Arithmétique dans les anneaux

I. Généralités et exemples

Exercice 1. — Soit $(A, +, \times)$ un anneau fini. Montrer que A est intègre ssi A est un corps.
[**Indication:** Pour $a \neq 0$ fixé, considérer l'application de multiplication par a.]

Exercice 2. — Soit k un corps et E une k-algèbre de dimension finie.

a) Montrer que E est intègre ssi E est un corps.

b) **Application :** Soit $x \in \mathbf{C}$ algébrique. Montrer que $\mathbf{Q}[x] := \{A(x),\ A \in \mathbf{Q}[X]\}$ est un sous-corps de $\mathbf{C}$. En pratique, comment calcule-t-on l'inverse d'un élément non nul ?

Exercice 3. — Montrer que les sous-ensembles de $\mathbf{C}$ suivants sont des anneaux intègres :

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

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

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

Exercice 4. — Soit A un anneau non nul. Montrer qu'il existe un unique morphisme d'anneaux $\varphi : \mathbf{Z} \to A$. L'unique entier $c > 0$ tel que $\ker \varphi = (c)$ s'appelle la *caractéristique* de A. Montrer que si A est intègre alors c est premier et que A est alors naturellement muni d'une structure de $\mathbf{Z}/c$-algèbre.
En déduire qu'un corps fini est automatiquement de cardinal une puissance d'un nombre premier.

II. Idéaux, anneaux quotients [Perrin]

Exercice 5. — **a)** Quels sont les sous-anneaux de $\mathbf{Z}$? Les idéaux ? Les quotients ?

b) Quels sont les sous-anneaux de $\mathbf{Z}/n$? Les idéaux ? Les quotients ?

c) Quels sont les idéaux et les quotients d'un corps ?

Exercice 6. — Soient m et $n \in \mathbf{Z}$ deux entiers.
Déterminer les idéaux $I = (m) + (n)$ et $J = (m) \cap (n)$.

Exercice 7. — Soient A, B deux anneaux et $f : A \to B$ un morphisme d'anneaux.

a) Montrer que $\ker f$ est un idéal de A.
Réciproquement, montrer que tout idéal de A est le noyau d'un certain morphisme.

b) Plus généralement, montrer que pour tout idéal $J \subset B$, $f^{-1}(J)$ est un idéal de A.
Montrer que si J est premier, alors $f^{-1}(J)$ aussi. Et si J est maximal ?

c) Montrer que si f est surjectif et $I \subset A$ est un idéal, alors $f(I) \subset B$ est un idéal. Que dire si I est premier ou maximal ?

Exercice 8. — Soit A un anneau et $I \subset A$ un idéal.
Montrer que l'on a une correspondance bijective entre les idéaux (premiers, maximaux) de l'anneau quotient A/I et les idéaux (premiers, maximaux) de A contenant I.

Exercice 9. — Soient A un anneau et $a, b \in A$. Montrer l'équivalence :

$$a \mid b \quad \Longleftrightarrow \quad (b) \subset (a).$$

Exercice 10. — 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 11. — 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 12. — Soit A un anneau non nul.

a) Montrer que l'ensemble des idéaux *stricts* de A est un ensemble inductif (pour la relation d'inclusion) non-vide.

b) En déduire que A admet un idéal maximal. Plus généralement, montrer que tout idéal $I \subset A$ est contenu dans un idéal maximal.

Exercice 13. — Soit A un anneau dont tous les idéaux stricts sont premiers.

a) Montrer que A est intègre.

b) Montrer que A est un corps.
[**Indication:** Pour $x \neq 0$, considérer l'idéal $\langle x^2 \rangle$.]

Exercice 14. — Soient A un anneau et $\mathcal{N} \subset A$ l'ensemble des éléments nilpotents de A.

a) Montrer que $\mathcal{N}$ est un idéal de A.

b) Soit $\mathfrak{p} \subset A$ un idéal premier. Montrer que $\mathcal{N} \subset \mathfrak{p}$.

c) Montrer l'égalité $\mathcal{N} = \bigcap_{\mathfrak{p} \text{ premier}} \mathfrak{p}$.
[**Indication:** Pour $\supset$, si $x \notin \mathcal{N}$, montrer que l'ensemble des idéaux de A ne rencontrant pas l'ensemble $\{1, x, \ldots, x^n, \ldots\}$ admet un élément maximal qui se trouve être un idéal premier de A.]

