Exercices - Théorie de Galois

Les exercices sont gradués : ⋆ application directe du cours, ⋆⋆ mise en œuvre, ⋆⋆⋆ problème, ⋆⋆⋆⋆ difficile.

Chapitre 1 - Groupes

Questions de cours

Q1. Démontrer la proposition 1.1 : dans un groupe, le neutre est unique et chaque élément possède un unique symétrique.

Q2. Énoncer la proposition 1.3, puis l'utiliser pour démontrer que $\mathfrak{A}_n$ est un sous-groupe de $\mathfrak{S}_n$, et que l'ensemble des permutations impaires n'en est pas un.

Q3. Démontrer la proposition 1.8 : le noyau et l'image d'un morphisme sont des sous-groupes, et un morphisme est injectif si et seulement si son noyau est trivial.

Q4. Démontrer la proposition 1.9, puis en déduire qu'il existe, à isomorphisme près, un unique groupe d'ordre p pour tout nombre premier p.

Q5. Démontrer que l'ordre d'une permutation est le PPCM des longueurs des cycles de sa décomposition.

Q6. Démontrer la propriété 1.15, puis en déduire le petit théorème de Fermat.

Exercice 1 ⋆

1. Les ensembles suivants, munis de la loi indiquée, sont-ils des groupes ? Justifier.

   (a) $(\mathbb{N}\,;+)$

   (b) $(\mathbb{Z}\,;\times)$

   (c) $(\mathbb{Q}^*\,;\times)$

   (d) l'ensemble des racines n-ièmes de l'unité, pour $\times$

   (e) $(\mathbb{Z}/6\mathbb{Z}\,;+)$

   (f) $(\mathbb{Z}/6\mathbb{Z}\setminus\{0\}\,;\times)$

2. Déterminer l'ordre de chacun des éléments de $\mathbb{Z}/12\mathbb{Z}$.

3. Déterminer l'ordre des permutations suivantes de $\mathfrak{S}_5$:

$$(1\ 2\ 3) \qquad (1\ 2)(3\ 4) \qquad (1\ 2\ 3\ 4\ 5) \qquad (1\ 2\ 3)(4\ 5)$$

Exercice 2 ⋆⋆

Soit p un nombre premier. Déterminer le nombre de sous-groupes du groupe $(\mathbb{Z}/p\mathbb{Z})^2$. Plus généralement, combien le groupe $(\mathbb{Z}/p\mathbb{Z})^n$ possède-t-il de sous-groupes d'ordre p ?

Exercice 3 ⋆

On travaille dans $\mathfrak{S}_n$.

1. Décomposer en produit de cycles à supports disjoints la permutation de $\mathfrak{S}_9$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 9 & 2 & 6 & 1 & 4 & 8 \end{pmatrix}$$

2. En déduire l'ordre de σ, puis sa signature.

3. Écrire $(1\ 2\ 3\ 4)$ comme produit de transpositions, de deux façons différentes. Que doivent avoir en commun ces deux écritures ?

4. Combien $\mathfrak{S}_4$ possède-t-il d'éléments de chaque ordre ? Dresser un tableau.

Exercice 4 ⋆⋆

1. Démontrer qu'un groupe d'ordre 4 est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à $(\mathbb{Z}/2\mathbb{Z})^2$.
2. Soit G un groupe dans lequel $x^2 = e$ pour tout x. Démontrer que G est abélien. Si G est fini, quel est son ordre possible ?
3. Donner un exemple de groupe non abélien d'ordre 6, et démontrer qu'il n'y en a qu'un à isomorphisme près.

Exercice 5 ⋆⋆

On note D_4 le groupe des isométries du carré, engendré par la rotation r d'angle $\frac{\pi}{2}$ et une symétrie axiale s.

1. Démontrer que $r^4 = s^2 = \mathrm{id}$ et $srs = r^{-1}$, puis que D_4 est d'ordre 8.
2. Dresser la liste des huit éléments et déterminer l'ordre de chacun.
3. Déterminer tous les sous-groupes de D_4. On en trouvera dix, et l'on tracera le treillis.

Exercice 6 ⋆⋆

1. Soit $n \geqslant 1$. Démontrer que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est isomorphe au groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$, et que son ordre vaut $\varphi(n)$.
2. Expliciter $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z})$ et $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z})$, et préciser leur structure.
3. Déterminer tous les sous-groupes de $\mathfrak{S}_4$ d'ordre 4. Combien y en a-t-il, et lesquels sont isomorphes entre eux ?

Chapitre 2 - Quotients, actions et résolubilité

Questions de cours

Q1. Énoncer les caractérisations de la proposition 2.1, puis démontrer qu'un sous-groupe d'indice 2 est distingué.

Q2. Énoncer et démontrer le premier théorème d'isomorphisme (théorème 2.2), puis en déduire que $\mathfrak{S}_n/\mathfrak{A}_n \simeq \mathbb{Z}/2\mathbb{Z}$ pour $n \geqslant 2$.

