

Exercices de Théorie de Galois

1. Polynômes, extensions de corps

1) Soient n un entier ≥ 1 et $F = a_0 + \cdots + a_n X^n$ un polynôme dans $\mathbb{Z}[X]$. On suppose que F a une racine r dans \mathbb{Q} . Posons $r = \frac{s}{t}$ où s et t sont deux entiers premiers entre eux. Montrer que t divise a_n et que s divise a_0 . En particulier, si $a_n = 1$, alors r est dans \mathbb{Z} et r divise a_0 .

Rappel 1. Soient K un corps et $F = a_0 + \cdots + a_n X^n$ un polynôme à coefficients dans K de degré $n \geq 1$.

1. Il existe une extension de K dans laquelle F possède n racines $\alpha_1, \dots, \alpha_n$ comptées avec multiplicités.
2. Si Δ est le discriminant de F , on a l'égalité

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

C'est un élément de K .

- 2) Soient K un corps et p, q deux éléments de K . On pose

$$F = X^3 + pX + q \in K[X].$$

Calculer le discriminant de F en fonction de p et q .

3) Soient K un corps de caractéristique différente de 2 et $F \in K[X]$ un polynôme unitaire de degré 3. Soit Δ le discriminant de F .

1. On suppose que F a une racine dans K et que Δ est un carré dans K . Montrer que F a toutes ses racines dans K .
2. Donner un contre exemple à l'assertion précédente si K est de caractéristique 2.
3. Supposons $K = \mathbb{R}$ et posons $F = X^3 + pX + q$. En déduire que les racines de F sont toutes réelles si et seulement si on a $4p^3 + 27q^2 \leq 0$.

4) On pose $F = X^3 - X + 1 \in \mathbb{C}[X]$. Déterminer les racines de F dans \mathbb{C} en utilisant les formules de Cardan.

5) Soient K un corps et X_1, X_2, X_3 des indéterminées. On pose

$$F = \sum_{i \neq j} X_i^2 X_j \in K[X_1, X_2, X_3].$$

1. Montrer que F est un polynôme symétrique et exprimer F en fonction des polynômes symétriques élémentaires σ_1, σ_2 et σ_3 .
2. Même question en prenant pour F le polynôme

$$F = \sum_{i \neq j} X_i^3 X_j \in K[X_1, X_2, X_3].$$

On rappelle que l'on a

$$\sigma_1 = X_1 + X_2 + X_3, \quad \sigma_2 = X_1 X_2 + X_2 X_3 + X_1 X_3 \quad \text{et} \quad \sigma_3 = X_1 X_2 X_3.$$

6) Soit α une racine dans \mathbb{C} du polynôme $X^3 - 2 \in \mathbb{Z}[X]$. On pose $K = \mathbb{Q}(\alpha)$.

1. Quel est le degré de K sur \mathbb{Q} ?
2. Montrer que $F = X^2 + X + 1$ est irréductible dans $K[X]$.
3. Soit j une racine de F . Quel est le degré de $\mathbb{Q}(\alpha, j)$ sur \mathbb{Q} ?
4. Montrer que l'on a $\mathbb{Q}(\alpha, j) = \mathbb{Q}(\alpha + j)$.
5. Déterminer le polynôme minimal de $\alpha + j$ sur \mathbb{Q} .

7) Soit K une extension de degré 2 de \mathbb{Q} i.e. une extension quadratique de \mathbb{Q} .

1. Montrer qu'il existe un entier d sans facteurs carrés tel que $K = \mathbb{Q}(\sqrt{d})$.
2. Soient d et d' deux entiers sans facteurs carrés tels que $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d'})$. Montrer que dd' est un carré dans \mathbb{Q} .

8) Soient L une extension d'un corps K et α un élément de L algébrique sur K de degré impair. Montrer que l'on a $K(\alpha) = K(\alpha^2)$.

9) Soient α une racine dans \mathbb{C} du polynôme $X^3 - X + 1 \in \mathbb{Z}[X]$ et K le corps $\mathbb{Q}(\alpha)$.

1. Quel est le degré de K sur \mathbb{Q} ?
2. On pose $a = 1 + \alpha$. En considérant l'endomorphisme de multiplication par a dans le \mathbb{Q} -espace vectoriel K , déterminer les coordonnées de l'inverse de a dans la base $B = (1, \alpha, \alpha^2)$.

