Anneaux

I. Anneaux intègres

Exercice 1. — Pour quelle valeur de l'entier n l'anneau $\mathbf{Z}/n\mathbf{Z}$ est-il intègre ?

Exercice 2. — Soit A un ensemble fini muni d'une structure d'anneau. Montrer que A est intègre ssi A un corps. Exemples ?

Exercice 3. — Soit F un anneau intègre et $E \subset F$ un sous-anneau qui est un corps et tel que F soit un E-ev de dimension finie. Montrer que F est un corps.
Application : Soit $x \in \mathbf{C}$ qui est racine d'un polynôme $P \in \mathbf{Q}[X]$. Montrer que

$$\mathbf{Q}[x] := \{A(x),\ A \in \mathbf{Q}[X]\} \subset \mathbf{C}$$

est un corps. Exemples.

Exercice 4. — Montrer que les sous-ensembles de $\mathbf{C}$ suivants sont des anneaux intègres :

a) $\mathbf{Z}[i] := \{a + \imath b,\ \ a, b \in \mathbf{Z}\}$.

b) Pour [1] $d \in \mathbf{Z}$, $\mathbf{Z}[\sqrt{d}] := \{a + b\sqrt{d},\ \ a, b \in \mathbf{Z}\}$.

c) Pour $d \in \mathbf{Z}$ non carré avec $d \equiv 1\ [4]$, $\mathbf{Z}[\frac{1+\sqrt{d}}{2}] := \{a + b\frac{1+\sqrt{d}}{2},\ \ a, b \in \mathbf{Z}\}$.

Exercice 5. — Soit X le sous-ensemble des éléments de $\mathbf{Q}[\imath]$ qui sont racines d'un polynôme unitaire de degré $\leqslant 2$ à coefficients entiers. Montrer que $X = \mathbf{Z}[\imath]$.

II. Unités

Exercice 6. — Quelles sont les unités de $\mathbf{Z}/n\mathbf{Z}$?

Exercice 7. — Soit A un anneau intègre et $A[X]$ (resp. $A[[X]]$) l'anneau des polynômes (resp. séries formelles) à coefficients dans A.

a) Montrer que le groupe des inversibles $A[X]^\times$ est naturellement isomorphe à $A^\times$.

b) Identifier $A[[X]]^\times$.

Exercice 8. — En utilisant l'application $\mathbf{C} \to \mathbf{R}$, $z \mapsto |z|^2 = z\overline{z}$, déterminer le groupe des éléments inversibles $\mathbf{Z}[\imath]^\times$.
Pour $d > 1$, déterminer le groupe $\mathbf{Z}[\sqrt{-d}]^\times$.

Exercice 9. — **[Norme]**
Soit $d \in \mathbf{Z}$ un entier qui n'est pas un carré parfait.

a) Justifier que l'anneau $\mathbf{Q}[\sqrt{d}] := \{a+b\sqrt{d},\ a, b \in \mathbf{Q}\}$ est un $\mathbf{Q}$-espace vectoriel de dimension 2 dont une base est $\{1, \sqrt{d}\}$. (En particulier les coefficients a et b ci-dessus sont uniques.)

b) Soit $N : \mathbf{Z}[\sqrt{d}] \to \mathbf{Z}$ l'application

$$a + b\sqrt{d} \to a^2 - db^2.$$

Montrer par un calcul que pour $\alpha, \beta \in \mathbf{Z}[\sqrt{d}]$ on a $N(\alpha\beta) = N(\alpha)N(\beta)$. (On dit que N est *multiplicative*.) Que retrouve-t-on si $d < 0$?

c) Soit $\alpha \in \mathbf{Z}[\sqrt{d}]$. Justifier que l'application $m_\alpha : \mathbf{Q}[\sqrt{d}] \to \mathbf{Q}[\sqrt{d}]$, $x \mapsto \alpha \cdot x$ est linéaire. Calculer son déterminant et retrouver le résultat de la question précédente sans calcul.

d) Montrer qu'un élément $\alpha \in \mathbf{Z}[\sqrt{d}]$ est inversible ssi $N(\alpha) = 1$ ou $N(\alpha) = -1$.

e) Trouver un sous-groupe d'ordre infini dans les groupes $\mathbf{Z}[\sqrt{2}]^\times$ et $\mathbf{Z}[\sqrt{3}]^\times$.

f) Soit $\alpha \in \mathbf{Z}[\sqrt{d}]$ tel que $|N(\alpha)|$ soit un nombre premier. Montrer que α est irréductible.