Q3. Démontrer la formule de conjugaison (proposition 2.3), puis en déduire que deux permutations sont conjuguées si et seulement si elles ont le même type.

Q4. Démontrer le théorème orbite-stabilisateur (théorème 2.4), puis établir l'équation aux classes et en déduire que le centre d'un p-groupe non trivial n'est pas réduit à l'élément neutre.

Q5. Démontrer la proposition 2.5 sur le groupe dérivé, puis établir que $D(\mathfrak{S}_n) = \mathfrak{A}_n$ pour $n \geqslant 2$.

Q6. Démontrer la simplicité de $\mathfrak{A}_5$ à l'aide de ses classes de conjugaison, en établissant la partition $60 = 1 + 15 + 20 + 12 + 12$.

Exercice 7 ⋆⋆⋆

Le théorème de Lagrange affirme que l'ordre d'un sous-groupe divise celui du groupe. Cet exercice montre que la réciproque est fausse.

1. Vérifier que $|\mathfrak{A}_4| = 12$, et que 6 divise 12.
2. Dresser la liste des douze éléments de $\mathfrak{A}_4$ avec leurs ordres.
3. Supposons qu'il existe $H \leqslant \mathfrak{A}_4$ d'ordre 6. Justifier que H est d'indice 2, donc distingué, et que $\mathfrak{A}_4/H$ est d'ordre 2.

4. En déduire que $x^2 \in H$ pour tout $x \in \mathfrak{A}_4$, puis compter les carrés des 3-cycles. Conclure.
5. Quel est, en revanche, le plus petit ordre d'un sous-groupe de $\mathfrak{A}_4$ contenant les trois doubles transpositions ?

Exercice 8 $\star\star$

Le *groupe des quaternions* $Q_8 = \{\pm 1\,;\pm \mathrm{i}\,;\pm \mathrm{j}\,;\pm \mathrm{k}\}$ est défini par les relations

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1 \qquad \mathrm{ij} = \mathrm{k}, \quad \mathrm{jk} = \mathrm{i}, \quad \mathrm{ki} = \mathrm{j}$$

l'élément -1 étant central et d'ordre 2.

1. Démontrer que $\mathrm{ji} = -\mathrm{k}$, puis que Q_8 n'est pas abélien.
2. Déterminer l'ordre de chacun des huit éléments. Combien Q_8 possède-t-il d'éléments d'ordre 2 ?
3. En déduire que Q_8 n'est isomorphe ni à $\mathbb{Z}/8\mathbb{Z}$, ni à D_4.
4. Déterminer tous les sous-groupes de Q_8. On en trouvera six.
5. Démontrer que *tous* sont distingués. Un groupe non abélien dont tout sous-groupe est distingué est dit *hamiltonien* : Q_8 est le plus petit.
6. Déterminer $Z(Q_8)$, puis identifier le quotient $Q_8/Z(Q_8)$.

Exercice 9 $\star\star\star$

Soit p un nombre premier. Le *groupe de Heisenberg* $H(\mathbb{F}_p)$ est l'ensemble des matrices

$$M(a\,;b\,;c) = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \qquad (a\,;b\,;c) \in \mathbb{F}_p^3$$

muni du produit matriciel.

1. Vérifier que $H(\mathbb{F}_p)$ est un groupe et que $\left|H(\mathbb{F}_p)\right| = p^3$. On explicitera $M(a\,;b\,;c)^{-1}$.
2. Démontrer que $M(a\,;b\,;c)\,M(a'\,;b'\,;c') = M\big(a+a'\,;\,b+b'\,;\,c+c'+ab'\big)$, et en déduire que le groupe n'est pas abélien.
3. Déterminer le centre de $H(\mathbb{F}_p)$ et identifier le quotient $H(\mathbb{F}_p)/Z$.
4. En posant $N = M(a\,;b\,;c) - I_3$, vérifier que $N^3 = 0$, puis démontrer que pour p *impair* :
$$M(a\,;b\,;c)^p = I_3$$
5. Conclure : pour p impair, $H(\mathbb{F}_p)$ est un groupe non abélien dans lequel $x^p = e$ pour tout x. Comparer avec la question 2 de l'exercice 4, et expliquer pourquoi il n'y a pas contradiction.
6. Que devient le résultat de la question 4 pour $p = 2$? Identifier alors $H(\mathbb{F}_2)$.

Exercice 10 $\star$

1. Décrire les éléments du quotient $\mathbb{Z}/12\mathbb{Z}$ modulo le sous-groupe $\langle 4\rangle$, et identifier ce quotient.
2. Identifier $\mathfrak{S}_3/\mathfrak{A}_3$, puis $D_4/\langle r^2\rangle$.
3. Soit G un groupe et $H \trianglelefteq G$. Démontrer que si G est abélien, alors G/H l'est. La réciproque est-elle vraie ?
4. Démontrer que $G/Z(G)$ cyclique entraîne G abélien. En déduire qu'un groupe d'ordre p^2 est abélien.