3. On pose $a = \alpha^2 - \alpha + 1$. En utilisant l'algorithme d'Euclide, déterminer les coordonnées de l'inverse de a dans B .

10) Soit P le polynôme $X^4 + X + 1 \in \mathbb{F}_2[X]$.

1. Montrer que P est irréductible.

On note K le corps $\mathbb{F}_2[X]/(P)$ et α la classe de X modulo (P) .

2. Déterminer le cardinal de K .
3. Quel est l'ordre de α dans le groupe K^* ?
4. Montrer que le polynôme $F = X^3 + X + 1$ est irréductible dans $K[X]$. Déterminer le cardinal de $K[X]/(F)$.

11) Soient L une extension finie de degré d d'un corps K et $F \in K[X]$ un polynôme de degré n irréductible sur K . Montrer que si d et n sont premiers entre eux, F est irréductible sur L .

12) Soient K et L deux extensions finies d'un corps k dont les degrés sont respectivement m et n . Soit Ω un corps contenant K et L . On note KL le composé de K et L dans Ω i.e. l'ensemble des sommes finies $\sum a_i b_i$ où $a_i \in K$ et $b_i \in L$.

1. Montrer que KL est un corps et que c'est le sous-corps de Ω engendré par K et L .
2. Montrer que KL est une extension finie de k de degré $\leq mn$.
3. Montrer que si m et n sont premiers entre eux, on a $[KL : k] = mn$.
4. Montrer qu'en général la conclusion de l'assertion 3 est fausse si m et n ne sont pas premiers entre eux.
5. Retrouver le résultat de l'exercice 11.

13) Soit K un corps fini de cardinal q : il existe un nombre premier p et un entier $n \geq 1$ tels que $q = p^n$. On note K^2 l'ensemble des éléments de K qui sont des carrés dans K i.e. l'ensemble des éléments de la forme x^2 où x est dans K .

1. Si $p = 2$ montrer que $K^2 = K$.
2. Si p est distinct de 2, montrer que $|K^2| = (q + 1)/2$.
3. En déduire que tout élément de K est la somme de deux carrés dans K .
4. Supposons $p \geq 3$. Montrer qu'un élément non nul $a \in K$ est un carré dans K si et seulement si on a $a^{\frac{q-1}{2}} = 1$.

14) Soit p un nombre premier. On pose

$$K = \mathbb{F}_p[X]/(X^2 + 1).$$

Montrer que si 4 divise $p - 3$, alors K est une extension de degré 2 de \mathbb{F}_p (on identifie ici \mathbb{F}_p et son image dans K).

15) Soient K un corps, a, b deux éléments de K et n un entier ≥ 2 . On pose

$$F = X^n + aX + b \in K[X].$$

L'objectif de cet exercice est de démontrer que le discriminant Δ de F est

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

1. Supposons que l'on ait $K = \mathbb{Q}(a, b)$ où a et b sont deux indéterminées. Soient α une racine de F dans une clôture algébrique de K et F' le polynôme dérivé de F . Démontrer l'égalité (1) en considérant le K -endomorphisme de $K(\alpha)$ de multiplication par $F'(\alpha)$.
2. En déduire l'égalité (1) dans le cas général.

16) Soient K un corps de caractéristique 0 et $F \in K[X]$ un polynôme irréductible sur K . Soient α et β deux racines distinctes de F dans une clôture algébrique de K .

1. Montrer que $\alpha - \beta$ n'est pas dans K .
2. Donner un contre exemple à l'assertion 1 si K est de caractéristique p .

17) Soient $\overline{\mathbb{Q}}$ la clôture algébrique de \mathbb{Q} dans \mathbb{C} et i une racine carrée de -1 . Montrer que l'on a

$$(\overline{\mathbb{Q}} \cap \mathbb{R})(i) = \overline{\mathbb{Q}}.$$

18) Soient K un corps, a un élément de K et p un nombre premier. On pose

$$F = X^p - a \in K[X].$$

1. Démontrer que si a n'est pas une puissance p -ième dans K , alors F est irréductible sur K .
2. L'assertion précédente est fausse si l'on remplace p par un entier qui n'est pas premier. Montrer en effet que le polynôme $X^4 + 4 \in \mathbb{Q}[X]$ est réductible sur \mathbb{Q} .