1. Lorsque d est un entier négatif, par convention, on pose $\sqrt{d} = \imath\sqrt{-d}$. Remarquer également que le cas où $d \geqslant 0$ est un carré parfait est particulièrement dégénéré.

III. Anneaux euclidiens

Exercice 10. — Soit d un entier non carré et $A = \mathbf{Z}[\sqrt{d}]$ l'anneau associé. Montrer qu'un entier $n \in \mathbf{Z}$ divise $a + b\sqrt{d}$ dans A ssi n divise a et b dans $\mathbf{Z}$.

Exercice 11. — Montrer que les anneaux suivants sont euclidiens pour la fonction $x \mapsto |N(x)|$ (N est définie à l'exercice 9) :

a) $\mathbf{Z}[i]$ ***b)*** $\mathbf{Z}[\sqrt{-2}]$ ***c)*** $\mathbf{Z}[\sqrt{2}]$

[**Indication:** Pour faire la division euclidienne de $a + b\sqrt{d}$ par $e + f\sqrt{d}$, considérer le quotient $\frac{a+b\sqrt{d}}{e+f\sqrt{d}} \in \mathbf{Q}[\sqrt{d}]$.]
A-t-on unicité de la division euclidienne ?

Exercice 12. — Trouver le pgcd des éléments de $\mathbf{Z}[\imath]$ suivants :

a) $4 + 6\imath$ et $5 + 7\imath$. ***b)*** $19 - 3\imath$ et $5 - 5\imath$.

c) $1 + 3\imath$ et 10. ***d)*** 13 et $2 + 3\imath$.

Exercice 13. — Montrer que deux entiers premiers entre eux dans $\mathbf{Z}$ le restent dans $\mathbf{Z}[\imath]$.

Exercice 14. — Soit $p \in \mathbf{N}$ un nombre premier impair.

a) On suppose $p \equiv 3\,[4]$. Montrer que p n'est pas somme de deux carrés dans $\mathbf{Z}$. En déduire que p est premier dans $\mathbf{Z}[\imath]$.

Dans toute la suite, on suppose $p \equiv 1\,[4]$.

b) Montrer que -1 est un carré dans $\mathbf{Z}/p$.
[**Indication:** Combien y a-t-il de carrés dans $\mathbf{Z}/p$? Montrer que les carrés non nuls sont exactement les racines du polynôme $X^{\frac{p-1}{2}} - 1$ dans le corps $\mathbf{Z}/p$.]

c) En déduire que p est le produit de deux nombres premiers non associés dans $\mathbf{Z}[\imath]$, puis que p est somme de deux carrés dans $\mathbf{Z}$.

d) De combien de façons p s'écrit-il comme somme de deux carrés dans $\mathbf{Z}$?

Exercice 15. — Soit $\Sigma \subset \mathbf{N}$ l'ensemble des entiers naturels qui sont somme de deux carrés.

a) Montrer que Σ est stable par multiplication.
[**Indication:** La norme $\mathbf{Z}[i] \to \mathbf{Z}$ est multiplicative.]

b) Soient $a, b \in \mathbf{N}$ et $n = a^2 + b^2 \in \Sigma$. On considère un diviseur premier p de n avec $p \equiv 3\,[4]$. En utilisant l'exercice ***14***, montrer que p^2 divise n.

c) En déduire que Σ est exactement l'ensemble des entiers dont les exposants des diviseurs premiers $\equiv 3\,[4]$ dans la décompostion en facteurs premiers sont pairs.

Exercice 16. — **Triplets pythagoriciens**
Soit $(x, y, z) \in \mathbf{Z}^3$ un triplet d'entiers *premiers entre eux* tels que

$$x^2 + y^2 = z^2.$$

a) Donner un exemple non trivial de tel triplet. Pourquoi "pythagoricien" ? Remarquer que si (x, y, z) est un tel triplet, alors $(\pm x, \pm y, \pm z)$ et $(\pm y, \pm x, \pm z)$ le sont aussi.

b) Montrer que z est impair et que parmi x et y, il y en a exactement un pair et un impair.
[**Indication:** Réduire modulo 4.]

c) Montrer que $x + \imath y$ et $x - \imath y$ sont premiers entre eux dans $\mathbf{Z}[\imath]$.
[**Indication:** Commencer par montrer que leur pgcd doit diviser 2.]

d) Montrer que $x + \imath y$ est, à un unité près, un carré de $\mathbf{Z}[\imath]$.

e) En déduire, qu'aux symétries de ***a)*** près, les triplets pythagoriciens sont exactement ceux de la forme :

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2,$$

avec u, v des entiers premiers entre eux, pas tous deux impairs et $u > v > 0$.

