on en déduit que $\tau(\alpha)$ est dans $\mathbb{Q}(\alpha)$. Par ailleurs, f étant irréductible, G agit transitivement sur l'ensemble des racines de f . Autrement dit, pour toute racine β de f il existe $\tau \in G$ tel que $\tau(\alpha) = \beta$. Ainsi, les racines de f sont dans $\mathbb{Q}(\alpha)$, d'où $K = \mathbb{Q}(\alpha)$.

4. Correspondance de Galois

44) 1. Soient a un générateur de G et H un sous-groupe de G . Soit δ le plus petit entier > 0 tel que a^δ appartienne à H . Le sous-groupe de G engendré par a^δ est contenu dans H . Montrons qu'il est égal à H . On considère pour cela un élément x de H . Il existe un entier $m \geq \delta$ tel que l'on ait $x = a^m$. Il existe des entiers q et r tels que l'on ait $m = \delta q + r$, avec $0 \leq r < \delta$. On déduit de là que a^r est dans H , et donc que r est nul. D'où $m = \delta q$, et x appartient au sous-groupe de G engendré par a^δ . D'où notre assertion.

2. Soit d un diviseur positif de n . D'abord il existe un sous-groupe H_d de G d'ordre d , à savoir le sous-groupe de G engendré par $a^{\frac{n}{d}}$. Démontrons que H_d est le seul sous-groupe d'ordre d de G . Soit H le sous-ensemble de G formé des éléments $x \in G$ tels que $x^d = e$ (l'élément neutre de G). C'est un sous-groupe de G et tout sous-groupe d'ordre d de G est contenu dans H . En particulier, tel est le cas de H_d et l'on a $|H| \geq d$. D'après l'assertion

1, H est cyclique. Soit y un générateur de H . Puisque l'on a $y^d = e$, l'ordre de y divise d et l'on a $|H| \leq d$. Il en résulte que $|H| = d$. Par suite, $H = H_d$ et c'est l'unique sous-groupe d'ordre d de G .

45) 1. L'extension K/\mathbb{Q} est galoisienne de degré 4 et $\text{Gal}(K/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ (cf. l'exercice 31). Le groupe $\text{Gal}(K/\mathbb{Q})$ possède ainsi trois sous-groupes d'ordre 2, de sorte qu'il y a exactement trois extensions de \mathbb{Q} de degré 2 contenues dans K , qui sont $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ et $\mathbb{Q}(\sqrt{6})$. Ce sont avec \mathbb{Q} et K les sous-corps de K .

2. Le polynôme considéré est irréductible sur \mathbb{Q} et son discriminant est 229 qui n'est pas un carré dans \mathbb{Z} . Il en résulte que K est une extension de \mathbb{Q} de degré 6 dont le groupe de Galois sur \mathbb{Q} est isomorphe à S_3 . Les sous-groupes propres de S_3 sont le groupe alterné A_3 et les trois sous-groupes d'ordre 2 engendrés chacun par une transposition. Les extensions de \mathbb{Q} contenues dans K , autres que \mathbb{Q} et K , sont donc $\mathbb{Q}(\sqrt{229})$ et les trois corps conjugués $\mathbb{Q}(\alpha)$, $\mathbb{Q}(\beta)$ et $\mathbb{Q}(\gamma)$, où α , β et γ sont les trois racines de f .

3. L'extension K/\mathbb{Q} est galoisienne de degré 6 (exercice 34). Son groupe de Galois G sur \mathbb{Q} est isomorphe à $(\mathbb{Z}/7\mathbb{Z})^*$ qui est cyclique d'ordre 6 : en effet, un générateur de ce groupe est la classe de 3 modulo 7. L'élément σ de G défini par l'égalité

$$\sigma(\zeta) = \zeta^3,$$

est donc un générateur de G . Ainsi G possède un unique sous-groupe H_1 d'ordre 2 et un unique sous-groupe H_2 d'ordre 3 (exercice 44). Notons K^{H_i} le sous-corps de K laissé fixe par H_i . Les extensions de \mathbb{Q} contenues dans K , autres que \mathbb{Q} et K , sont donc les deux corps K^{H_i} . L'extension K/K^{H_i} est galoisienne de degré l'ordre de H_i .