19) (Le critère d'Eisenstein sur \mathbb{Z}) Soit $F = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$ un polynôme de degré $n \geq 1$ tels que les coefficients a_i soient premiers entre eux dans leur ensemble. Soit p un nombre premier. On suppose que

$$a_i \equiv 0 \pmod{p} \quad \text{si} \quad i = 0, \dots, n-1, \quad a_0 \not\equiv 0 \pmod{p^2} \quad \text{et} \quad a_n \not\equiv 0 \pmod{p}.$$

Montrer que F est irréductible dans $\mathbb{Z}[X]$.

[Il peut être utile de rappeler ici que dans un anneau commutatif unitaire A , un élément a de A est dit irréductible s'il n'est pas inversible et si l'égalité $a = bc$ entraîne que b ou c est inversible].

Tout polynôme non constant de $\mathbb{Z}[X]$ qui est irréductible dans $\mathbb{Z}[X]$ l'est aussi dans $\mathbb{Q}[X]$ (ce résultat sera démontré plus loin dans le cours). Le polynôme F est donc irréductible dans $\mathbb{Q}[X]$.

20) Soit p un nombre premier.

1. Soit u un élément non nul de \mathbb{F}_p . Montrer que le polynôme $X^p - X + u \in \mathbb{F}_p[X]$ est irréductible sur \mathbb{F}_p .
2. Soit a un entier non divisible par p . En déduire que le polynôme $X^p - X + a \in \mathbb{Q}[X]$ est irréductible sur \mathbb{Q} .

21) Soient K un corps et F un polynôme à coefficients dans K de degré n . Montrer que F est irréductible sur K si et seulement si F n'a pas de racines dans les extensions de K dont le degré sur K est $\leq n/2$.

22) On pose $F = X^4 + 1 \in \mathbb{Z}[X]$.

1. Montrer que F est irréductible dans $\mathbb{Z}[X]$.
2. Montrer que pour tout nombre premier p , le polynôme de $\mathbb{F}_p[X]$ déduit de F en réduisant ses coefficients modulo p est réductible dans $\mathbb{F}_p[X]$.
3. Soient a et b deux entiers relatifs tels que a , b et ab ne soient pas des carrés dans \mathbb{Z} . Montrer que pour tout nombre premier p , le polynôme

$$(X^2 - a)(X^2 - b)(X^2 - ab) \in \mathbb{Z}[X],$$

a une racine modulo p (bien qu'il n'ait pas de racines dans \mathbb{Z}).

23) Soient p un nombre premier et ζ une racine primitive p -ième de l'unité dans \mathbb{C} . On pose $K = \mathbb{Q}(\zeta)$.

1. Montrer que le polynôme

$$\Phi_p(X) = \sum_{i=0}^{p-1} X^i \in \mathbb{Z}[X]$$

est irréductible sur \mathbb{Q} . En déduire que K est une extension finie de \mathbb{Q} de degré $p - 1$.

2. Montrer que $\cos \frac{2\pi}{p}$ appartient à K .
3. Quel est le degré de l'extension $\mathbb{Q}(\cos \frac{2\pi}{p})/\mathbb{Q}$?
4. Montrer que $\mathbb{Q}(\cos \frac{2\pi}{5}) = \mathbb{Q}(\sqrt{5})$.
5. Déterminer le polynôme minimal sur \mathbb{Q} de $2 \cos \frac{2\pi}{7}$.

2. Séparabilité

24) Soient K un corps, $F = X^3 - 3X - 1 \in K[X]$ et α une racine de F dans une clôture algébrique de K . Montrer que $K(\alpha)$ est une extension séparable de K .

25) Soient K un corps de caractéristique un nombre premier p et f un polynôme irréductible sur K . Montrer que f n'est pas séparable si et seulement si il existe g dans $K[X]$ tel que $f(X) = g(X^p)$.

26) Soient K un corps de caractéristique un nombre premier p et L une extension finie de K de degré non divisible par p . Montrer que L est séparable sur K .

27) Soient K un corps de caractéristique 0 et α, β deux éléments algébriques sur K . Montrer qu'il existe $n \in \mathbb{Z}$ tel que $\alpha + n\beta$ soit un élément primitif de l'extension $K(\alpha, \beta)$.