Exercice 15. — **[Théorème chinois]**
Soit A un anneau et I_1, I_2 deux idéaux étrangers ($I_1 + I_2 = A$.)

a) Montrer qu'on a des morphismes de réduction naturels $\rho_i : A/(I_1 \cap I_2) \to A/I_i$.

b) Montrer que le morphisme produit $\rho_1 \times \rho_2 : \rho_i : A/(I_1 \cap I_2) \to A/I_1 \times A/I_2$ est un isomorphisme.
Généraliser à une famille d'idéaux $I_1, \ldots I_n$.

Exercice 16. — Montrer que pour d un entier qui n'est pas un carré parfait, on a des isomorphismes d'anneaux :

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

Que dire si $d = c^2$ est un carré parfait ?

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.

Exercice 17. — 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) $\mathbf{Q}[X,Y]/(X^2-Y)$.

Exercice 18. — Les anneaux suivants sont-il intègres ?

a) $\mathbf{Q}[X]/(X^3)$.

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

Exercice 19. — Montrer que l'idéal (X) de $\mathbf{Q}[X,Y]$ est premier mais pas maximal.

Exercice 20. — **[Un exemple de non noethérianité.]**
Soient A l'anneau des fonctions continues $\mathcal{C}^0(\mathbf{R},\mathbf{R})$.
Montrer que l'idéal des fonctions à cupport compact n'est pas de type fini.

Exercice 21. — 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 *1.*]
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.

III. Anneaux arithmétiques

Exercice 22. — 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) Pour A intègre, 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 23. — 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 24. — 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 25. — **[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.

Exercice 26. — Montrer que les anneaux suivants sont euclidiens pour la fonction $x \mapsto |N(x)|$ (N est définie à l'exercice 25) :

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

Exercice 29. — 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 30. — 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 ***29***, montrer que p^2 divise n et que $\frac{n}{p^2} \in \Sigma$.

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 31. — **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 primitifs s'écrivent de manière unique :

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

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

f) Montrer que $9^2 + 12^2 = 15^2$, mais que le triplet $(9, 12, 15)$ n'est pas de la forme précédente. Lever l'apparente contradiction.

Exercice 32. — 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 33. — 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 34. — Décomposer en produits d'éléments irréductibles les entiers $2, 3, 5, 7, 11, 13, 17 \ldots$

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

Exercice 35. — **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.

Exercice 36. — Le but de cet exercice est d'étudier l'ensemble Σ suivant :

$$\Sigma := \{n \in \mathbf{N}, \exists\ a, b \in \mathbf{Z},\ n = a^2 + 2b^2\}.$$

Pour cela, on considère le sous-anneau $A = \mathbf{Z}[i\sqrt{2}] := \{a + ib\sqrt{2}, a, b \in \mathbf{Z}\} \subset \mathbf{C}$.
On note $N : A \to \mathbf{N}$ l'application $a + ib\sqrt{2} \mapsto a^2 + 2b^2$.

a) Montrer que l'anneau A est euclidien relativement à l'application N.

b) Soit $z \in A$ un élément tel que $N(z)$ soit un entier premier. Montrer que z est irréductible dans A.

c) Soit $p \in \mathbf{N}$ un nombre premier. Montrer que p appartient à Σ ssi p est réductible dans l'anneau A.

d) Montrer que p est réductible dans A ssi -2 est un carré dans $\mathbf{Z}/p\mathbf{Z}$.

e) Quelle est la décomposition en produits d'irréductibles de A des éléments suivants :

i) 2 **ii)** 3 **iii)** 5.

f) Montrer que Σ est stable par multiplication, c'est-à-dire que pour tous m, $n \in \Sigma$, l'entier mn est encore dans Σ.

g) Soit $n \in \Sigma$ et p un diviseur premier de n. Montrer que si p est irréductible dans A alors $p^2 | n$ et $\frac{n}{p^2} \in \Sigma$.

h) En déduire une condition nécessaire et suffisante sur la décomposition en facteurs premiers d'un entier n pour qu'il appartienne à Σ.

Exercice 37. — 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 38. — Dans l'anneau $A = \mathbf{Z}[\imath\sqrt{3}]$ on a l'égalité :

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

a) Montrer que les éléments $2, 1 + \imath\sqrt{3}$ et $1 - \imath\sqrt{3}$ sont irréductibles non associés dans A et qu'ils ne sont pas premiers.
[**Indication:** Pour l'irréductibilité, utiliser la norme.]

b) L'anneau A est-il euclidien ? principal ?

c) Montrer que 2 (resp. $(1 + \imath\sqrt{3})$) est un diviseur commun à 4 et $2 \cdot (1 + \imath\sqrt{3})$ dans A et qu'il est maximal (c'est-à-dire que tout diviseur commun qu'il divise lui est associé). En déduire que ces deux éléments n'ont pas de pgcd dans A.

d) L'idéal $(4) + (2 \cdot (1 + \imath\sqrt{3}))$ est-il principal ? Et $(2) + (1 + \imath\sqrt{3})$?