Exercice 17. — Montrer que les éléments premiers de $\mathbf{Z}[\imath]$ sont (aux unités près) les entiers premiers $p \equiv 3\,[4]$ et les $a + \imath b$ tels que $a^2 + b^2$ soit premier.
[**Indication:** Vérifier que ceux-ci sont bien premiers. Réciproquement, si $z \in \mathbf{Z}[\imath]$ est premier, considérer les diviseurs premiers (dans $\mathbf{Z}$) de $N(z)$.]

Exercice 18. — Décomposer les éléments suivants en produits de facteurs premiers :

a) $1 + 3\imath$ ***b)*** $11 + \imath$ ***c)*** $4 + 3\imath$ ***d)*** $3 + 5\imath$.

Exercice 19. — Décomposer en produits d'éléments irréductibles les entiers $2, 3, 5, 7, 11, 13, 17 \ldots$

a) Dans $\mathbf{Z}[\sqrt{-2}]$. ***b)*** Dans $\mathbf{Z}[\sqrt{2}]$.

IV. Idéaux

Exercice 20. — Soient A un anneau et $a, b \in A$. Montrer l'équivalence :

$$a \,|\, b \quad \Longleftrightarrow \quad (b) \subset (a).$$

Exercice 21. — Trouver un générateur pour les idéaux suivants :

a) Dans $\mathbf{Z}$, $I = (14, 22)$ et $J = (14) \cap (22)$.

b) Dans $\mathbf{Z}[\imath]$, $I = (15 + 10\imath, 1 + 13\imath)$ et $J = (15 + 10\imath) \cap (1 + 13\imath)$.

c) Dans $\mathbf{Q}[X]$, $I = (X^2 + 1, X^2 + X + 1)$ et $J = (X^2 + 1) \cap (X^2 + X + 1)$.

Exercice 22. — Soient $\mathfrak{a}$ et $\mathfrak{b}$ des idéaux d'un anneau A. Montrer qu'on a $\mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$.
Donner des exemples où l'on n'a pas égalité.

Exercice 23. — Soit $f : \mathbf{Q}[X, Y] \to \mathbf{Q}$, $P(X, Y) \mapsto P(2, 3)$.
Vérifier que f est un morphisme d'anneaux et déterminer $\ker f$.

V. Anneaux quotients

Exercice 24. — Soit A un anneau et $I \subsetneq A$ un idéal strict.

a) Montrer que I est premier ssi l'anneau A/I est intègre.

b) Montrer que I est maximal ssi l'anneau A/I est un corps.

Exercice 25. — Montrer que pour d un entier qui n'est pas un carré parfait, on a des isomorphismes d'anneaux :

$$\mathbf{Q}[X]/(X^2 - d) \cong \mathbf{Q}[\sqrt{d}] \quad \text{et} \quad \mathbf{Z}[X]/(X^2 - d) \cong \mathbf{Z}[\sqrt{d}].$$

Exercice 26. — Identifier les anneaux suivants :

a) $\mathbf{Z}/(14, 21)$. ***b)*** $\mathbf{Z}[\imath]/(1 + \imath)$.

c) Pour $n \in \mathbf{Z}$, $\mathbf{Z}[X]/(n, X)$. ***d)*** $\mathbf{Q}[X, Y]/(X - 1, Y - 2)$.

e) $Q[X, Y]/(Y)$.

Exercice 27. — Les anneaux suivants sont-il intègres ?

a) $\mathbf{Q}[X]/(X^3)$. ***b)*** $\mathbf{Q}[X]/(X^2 + 1)$.

Exercice 28. — ***a)*** Déterminer le nombre d'éléments de l'anneau $\mathbf{Z}[\imath]/(3)$.

b) Expliciter les lois d'addition et de multiplication de $\mathbf{Z}[\imath]/(3)$ et vérifier que c'est un corps.

c) L'anneau $\mathbf{Z}[\imath]/(5)$ est-il un corps ?

d) Plus généralement, pour $p \in \mathbf{Z}$ un nombre premier, montrer que l'anneau $\mathbf{Z}[\imath]/(p)$ est isomorphe à $(\mathbf{Z}/p\,[X])/(X^2 + 1)$. En déduire que $\mathbf{Z}[\imath]/(p)$ est un corps ssi -1 n'est pas un carré modulo p.