Exercice 11 ⋆⋆

1. Dresser la liste des classes de conjugaison de $\mathfrak{S}_4$, avec leurs cardinaux. Vérifier que la somme vaut 24.
2. Faire de même pour $\mathfrak{S}_5$. On trouvera sept classes.
3. En déduire, sans calcul supplémentaire, les sous-groupes distingués possibles de $\mathfrak{S}_4$: un sous-groupe distingué est une réunion de classes de conjugaison contenant id, dont le cardinal divise 24.

Exercice 12 ⋆⋆

1. Énoncer le théorème de Cauchy, puis l'appliquer pour montrer qu'un groupe d'ordre 15 contient un élément d'ordre 3 et un élément d'ordre 5.
2. Soit G d'ordre 15. À l'aide des théorèmes de Sylow, démontrer que G possède un unique 3-Sylow et un unique 5-Sylow, puis que $G \simeq \mathbb{Z}/15\mathbb{Z}$.
3. Soit G d'ordre 12. Démontrer que G n'est pas simple. On discutera selon le nombre de 3-Sylow.
4. Démontrer qu'un groupe d'ordre pq, avec $p < q$ premiers et $p \nmid q - 1$, est cyclique.

Exercice 13 ⋆⋆⋆

Démontrer qu'un groupe fini qui possède au plus un sous-groupe de chaque ordre est cyclique. On pourra commencer par le cas où l'ordre du groupe est une puissance d'un nombre premier.

Exercice 14 ⋆⋆⋆⋆

Soit G un groupe d'ordre 60 possédant plus d'un 5-Sylow. Démontrer que G est simple.

Exercice 15 ⋆⋆⋆

Soit p un nombre premier. Le *groupe affine* de $\mathbb{F}_p$ est

$$\mathrm{Aff}(\mathbb{F}_p) = \{\varphi_{a,b} : x \mapsto ax + b \mid a \in \mathbb{F}_p^*,\ b \in \mathbb{F}_p\}$$

muni de la composition.

1. Démontrer que c'est un groupe d'ordre $p(p-1)$, non abélien dès que $p \geqslant 3$.
2. Démontrer que le sous-groupe T des translations est distingué, isomorphe à $\mathbb{Z}/p\mathbb{Z}$, et que le quotient est isomorphe à $\mathbb{F}_p^*$.
3. En déduire que $\mathrm{Aff}(\mathbb{F}_p)$ est résoluble, en exhibant une suite de résolubilité.
4. Déterminer $Z\big(\mathrm{Aff}(\mathbb{F}_p)\big)$ pour $p \geqslant 3$.
5. Traiter le cas $p = 3$: quel groupe déjà rencontré reconnaît-on ?
6. Faire agir $\mathrm{Aff}(\mathbb{F}_p)$ sur $\mathbb{F}_p$. Démontrer que l'action est transitive, et que le stabilisateur de 0 est isomorphe à $\mathbb{F}_p^*$. Vérifier la formule orbite-stabilisateur.

Pour $p = 5$, ce groupe réapparaîtra à l'exercice 37 comme groupe de Galois de $X^5 - 2$ sur $\mathbb{Q}$.

Exercice 16 ⋆⋆⋆

On pose $G = \mathrm{SL}_2(\mathbb{F}_3)$, groupe des matrices de $\mathcal{M}_2(\mathbb{F}_3)$ de déterminant 1.

1. Démontrer que $|G| = 24$. On comptera d'abord les couples $(u\,;v)$ de vecteurs formant une base de $\mathbb{F}_3^2$, puis on tiendra compte de la condition sur le déterminant.
2. Démontrer que $-I_2$ est le *seul* élément d'ordre 2 de G. On résoudra $A^2 = I_2$ avec $\det A = 1$.

3. Combien $\mathfrak{S}_4$ possède-t-il d'éléments d'ordre 2 ? En déduire que G et $\mathfrak{S}_4$ ne sont pas isomorphes, bien qu'ils soient de même ordre.
4. Démontrer que $\{\pm I_2\}$ est distingué dans G, et que le quotient est d'ordre 12. On admettra qu'il est isomorphe à $\mathfrak{A}_4$.
5. Le groupe G est-il résoluble ? Justifier à l'aide du théorème 2.8 et de la question précédente.
6. Pourquoi cet exemple montre-t-il que l'ordre d'un groupe ne détermine pas sa structure, même lorsqu'il est petit ?

Exercice 17 $\star\star\star$

Soit $\mathbb{F}$ un corps fini et $n \geqslant 1$. Démontrer que le groupe des matrices triangulaires supérieures inversibles de taille n à coefficients dans $\mathbb{F}$ est résoluble.

Chapitre 3 - Anneaux, corps et polynômes

Questions de cours

Q1. Démontrer la proposition 3.1 : le noyau d'un morphisme d'anneaux est un idéal, et les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$.

Q2. Démontrer le théorème 3.2, puis en déduire que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Q3. Démontrer que la caractéristique d'un corps est nulle ou première (proposition 3.2), puis le « rêve du débutant » (proposition 3.3).

