Vincent Beck —Patrick Le Meur

Examen

Motivation

Soit $P \in k[X]$ à coefficients dans un corps k. Ce problème étudie le groupe de Galois de P. Il se décompose selon les parties suivantes :

0 De brefs rappels sur des notions utiles. Ces rappels peuvent être utilisés librement sans démonstration.

1 Des préliminaires sur les polynômes en plusieurs indéterminées, et notamment sur les polynômes symétriques. Ces résultats techniques jouent un rôle essentiel dans la Partie 2, et, dans une moindre mesure, dans la Partie 3.

2 On propose une méthode pour « calculer »le groupe de Galois d'un polynôme $P \in k[X]$: Supposons que P est scindé à racines simples $x_1, \dots, x_n$ dans son corps de décomposition K. Pour déterminer le groupe de Galois, on introduit le polynôme $f := \prod_{\sigma \in \mathfrak{S}_n} \big(X - (x_{\sigma(1)}T_1 + \cdots + x_{\sigma(n)}T_n)\big) \in K[X, T_1, \dots, T_n]$. Le groupe $\mathrm{Gal}_k(P)$ est alors caractérisé, comme sous-groupe de $\mathfrak{S}_n$, grâce aux facteurs irréductibles de f.

3 Soient $P \in \mathbb{Z}[X]$ un polynôme unitaire et p un entier premier impair. On note $\overline{P} \in \mathbb{F}_p[X]$ le polynôme obtenu par réduction des coefficients modulo p. Grâce à la caractérisation de la Partie 2, on montre que $\mathrm{Gal}_{\mathbb{F}_p}(\overline{P})$ est isomorphe à un sous-groupe de $\mathrm{Gal}_{\mathbb{Q}}(P)$.

4 On étudie les groupes qui peuvent apparaître comme groupe de Galois d'un polynôme de $\mathbb{Q}[X]$ irréductible de degré 5. La Partie 3 permet d'affiner cette étude.

5 Dans cette dernière partie, on constate sur des exemples que les groupes mis en évidence dans la partie précédente sont réellement des groupes de Galois de polynômes irréductibles de degré 5.

0 Rappels

Rappel — Action de groupes. Soient G un groupe agissant sur X et $x \in X$. On note $\mathcal{O}(x) = \{gx, \quad g \in G\}$ l'orbite de x sous l'action de G et $G_x = \{g \in G, \quad gx = x\}$ le stabilisateur de x. L'application

$$\varphi_x : \begin{cases} G/G_x \longrightarrow \mathcal{O}(x) \\ gG_x \longmapsto gx \end{cases}$$

est bien définie (si $gG_x = g'G_x$ alors $gx = g'x$) et est une bijection.

Rappel — Normalisateur. Soient G un groupe et H un sous-groupe de G. L'ensemble

$$N_G(H) = \big\{g \in G, \qquad gHg^{-1} = H\big\}$$

est un sous-groupe de G contenant H. De plus, H est distingué dans $N_G(H)$ et tout sous-groupe de G contenant H et dans lequel H est distingué est contenu dans $N_G(H)$. En fait, $N_G(H)$ est le stabilisateur de H pour l'action de G par conjugaison sur l'ensemble de ses sous-groupes.

Rappel — Théorèmes de Sylow. Soit G un groupe fini d'ordre $p^\alpha m$ avec p premier et $m \wedge p = 1$.

(i) Il existe un sous-groupe de G d'ordre p^α.

(ii) Les sous-groupes de G d'ordre p^α sont conjugués. Conséquence : G admet un unique sous-groupe d'ordre p^α si et seulement si celui-ci est distingué.

(iii) Tout sous-groupe de G dont l'ordre est une puissance de p est contenu dans un sous-groupe de G d'ordre p^α.

(iv) Si $p \mid |G|$ (c'est-à-dire si $\alpha > 0$), il existe un élément d'ordre p dans G.

