École Polytechnique 2022-2023

Algèbre et théorie de Galois

Feuille d'exercices 2

Exercice 1. (Théorème de Lagrange) Soient G un groupe fini et $x \in G$. L'ordre de x est le plus petit entier $n \geq 1$ tel que $x^n = e$.

1. Montrer que l'ordre de x divise le cardinal du groupe.
2. Montrer que tout groupe fini d'ordre premier est cyclique, c'est-à-dire de la forme $\mathbf{Z}/p\mathbf{Z}$ pour un nombre premier p.

Exercice 2. Soit $G \subseteq O_3(\mathbf{R})$ le sous-groupe des isométries préservant un tétraèdre régulier de centre 0.

1. Montrer que l'action de G sur l'ensemble T des sommets du tétraèdre définit un morphisme injectif $\varphi : G \to \mathfrak{S}(T)$, où $\mathfrak{S}(T)$ dénote l'ensemble des permutations de l'ensemble T.
2. Soient $x \neq y$ dans T et $s \in O_3(\mathbf{R})$ la symétrie orthogonale hyperplane échangeant x et y. Montrer que $s \in G$ et déterminer $\varphi(s)$.
3. En déduire que φ est un isomorphisme.
4. En considérant l'ensemble des paires d'arêtes opposées du tétraèdre, démontrer l'existence d'un morphisme de groupes surjectif $f : S_4 \to S_3$.
5. Déterminer explicitement $K := \mathrm{Ker}(f)$ et montrer que $K \simeq (\mathbf{Z}/2\mathbf{Z})^2$.

Exercice 3. (Équation aux classes) Soient X un ensemble et G un groupe agissant sur X, l'action étant notée $(g, x) \mapsto g \cdot x$. Si $x \in X$ on note $G \cdot x = \{g \cdot x, g \in G\} \subset X$ (orbite de x sous G) et $G_x = \{g \in G : g \cdot x = x\} \subset G$ (stabilisateur de x dans G). On note enfin $x \sim y$ si il existe $g \in G$ tel que $y = g \cdot x$.

1. Montrer que $\sim$ est une relation d'équivalence sur X. En déduire que si $\Theta \subset X$ est un ensemble de représentants des classes de cette relation, et si X est fini, alors $|X| = \sum_{x \in \Theta} |G \cdot x|$.
2. Supposons G fini. Montrer que pour tout $x \in X$, $|G| = |G \cdot x| \times |G_x|$. Si X est fini, en déduire que $|X| = \sum_{x \in \Theta} \frac{|G|}{|G_x|}$ (équation aux classes).
3. (Points fixes d'un p-groupe) On note $X^G = \{x \in X : \forall g \in G, g \cdot x = x\}$. Montrer que si X et G sont finis, et si $|G|$ est une puissance d'un nombre premier p, alors $|X| \equiv |X^G| \pmod{p}$.
4. En considérant l'action par conjugaison de G sur lui-même, montrer que si G est un p-groupe (c'est-à-dire fini, de cardinal une puissance d'un nombre premier p), alors le centre de G est non trivial. (On rappelle que le centre d'un groupe est l'ensemble des éléments qui commutent avec tous les autres.)

Exercice 4. (Lemme de Cauchy) Soient G un groupe fini et p un nombre premier divisant $|G|$. On se propose de montrer que G contient un élément d'ordre p.

1. On considère $X = \{(x_1, \ldots, x_p) \in G^p, x_1 \cdots x_p = 1\}$. Calculer $|X|$.

2. Montrer que $(i, (x_j)) \mapsto (x_{j+i})$ (les indices étant pris modulo p) définit une action du groupe $\mathbf{Z}/p\mathbf{Z}$ sur l'ensemble X.

3. Conclure en utilisant le (iii) de l'exercice précédent.

Exercice 5. (Groupe diédral) Soient $n \geq 3$ un entier, $P \subseteq \mathbf{R}^2$ un polygone régulier à n sommets centré en 0, et $D_n \subseteq O_2(\mathbf{R})$ le sous-groupe des isométries préservant P.

1. Montrer que l'ensemble $D_n^+ \subset D_n$ constitué des rotations est un sous-groupe distingué, et qu'il est isomorphe à $\mathbf{Z}/n\mathbf{Z}$.

2. Montrer que $D_n \backslash D_n^+$ est constitué de symétries, et que ces symétries forment une ou deux classes de conjugaison.

3. Montrer que $|D_n| = 2n$.

Exercice 6. (Idéal nilpotent) Soit A un anneau.

1. Soit I un idéal de A. Montrer qu'il existe une bijection entre les idéaux de A contenant I et les idéaux de A/I.

2. Soit N l'ensemble des éléments nilpotents de A (i.e. les éléments $x \in A$ tel qu'il existe $n \geq 1$ avec $x^n = 0$). Montrer que N est un idéal de A.

   On dit que l'anneau A est réduit si $N = \{0\}$.

3. Soit $A^{red} = A/N$. Montrer que A^{red} est réduit.

4. Montrer qu'il existe une bijection entre les idéaux premiers de A et ceux de A^{red}.

Exercice 7. (Lemme de Gauß) On dit qu'un polynôme à coefficients dans un anneau (quelconque) est **primitif** si l'idéal engendré par ses coefficients est l'anneau tout entier.

1. Soit p un nombre premier et $f, g \in \mathbf{Z}[T]$ tels que p ne divise pas tous les coefficients de f ni de g. Montrer qu'il en est alors de même pour fg.

2. En déduire que le produit de deux polynômes primitifs dans $\mathbf{Z}[T]$ est primitif.

3. Montrer que tout polynôme non nul f de $\mathbf{Q}[T]$ s'écrit de manière unique sous la forme $f = c(f)F$ avec F dans $\mathbf{Z}[T]$ primitif et $c(f) \in \mathbf{Q}_{>0}$. Vérifier que $c(f) \in \mathbf{Z}$ si $f \in \mathbf{Z}[T]$. Le rationnel $c(f)$ s'appelle le **contenu** de P.

4. Montrer que pour $f, g \in \mathbf{Q}[T]$, $c(fg) = c(f)c(g)$.

5. Un polynôme $f \in \mathbf{Z}[T]$ est dit irréductible dans $\mathbf{Z}[T]$ s'il ne se factorise pas sous la forme $f = gh$ avec g et h différents de ± 1. Montrer que si f est irréductible dans $\mathbf{Z}[T]$, alors il est irréductible dans $\mathbf{Q}[T]$.

Exercice 8. (Critère de [Schönemann-]Eisenstein)

1. Soit $f = a_0 + a_1 T + \cdots + a_{n-1}T^{n-1} + T^n \in \mathbf{Z}[T]$ un polynôme unitaire. Supposons qu'il existe un nombre premier p divisant $a_0, a_1, \cdots, a_{n-1}$ mais tel que p^2 ne divise pas a_0. Montrer que f est irréductible dans $\mathbf{Q}[T]$. (On pourra utiliser le lemme de Gauß.)

2. Montrer que pour tout entier n, il existe un polynôme irréductible de degré n dans $\mathbf{Q}[T]$.