Q4. Démontrer que $K[X]$ est principal (théorème 3.4), puis qu'un polynôme non nul de degré n possède au plus n racines dans K (proposition 3.6).

Q5. Démontrer le lemme de Gauss et le critère d'Eisenstein (théorème 3.6), puis l'appliquer à Φ_p après le changement de variable $X \mapsto X + 1$.

Exercice 18 ⋆

1. Effectuer la division euclidienne de $X^4 + X^3 + 2X + 1$ par $X^2 + 1$ dans $\mathbb{Q}[X]$.
2. Déterminer le PGCD de $X^4 - 1$ et $X^6 - 1$ dans $\mathbb{Q}[X]$, puis une relation de Bézout.
3. Donner un polynôme de degré 2 ayant quatre racines dans $\mathbb{Z}/8\mathbb{Z}$. Pourquoi n'y a-t-il pas contradiction ?

Exercice 19 ⋆⋆

1. Les polynômes suivants sont-ils irréductibles sur $\mathbb{Q}$? Justifier par le critère le plus économique.

   (a) $X^2 - 2$
   (b) $X^3 - 3X - 1$
   (c) $X^4 + 1$
   (d) $X^5 - 4X + 2$
   (e) $X^4 + X^3 + X^2 + X + 1$
   (f) $X^4 + 4$

2. Démontrer que $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais réductible sur $\mathbb{F}_p$ pour *tout* nombre premier p. On traitera d'abord le cas $p = 2$.
3. Énoncer le critère d'Eisenstein et l'appliquer à $\Phi_p(X) = X^{p-1} + \cdots + X + 1$ après le changement de variable $X \mapsto X + 1$.
4. Démontrer que la réduction modulo p fournit un critère d'irréductibilité, et l'appliquer à $X^3 + X + 1$ sur $\mathbb{Q}$ en réduisant modulo 2.

Exercice 20 ⋆

Soit α la classe de X dans $\mathbb{Q}[X]/(X^3 - X^2 + X + 2)$. Justifier que ce quotient est un corps, puis exprimer $(\alpha^2 + \alpha + 1)(\alpha^2 - \alpha)$ et $(\alpha - 1)^{-1}$ sous la forme $a\alpha^2 + b\alpha + c$, avec $a, b, c \in \mathbb{Q}$.

Exercice 21 ⋆⋆

1. Construire explicitement $\mathbb{F}_4$ comme $\mathbb{F}_2[X]/(X^2 + X + 1)$: dresser les tables d'addition et de multiplication.
2. Vérifier que le groupe multiplicatif $\mathbb{F}_4^*$ est cyclique et en exhiber un générateur.
3. Construire $\mathbb{F}_8$ comme $\mathbb{F}_2[X]/(X^3 + X + 1)$. Combien d'éléments ? Quel est l'ordre de la classe de X ?
4. Construire $\mathbb{F}_9$ comme $\mathbb{F}_3[X]/(X^2 + 1)$, après avoir vérifié l'irréductibilité.

Exercice 22 ⋆⋆

1. Dresser la liste des polynômes unitaires de degré 2 de $\mathbb{F}_2[X]$, et déterminer lesquels sont irréductibles.
2. Faire de même en degré 3. Combien en trouve-t-on ?
3. Soit p un nombre premier. Pour tout entier $d \geqslant 1$, on note N_d le nombre de polynômes unitaires irréductibles de degré d de $\mathbb{F}_p[X]$. Démontrer que, pour tout entier $n \geqslant 1$, on a $\sum_{d|n} d\, N_d = p^n$, la somme portant sur les diviseurs positifs d de n. On pourra établir que $X^{p^n} - X$ est le produit des polynômes unitaires irréductibles de $\mathbb{F}_p[X]$ dont le degré divise n.
4. En déduire N_1, N_2, N_3 et N_4 sur $\mathbb{F}_2$, et comparer aux questions 1 et 2.

Chapitre 4 - Extensions de corps

Questions de cours

Q1. Démontrer le théorème 4.1 de multiplicativité des degrés.

Q2. Démontrer le théorème 4.2 : le polynôme minimal est irréductible, et $K(\alpha) \simeq K[X]/(\mu_\alpha)$ admet $(1\,;\alpha\,;\ldots\,;\alpha^{n-1})$ pour base.

Q3. Démontrer la proposition 4.3 : une extension finie est algébrique, et les éléments algébriques sur K forment un corps.

Q4. Démontrer la proposition 4.4 de prolongement des isomorphismes, puis en déduire le théorème 4.4 d'unicité du corps de décomposition.

Q5. Énoncer le critère de Wantzel (théorème 4.5), puis démontrer l'impossibilité de la duplication du cube et de la trisection de l'angle $\dfrac{\pi}{3}$.

Q6. Démontrer qu'une extension de degré premier n'admet aucun corps strictement intermédiaire.

Exercice 23 ⋆

1. Déterminer le polynôme minimal sur $\mathbb{Q}$ de chacun des nombres ci-dessous, en justifiant à chaque fois l'irréductibilité.