Rappel — Polynômes symétriques. Soient A un anneau intègre et $n \geqslant 1$ un entier. Alors $\mathfrak{S}_n$ agit naturellement sur $A[X_1, \dots, X_n]$, avec $\sigma.1 = 1$ et $\sigma.X_i = X_{\sigma(i)}$ pour tout i. L'anneau des polynômes symétriques est $A[X_1, \dots, X_n]^{\mathfrak{S}_n} := \{P \in A[X_1, \dots, X_n] \mid \sigma.P = P$ pour tout $\sigma \in \mathfrak{S}_n\}$. Si, pour chaque i, on note

$\Sigma_i : \sum_{1 \leqslant j_1 < \cdots < j_n \leqslant n} X_{j_1} \cdots X_{j_i}$ le i-ème polynôme symétrique élémentaire en $X_1, \ldots, X_n$, alors il existe un unique morphisme d'anneaux :

$$\begin{cases} A[X_1, \ldots, X_n] \longrightarrow A[X_1, \ldots, X_n]^{\mathfrak{S}_n} \\ 1 \longmapsto 1 \\ X_i \longmapsto \Sigma_i \,. \end{cases}$$

Ce morphisme est un isomorphisme.

Rappel — Discriminant. Soit $P \in k[X]$ un polynôme unitaire de degré n et $(\alpha_i)_{1 \leq i \leq n}$ les racines (comptées avec multiplicité) de P dans un corps de décomposition. L'élément $D \in k$ définit ci-dessous s'appelle le discriminant de P :

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

Pour $i \in \mathbb{NN}$, on note $s_i = {\alpha_1}^i + \cdots + {\alpha_n}^i \in k$. On rappelle que

$$D = \begin{vmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & & \ddots & \vdots \\ s_{n-1} & \cdots & \cdots & s_{2n-2} \end{vmatrix}$$

On rappelle aussi que, lorsque P est séparable, $\mathrm{Gal}_k(P) \subset \mathfrak{A}_n$ si et seulement si D est un carré dans k.

1 Préliminaires

Exercice 1 — Question de cours.

a) Soient k un corps et $P \in k[X]$ un polynôme de degré n. Montrer que $[\mathrm{Dec}_k(P) : k] \leqslant n!$.

b) Montrer que le sous-corps $k(X_1, \ldots, X_n)^{\mathfrak{S}_n}$ de $k(X_1, \ldots, X_n)$ coïncide avec le sous-corps $k(\Sigma_1, \ldots, \Sigma_n)$ engendré par les polynômes symétriques élémentaires.

c) Soient $P, Q \in k[X]$ deux polynômes unitaires premiers entre eux. Exprimer $\mathrm{Gal}_k(PQ)$ en fonction de $\mathrm{Gal}_k(P)$ et $\mathrm{Gal}_k(Q)$.

d) Soient $p_1, \ldots, p_n$ des entiers premiers, deux à deux distincts et $P = (X^2 - p_1) \cdots (X^2 - p_n) \in \mathbb{Q}[X]$. Calculer $\mathrm{Gal}_{\mathbb{Q}}(P)$. Lorsque $n = 3$, déterminer les sous-corps de $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$?

Exercice 2 — Fractions rationelles. Soit $(K : k)$ une extension algébrique.

a) Montrer que $(K(X_1, \ldots, X_n) : k(X_1, \ldots, X_n))$ est une extension algébrique.

b) Soit $x \in K(X_1, \ldots, X_n)$. Montrer que $x \in K$ si et seulement si x est algébrique sur k.

c) En déduire qu'on peut définir un morphisme de groupes

$$\Psi : \begin{cases} \mathrm{Aut}_{k(X_1, \ldots, X_n)}(K(X_1, \ldots, X_n)) \longrightarrow \mathrm{Aut}_k(K) \\ \sigma \longmapsto \sigma_K \end{cases}$$

où σ_K désigne la restriction de σ à K. Montrer que Ψ est bijectif.

d) On suppose que $(K : k)$ est une extension séparable. Montrer que $(K(X_1, \ldots, X_n) : k(X_1, \ldots, X_n))$ l'est aussi.

e) On suppose que $(K : k)$ est une extension normale. Montrer que $(K(X_1, \ldots, X_n) : k(X_1, \ldots, X_n))$ l'est aussi.

f) En déduire que si $(K : k)$ est une extension galoisienne, $(K(X_1, \ldots, X_n) : k(X_1, \ldots, X_n))$ l'est aussi. Que peut-on dire de plus si $[K : k]$ est fini ?