Exercice 39. — 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 40. — 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.

Exercice 41. — **Entiers algébriques, [Samuel]**
Soit $\mathcal{E}$ l'ensemble des éléments de $\mathbf{C}$ qui sont racine d'un polynôme *unitaire* à coefficients *entiers*.

a) Montrer que $\sqrt{n}$ et $e^{\frac{2\imath\pi}{n}}$ sont des entiers algébriques.

b) Pour $x \in \mathbf{C}$ entier algébrique, montrer que l'ensemble $\mathbf{Z}[x] := \{P(x),\ P \in \mathbf{Z}[X]\}$ est un sous-groupe abélien de $\mathbf{C}$ qui est de type fini et non-nul.
Montrer que pour tout $y \in \mathbf{Z}[x]$, le complexe xy est encore dans $\mathbf{Z}[x]$.

c) Réciproquement, soit $x \in \mathbf{C}$ tel qu'il existe un sous-groupe non-nul $A \subset \mathbf{C}$ qui est de type fini et tel que $xA \subset A$. Montrer que x est un entier algébrique.
[**Indication:** En choisissant une base de A, la multiplication par x devient une matrice à coefficients entiers. Une telle matrice admet toujours un polynôme annulateur entier !]

d) En déduire que l'ensemble des entiers algébriques est un sous-anneau de $\mathbf{C}$.

e) Déterminer $\mathcal{E} \cap \mathbf{Q}$.
Application : Soit ρ le caractère d'une représentation. On suppose que ρ est à valeurs dans $\mathbf{Q}$. Montrer que ρ est en fait à valeurs entières.

f) Pour d entier, non carré parfait, on se propose de déterminer $\mathcal{E} \cap \mathbf{Q}[\sqrt{d}]$.

i) Montrer que d se factorise uniquement sous la forme $d = e^2\tilde{d}$ où $e \in \mathbf{N}$ et $\tilde{d} \in \mathbf{Z}$ est sans facteur carré. Montrer qu'alors $\mathbf{Q}[\sqrt{d}] = \mathbf{Q}[\sqrt{\tilde{d}}]$ et que $\{1, \sqrt{\tilde{d}}\}$ en est une $\mathbf{Q}-$base.

ii) Soit $\alpha = a+b\sqrt{\tilde{d}}$ pour $a, b \in \mathbf{Q}$. Montrer que α est entier ssi $2a \in \mathbf{Z}$ et $a^2-\tilde{d}b^2 \in \mathbf{Z}$.
[**Indication:** Remarquer que si α est entier, alors $\overline{\alpha} := a - b\sqrt{\tilde{d}}$ est aussi entier.]

iii) En déduire que $\mathcal{E} \cap \mathbf{Q}[\sqrt{d}] = \begin{cases} \mathbf{Z}[\sqrt{\tilde{d}}] & \text{si } \tilde{d} \not\equiv 1[4] \\ \mathbf{Z}[\frac{1+\sqrt{\tilde{d}}}{2}] & \text{si } \tilde{d} \equiv 1[4] \end{cases}$.
[**Indication:** Commencer par montrer que si α est entier, alors $2b \in \mathbf{Z}$.]

iv) Application numérique : quels sont les entiers de $\mathbf{Q}[i]$, $\mathbf{Q}[\sqrt{5}]$ et $\mathbf{Q}[\sqrt{12}]$?

IV. Anneaux principaux, anneaux factoriels

Exercice 42. — Soit A un anneau intègre et $a, b \in A$ deux éléments.

a) Montrer que si a et b admettent un ppcm μ, alors ils admettent aussi un pgcd δ et que $\mu\delta$ est associé à ab.

b) Montrer que dans $A = \mathbf{Z}[i\sqrt{5}]$, $a = 1 - i\sqrt{5}$ et $b = 2$ ont un pgcd, mais pas de ppcm.

c) Montrer que si A est factoriel, a et b admettent toujours un ppcm (et un pgcd !).

Exercice 43. — 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 44. — **a)** Si k est un corps, montrer que $k[X]$ est principal.

b) Si A est un anneau intègre, montrer que $A[X]$ est principal ssi A est un corps.

Exercice 45. — Montrer qu'un anneau principal est toujours noethérien.

Exercice 46. — Montrer que l'anneau des nombres décimaux $\mathbf{Z}[\frac{1}{10}] \subset \mathbf{Q}$ est principal.

