Exercices de théorie de Galois 2

Exercice 1. — *Quel est le groupe de Galois du polynôme* $(X^4+1)(X^4-2)$ *?*

Exercice 2. — *Montrez en réduisant modulo* 2 *et* 3*, que le groupe de Galois de* X^5-X-1 *est* $\mathfrak{S}_5$*.*

Exercice 3. — *Donner le groupe du Galois du polynôme*

1) X^3-3X+1 *;*

2) X^3+3X+1*.*

Exercice 4. — *Soit* $P(X)=X^4-X-1\in\mathbb{Q}[X]$*.*

1) Montrer que P *est irréductible sur* $\mathbb{Q}$*.*

2) Montrer que le groupe de Galois G *de* P *n'est pas contenu dans* $\mathcal{A}_4$*.*

3) Factoriser P *sur* $\mathbb{F}_7$ *et en déduire que* $G\simeq\mathfrak{S}_4$*.*

Exercice 5. — *Soit* $P(X)=X^4+8X+12$ *sur* $\mathbb{Q}$*.*

1) Factoriser P *sur* $\mathbb{F}_5$ *et* $\mathbb{F}_{17}$ *et en déduire que* P *est irréductible sur* $\mathbb{Q}$*.*

2) Montrer que le groupe de Galois G *de* P *est isomorphe à* $\mathcal{A}_4$*.*

Exercice 6. — *Soit* $P(X)=X^5-X-1$ *sur* $\mathbb{Q}$*.*

1) Montrer que P *est irréductible.*

2) En étudiant la factorisation de P *modulo* 2*, montrer que le groupe de Galois* G *de* P *est isomorphe à* $\mathfrak{S}_5$*.*

Exercice 7. — *Montrer que* X^5-4X-1 *a toutes ses racines, sauf* 2*, dans* $\mathbb{F}_{19}$ *et en déduire que son groupe de Galois est* $\mathfrak{S}_5$*.*
Remarque : dans l'exercice précédent, on peut aussi vérifier, par ordinateur, que X^5-X-1 *a toutes ses racines, sauf* 2*, dans* $\mathbb{F}_{163}$*.*

Exercice 8. — *Soit* $P(X)\in k[X]$ *unitaire de degré* 4 *et irréductible sur* k*. On note* E *son corps de décomposition et* $x_1,\cdots,x_4$ *ses racines dans* E*. On considère son groupe de Galois* G *comme un sous-groupe de* $\mathfrak{S}_4$*.*

1) On pose

$$\begin{cases}\alpha = x_1x_2+x_3x_4\\ \beta = x_1x_3+x_2x_4\\ \gamma = x_1x_4+x_2x_3.\end{cases}$$

Montrer que V_4 *le sous-groupe de* $\mathfrak{S}_4$ *engendré par les doubles transpositions est égal au stabilisateur de* α,β,γ*.*

2) Quel est le groupe de Galois de $k[\alpha,\beta,\gamma]/k$*.*

3) On pose $g(X)=(X-\alpha)(X-\beta)(X-\gamma)\in M[X]$ *avec* $M=k[\alpha,\beta,\gamma]$*. Montrer que si* $P(X)=X^4+bX^3+cX^2+dX+e$ *alors*

$$g(X)=X^3-cX^2+(bd-4e)X-b^2e+4ce-d^2,$$

et que g *et* P *ont le même discriminant.*

4) Soit $P(X) = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$ *de sorte que* $g(X) = (X-4)(X^2-8)$*. Montrer que* $G \simeq \mathbb{Z}/4\mathbb{Z}$*.*

5) Soit $P(X) = X^4 - 10X^2 + 4 \in \mathbb{Q}[X]$ *; montrer que* $g(X) = (X+10)(X+4)(X-4)$ *et en déduire que* $G = V_4$*.*

6) Soit $P(X) = X^4 - 2$ *; montrer que* $g(X) = X^3 + 8X$ *et en déduire que* $G = D_4$*.*

1 Noter que $\zeta_9 = \frac{1+i}{\sqrt{2}}$ et donc le corps de décomposition est celui de $X^4 + 1$ avec pour groupe de Galois D_4.