Vérifions que l'on a $K^{H_2} = \mathbb{Q}(\sqrt{-7})$. Puisque H_2 est d'ordre 3, on a

$$H_2 = \{1_K, \sigma^2, \sigma^4\}.$$

Posons

$$\alpha = \zeta + \sigma^2(\zeta) + \sigma^4(\zeta).$$

On a $\sigma^2(\alpha) = \alpha$, de sorte que α appartient à K^{H_2} . Par ailleurs, on a

$$\alpha = \zeta + \zeta^2 + \zeta^4,$$

qui est un élément de degré 2 sur \mathbb{Q} : α n'est pas dans \mathbb{Q} , sinon ζ serait racine d'un polynôme de degré 4 à coefficients dans \mathbb{Q} , ce qui n'est pas. Puisque K^{H_2} est une extension quadratique de \mathbb{Q} , on en déduit que α est un élément primitif de K^{H_2} . Par ailleurs, le conjugué de α sur \mathbb{Q} est $\sigma(\alpha) = \zeta^3 + \zeta^5 + \zeta^6$. Le polynôme minimal de α sur \mathbb{Q} est donc $(X - \alpha)(X - \sigma(\alpha))$ i.e. $X^2 + X + 2$. Cela entraîne notre assertion.

Pour déterminer K^{H_1} , on peut s'inspirer du procédé précédent, ou bien utiliser l'exercice 23 : le corps $\mathbb{Q}(\cos \frac{2\pi}{7})$ est une extension de \mathbb{Q} de degré 3 contenue dans K . Il en résulte que l'on a

$$K^{H_1} = \mathbb{Q}\left(\cos \frac{2\pi}{7}\right).$$

4. On vérifie que le polynôme minimal de ζ sur \mathbb{Q} est $X^4 + 1$. Le corps K est donc une extension de degré 4 de \mathbb{Q} . Les racines quatrièmes de l'unité sont dans K , autrement dit $\mathbb{Q}(i)$ est contenu dans K . Par ailleurs, on a

$$\exp\left(\frac{\pi i}{4}\right) + \exp\left(-\frac{\pi i}{4}\right) = 2 \cos \frac{\pi}{4} = \sqrt{2}.$$

Par conséquent, $\mathbb{Q}(\sqrt{2})$ est aussi contenu dans K . On en déduit que $\text{Gal}(K/\mathbb{Q})$ n'est pas cyclique, car sinon K contiendrait un unique corps quadratique. Le groupe $\text{Gal}(K/\mathbb{Q})$ est donc isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$, et il existe exactement trois extensions quadratiques de \mathbb{Q} contenues dans K . Ce sont les corps $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{-2})$. D'où l'exercice.

46) 1. Cette assertion a déjà été démontré dans la question 5 de l'exercice 32 : avec les notations de cet exercice, il suffit de prendre $b = a^2 - t^2$.

2. L'extension K/\mathbb{Q} est galoisienne de groupe de Galois G isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. D'après le théorème de correspondance de Galois, les sous-corps de K autres que \mathbb{Q} et K sont donc trois extensions quadratiques de \mathbb{Q} que l'on va maintenant déterminer.

Posons comme ci-dessus $b = a^2 - t^2$. Soient \sqrt{b} une racine carrée de b dans \mathbb{C} et α une racine carrée de $a + \sqrt{b}$ dans \mathbb{C} . On a $F(\pm\alpha) = 0$ et $K = \mathbb{Q}(\alpha)$. Vérifions que les extensions quadratiques cherchées sont

$$\mathbb{Q}(\sqrt{b}), \quad \mathbb{Q}(\sqrt{2(a+t)}) \quad \text{et} \quad \mathbb{Q}(\sqrt{2(a-t)}).$$