   (a) $\sqrt[3]{5}$ (c) $\zeta_5 = \mathrm{e}^{2\mathrm{i}\pi/5}$

   (b) $\mathrm{i}\sqrt{3}$ (d) $1+\sqrt{2}$

2. Déterminer le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}(\sqrt{3})$, puis sur $\mathbb{Q}(\sqrt{2})$.

Exercice 24 ⋆⋆⋆

Soit F un corps de caractéristique différente de 2. Pour toute extension E de F de degré 2, on note $S(E)$ l'ensemble des $a \in F^*$ qui sont des carrés dans E.

1. Démontrer que $S(E)$ est un sous-groupe de F^* contenant $F^{*2} = \{x^2\ ;\ x \in F^*\}$.
2. Démontrer que deux extensions E et E' de F de degré 2 sont F-isomorphes si et seulement si $S(E) = S(E')$.
3. En déduire qu'il existe une infinité d'extensions de $\mathbb{Q}$ de degré 2, deux à deux non isomorphes.

Exercice 25 ⋆⋆⋆

Soit K un corps et $f \in K[X]$ un polynôme de degré p premier. On suppose que, pour toute extension L de K, dès que f possède une racine dans L, il est scindé sur L. Démontrer que f est irréductible sur K ou possède une racine dans K.

Exercice 26 ⋆⋆

Déterminer le corps de décomposition L de $X^5 - 2$ sur $\mathbb{Q}$, ainsi que son degré $[L : \mathbb{Q}]$.

Exercice 27 ⋆⋆

Démontrer que ni l'heptagone régulier ni l'ennéagone régulier ne sont constructibles à la règle et au compas. Pourquoi la quadrature du cercle échappe-t-elle à ce type de raisonnement ?

Chapitre 5 - Séparabilité, normalité, corps finis

Questions de cours

Q1. Démontrer les propositions 5.1 et 5.2, puis en déduire que tout corps de caractéristique nulle est parfait.

Q2. Démontrer que $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale, et que sa clôture normale dans $\mathbb{C}$ est de degré 6.

Q3. Démontrer que tout corps fini a pour cardinal une puissance d'un nombre premier, puis énoncer le théorème 5.3 de classification.

Q4. Démontrer la proposition 5.5 : les sous-corps de $\mathbb{F}_{p^n}$ sont les $\mathbb{F}_{p^d}$ pour $d \mid n$.

Q5. Démontrer le théorème 5.4 : le groupe multiplicatif d'un corps fini est cyclique.

Q6. Énoncer le théorème de l'élément primitif (théorème 5.5), puis déterminer un élément primitif de $\mathbb{Q}(\sqrt{2}\,;\sqrt{3})$ sur $\mathbb{Q}$.

Exercice 28 ⋆⋆

1. Démontrer que toute extension de degré 2 est normale.
2. Donner un exemple de tour $K \subseteq M \subseteq L$ où L/M et M/K sont normales sans que L/K le soit. On pourra prendre $K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt{2})$, $L = \mathbb{Q}(\sqrt[4]{2})$.

Exercice 29 ⋆

1. Déterminer tous les sous-corps de $\mathbb{F}_{64}$, et tracer le treillis correspondant.
2. Même question pour $\mathbb{F}_{3^{12}}$.

Exercice 30 ⋆⋆

1. Déterminer tous les générateurs de $\mathbb{F}_7^*$, puis de $\mathbb{F}_{11}^*$.
2. Combien $\mathbb{F}_q^*$ possède-t-il de générateurs ? Exprimer la réponse à l'aide de l'indicatrice d'Euler.
3. Démontrer le théorème de Wilson : $(p-1)! \equiv -1\ [p]$ pour p premier. On appariera chaque élément avec son inverse.
4. En déduire la valeur de 6! modulo 7, et vérifier par le calcul direct.

Exercice 31 ⋆⋆⋆

Soit p un nombre premier impair. Démontrer que -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1\ [4]$, puis que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1\ [8]$. On pourra considérer une racine primitive huitième de l'unité x dans une extension de $\mathbb{F}_p$, et l'élément $x + x^{-1}$.

Exercice 32 ⋆⋆

Soit p un nombre premier et $n \geqslant 1$ un entier premier à p. Démontrer que le corps de décomposition de $X^n - 1$ sur $\mathbb{F}_p$ est $\mathbb{F}_{p^d}$, où d est l'ordre de $\overline{p}$ dans le groupe $(\mathbb{Z}/n\mathbb{Z})^*$. Déterminer le corps engendré sur $\mathbb{F}_3$ par une racine primitive septième de l'unité. Que devient le corps de décomposition lorsqu'on remplace $X^n - 1$ par $X^{p^m} - 1$?

Exercice 33 ⋆⋆⋆

1. Déterminer un élément primitif de $\mathbb{Q}(\sqrt[3]{2}\,;\mathrm{j})$ sur $\mathbb{Q}$, où $\mathrm{j} = \mathrm{e}^{2\mathrm{i}\pi/3}$.
2. Démontrer que l'extension $\mathbb{F}_p(T\,;S)/\mathbb{F}_p(T^p\,;S^p)$ est finie mais n'admet *aucun* élément primitif. On montrera qu'elle possède une infinité de corps intermédiaires.
3. Quelle hypothèse du théorème 5.5 est ici mise en défaut ?

