Université de Bordeaux

Master Agrégation
Révisions : anneaux factoriels et extensions de corps

Tous les anneaux considérés sont supposés commutatifs et unitaires.

Exercice 1. Montrer que tout sous-anneau de $\mathbf{Q}$ est principal.

Exercice 2. Soit A un anneau. Montrer que A est un corps si et seulement si $A[X]$ est un anneau principal (pour $a \in A$, on pourra considérer l'idéal de $A[X]$ engendré par a et X).

Exercice 3. (1) Soient A un anneau intègre et $\pi \in A$ un élément premier. Montrer que π est irréductible.
(2) Soient A un anneau principal et π un élément irréductible. Montrer que l'idéal $\langle \pi \rangle$ est maximal.

Exercice 4. Montrer que $\mathbf{Z}[i\sqrt{5}] = \left\{a + ib\sqrt{5}\right\}_{a,b\in\mathbf{Z}} \subset \mathbf{C}$ est un anneau non factoriel.

Exercice 5. (1) Soient A un anneau euclidien, et $\phi\colon A\backslash\{0\} \to \mathbf{N}$ un stathme euclidien. Supposons en outre que A n'est pas un corps.

(a) Justifier l'existence de $x \in E := A\backslash(\{0\} \cup A^\times)$ tel que $\phi(x) = \min_{y\in E} \phi(y)$.

(b) Notons $\pi\colon A \to A/\langle x\rangle$ la surjection canonique. Montrer que $\pi(\{0\} \cup A^\times) = A/\langle x\rangle$.

Posons $\theta = \frac{1+i\sqrt{19}}{2} \in \mathbf{C}$ et $A = \{a + b\theta\}_{a,b\in\mathbf{Z}}$.

(2) Calculer le polynôme minimal P de θ sur $\mathbf{Q}$.
(3) Construire un isomorphisme $\mathbf{Z}[X]/\langle P\rangle \xrightarrow{\sim} A$.

Si $z \in \mathbf{Q}(\theta)$, on pose $N(z) = |z|^2$ (où $|z|$ désigne le module du nombre complexe z).

(4) Montrer que l'application N est multiplicative, et que $N(A) \subset \mathbf{N}$.
(5) Montrer que $A^\times = \{\pm 1\}$.
(6) Supposons A euclidien.

(a) En utilisant la question (1), montrer qu'il existe $x \in A$ tel que $A/\langle x\rangle$ est isomorphe à $\mathbf{Z}/2\,\mathbf{Z}$ ou $\mathbf{Z}/3\,\mathbf{Z}$.

(b) Montrer que cela implique que P a une racine dans $\mathbf{Z}/2\,\mathbf{Z}$ ou $\mathbf{Z}/3\,\mathbf{Z}$, et en déduire une contradiction.

(7) Montrer que l'idéal $2A$ est maximal dans A.
(8) Soient $a \in A$ et $b \in A\backslash\{0\}$. Posons $z = \frac{a}{b} \in \mathbf{Q}(\theta)$. Écrivons $z = x + y\theta$ avec $x, y \in \mathbf{Q}$, notons v l'entier le plus proche de y, et posons $y' = y - v$ (on a donc $|y'| \leqslant \frac{1}{2}$).

(a) Supposons $|y'| \leqslant \frac{1}{3}$ et notons u l'entier le plus proche de $x + \frac{y-v}{2}$. Montrer que $N(z - (u + v\theta)) < 1$. En déduire qu'il existe $q, r \in A$ avec $N(r) < N(b)$, tels que $a = bq + r$.

(b) Supposons $\frac{1}{3} < |y'| \leqslant \frac{1}{2}$. Montrer qu'il existe $v'' \in \mathbf{Z}$ tel que $|2y - v''| < \frac{1}{3}$. En déduire qu'il existe $q, r \in A$ avec $N(r) < N(b)$, tels que $2a = bq + r$.

(9) Montrer que A est principal [indication : si $I \subset A$ est un idéal non nul, on considérera un élément de norme minimale dans $I\backslash\{0\}$].

Exercice 6. (Lemme de Gauss) Soient A un anneau factoriel et $P, Q \in A[X]$. Démontrer que si P et Q sont primitifs, alors PQ est primitif.

Exercice 7. Soient A un anneau intègre, $K = \mathsf{Frac}(A)$ et $P \in A[X]$ de degré $d \geqslant 1$.
(1) Montrer que si P est premier dans $A[X]$, alors il est premier dans $K[X]$.
(2) Supposons P primitif. Montrer que si P est irréductible dans $K[X]$, alors il est irréductible dans $A[X]$.

Exercice 8. (1) Soient A un anneau factoriel, K son corps des fractions et $P(X) \in A[X]$ unitaire. Montrer que si $P(X) = P_1(X)P_2(X)$ avec $P_1, P_2 \in K[X]$ unitaires, alors on a $P_1, P_2 \in A[X]$.
(2) En déduire que $\mathbf{Z}[2\sqrt{2}] = \left\{a + 2\sqrt{2}b\right\}_{a,b\in\mathbf{Z}}$ n'est pas factoriel.