Notons $\pm\beta$ les deux autres racines de F dans \mathbb{C} . On a $(\alpha\beta)^2 = t^2$, et l'on peut choisir t de sorte que

$$\alpha\beta = t.$$

De l'égalité $\alpha^2 = a + \sqrt{b}$, on déduit que $\mathbb{Q}(\sqrt{b})$ est contenu dans K . Par ailleurs, b n'est pas un carré dans \mathbb{Q} , sinon α^2 serait dans \mathbb{Q} et K serait une extension de degré 2 de \mathbb{Q} , ce qui n'est pas. Ainsi $\mathbb{Q}(\sqrt{b})$ est l'une des trois extensions quadratiques cherchées. On écrit ensuite que

$$2a = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2t,$$

d'où l'on déduit que

$$(1) \quad (\alpha + \beta)^2 = 2(a + t).$$

Ainsi $\mathbb{Q}(\sqrt{2(a+t)})$ est contenu dans K . Démontrons que c'est une extension de degré 2 de \mathbb{Q} distincte de $\mathbb{Q}(\sqrt{b})$.

a) Vérifions d'abord que $2(a+t)$ n'est pas un carré dans \mathbb{Q} . Dans le cas contraire, d'après (1), $\alpha + \beta$ est dans \mathbb{Q} et est donc fixé par les éléments de G . Soit σ l'élément de G défini par l'égalité $\sigma(\alpha) = -\alpha$. On a

$$\sigma(\beta) = \sigma\left(\frac{t}{\alpha}\right) = -\frac{t}{\alpha} = -\beta.$$

Par suite, on a $\sigma(\alpha + \beta) = -(\alpha + \beta)$ qui est distinct de $\alpha + \beta$ car $\alpha \neq -\beta$. D'où une contradiction et notre assertion.

b) Vérifions que $\mathbb{Q}(\sqrt{2(a+t)}) \neq \mathbb{Q}(\sqrt{b})$. Supposons le contraire. Dans ce cas, il existe $u \in \mathbb{Q}$ tel que $2(a+t) = bu^2$. D'après (1), on a donc

$$(\alpha + \beta)^2 = bu^2.$$

Il en résulte que $\alpha + \beta$ appartient à $\mathbb{Q}(\sqrt{b})$. Soit τ l'élément de G autre que l'identité qui fixe $\mathbb{Q}(\sqrt{b})$. On a $\tau(\alpha^2) = a + \tau(\sqrt{b}) = a + \sqrt{b} = \alpha^2$, d'où $\tau(\alpha) = \pm\alpha$. Puisque τ n'est pas l'identité, on a donc $\tau(\alpha) = -\alpha$ et l'on obtient

$$\tau(\beta) = \tau\left(\frac{t}{\alpha}\right) = \frac{t}{\tau(\alpha)} = -\frac{t}{\alpha} = -\beta.$$

On en déduit que $\tau(\alpha + \beta) = -(\beta + \alpha)$ qui est distinct de $\alpha + \beta$, ce qui conduit de nouveau à une contradiction et prouve l'assertion.

Il résulte de ce qui précède que les extensions quadratiques cherchées sont $\mathbb{Q}(\sqrt{b})$, $\mathbb{Q}(\sqrt{2(a+t)})$ et $\mathbb{Q}(\sqrt{2b(a+t)})$. L'égalité $2b(a+t) = 2(a-t)(a+t)^2$ entraîne alors le résultat annoncé.

47) 1. On vérifie que l'on a

$$a^2 = (1, 3)(2, 4), \quad a^3 = (1, 4, 3, 2), \quad ab = (1, 2)(3, 4), \quad a^2b = (1, 3), \quad a^3b = (1, 4)(3, 2).$$

Il en résulte que l'ensemble $\{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, qui est contenu dans D_4 , est de cardinal 8. Puisque D_4 est distinct de \mathbb{A}_4 , le groupe D_4 n'est pas d'ordre 12. On en déduit que D_4 est d'ordre 8 ou est égal à \mathbb{S}_4 . Par ailleurs, l'ensemble $S := \{\{1, 3\}, \{2, 4\}\}$ est stabilisé par a et b , donc les éléments de D_4 stabilisent aussi S . Il en résulte que D_4 n'est pas \mathbb{S}_4 tout entier car par exemple la transposition $(1, 2)$ ne stabilise pas S . On déduit que D_4 est d'ordre 8, ce qui entraîne le résultat.