Chapitre 6 - La correspondance de Galois

Questions de cours

Q1. Démontrer la proposition 6.2 : pour toute extension finie, $|\mathrm{Aut}(L/K)| \leqslant [L : K]$.

Q2. Démontrer le théorème 6.1 de Dedekind, puis en déduire le théorème 6.2 d'Artin.

Q3. Énoncer le théorème 6.3, qui caractérise les extensions galoisiennes, puis le théorème fondamental 6.4.

Q4. Retrouver le groupe de Galois et le treillis des sous-corps de $\mathbb{Q}(\sqrt[3]{2}\,;\mathrm{j})$, puis de $\mathbb{Q}(\sqrt[4]{2}\,;\mathrm{i})$.

Exercice 34 ⋆⋆

Déterminer le polynôme minimal de $\sqrt{2}+\sqrt{3}+\sqrt{5}$ sur $\mathbb{Q}$.

Exercice 35 ⋆⋆

Déterminer le groupe de Galois du polynôme X^4+X^3+1 sur chacun des corps $\mathbb{F}_2$, $\mathbb{F}_3$ et $\mathbb{F}_4$.

Exercice 36 ⋆⋆⋆

Démontrer que le groupe de Galois de X^6+3 sur $\mathbb{Q}$ est isomorphe à $\mathfrak{S}_3$. Démontrer ensuite que ce polynôme, irréductible sur $\mathbb{Q}$, est réductible sur $\mathbb{F}_p$ pour tout nombre premier p.

Exercice 37 ⋆⋆⋆

Déterminer le groupe de Galois de X^5-2 sur $\mathbb{Q}$, dont l'exercice 26 a calculé le corps de décomposition. On le comparera au groupe affine $\mathrm{Aff}(\mathbb{F}_5)$ de l'exercice 15.

Exercice 38 ⋆⋆⋆

Soit K un corps de caractéristique $p>0$, $a \in K$ et $f = X^p - X - a$. On suppose que f n'a aucune racine dans K. Démontrer que f est irréductible sur K, que son corps de décomposition est engendré par n'importe laquelle de ses racines, et que son groupe de Galois est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. En déduire que $X^p - X - 1$ est irréductible sur $\mathbb{Q}$ pour tout nombre premier p.

Exercice 39 ⋆⋆⋆

Soit $n \geqslant 1$, et t, u deux indéterminées. Démontrer que l'extension $\mathbb{C}(t\,;u)/\mathbb{C}(t^n\,;u^n)$ est galoisienne, et déterminer son groupe de Galois.

Exercice 40 ⋆⋆⋆

Soient $a, b \in \mathbb{Q}$ tels que $b>0$ ne soit pas le carré d'un rationnel et que $a+\sqrt{b}>0$. On dit que $\alpha = \sqrt{a+\sqrt{b}}$ se *désimbrique* s'il appartient à un corps de la forme $\mathbb{Q}(\sqrt{c_1}\,;\ldots\,;\sqrt{c_k})$, avec $c_1,\ldots,c_k \in \mathbb{Q}$. Démontrer que α se désimbrique si et seulement si a^2-b est le carré d'un rationnel. Lesquels des nombres suivants se désimbriquent ? Le cas échéant, en donner une écriture sans radical emboîté.

$$\sqrt{2+\sqrt{11}} \qquad \sqrt{6+\sqrt{11}} \qquad \sqrt{11+6\sqrt{2}} \qquad \sqrt{11+\sqrt{6}}$$

Exercice 41 ⋆⋆⋆⋆

Soit K un corps, $L = K(X_1\,;X_2\,;X_3\,;X_4)$ le corps des fractions rationnelles en quatre indéterminées, et $M = K(s_1\,;s_2\,;s_3\,;s_4)$ le sous-corps engendré par les fonctions symétriques élémentaires. Démontrer que $\theta = X_1X_3 + X_2X_4$ possède un polynôme minimal de degré 3 sur M, et l'expliciter à l'aide de s_1, s_2, s_3 et s_4. Démontrer ensuite que le corps des invariants du sous-groupe de $\mathfrak{S}_4$ engendré par (1 2 3 4) et (1 3) est $M(\theta)$.

Exercice 42 ⋆⋆⋆⋆

On pose $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ et $E = \mathbb{Q}(\alpha)$. Démontrer que $E/\mathbb{Q}$ est une extension galoisienne de degré 8, dont le groupe de Galois est isomorphe au groupe des quaternions Q_8 de l'exercice 8.

Chapitre 7 - Résolubilité par radicaux

Questions de cours

Q1. Démontrer la proposition 7.1 : $X^n - 1 = \prod_{d|n} \Phi_d$ et $\Phi_n \in \mathbb{Z}[X]$.