28) Soient X et Y deux indéterminées et p un nombre premier. On pose

$$K = \mathbb{F}_p(X^p, Y^p) \quad \text{et} \quad L = \mathbb{F}_p(X, Y).$$

1. Montrer que L est une extension finie de K de degré p^2 .
2. Montrer qu'il n'existe pas d'élément $\theta \in L$ tel que $L = K(\theta)$.

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

Rappel 2. Soient K un corps, Ω une clôture algébrique de K et L une extension (finie) de K contenue dans Ω . Notons $\text{Aut}(L/K)$ le groupe des automorphismes de L qui fixent K . C'est un sous-groupe du groupe des automorphismes de L . On dit que L est une extension normale de K si pour tout plongement σ de L dans Ω égal à l'identité sur K , on a $\sigma(L) = L$. On dit que L est une extension galoisienne de K , si l'une des deux conditions équivalentes suivantes est satisfaite :

- (i) l'extension L/K est normale et séparable ;
- (ii) le sous-corps de L laissé fixe par $\text{Aut}(L/K)$ est le corps K .

Dans le cas où l'extension L/K est galoisienne, le groupe $\text{Aut}(L/K)$ s'appelle le groupe de Galois de L sur K . On le note $\text{Gal}(L/K)$. Si L/K est une extension finie, $\text{Gal}(L/K)$ est un groupe fini dont l'ordre est le degré de L sur K .

Supposons que K soit de caractéristique 0 ou un corps fini. Soient f un polynôme à coefficients dans K de degré $n \geq 1$ et L son corps de décomposition dans Ω . L'extension L/K est galoisienne. On appelle groupe de Galois de f , le groupe $\text{Gal}(L/K)$. On le note souvent $\text{Gal}(f)$. Soient r le nombre de racines distinctes de f dans Ω et $R = \{\alpha_1, \dots, \alpha_r\}$ l'ensemble de ces racines (on a donc choisi implicitement une numérotation des racines de

f). Le groupe $\text{Gal}(f)$ agit sur R . Soit \mathbb{S}_r le groupe symétrique sur $\{1, \dots, r\}$. L'application $\text{Gal}(f) \rightarrow \mathbb{S}_r$ qui à σ associe la permutation déduite de σ par son action sur les α_i est un homomorphisme injectif de groupes. Ainsi, $\text{Gal}(f)$ s'identifie à un sous-groupe de \mathbb{S}_r . Un changement de numérotation des racines transforme l'image de $\text{Gal}(f)$ dans \mathbb{S}_r en un sous-groupe conjugué. Les orbites de R correspondent aux facteurs irréductibles de f . En particulier, $\text{Gal}(f)$ agit transitivement sur R si et seulement si f est irréductible sur K . Dans ce cas, on a $r = n$ et $\text{Gal}(f)$ s'identifie à un sous-groupe de \mathbb{S}_n .

Rappel 3. Soit p un nombre premier. Soit f un polynôme unitaire de degré n dans $\mathbb{Z}[X]$. Soit \bar{f} le polynôme de $(\mathbb{Z}/p\mathbb{Z})[X]$ déduit de f par réduction via l'homomorphisme $\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$. On suppose que \bar{f} est séparable. Soit

$$\bar{f} = \prod_{i=1}^t \bar{f}_i,$$

la décomposition de \bar{f} en produit de polynômes irréductibles dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Notons n_i le degré de \bar{f}_i . Alors, f est séparable et $\text{Gal}(f)$ étant identifié à un sous-groupe de \mathbb{S}_n , il existe t cycles $\sigma_1, \dots, \sigma_t$ de \mathbb{S}_n à supports disjoints, tels que, σ_i soit d'ordre n_i et que le produit $\sigma_1 \cdots \sigma_t$ appartienne à $\text{Gal}(f)$.

29) Déterminer le groupe des automorphismes de \mathbb{R} .

30) On pose $F = X^4 - 2X^2 - 1 \in \mathbb{Q}[X]$. Soient α une racine de F dans \mathbb{C} et K le corps $\mathbb{Q}(\alpha)$. Montrer que K/\mathbb{Q} est une extension de degré 4 qui n'est pas galoisienne.