2 $X^5 - X - 1$ n'a pas de racines dans $\mathbb{F}_2$ mais il en a dans $\mathbb{F}_4$ comme on peut par exemple le voir calculant le pgcd de $X^5 - X - 1$ avec $X^4 - X$. Ainsi $X^5 - X - 1$ se factorise en un produit de deux facteurs irréductibles de degré 2 et 3. On en déduit alors que G contient une permutation de type $(12)(345)$ et donc en passant au cube, une transposition.

Modulo 3, $X^5 - X - 1$ reste irréductible, de sorte que G contient un 5-cycle.

Par ailleurs comme 5 est premier quitte à prendre une puissance du 5-cycle trouvé, on peut supposer le 5-cycle et la transposition respectivement égale à (12) et (12345). On conclut en remarquant que $\mathfrak{S}_n$ est engendré par (12) et $(12\cdots n)$.

3 Notons tout d'abord que les deux polynômes proposés n'ont pas de solution dans $\mathbb{Z}$ et sont donc irréductibles sur $\mathbb{Z}$. On calcule le discriminant de P ce qui donne

1) $\Delta(P) = -4(-3)^3 - 27 = 81 = 9^2$ et donc $\mathrm{Gal}(P) = \mathcal{A}_3$

2) $\Delta(P) = -4.3^3 - 27 = -135$ et donc $\mathrm{Gal}(P)$ n'est pas contenu dans $\mathcal{A}_3$; comme son cardinal est un multiple de 3 on a donc $\mathrm{Gal}(P) = \mathfrak{S}_3$.

4 1) Comme P est irréductible modulo 2, il est irréductible.

2) On calcule le discriminant de P ce qui donne -283.

3) Modulo 7, on a la factorisation en irréductible

$$X^4 - X - 1 = (X+4)(X^3 + 3X^2 + 2X + 5)$$

de sorte que G contient un 3-cycle et donc son cardinal est divisible par $3 \vee 4 = 12$ et comme il n'est pas contenu dans $\mathcal{A}_4$, il est égal à $\mathfrak{S}_4$.

5 1) Modulo 5, on a la factorisation en irréductible

$$X^4 + 8X + 12 = (X+1)(X^3 + 4X^2 + X + 2)$$

alors que modulo 17

$$X^4 + 8X + 12 = (X^2 + 4X + 7)(X^2 + 13X + 9).$$

Les factorisations étant incompatibles on en déduit que P est irréductible.

2) Le discriminant de P est 576^2 de sorte que le cardinal de G est soit 4 soit 12. Or la factorisation dans $\mathbb{F}_5$ nous fournit l'existence d'un 3-cycle et donc $G = \mathcal{A}_4$.

6 1) On vérifie que P est irréductible sur $\mathbb{F}_3$ et donc P est irréductible sur $\mathbb{Q}$.

2) Modulo 2, on a

$$X^5 - X - 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$$

et donc G contient une permutation de typer $(2,3)$, i.e. un élément d'ordre 6. Ainsi le cardinal de G est divisible par 30 et donc égal soit à $30, 60$ ou 120. Comme il n'y a pas de sous-groupe d'ordre 30 dans $\mathfrak{S}_5$ il suffit de calculer le discriminant de P qui est égal à 19.151 qui n'est pas un carré et donc $G \simeq \mathfrak{S}_5$.

7 Comme P est irréductible et que 5 est premier, G contient un 5-cycle. Sa factorisation modulo 19 nous fournit une transposition et donc $G \simeq \mathfrak{S}_5$.

8 1) L'action de G est transitive sur $\{\alpha, \beta, \gamma\}$ de sorte que le stabilisateur de α est alors un sous-groupe de cardinal 8 soit un 2-Sylow et le stabilisateur cherché est l'intersection des trois 2-Sylow de $\mathfrak{S}_4$ qui est V_4 (car V_4 est de cardinal 4 et distingué dans $\mathfrak{S}_4$ et que les 2-Sylow sont distingués dans $\mathfrak{S}_4$).

2) Le groupe de Galois est alors $G/(G \cap V_4)$.

3)

4) En tant que polynôme d'Eisentein P est irréductible. On a $M = \mathbb{Q}[\sqrt{2}]$ et donc $G/(V_4 \cap G)$ est de cardinal 2. Considérant la liste des sous-groupes de $\mathfrak{S}_4$ on en déduit que $G \simeq D_4$ ou $G \simeq \mathbb{Z}/4\mathbb{Z}$. Or comme P est réductible sur M alors $G \simeq \mathbb{Z}/4\mathbb{Z}$.