Q2. Énoncer le théorème 7.2, puis en déduire que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

Q3. Démontrer que tout polynôme de degré au plus 4 est résoluble par radicaux, et interpréter la méthode de Cardan comme une tour de radicaux.

Q4. Démontrer la proposition 7.5, puis en déduire le théorème d'Abel-Ruffini.

Q5. Énoncer le théorème de Gauss-Wantzel sur les polygones réguliers constructibles.

Q6. Démontrer le théorème fondamental de l'algèbre à l'aide de la théorie de Galois (théorème 7.8).

Exercice 43 ⋆

1. Calculer Φ_n pour n allant de 1 à 12, en utilisant la relation $X^n - 1 = \prod_{d|n} \Phi_d$.
2. Vérifier que $\deg \Phi_n = \varphi(n)$ dans chacun de ces cas.
3. Démontrer que $\Phi_{2m}(X) = \Phi_m(-X)$ pour m impair supérieur à 1, et le vérifier sur Φ_6 et Φ_{10}.

Exercice 44 ⋆⋆⋆⋆

1. Démontrer que $\mathbb{Q}(\zeta_{15})/\mathbb{Q}$ est galoisienne, et déterminer son degré.
2. Démontrer que $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q}) \simeq (\mathbb{Z}/15\mathbb{Z})^*$, puis identifier la structure de ce groupe.
3. En déduire le nombre de corps intermédiaires, et déterminer ceux de degré 2 sur $\mathbb{Q}$.
4. Démontrer que $\mathbb{Q}(\zeta_{15})$ contient $\mathbb{Q}(\sqrt{5})$, et expliciter $\sqrt{5}$ en fonction de ζ_5.
5. Plus généralement, démontrer que $\mathbb{Q}(\zeta_p)$ contient un unique sous-corps quadratique pour p premier impair, et préciser lequel selon la classe de p modulo 4.

Exercice 45 ⋆⋆⋆

On étudie l'extension $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$, où $\zeta_{16} = \mathrm{e}^{2\mathrm{i}\pi/16}$.

1. Justifier que $\Phi_{16} = X^8 + 1$, puis que $[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}] = 8$.
2. Déterminer la structure du groupe $(\mathbb{Z}/16\mathbb{Z})^*$: on calculera l'ordre de chacun de ses huit éléments.
3. En déduire que $\mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$ *n'est pas cyclique*, contrairement à $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ pour p premier impair.
4. Combien $\mathbb{Q}(\zeta_{16})$ possède-t-il de sous-corps quadratiques ? Les expliciter.
5. Plus généralement, démontrer que $(\mathbb{Z}/2^k\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$ pour $k \geqslant 3$. On montrera que 5 est d'ordre 2^{k-2} et que $-1 \notin \langle 5 \rangle$.
6. Quelle conséquence ce résultat a-t-il sur la constructibilité du polygone régulier à 16 côtés ?

Exercice 46 ⋆⋆

1. Déterminer $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ et vérifier qu'il est cyclique d'ordre 6.
2. En déduire le nombre de corps intermédiaires entre $\mathbb{Q}$ et $\mathbb{Q}(\zeta_7)$, et les déterminer tous.
3. Expliciter le sous-corps de degré 3 à l'aide de sommes de racines de l'unité — les *périodes de Gauss*.
4. Démontrer que toute extension abélienne de $\mathbb{Q}$ obtenue ainsi est résoluble par radicaux.

Exercice 47 ⋆⋆⋆

Démontrer que $\mathbb{Q}\Big(\sqrt{2+\sqrt{2+\sqrt{2}}}\Big)$ est une extension galoisienne de $\mathbb{Q}$, et déterminer son groupe de Galois.

Exercice 48 ⋆⋆⋆

Soit K un corps, p un nombre premier distinct de la caractéristique de K, et ζ une racine primitive p-ième de l'unité dans une extension de K. Soit $a \in K$. Démontrer que $X^p - a$ est irréductible sur K si et seulement s'il l'est sur $K(\zeta)$. Le résultat subsiste-t-il lorsque l'exposant n'est pas premier ?

Exercice 49 ⋆⋆⋆

On pose $P = X^3 - 3X + 1$.

1. Démontrer que P est irréductible sur $\mathbb{Q}$, et qu'il possède *trois* racines réelles.
2. Calculer le discriminant $\Delta = -4p^3 - 27q^2$ de P, et vérifier que c'est un carré parfait.
3. On admet que le groupe de Galois d'un polynôme séparable est contenu dans $\mathfrak{A}_n$ si et seulement si son discriminant est un carré. En déduire que $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, où L est le corps de décomposition.
4. En déduire que $[L : \mathbb{Q}] = 3$ et que $L = \mathbb{Q}(\alpha)$ pour n'importe quelle racine α : les trois racines s'expriment rationnellement les unes en fonction des autres. Vérifier que $\alpha^2 - 2$ est encore racine de P.
5. Démontrer que $2\cos\dfrac{2\pi}{9}$ est racine de P, à l'aide de la formule $\cos(3\theta) = 4\cos^3\theta - 3\cos\theta$.
6. *Le casus irreducibilis.* Les trois racines sont réelles, et pourtant la formule de Cardan les exprime au moyen de racines cubiques de nombres *complexes*. Expliquer pourquoi, en observant que $L \subset \mathbb{R}$ mais que L ne contient aucune racine carrée de Δ absente de $\mathbb{Q}$.