31) On pose $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

1. Montrer que K est une extension galoisienne de \mathbb{Q} .
2. Expliciter le groupe $\text{Gal}(K/\mathbb{Q})$.

32) Soient a et b deux entiers relatifs. Soient \sqrt{b} une racine carrée de b dans \mathbb{C} et α une racine carrée de $a + \sqrt{b}$ dans \mathbb{C} .

1. Montrer que si $a^2 - b$ est un carré dans \mathbb{Z} , l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne de degré au plus 4.
2. Supposons $(a, b) = (7, 16)$. Montrer que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne (bien que $a^2 - b = 33$ ne soit pas un carré dans \mathbb{Z}).
3. Si $(a, b) = (4, 3)$ montrer que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ n'est pas galoisienne.

On pose $F = X^4 - 2aX^2 + a^2 - b \in \mathbb{Z}[X]$.

4. Calculer le discriminant de F .

On suppose que F est irréductible sur \mathbb{Q} .

5. Montrer que si $a^2 - b$ est un carré dans \mathbb{Z} , l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.
6. Montrer que si $a^2 - b$ appartient à $b\mathbb{Z}^2$, l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne de groupe de Galois isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

33) Pour tout entier $n \geq 3$ déterminer une extension non galoisienne de \mathbb{Q} de degré n .

34) Soient p un nombre premier et ζ une racine primitive p -ième de l'unité dans \mathbb{C} .

1. Montrer que $\mathbb{Q}(\zeta)$ est une extension galoisienne de \mathbb{Q} de degré $p - 1$.
2. Montrer que le groupe de Galois $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$.

35) Soient p un nombre premier et $F = X^p - 2 \in \mathbb{Q}[X]$. Quel est le degré sur \mathbb{Q} du corps de décomposition de F dans \mathbb{C} ?

36) Soient K un corps et Ω une clôture algébrique de K . Soient F un polynôme à coefficients dans K de degré $n \geq 1$ et Δ son discriminant. Montrer que $K(\sqrt{\Delta})$ est contenu dans le corps de décomposition de F dans Ω .

37) Soit f un polynôme unitaire irréductible de degré n à coefficients dans \mathbb{Q} . On identifie $\text{Gal}(f)$ à un sous-groupe de \mathbb{S}_n . Montrer que $\text{Gal}(f)$ est contenu dans \mathbb{A}_n (le sous-groupe alterné de \mathbb{S}_n) si et seulement si le discriminant de f est un carré dans \mathbb{Q} .

38) Soient F un polynôme de degré 3 à coefficients dans \mathbb{Q} irréductible sur \mathbb{Q} , Δ son discriminant et α une racine de F dans \mathbb{C} .

1. Montrer que le corps de décomposition de F est $\mathbb{Q}(\sqrt{\Delta}, \alpha)$.
2. En déduire que l'extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ est galoisienne si et seulement si Δ est un carré dans \mathbb{Q} .
3. Expliciter une extension galoisienne (resp. non galoisienne) de \mathbb{Q} de degré 3.
4. Montrer que le groupe de Galois sur $\mathbb{Q}(\sqrt{-19})$ du polynôme $X^3 - 2X + 2$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}$.

39) Soit f le polynôme $X^4 + 8X + 12 \in \mathbb{Q}[X]$.

1. Montrer que f est irréductible sur \mathbb{Q} .
2. Montrer que $\text{Gal}(f)$ est isomorphe à \mathbb{A}_4 .
3. Soit L le corps de décomposition de f dans \mathbb{C} . Montrer qu'il n'existe pas d'extension quadratique de \mathbb{Q} contenue dans L .

40) Soit f le polynôme $X^4 + X + 1 \in \mathbb{Q}[X]$.

1. Montrer que f est irréductible sur \mathbb{Q} .

2. Montrer que $\text{Gal}(f)$ est isomorphe à \mathbb{S}_4 .
3. Soit α une racine de f dans \mathbb{C} . Montrer qu'il n'existe pas d'extension quadratique de \mathbb{Q} contenue dans $\mathbb{Q}(\alpha)$.

41) Soient ℓ et p deux nombres premiers distincts. On note

$$\Phi_p = \sum_{i=0}^{p-1} X^i \in \mathbb{F}_\ell[X],$$

le p -ième polynôme cyclotomique à coefficients dans \mathbb{F}_ℓ .