Exercice 9. Montrer que l'anneau $\mathbf{R}[X, Y, Z]/\langle X^2 + Y^2 + Z^2\rangle$ est intègre.

Exercice 10. Posons $A = \mathbf{Z}[i\sqrt{2}] = \left\{x + i\sqrt{2}y\right\}_{x,y\in\mathbf{Z}}$. C'est un sous-anneau de $\mathbf{C}$.

(1) Montrer soigneusement que A, muni du stathme défini par $N(x + yi\sqrt{2}) = x^2 + 2y^2$ est un anneau euclidien [on pourra illustrer la preuve par un dessin].
(2) Déterminer $A^\times$.
(3) Montrer que $i\sqrt{2}$ est irréductible dans A.

Soit $(x, y) \in \mathbf{Z}^2$ tel que $x^3 = y^2 + 2$.

(4) Soit $\pi \in A$ un élément irréductible divisant $y + i\sqrt{2}$ et $y - i\sqrt{2}$.
   (a) Montrer qu'on a $\pi = \pm i\sqrt{2}$.
   (b) En déduire que y est pair, et trouver une contradiction.
(5) En déduire $\mathsf{pgcd}(y + i\sqrt{2}, y - i\sqrt{2})$.
(6) Montrer que $y + i\sqrt{2}$ est un cube dans A.
(7) En déduire que les seules solutions de l'équation $x^3 = y^2 + 2$ sont $(3, \pm 5)$.

Exercice 11. Posons $A = \mathbf{R}[X]$ et $B = \mathbf{R}[X, Y]/\langle X^4 + Y^2 - 1\rangle$. On note x et y les images de X et de Y dans B.
(1) Montrer que B est intègre.
(2) Monter que l'unique morphisme $A \to B$ qui envoie X sur x est injectif. Il induit donc un isomorphisme $A \xrightarrow{\sim} \mathbf{R}[x] \subset B$.
(3) Montrer que $B = \mathbf{R}[x] \oplus \mathbf{R}[x]y$. Tout élément de B s'écrit donc de façon unique sous la forme $P(x) + Q(x)y$ avec $P, Q \in \mathbf{R}[X]$.
(4) Si $\alpha = P(x) + Q(x)y$, on pose $\overline{\alpha} = P(x) - Q(x)y$. Montrer que $\alpha \mapsto \overline{\alpha}$ est un automorphisme de l'anneau B.
(5) Montrer que pour tout $\alpha \in A$, on a $N(\alpha) := \alpha\overline{\alpha} \in \mathbf{R}[x]$, puis que $N\colon B \to \mathbf{R}[x]$ est multiplicative (*i.e.* que $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$).
(6) Détermier $B^\times$.
(7) Montrer que x est irréductible dans A.
(8) L'anneau B est-il factoriel ?

Exercice 12. Soit $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbf{Z}[X]$.
(1) Démontrer que toutes ses racines rationnelles sont entières.
(2) Démontrer que toute racine entière de $P(X)$ divise a_0.
(3) Soit a un entier. Le polynôme $X^3 - aX + 1$ est-il irréductible dans $\mathbf{Q}[X]$?
(4) Déterminer la décomposition de $P(X) = 2X^5 - 7X^4 + 9X^3 - 9X^2 + 7X - 2$ en facteurs irréductibles dans $\mathbf{Z}[X]$.

Exercice 13. (Critère d'irréductibilité par réduction). Soient A un anneau intègre, K son corps des fractions et $P(X) = a_d X^d + \cdots + a_0 \in A[X]$ de degré $d > 0$. On suppose qu'il existe $\pi \in A$ premier ne divisant pas a_d et tel que $\overline{P}(X) = \overline{a}_d X^d + \cdots + \overline{a}_0 \in (A/\pi A)[X]$ soit irréductible dans $(A/\pi A)[X]$.
(1) Montrer que si P est primitif, alors P est irréductible dans $A[X]$.
(2) Prouver que si A est factoriel, alors P est irréductible dans $K[X]$.
(3) En déduire que $X^5 + X^2 - 2X - 1$ est irréductible dans $\mathbf{Q}[X]$.

Exercice 14. (Critère d'Eisenstein) Soient A un anneau intègre, K son corps des fractions et $P(X) = a_d X^d + \cdots + a_0 \in A[X]$ de degré $d > 1$. On suppose qu'il existe $\pi \in A$ premier tel que :
(i) π ne divise pas a_d ;
(ii) π divise a_i pour tout $i \in \{0, \ldots, d-1\}$;
(iii) π^2 ne divise pas a_0.
(1) Montrer que si P est primitif, alors P est irréductible dans $A[X]$.
(2) Prouver que si A est factoriel, alors P est irréductible dans $K[X]$.
(3) En déduire que $X^4 - 10X^3 + 4X + 6$ est irréductible dans $\mathbf{Q}[X]$.

Exercice 15. Soit $P(X) = X^5 + X^4 + 3X^2 + 1 \in \mathbf{Z}[X]$. En factorisant l'image $\overline{P}$ de P dans $\mathbf{F}_2[X]$, montrer que P est irréductible dans $\mathbf{Q}[X]$.