Exercice 50 ⋆⋆⋆⋆

On pose $P = X^4 + 8X + 12$. Cet exercice détermine son groupe de Galois G.

1. Démontrer que P n'a pas de racine rationnelle, puis qu'il est irréductible sur $\mathbb{Q}$. On écartera aussi la factorisation en deux facteurs de degré 2.
2. En déduire que G est un sous-groupe *transitif* de $\mathfrak{S}_4$. Dresser la liste des sous-groupes transitifs de $\mathfrak{S}_4$: on en trouvera cinq, à savoir $\mathbb{Z}/4\mathbb{Z}$, le groupe de Klein V, D_4, $\mathfrak{A}_4$ et $\mathfrak{S}_4$.
3. Calculer le discriminant de P et vérifier que $331\,776 = 576^2$. En déduire que $G \subseteq \mathfrak{A}_4$.
4. Il reste V et $\mathfrak{A}_4$. La *résolvante cubique* de $X^4 + pX + q$ est $R = X^3 - 4qX - p^2$. L'écrire ici, et démontrer qu'elle est irréductible sur $\mathbb{Q}$.
5. On admet que G est contenu dans V si et seulement si R est scindé sur $\mathbb{Q}$. Conclure que $G \simeq \mathfrak{A}_4$, puis donner $[L : \mathbb{Q}]$.
6. Pourquoi ce groupe est-il « atypique » ? On comparera avec les exemples $X^4 - 2$, $X^4 + 1$ et $X^4 - 5X^2 + 6$ rencontrés dans le cours.

Exercice 51 ⋆⋆⋆

Démontrer que le groupe de Galois de $X^5 + 20X^2 - 2$ sur $\mathbb{Q}$ est $\mathfrak{S}_5$. Soit ensuite K une extension finie de $\mathbb{Q}$ de degré premier $q \geqslant 7$: démontrer que le groupe de Galois de ce polynôme sur K est encore $\mathfrak{S}_5$.

Exercice 52 ⋆⋆⋆

On pose $P = X^5 - 5X + 12$. Contrairement à $X^5 - 4X + 2$, ce polynôme est *résoluble par radicaux*.

1. Démontrer que P est irréductible sur $\mathbb{Q}$. On pourra réduire modulo un nombre premier bien choisi.
2. Démontrer que P possède exactement une racine réelle, en étudiant les variations.
3. Calculer le discriminant et vérifier que $64\,000\,000 = 8000^2$. En déduire que $G \subseteq \mathfrak{A}_5$.
4. Dresser la liste des sous-groupes transitifs de $\mathfrak{A}_5$: on trouvera $\mathbb{Z}/5\mathbb{Z}$, le groupe diédral D_5 d'ordre 10, et $\mathfrak{A}_5$.
5. La conjugaison complexe fixe une racine et échange les autres deux à deux : quelle est sa structure de cycles ? En déduire que $G \neq \mathbb{Z}/5\mathbb{Z}$.
6. On admet que, pour presque tout premier p, la structure de cycles du Frobenius se lit sur la factorisation de P modulo p. Les motifs observés pour $p < 200$ sont (5), (1 ; 2 ; 2) et (1 ; 1 ; 1 ; 1 ; 1), jamais (1 ; 1 ; 3). Qu'en déduit-on sur les ordres des éléments de G, et donc sur G ?
7. Conclure que $G \simeq D_5$, puis que P *est* résoluble par radicaux. Quelle morale en tirer sur le théorème d'Abel-Ruffini ?

Exercice 53 ⋆⋆⋆

1. Déterminer tous les entiers n compris entre 3 et 30 pour lesquels le polygone régulier à n côtés est constructible.
2. Justifier chacune des exclusions : 7, 9, 11, 13, 14, 18, 19, 21, 22, 23, 25, 26, 27, 28, 29.
3. Démontrer que si $2^k + 1$ est premier, alors k est une puissance de 2. On appelle *nombres de Fermat* les entiers $F_m = 2^{2^m} + 1$.
4. Les cinq premiers nombres de Fermat sont-ils tous premiers ? Que sait-on aujourd'hui de cette question, et quelle conséquence cela a-t-il sur la liste des polygones constructibles ?

Exercice 54 ⋆⋆⋆

Pour quels entiers $n \geqslant 1$ peut-on trisecter à la règle et au compas un angle de mesure $\dfrac{2\pi}{n}$?

Exercice 55 ⋆⋆⋆

Démontrer que, pour tout entier $n \geqslant 2$, le polynôme $X^n + X + 3$ est irréductible sur $\mathbb{Q}$. Déterminer son groupe de Galois pour $n \leqslant 4$, en admettant les critères utilisés aux exercices 49 et 50.