1. Soit F un facteur irréductible de Φ_p dans $\mathbb{F}_\ell[X]$. Montrer que le degré de F est égal à l'ordre de la classe de ℓ dans $(\mathbb{Z}/p\mathbb{Z})^*$.
2. En déduire que Φ_p est irréductible sur \mathbb{F}_ℓ si et seulement si la classe de ℓ modulo p est un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$.
3. Quels sont les nombres premiers ℓ pour lesquels Φ_5 soit irréductible sur \mathbb{F}_ℓ ?

42) Soient p un nombre premier et f un polynôme irréductible de $\mathbb{Q}[X]$ de degré p . Soit K le corps de décomposition de f dans \mathbb{C} . On suppose que f possède exactement deux zéros non réels. Montrer que le groupe de Galois de K sur \mathbb{Q} est isomorphe à \mathbb{S}_p .

Application. Montrer que le groupe de Galois du polynôme $f = X^5 - 4X^3 - 2 \in \mathbb{Q}[X]$ est isomorphe à \mathbb{S}_5 .

43) Soient f un polynôme irréductible de $\mathbb{Q}[X]$ et K le corps de décomposition de f dans \mathbb{C} . On suppose que le groupe de Galois de K sur \mathbb{Q} est abélien. Montrer que pour toute racine α de f , on a $K = \mathbb{Q}(\alpha)$.

4. Correspondance de Galois

44) Soit G un groupe cyclique d'ordre n .

1. Montrer que tout sous-groupe de G est cyclique.
2. Montrer que pour tout diviseur positif d de n , il existe un unique sous-groupe de G d'ordre d .

45) Décrire les extensions de \mathbb{Q} contenues dans K dans les cas suivants :

1. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$;
2. K est le corps de décomposition du polynôme $X^3 - 4X + 1 \in \mathbb{Q}[X]$;
3. $K = \mathbb{Q}(\zeta)$, où ζ est une racine primitive 7-ième de l'unité de \mathbb{C} .
4. $K = \mathbb{Q}(\zeta)$, où ζ est une racine primitive 8-ième de l'unité de \mathbb{C} .

46) Soient a et t des entiers. Posons $F = X^4 - 2aX^2 + t^2 \in \mathbb{Z}[X]$ et notons K le corps de décomposition de F dans \mathbb{C} . On suppose que F est irréductible sur \mathbb{Q} .

1. Montrer que le groupe de Galois de K sur \mathbb{Q} est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$.
2. Décrire les sous-corps de K .

47) Soit D_4 le sous-groupe de \mathbb{S}_4 engendré le 4-cycle $a = (1, 2, 3, 4)$ et la transposition $b = (2, 4)$.

1. Montrer que l'on a (où e est l'élément de neutre de \mathbb{S}_4)

$$D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

On l'appelle le groupe diédral d'ordre 8. C'est l'un des deux groupes non abéliens d'ordre 8.

2. Montrer que D_4 possède exactement dix sous-groupes :

$$\begin{aligned} &\{e\}, \quad \{e, b\}, \quad \{e, ab\}, \quad \{e, a^2\}, \quad \{e, a^2b\}, \quad \{e, a^3b\}, \\ &\{e, a, a^2, a^3\}, \quad \{e, a^2, ab, a^3b\}, \quad \{e, a^2, b, a^2b\}, \quad D_4. \end{aligned}$$

Considérons alors un nombre premier p et posons $f = X^4 - p \in \mathbb{Q}[X]$. Soient L le corps de décomposition de f dans \mathbb{C} et G le groupe de Galois de L sur \mathbb{Q} .

3. Montrer que G est isomorphe à D_4 .
4. Pour chaque sous-groupe H de G expliciter le sous-corps de L laissé fixe par H . En déduire la liste des extensions de \mathbb{Q} contenues dans L .
5. Déterminer un élément primitif de L .

48) Soient p un nombre premier impair et ξ une racine primitive p -ième de l'unité dans \mathbb{C} . On rappelle que le polynôme minimal de ξ sur \mathbb{Q} est le p -ième polynôme cyclotomique

$$\Phi_p = \sum_{i=0}^{p-1} X^i \in \mathbb{Z}[X].$$

1. Montrer que le discriminant Δ de Φ_p est

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

2. Montrer qu'il existe une unique extension quadratique L de \mathbb{Q} contenue dans $\mathbb{Q}(\xi)$. Déterminer L .