Exercice 3 — Polynômes symétriques. Soient k un corps, $n \geqslant 1$ un entier et $k[X_1, \ldots, X_n, T_1, \ldots, T_n, X]$ l'anneau des polynômes en les indéterminées $X_1, \ldots, X_n, T_1, \ldots, T_n, X$, à coefficients dans k. Pour $\sigma \in \mathfrak{S}_n$, on note U_σ le polynôme suivant :

$$U_\sigma := X_{\sigma(1)} T_1 + \cdots + X_{\sigma(n)} T_n \,.$$

Soit F le polynôme :

$$F := \prod_{\sigma \in \mathfrak{S}_n} (X - U_\sigma) \,.$$

Ainsi, $F \in k[X_1, \ldots, X_n][T_1, \ldots, T_n, X]$. Le but de l'exercice est de montrer que $F \in k[\Sigma_1, \ldots, \Sigma_n][T_1, \ldots, T_n, X]$. À cette fin, nous fixons une énumération $\mathfrak{S}_n = \{\sigma_1, \ldots, \sigma_{n!}\}$ des éléments du groupe symétrique.

a) Pour $i = 1, \dots, n!$, soit S_i le i-ème polynôme symétrique en les U_{σ_i} :

$$S_i := \sum_{1 \leqslant j_1 < \cdots < j_i \leqslant n!} U_{\sigma_{j_1}} \cdots U_{\sigma_{j_i}} \ .$$

Exprimer F en fonction de X et des S_i.

b) Soit $i \in \{1, \dots, n!\}$. Pour simplifier, on note A l'anneau $k[T_1, \dots, T_n]$. Montrer que $S_i \in A[X_1, \dots, X_n]^{\mathfrak{S}_n}$.

c) En déduire que $F \in k[\Sigma_1, \dots, \Sigma_n][T_1, \dots, T_n, X]$.

On fixe $P_1, \dots, P_{n!} \in k[X_1, \dots, T_n][X_1, \dots, X_n]$ des polynômes tels que :

$$F = X^{n!} - P_1(\Sigma_1, \dots, \Sigma_n) X^{n!-1} + \cdots + (-1)^{n!} P_{n!}(\Sigma_1, \dots, \Sigma_n) \ ,$$

où $P_i(\Sigma_1, \dots, \Sigma_n) \in k[T_1, \dots, T_n]$ est obtenu à partir de P_i en remplaçant chaque X_j par Σ_j.

d) On suppose que $k = \mathbb{Q}$, justifier que $P_i \in \mathbb{Z}[X_1, \dots, X_n, T_1, \dots, T_n]$, pour tout i.

2 Caractérisation des permutations des racines d'un polynôme qui proviennent du groupe de Galois

Soient k un corps, $P \in k[X]$ un polynôme unitaire non constant et séparable et K un corps de décomposition de P sur k. Dans K, on fixe une décomposition $P = \prod_{i=1}^{n} (X - x_i)$, où $x_1, \dots, x_n \in K$ sont supposés deux à deux distincts. L'action du groupe de Galois $\mathrm{Gal}_k(P) = \mathrm{Gal}(K : k)$ sur $\{x_1, \dots, x_n\}$ définit donc un morphisme injectif de groupes :

$$\mathrm{Gal}_k(P) \hookrightarrow \mathfrak{S}_n \ .$$

L'objectif de cette partie est de caractériser les permutations $\sigma \in \mathfrak{S}_n$ qui proviennent, par ce morphisme, d'un élément du groupe de Galois.

On rappelle que l'application $g \mapsto g_{|K}$ est un isomorphisme de groupes de $\mathrm{Gal}(K(T_1, \dots, T_n) : k(T_1, \dots, T_n))$ vers $\mathrm{Gal}(K : k)$ (voir l'Exercice **??**).

Étant donné $\sigma \in \mathfrak{S}$, on note $u_\sigma \in K[T_1, \dots, T_n]$ le polynôme suivant :

$$u_\sigma := x_{\sigma(1)} T_1 + \cdots + x_{\sigma(n)} T_n \ .$$

Exercice 4 — Polynôme minimal de u_σ. Soit $\sigma \in \mathfrak{S}_n$.

a) Montrer que le polynôme $m_\sigma := \prod_{g \in \mathrm{Gal}_k(P)} (X - g(u_\sigma)) \in K[T_1, \dots, T_n][X]$ annule u_σ.

b) Dans cette question seulement, on suppose que $k = \mathbb{Q}$ et que $P = X^2 + 1$. Calculer u_σ et m_σ pour toute permutation $\sigma \in \mathfrak{S}_2$.

c) Montrer que $m_\sigma \in k[T_1, \dots, T_n][X]$.

d) Quel est le polynôme minimal de $u_\sigma \in K(T_1, \dots, T_n)$ sur $k(T_1, \dots, T_n)$?

e) Montrer que $K(T_1, \dots, T_n)$ est engendré par u_σ sur $k(T_1, \dots, T_n)$.