2. Soit H un sous-groupe de D_4 distinct de $\{e\}$ et de D_4 . Son ordre est 2 ou 4. D'après les égalités ci-dessus, les éléments d'ordre 2 de D_4 sont b, ab, a^2, a^2b et a^3b . On obtient ainsi

les cinq sous-groupes d'ordre 2 annoncés. Supposons que H soit d'ordre 4. Puisque H est d'indice 2 dans D_4 , il est distingué dans D_4 , de sorte que H est le noyau d'un morphisme de groupes surjectif de D_4 sur $\mathbb{Z}/2\mathbb{Z}$. Il y a trois tels morphismes qui correspondent aux choix des images de a et b dans $\mathbb{Z}/2\mathbb{Z}$. On en déduit qu'il existe trois sous-groupes d'ordre 4 dans D_4 . On vérifie par ailleurs que l'on a les égalités $(ab)(a^3b) = a^2$ et $b(a^2b) = a^2$. Cela entraîne notre assertion.

3. Le polynôme f est irréductible sur \mathbb{Q} d'après le critère d'Eisenstein. Soit α une racine réelle de f et i une racine carrée de -1 dans \mathbb{C} . Les racines de f sont $\alpha, i\alpha, -\alpha, -i\alpha$, de sorte que l'on a

$$L = \mathbb{Q}(i, \alpha).$$

Le corps $\mathbb{Q}(\alpha)$ est contenu dans \mathbb{R} et est de degré 4 sur \mathbb{Q} . Puisque i n'est pas dans $\mathbb{Q}(\alpha)$, le polynôme minimal de i sur $\mathbb{Q}(\alpha)$ est $X^2 + 1$. Par suite, le degré de L sur \mathbb{Q} est égal à 8. Ainsi, le groupe G est d'ordre 8. Un élément s de G est entièrement déterminé par $s(\alpha)$ et $s(i)$. Soient σ et τ les éléments de G définis par les égalités

$$\sigma(i) = i, \quad \sigma(\alpha) = i\alpha \quad \text{et} \quad \tau(i) = -i, \quad \tau(\alpha) = \alpha.$$

Les éléments σ et τ sont respectivement d'ordre 4 et 2. Notons encore e l'élément neutre de G . On vérifie que les éléments $e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau$ sont distincts deux à deux. On a ainsi

$$G = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}.$$

On en déduit qu'il existe un unique morphisme de groupes $\varphi : G \rightarrow \mathbb{S}_4$ tel que $\varphi(\sigma) = a$ et $\varphi(\tau) = b$. C'est un isomorphisme de G sur D_4 .

4. Étant donné un sous-groupe H de G , on note L^H le sous-corps de L laissé fixe par H . Rappelons que l'extension L/L^H est galoisienne de degré l'ordre de H .

Si $H = \{e\}$, on a $L^H = L$ et si $H = G$, on a $L^H = \mathbb{Q}$.

Si $H = \{e, \sigma, \sigma^2, \sigma^3\}$, le degré de L^H/\mathbb{Q} vaut 2 et le corps $\mathbb{Q}(i)$ est laissé fixe par H . On a donc $L^H = \mathbb{Q}(i)$.

Si $H = \{e, \sigma^2, \tau, \sigma^2\tau\}$, le corps $\mathbb{Q}(\alpha^2)$ est contenu dans L^H et le degré de l'extension $\mathbb{Q}(\alpha^2)/\mathbb{Q}$ est égal à 2 : en effet, le polynôme minimal de α^2 sur \mathbb{Q} est $X^2 - p$. On a donc $L^H = \mathbb{Q}(\alpha^2)$ i.e. $L^H = \mathbb{Q}(\sqrt{p})$.

Si $H = \{e, \sigma^2, \sigma\tau, \sigma^3\tau\}$, on vérifie comme ci-dessus que $L^H = \mathbb{Q}(i\alpha^2)$, autrement dit, que $L^H = \mathbb{Q}(\sqrt{-p})$.

Si $H = \{e, \tau\}$, on a $L^H = \mathbb{Q}(\alpha)$.