VI. Eléments irréductibles et premiers

Exercice 29. — Soit A un anneau et x un élément non inversible de A.

a) Montrer que x est premier ssi l'idéal (x) est premier.

b) Montrer que x est irréductible ssi l'idéal (x) est maximal parmi les idéaux principaux.

c) En déduire que pour un anneau principal ces deux notions coïncident.

Exercice 30. — Dans l'anneau $A = \mathbf{Z}[\sqrt{-5}]$ on a l'égalité :

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

a) Montrer que les éléments $2, 3, 1 + \sqrt{-5}$ et $1 - \sqrt{-5}$ sont irréductibles non associés dans A et qu'ils ne sont pas premiers.

b) L'idéal (2) de A est-il premier ?

c) Montrer que les idéaux $I_1 = (2, 1 + \sqrt{-5})$, $I_2 = (2, 1 - \sqrt{-5})$, $I_3 = (3, 1 + \sqrt{-5})$ et $I_4 = (3, 1 - \sqrt{-5})$ de A sont premiers.

d) Montrer que $I_1 \cdot I_2 = (2)$, que $I_3 \cdot I_4 = (3)$, que $I_1 \cdot I_3 = (1 + \sqrt{-5})$ et que $I_2 \cdot I_4 = (1 - \sqrt{-5})$.

e) Montrer que les idéaux I_1, I_2, I_3 et I_4 ne sont pas principaux.

Exercice 31. — Dans l'anneau $A = \mathbf{Z}[\sqrt{-14}]$ on a l'égalité :

$$3 \cdot 3 \cdot 3 \cdot 3 = (5 + 2\sqrt{-14}) \cdot (5 - 2\sqrt{-14}).$$

a) Montrer que les éléments $3, 5 + 2\sqrt{-14}$ et $5 - 2\sqrt{-14}$ sont irréductibles non associés dans A et qu'ils ne sont pas premiers.

b) Montrer que les idéaux $I_1 = (3, 5 + 2\sqrt{-14})$ et $I_2 = (3, 5 - 2\sqrt{-14})$ de A sont premiers.

Exercice 32. — Soit $\varphi : k[X, Y] \to k[T]$, $P(X, Y) \mapsto P(T^2, T^3)$.

a) Vérifier que φ est un morphisme d'anneaux et identifier son image $A \subset k[T]$.

b) Montrer que T^2, T^3 sont des éléments irréductibles de A, mais qu'ils ne sont pas premiers.

c) Montrer que l'idéal (T^2, T^3) de A est premier et n'est pas principal.

VII. Idéaux maximaux

Exercice 33. — Soit $f : A \to B$ un morphisme d'anneaux, I un idéal de B et $J = f^{-1}(I) \subset A$.

a) Montrer que si I est premier alors J aussi.

b) Que dire de J si I est maximal ? Et si f est surjective ?

Exercice 34. — Soit A un anneau. On suppose que le groupe sous-jacent $(A, +)$ est isomorphe à $\mathbf{Z}^n$, pour un certain $n \in \mathbf{N}$. Soit $\mathfrak{p}$ un idéal premier de A qui contient un entier non nul $k := k \cdot 1_A$. Montrer que $\mathfrak{p}$ est un idéal maximal.
[**Indication:** Montrer que $A/\mathfrak{p}$ est fini, *c.f.* exercice *2.*]

Application : Montrer que pour $d \in \mathbf{Z}$ (resp. $d \equiv 1[4]$), tout idéal premier $\mathfrak{p}$ non nul de $\mathbf{Z}[\sqrt{d}]$ (resp. $\mathbf{Z}[\frac{1+\sqrt{d}}{2}]$) est maximal.

Exercice 35. — Soit k un corps et $\mathfrak{p}$ un idéal premier non nul de $k[X]$. Montrer que $\mathfrak{p}$ est maximal.

Exercice 36. — Montrer que l'idéal (X) de $\mathbf{Q}[X, Y]$ est premier mais pas maximal.