On définit $f \in K[T_1, \dots, T_n][X]$ comme étant le polynôme :

$$f := \prod_{\sigma \in \mathfrak{S}_n} (X - u_\sigma) \ .$$

Exercice 5 — Le polynôme f est à coefficients dans $k[T_1, \dots, T_n]$.

a) Montrer que f est, en tant que polynôme en X, sans facteur carré.

b) Exprimer f en fonction du polynôme F étudié à l'Exercice **??**.

c) En déduire que f est, en tant que polynôme en X, à coefficients dans $k[T_1, \dots, T_n]$ et unitaire.

d) Quelle est la décomposition de f en produit d'irréductibles ?

Exercice 6 — Permutations provenant du groupe de Galois. Dans toute la suite, on note $(\sigma, P) \mapsto \sigma.P$ l'action usuelle de $\mathfrak{S}_n$ sur $k(T_1, \dots, T_n)$ par permutation des coordonnées ($\sigma.T_i = T_{\sigma(i)}$).

a) Montrer que $\sigma.f = f$ pour tout $\sigma \in \mathfrak{S}_n$.

b) Exprimer simplement $\sigma.u_{\sigma'}$ et $\sigma.m_{\sigma'}$ pour $\sigma, \sigma' \in \mathfrak{S}_n$.

c) Soit Q un facteur irréductible unitaire de f dans l'anneau factoriel $k[T_1, \dots, T_n][X]$. Montrer qu'il existe $\sigma \in \mathfrak{S}_n$ tel que $Q = m_\sigma$.

d) Soit $g \in \mathrm{Gal}_k(P)$, et soit $\tau \in \mathfrak{S}_n$ la permutation telle que $g(x_i) = x_{\tau(i)}$. Montrer que $\tau.m_{id} = m_{id}$.

e) Soit $\tau \in \mathfrak{S}_n$ une permutation telle que $\tau.m_{id} = m_{id}$. Montrer qu'il existe $g \in \mathrm{Gal}_k(P)$ tel que $x_{\tau(i)} = g(x_i)$.

f) Soit $\sigma, \tau \in \mathfrak{S}_n$ telles que $\tau.m_\sigma = m_\sigma$. Montrer qu'il existe $g \in \mathrm{Gal}_k(P)$ tel que $g(x_i) = x_{\sigma\tau\sigma^{-1}(i)}$ pour tout i.

On a ainsi caractérisé l'image du morphisme de groupes

$$\begin{cases} \mathrm{Gal}_k(P) \longrightarrow \mathfrak{S}_n \\ \qquad g \longmapsto \sigma \text{ tel que } g(x_i) = x_{\sigma(i)} \text{ pour tout } i. \end{cases}$$

3 Groupe de Galois après réduction modulo p des coefficients

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré n. On garde les notations $(x_1, \dots, x_n, f, u_\sigma)$ introduites à la partie précédente. Soit p un entier premier impair. Étant donné un polynôme Q à coefficients dans $\mathbb{Z}$ (en une ou plusieurs indéterminées), on notera $\overline{Q}$ le polynôme obtenu à partir de Q par réduction des coefficients modulo p. Dans cette partie, on suppose que $\overline{P} = (X - \xi_1) \cdots (X - \xi_n)$ dans un corps de décomposition de $\overline{P}$ sur $\mathbb{F}_p$, avec $\xi_1, \dots \xi_n$ deux à deux distincts.

Exercice 7 — On peut tout réduire modulo p.

a) Justifier que $f \in \mathbb{Z}[T_1, \dots, T_n, X]$.

b) Pour $\sigma \in \mathfrak{S}_n$, soit $\upsilon_\sigma = \xi_{\sigma(1)}T_1 + \cdots + \xi_{\sigma(n)}T_n$. Montrer que $\overline{f} = \prod_{\sigma \in \mathfrak{S}_n} (X - \upsilon_\sigma)$. En déduire que $\overline{f}$ est sans facteur carré (comme polynôme en X).