Exercice 16. Montrer que si $a_1, \ldots, a_n \in \mathbf{Z}$ sont deux à deux distincts, alors le polynôme $(X - a_1) \cdots (X - a_n) - 1$ est irréductible dans $\mathbf{Z}[X]$.

Exercice 17. Soient K un corps, L/K une extension de degré m et $P \in K[X]$ irréductible de degré d.
(1) On suppose m et d premiers entre eux. Montrer que P est irréductible dans $L[X]$ (on pourra considérer une extension de L engendrée par une racine de P).
(2) Que se passe-t-il si m et d ne sont pas premiers entre eux ?
(3) Prouver que le polynôme $X^{12} + 30X^8 + 36X + 24$ est irréductible sur $\mathbf{Q}\left(\sqrt[5]{7}\right)$.

Exercice 18. Posons $\alpha = \sqrt{1 + \sqrt{3}} \in \mathbf{R}$.
(1) Trouver le polynôme minimal P de α sur $\mathbf{Q}$.
(2) Démontrer que $K = \mathbf{Q}(\alpha, i\sqrt{2})$ est une extension de décomposition de $P \in \mathbf{Q}[X]$.
(3) Calculer le degré de K sur $\mathbf{Q}$.

Exercice 19. Posons $K = \mathbf{Q}(\sqrt{2}, \sqrt[3]{7}) \subset \mathbf{R}$.
(1) Que vaut $[K : \mathbf{Q}]$?
(2) Donner une base de K vu comme $\mathbf{Q}$-espace vectoriel.
(3) En déduire que le polynôme minimal de $\alpha := \sqrt{2} + \sqrt[3]{7}$ sur $\mathbf{Q}$ n'est pas de degré 2 ou 3.
(4) En déduire que $K = \mathbf{Q}(\alpha)$ et calculer le polynôme minimal de α sur $\mathbf{Q}$.

Exercice 20. Soient $P \in \mathbf{Q}[X]$ irréductible unitaire de degré d et $K \subset \mathbf{C}$ une extension de $\mathbf{Q}$ contenant une racine α de P. Supposons que K ne contient pas de racine cubique de α.
(1) Montrer que le polynôme $X^3 - \alpha$ est irréductible sur $\mathbf{Q}(\alpha)$.
(2) Soit $\beta \in \mathbf{C}$ une racine cubique de α. Calculer $[\mathbf{Q}(\beta) : \mathbf{Q}]$ en fonction de d, et en déduire que $P(X^3)$ est irréductible sur $\mathbf{Q}$.

Exercice 21. Soit K un corps, $a \in K$, et p un nombre premier. Montrer que le polynôme $X^p - a$ est irréductible dans $K[X]$ si et seulement s'il n'a pas de racine dans K.

Exercice 22. On pose $K = \mathbf{R}(Y)$ et $P(X,Y) = X^4 + X^2 + Y^6$. Soit L une extension de décomposition de $P \in K[X]$.
(1) On choisit une racine f de P dans L. Prouver que $L = K(f)$.
(2) Démontrer que P est irréductible dans $\mathbf{R}[X,Y]$. Quel est le degré de L sur K ?

Exercice 23. Soient K un corps, L une extension algébrique de K et $\sigma\colon L \to L$ un K-morphisme.
(1) Soient $y \in L$ et P le polynôme minimal de y sur K. Notons R l'ensemble des racines de P dans L. Montrer que $\sigma(R) = R$.
(2) En déduire que σ est bijective.

Exercice 24. Soit p un nombre premier. On pose $Q(X) = X^6 + p^2$, on choisit une racine complexe α de Q et on pose $K = \mathbf{Q}(\alpha)$.
(1) Prouver que $i \in K$.
(2) Démontrer que K contient une racine du polynôme $X^3 - p$.
(3) En déduire le degré de K sur $\mathbf{Q}$. Le polynôme $\mathbf{Q}$ est-il irréductible dans $\mathbf{Q}[X]$?

Exercice 25. Soit K un corps fini de cardinal q. Montrer que $\prod_{\alpha \in K} (X - \alpha) = X^q - X$ dans $K[X]$.

Exercice 26. On pose $K = \mathbf{F}_2[Y]/\langle Y^4 + Y + 1\rangle$ et on note α la classe de Y dans K. Posons $\beta = \alpha^2 + \alpha$.
(1) Montrer que K est un corps.
(2) Trouver le polynôme minimal de β sur $\mathbf{F}_2$. Quel est le cardinal de $\mathbf{F}_2(\beta)$?
(3) Factoriser $X^3 + 1$ dans $K[X]$.
(4) Quel est le polynôme minimal de α sur $\mathbf{F}_2(\beta)$?

Exercice 27. On pose $A = \mathbf{F}_3[Y]/\langle Y^4 + Y - 1\rangle$ et on note α la classe de Y dans A.
(1) Calculer α^{16} et α^{40}.
(2) En déduire que A est un corps.
(3) Trouver le polynôme minimal de $\alpha + 1$ sur $\mathbf{F}_3$.
(4) Quel est le degré de α^{10} sur $\mathbf{F}_3$?