VIII. Le groupe $(\mathbf{Z}/n)^\times$

Exercice 37. — Soit n un entier.

a) Soit $m \in \mathbf{Z}$. Montrer que l'on a $\overline{m} \in (\mathbf{Z}/n)^\times$ ssi n et m sont premiers entre eux.

b) Si $n = p^\alpha$ avec p premier, quel est le cardinal de $(\mathbf{Z}/n)^\times$?

c) On suppose que la décomposition de n en produits de facteurs premiers est $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Montrer que l'on a un isomorphisme de groupes :

$$(\mathbf{Z}/n)^\times \cong (\mathbf{Z}/p_1^{\alpha_1})^\times \times \cdots \times (\mathbf{Z}/p_k^{\alpha_k})^\times.$$

En déduire une formule pour le cardinal de $(\mathbf{Z}/n)^\times$.

Exercice 38. — Soit p un nombre premier. On va montrer que $(\mathbf{Z}/p)^\times$ est cyclique.

a) En utilisant le cours sur les $\mathbf{Z}$-modules, justifier qu'il existe un entier $r > 0$ et des entiers $d_1 \,|\, d_2 \,|\, \cdots \,|\, d_r$ tels que l'on ait un isomorphisme de groupes :

$$(\mathbf{Z}/p)^\times \cong (\mathbf{Z}/d_1) \times \cdots \times (\mathbf{Z}/d_r).$$

(**Attention :** c'est un isomorphisme entre un groupe multiplicatif et un groupe additif !)

b) En considérant le polynôme $X^{d_r} - 1$, montrer que $d_r = p - 1$.

c) En déduire un isomorphisme de groupes $(\mathbf{Z}/p)^\times \cong \mathbf{Z}/(p-1)$.

d) Donner tous les générateurs des groupes $(\mathbf{Z}/5)^\times$, $(\mathbf{Z}/7)^\times$ et $(\mathbf{Z}/11)^\times$.

Exercice 39. — Soient p un nombre premier *impair* et $k > 0$ un entier. On va montrer que le groupe $(\mathbf{Z}/p^k)^\times$ est cyclique.
Soit $\varphi : \mathbf{Z}/p^k \to \mathbf{Z}/p$ le morphisme de "réduction modulo p", *i.e.* : $\varphi(x \mod p^k) = x \mod p$.

a) Vérifier que φ est un morphisme d'anneaux bien défini.

b) Vérifier que φ induit (par restriction) un morphisme de groupes $\psi : (\mathbf{Z}/p^k)^\times \to (\mathbf{Z}/p)^\times$. Montrer que ψ est surjectif.

c) En utilisant l'exercice *38*, montrer qu'il existe un élément g d'ordre $p-1$ dans $(\mathbf{Z}/p^k)^\times$.
[**Indication:** Soit x un générateur de $(\mathbf{Z}/p)^\times$, montrer qu'un élément y tel que $\psi(y) = x$ est d'ordre multiple de $p-1$ et considérer les puissances de y.]

d) Soit $\langle g \rangle$ le sous-groupe engendré par g et soit Γ le noyau de ψ. Montrer que l'application

$$\begin{array}{ccc} \langle g \rangle \times \Gamma & \to & (\mathbf{Z}/p^k)^\times \\ (a, b) & \mapsto & a \cdot b \end{array}$$

est un isomorphisme de groupes.

e) Montrer que pour tout entier $\ell \geqslant 0$, on a $(1+p)^{p^\ell} \equiv 1 + p^{\ell+1}\ [p^{\ell+2}]$.

f) Déduire de la question précédente que $\overline{1+p}$ engendre Γ.

g) En déduire que $(\mathbf{Z}/p^k)^\times$ est cyclique et même que l'élément $g \cdot \overline{(1+p)}$ en est un générateur.

h) Déterminer un générateur pour les groupes $(\mathbf{Z}/5^3)^\times$, $(\mathbf{Z}/7^2)^\times$ et $(\mathbf{Z}/11^3)^\times$.

Exercice 40. — ***a)*** Déterminer les groupes $(\mathbf{Z}/2)^\times$, $(\mathbf{Z}/4)^\times$ et $(\mathbf{Z}/8)^\times$. Sont-ils cycliques ?

b) Où la démonstration de l'exercice *39* ne marche-t-elle plus pour $p = 2$?

Exercice 41. — Décomposer les groupes suivants en produits de p-groupes :

a) $(\mathbf{Z}/14)^\times$ ***b)*** $(\mathbf{Z}/15)^\times$ ***c)*** $(\mathbf{Z}/72)^\times$