Supposons $H = \{e, \sigma\tau\}$. Posons $\beta = (1 + i)\alpha$. On a $\sigma\tau(\beta) = \beta$. Par ailleurs, le polynôme minimal de β sur \mathbb{Q} est $X^4 + 4p$, donc le degré de $\mathbb{Q}(\beta)/\mathbb{Q}$ est 4. On en déduit que $L^H = \mathbb{Q}(\beta)$.

Supposons $H = \{e, \sigma^2\}$. Posons $\gamma = i + \alpha^2$. Vérifions que $L^H = \mathbb{Q}(\gamma)$. D'abord on a $\sigma^2(\gamma) = \gamma$. Par ailleurs, on vérifie que $\mathbb{Q}(i)\mathbb{Q}(\sqrt{p}) = \mathbb{Q}(\gamma)$, d'où l'on déduit que le degré de γ sur \mathbb{Q} est 4, ce qui entraîne l'assertion.

Si $H = \{e, \sigma^2\tau\}$, le corps $\mathbb{Q}(i\alpha)$ est contenu dans L^H . Puisque le degré de $i\alpha$ sur \mathbb{Q} est 4, on a l'égalité $L^H = \mathbb{Q}(i\alpha)$.

Supposons $H = \{e, \sigma^3\tau\}$. Posons $\lambda = (1 - i)\alpha$. On a $\sigma^3\tau(\lambda) = \lambda$. Le polynôme minimal de λ étant $X^4 + 4p$, il en résulte que $L^H = \mathbb{Q}(\lambda)$.

Conclusion. Il existe dix extensions de \mathbb{Q} contenues dans L . Ce sont

$$\mathbb{Q}, \quad \mathbb{Q}(i), \quad \mathbb{Q}(\sqrt{p}), \quad \mathbb{Q}(\sqrt{-p}),$$

$$\mathbb{Q}(i + \sqrt{p}), \quad \mathbb{Q}(\alpha), \quad \mathbb{Q}(i\alpha), \quad \mathbb{Q}((1 + i)\alpha), \quad \mathbb{Q}((1 - i)\alpha), \quad L.$$

5. L'élément $\theta = i + \alpha$ est un élément primitif de L . En effet, $\mathbb{Q}(\theta)$ est contenu dans L . Par ailleurs, on vérifie que pour tous σ_i et σ_j distincts dans G , on a $\sigma_i(\theta) \neq \sigma_j(\theta)$. Le polynôme minimal de θ sur \mathbb{Q} a donc au moins huit racines. On en déduit qu'il est de degré 8, d'où notre assertion.

48) Posons $n = p - 1$ et notons μ_p le sous-groupe des racines p -ièmes de l'unité de \mathbb{C}^* . On a l'égalité

$$(1) \quad \Delta = (-1)^{\frac{n(n-1)}{2}} \prod_{\zeta \in \mu_p, \zeta \neq 1} \Phi'_p(\zeta).$$

On a

$$\Phi_p = \frac{X^p - 1}{X - 1}.$$

Par suite, pour tout $\zeta \in \mu_p, \zeta \neq 1$, on a

$$(2) \quad \Phi'_p(\zeta) = \frac{p\zeta^{p-1}}{\zeta - 1}.$$

On a

$$(3) \quad \prod_{\zeta \in \mu_p, \zeta \neq 1} \zeta = (-1)^{p-1} = 1.$$

Par ailleurs, pour tout $\zeta \in \mu_p, \zeta \neq 1$, $\zeta - 1$ est racine du polynôme $\Phi_p(X + 1)$. Il en résulte l'égalité

$$(4) \quad \prod_{\zeta \in \mu_p, \zeta \neq 1} (\zeta - 1) = p.$$

On déduit alors des égalités (1) à (4) que l'on a

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

ce qui entraîne le résultat.

2. Le degré de K sur \mathbb{Q} est $p-1$, qui est pair, et le groupe de Galois $\text{Gal}(K/\mathbb{Q})$ est cyclique d'ordre $p-1$. Il existe donc un unique sous-groupe de $\text{Gal}(K/\mathbb{Q})$ d'ordre $(p-1)/2$, ce qui implique l'existence d'une unique extension quadratique L de \mathbb{Q} contenue dans K . On déduit alors de l'exercice 36 et de l'assertion 1, que l'on a

$$L = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right).$$