Dans la suite, on pose $\mu_\sigma := \prod_{g \in \mathrm{Gal}_{\mathbb{F}_p}(\overline{P})} (X - g(\upsilon_\sigma))$. Ainsi, les résultats concernant f, u_σ, m_σ (obtenus dans la partie précédente) restent valables pour $\overline{f}, \upsilon_\sigma, \mu_\sigma$. On rappelle que $\mathfrak{S}_n$ agit sur les polynômes en $X, T_1, \dots, T_n$ par permutation des indéterminées $T_1, \dots, T_n$ (comme dans l'Exercice **??**).

Exercice 8 — Inclusion de groupes de Galois. Soit $\tau \in \mathfrak{S}_n$. On suppose que $\tau.\mu_{id} = \mu_{id}$.

a) Justifier qu'il existe $\sigma \in \mathfrak{S}_n$ tel que μ_{id} divise $\overline{m_\sigma}$ dans $\mathbb{F}_p[T_1, \dots, T_n][X]$.

b) Soit $\sigma' \in \mathfrak{S}_n$ distinct de σ. Montrer que $\overline{m_\sigma}$ et $\overline{m_{\sigma'}}$ sont premiers entre eux dans $\mathbb{F}_p[T_1, \dots, T_n][X]$.

c) En déduire que $\tau.m_\sigma = m_\sigma$.

d) En déduire l'existence d'un morphisme injectif de groupes $\mathrm{Gal}_{\mathbb{F}_p}(\overline{P}) \to \mathrm{Gal}_{\mathbb{Q}}(P)$.

e) Que peut-on dire de la classe d'isomorphisme de $\mathrm{Gal}_{\mathbb{F}_p}(\overline{P})$? (On pourra utiliser la question c de l'exercie **??**).

4 Résolubilité des polynômes de degré 5

Exercice 9 — Étude des sous-groupes de $\mathfrak{S}_5$ dont le cardinal est divisible par 5.

a) Donner les décompositions en cycles à support disjoint d'un élément d'ordre 5 et d'un élément d'ordre 4 de $\mathfrak{S}_5$. En déduire que tous les éléments d'ordre 5 (resp. d'ordre 4) sont conjugués dans $\mathfrak{S}_5$.

b) Déterminer le sous-groupe de $\mathfrak{S}_5$ engendré par l'ensemble des 5-cycles (on pourra par exemple utiliser le fait que $\mathfrak{A}_5$ est simple).

c) Soit $\sigma \in \mathfrak{S}_5$ d'ordre 5 (resp. d'ordre 4). Déterminer les éléments de $\mathfrak{S}_5$ qui commutent avec σ.

d) Déterminer le nombre d'éléments d'ordre 5 (resp. d'ordre 4) de $\mathfrak{S}_5$. En déduire le nombre de 5-Sylow de $\mathfrak{S}_5$.

e) En utilisant les questions précédentes, déterminer le cardinal du normalisateur N du groupe $\langle (1, 2, 3, 4, 5) \rangle$ (on pourra considérer l'action de $\mathfrak{S}_5$ par conjugaison sur l'ensemble de ses 5-Sylow et les rappels « Action de groupes »et « Normalisateur »).

f) Exhiber les éléments de N : en particulier, montrer que N contient un élément d'ordre 4. Déterminer les sous-groupes d'ordre 5 et d'ordre 10 de N. Montrer que les éléments d'ordre 2 de N sont tous conjugués dans $\mathfrak{S}_5$ (et pour les courageux, montrer qu'ils sont conjugués dans G).

Pour la suite de l'exercice, on fixe un sous-groupe G de $\mathfrak{S}_5$ dont le cardinal est divisible par 5.

g) Quels sont les cardinaux possibles pour G ?

h) Quels sont les possibilités pour le nombre de 5-Sylow dans G ?

i) Dans cette question, on suppose que G a 6 5-Sylow. Montrer que $G = \mathfrak{A}_5$ ou $G = \mathfrak{S}_5$ (on pourra utiliser la question b).

j) Dans cette question, on suppose que G a un seul 5-Sylow. Montrer que G est contenu dans le normalisateur dans $\mathfrak{S}_5$ de son 5-Sylow. Quels sont les cardinaux possibles pour G ? Montrer que $G \subset \mathfrak{A}_5$ si et seulement si $|G| \in \{5, 10\}$.

k) Parmi les groupes G possibles, lesquels sont résolubles ?

l) On suppose que G contient une transposition. Montrer que $G = \mathfrak{S}_5$.

