

Feuille d'exercices 2

Les anneaux sont supposés commutatifs et unitaires.

Exercice 1. (Équation aux classes) Soient X un ensemble et G un groupe agissant sur X , l'action étant notée $(g, x) \mapsto g.x$. Si $x \in X$ on note $O_x = \{g.x : g \in G\} \subset X$ l'orbite de x sous G et $\text{Stab}_x = \{g \in G : g.x = x\} \subset G$ le stabilisateur de x dans G . On note enfin $x \sim y$ si il existe $g \in G$ tel que $y = g.x$.

(i) Montrer que $\sim$ est une relation d'équivalence sur X et que $x \sim y$ si et seulement si $O_x = O_y$. On note X/G l'ensemble des classes d'équivalence et pour chaque $e \in X/G$, O_e l'orbite correspondante.

(ii) Montrer que si $x \sim y$, les stabilisateurs Stab_x et Stab_y sont conjugués dans G . Si G est fini, on note n_e le cardinal de Stab_x pour tout x dans la classe e .

(iii) Montrer que si X est fini, alors $|X| = \sum_{e \in X/G} |O_e|$.

(iv) Supposons G fini. Montrer que pour tout $x \in X$, $|G| = |O_x| \cdot |\text{Stab}_x|$. Si X est fini, en déduire que $|X| = \sum_{e \in X/G} \frac{|G|}{n_e}$ (« équation aux classes »).

(iv) (Points fixes d'un p -groupe) On note $\text{Fix}_G(X) = \{x \in X : g.x = x \text{ pour tout } g \in G\}$. Montrer que si X est fini et G est un p -groupe (c'est-à-dire fini de cardinal une puissance d'un nombre premier p), alors $|X| \equiv |\text{Fix}_G(X)| \pmod{p}$.

(v) En considérant l'action par conjugaison de G sur lui-même, montrer que si G est un p -groupe, alors le centre de G est non trivial.

(vi) En déduire que tout p -groupe est résoluble.

Exercice 2. (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 .

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

(ii) 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 .

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

Exercice 3. Soient A un anneau intègre et $A[T]$ l'anneau des polynômes à coefficients dans A .

(i) Montrer que $A[T]$ est intègre, et que ce n'est pas un corps.

(ii) Quels sont les éléments inversibles de $A[T]$?

Exercice 4. (i) Montrer qu'un anneau fini intègre est un corps.

(ii) Plus généralement, montrer qu'une algèbre de dimension finie sur un corps et intègre est un corps.

(iii) Pourquoi « plus généralement » ?

Exercice 5. (Contenu de Gauß d'un polynôme) On dit qu'un polynôme $P(T) \in \mathbf{Z}[T]$ non nul est primitif si ses coefficients sont premiers entre eux dans leur ensemble.

(i) Montrer que le produit de deux polynômes primitifs est primitif. (On pourra réduire modulo des nombres premiers.)

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

- (iii) Montrer que pour $P, Q \in \mathbf{Q}[T]$, $c(PQ) = c(P)c(Q)$.
- (iv) (Lemme de Gauß) Un polynôme $P \in \mathbf{Z}[T]$ est dit irréductible dans $\mathbf{Z}[T]$ si il ne se factorise pas sous la forme $P = QR$ avec Q et R différents de ± 1 . Montrer que si P est irréductible dans $\mathbf{Z}[T]$, alors il est irréductible dans $\mathbf{Q}[T]$.

Exercice 6. (Critère de [Schönemann-]Eisenstein)

- (i) Soit $P = a_0 + a_1T + \cdots + a_nT^n \in \mathbf{Z}[T]$ un polynôme non constant. Supposons qu'il existe un nombre premier p tel que p divise $a_0, a_1, \dots, a_{n-1}$, p ne divise pas a_n , et p^2 ne divise pas a_0 . Montrer que P est irréductible dans $\mathbf{Q}[T]$ (on pourra utiliser le lemme de Gauß).
- (ii) Montrer que pour tout entier n , il existe un polynôme irréductible de degré n dans $\mathbf{Q}[T]$.

Exercice 7. Soit $P \in \mathbf{Z}[T]$ un polynôme unitaire.

- (i) Soit p un nombre premier. Supposons que $P \bmod p$ est irréductible dans $\mathbf{F}_p[T]$. Montrer que P est irréductible dans $\mathbf{Q}[T]$. Contre-exemple si P n'est pas unitaire.
- (ii) Soient p et ℓ des nombres premiers. Supposons que $P \bmod p = AB \in \mathbf{F}_p[T]$, $P \bmod \ell = CD \in \mathbf{F}_\ell[T]$, avec A, B, C et D irréductibles. Supposons de plus que $\{\deg(A), \deg(B)\} \neq \{\deg(C), \deg(D)\}$. Montrer que P est irréductible dans $\mathbf{Q}[T]$.

Exercice 8. (Application) (i) Lister les polynômes irréductibles unitaires de degré ≤ 3 dans $\mathbf{F}_2[T]$ et ceux de degré ≤ 2 dans $\mathbf{F}_3[T]$.

- (ii) Montrer que $T^4 + T^2 + T + 1$ est irréductible dans $\mathbf{F}_3[T]$.
- (iii) Montrer que le polynôme $T^5 + 3T^4 - 2T^3 + 4T^2 - 2T + 3$ est irréductible dans $\mathbf{Q}[T]$.
- (iv) Soit p un nombre premier. Montrer que le nombre de polynômes irréductibles unitaires de degré ≤ 3 dans $\mathbf{F}_p[T]$ est $\frac{1}{3}p^3 + \frac{1}{2}p^2 + \frac{1}{6}p$.

Exercice 9. (i) Montrer que les $\mathbf{R}$ -algèbres $\mathbf{R} \times \mathbf{R}$, $\mathbf{C}$ et $\mathbf{R}[X]/(X^2)$ ne sont pas isomorphes (on pourra considérer leurs diviseurs de 0 et leurs éléments nilpotents).

- (ii) Soient $a, b \in \mathbf{R}$. Montrer que $\mathbf{R}[X]/(X^2 + aX + b)$ est isomorphe à l'une de ces trois $\mathbf{R}$ -algèbres.
- (iii) En déduire que toute $\mathbf{R}$ -algèbre de dimension 2 est isomorphe à une, et une seule, des algèbres du (i).

Exercice 10. (i) Soient k un corps et A une k -algèbre de dimension finie. Montrer que l'ensemble $\text{Specmax}(A)$ des idéaux maximaux de A est fini, de cardinal au plus $[A : k] = \dim_k(A)$. (Indication : on pourra utiliser le théorème chinois.)

- (ii) À quelle condition a-t-on égalité ?

Exercice 11. Soit A un anneau commutatif. On rappelle qu'un *idempotent* de A est un élément e tel que $e^2 = e$.

- (i) Montrer que l'ensemble $B = \text{Idem}(A)$ muni de l'addition $e \boxplus e' := (e + e')^2$ et de la multiplication $e \boxtimes e' := ee'$ est un anneau.
- (ii) Montrer que tout idéal premier $\mathfrak{p}$ de B est maximal, et que $B/\mathfrak{p}$ est isomorphe à $\mathbf{F}_2$.
- (iii) Montrer que l'ensemble $\pi_0(A) = \text{Spec}(\text{Idem}(A))$ des idéaux premiers de $\text{Idem}(A)$ est un singleton si et seulement si A a exactement deux idempotents.