Exercice 10 — Groupe de Galois d'un polynôme irréductible de degré 5. Soit $P \in \mathbb{Q}[X]$ un polynôme unitaire irréductible de degré 5. On note $G = \mathrm{Gal}_{\mathbb{Q}}(P)$.

a) Montrer que $|G|$ est divisible par 5.

b) On suppose que le discriminant de P est un carré dans $\mathbb{Q}$. Montrer que le cardinal du groupe de Galois est 5, 10 ou 60.

c) On suppose que P a exactement deux racines complexes non réelles. Montrer que $G = \mathfrak{S}_5$.

d) On suppose que P a exactement quatre racines complexes non réelles. Montrer que le cardinal du groupe de Galois est 10, 20, 60 ou 120.

e) Supposons que $P \in \mathbb{Z}[X]$ et que p est un entier premier impair. Soit $\overline{P} \in \mathbb{F}_p[X]$ le polynôme déduit de P par réduction des coefficients modulo p. On suppose que $\overline{P}$ a un facteur irréductible de degré 3 dans $\mathbb{F}_p[X]$. En fonction du discriminant de P, donner la classe d'isomorphisme de $\mathrm{Gal}_{\mathbb{Q}}(P)$.

5 Applications

Exercice 11 — Exemples concrets. Dans chacun des cas suivants, montrer que P est irréductible dans $\mathbb{Q}[X]$ et calculer $\mathrm{Gal}_{\mathbb{Q}}(P)$.

a) $P = X^5 - 4$.

b) $P = X^5 + 20X + 16$ (on pourra calculer le discriminant, puis chercher des racines de $\overline{P}$ pour $p = 7$).

c) $P = X^5 - 4X + 2$ (on pourra déterminer le tableau des variations de $x \mapsto P(x)$).

d) $P = X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$ (on pourra montrer que si α est une racine primitive 11-ème de l'unité, alors P est le polynôme minimal de $\alpha + \alpha^{-1}$).

Exercice 12 — Un exemple plus délicat. Soit $P = X^5 - 5X + 12$. On veut calculer $\mathrm{Gal}_{\mathbb{Q}}(P)$.

a) Montrer que $\mathrm{Gal}_{\mathbb{Q}}(P)$ est isomorphe à un sous-groupe de $\mathfrak{A}_5$.

b) Soit $p = 3$. En décomposant $\overline{P}$ en produit de polynômes irréductibles dans $\mathbb{F}_3[X]$, montrer que $\mathrm{Gal}_{\mathbb{Q}}(P)$ contient un élément d'ordre 2. En déduire que $\mathrm{Gal}_{\mathbb{Q}}(P)$ est isomorphe à D_{10} (le groupe des isométries d'un pentagone régulier) ou à $\mathfrak{A}_5$.

Soient x_1, x_2, x_3, x_4, x_5 les racines deux à deux distinctes de P dans $\mathbb{C}$. On pose $Q := \prod_{1 \leqslant i < j \leqslant 5} (X - (x_i + x_j))$.

c) Montrer que Q est un polynôme à coefficients dans $\mathbb{Q}$ et qu'il est à racines simples dans $\mathbb{C}$.

d) Montrer que $\mathbb{Q}(x_1, x_2, x_3, x_4, x_5)$ est un corps de décomposition de Q (on pourra exprimer les x_i en fonction des coefficients de P et des racines de Q).

Dans la suite, on admet Q n'est pas irréductible dans $\mathbb{Q}[X]$.

e) Montrer que si $\mathrm{Gal}_{\mathbb{Q}}(P)$ était isomorphe à $\mathfrak{A}_5$, alors ce groupe de Galois agirait transitivement sur l'ensemble des racines de Q.

f) En déduire la classe d'isomorphisme de $\mathrm{Gal}_{\mathbb{Q}}(P)$.

Exercice 13 — Résolubilité. On dit du polynôme $P \in \mathbb{Q}[X]$ qu'il est résoluble si son corps de décomposition sur $\mathbb{Q}$ est résoluble. Pour chacun des cinq exemples ci-dessus, quels sont les polynômes qui sont résolubles ?