Exercice 47. — Soit $A = \mathbf{C}[X, \frac{1}{X}] \subset \mathbf{C}(X)$ l'anneau des polynômes de Laurent.

a) Montrer que A est principal.

b) Montrer que A est isomorphe à $\mathbf{C}[X, Y]/(XY - 1)$, puis à $\mathbf{C}[X, Y]/(X^2 + Y^2 - 1)$.

c) Par contre, montrer que l'anneau $\mathbf{R}[X, Y]/(X^2 + Y^2 - 1)$ n'est pas factoriel.
[**Indication:** Définir une norme sur cet anneau.]

Exercice 48. — Soit A un anneau euclidien et $v : A - 0 \to \mathbf{N}$ l'application associée.

a) Si A n'est pas un corps, soit $x \in A \setminus A^\times$ avec $v(x)$ minimal. Montrer que la restriction de la projection canonique $A^\times \bigcup\{0\} \to A/(x)$ est surjective.

b) En déduire que l'anneau $A := \mathbf{R}[X, Y]/(X^2 + Y^2 + 1)$ n'est pas euclidien.
[**Indication:** Montrer que $A^\times = \mathbf{R}^*$ en définissant une norme sur A.]
On peut montrer cependant que A est principal [Perrin].

V. Equations diophantiennes

Exercice 49. — **[Lemme préliminaire pour certaines équations diophantiennes]**
Soit A un anneau factoriel. On suppose que x,$y \in A$ sont premiers entre eux et qu'il existe $z \in A$ tel que $xy = z^k$.

a) Montrer qu'il existe deux unités $u, v \in A^\times$ et deux éléments $x_0, y_0 \in A$ tel que l'on ait $x = ux_0^k$ et $y = vy_0^k$.
Montrer par un exemple, qu'on ne peut pas omettre u et v.

b) Si de plus $A^\times$ est un ensemble fini et de cardinal premier à k, montrer qu'il existe $x_1, y_1 \in A$ tels que $x = x_1^k$ et $y = y_1^k$.
[**Indication:** Que dire du morphisme $A^\times \to A^\times, u \mapsto u^k$?]

Exercice 50. — **[Une équation de Mordell]**
Le but est de montrer que l'équation diophantienne $y^2 = x^3 - 2$ admet pour uniques solutions $(x = 3, y = \pm 5)$.

a) En raisonnant modulo 8, montrer que x est impair.

b) Rappeler pourquoi l'anneau $A := \mathbf{Z}[\sqrt{-2}]$ est euclidien et quelles sont ses unités.

c) Montrer que les éléments $y + i\sqrt{2}$ et $y - i\sqrt{2} \in A$ sont premiers entre eux.

d) En utilisant l'ex. ***49***, montrer qu'il existe $n, m \in \mathbf{Z}$ tels que :

$$y = m(m^2 - 6n^2) \qquad \text{et} \qquad 1 = n(3m^2 - 2n^2).$$

e) Conclure.

Exercice 51. — **[Fermat, généralités]**
Le théorème de Fermat énonce que pour $n \geqslant 3$, les solutions de l'équation $x^n + y^n = z^n$ sont triviales.

a) Quelles sont les solutions triviales ?

b) Montrer qu'il suffit d'établir l'assertion pour $n = 4$ et n premier impair.

c) Montrer qu'il suffit de prouver l'assertion pour x, y premiers entre eux.

Exercice 52. — **[Fermat, $n = 4$ [Hindry]]**
Le but est de montrer que l'équation

$$x^4 + y^4 = z^2$$

n'a pas de solution avec $xyz \neq 0$. On reprend les résultats de l'ex ***31***.

a) Soit x, y, z une solution primitive avec $z > 0$ minimal. Montrer qu'il existe des entiers $u > v > 0$ premiers entre eux et de parités différentes tels que $x^2 = u^2 - v^2, y^2 = 2uv, z = u^2 + v^2$.

b) Montrer que u est impair et v pair, disons $v = 2w$.

c) Montrer que u et w sont des carrés, disons $u = z_1^2$, $w = a^2$.

d) Montrer qu'il existe des entiers b, c premiers entre eux tels que $x = b^2 - c^2$, $v = 2bc$ et $u = b^2 + c^2$, puis que b et c sont des carrés.

e) En déduire x_1, y_1 tels que $x_1^4 + y_1^4 = z_1^2$ et conclure.

Exercice 53. — **[Fermat, $n = 3$ [Hindry]]**
On travaille dans l'anneau $A := \mathbf{Z}[j]$ avec $j = e^{\frac{2i\pi}{3}}$ et on se propose de montrer que toute solution dans A de l'équation de Fermat pour $n = 3$ vérifie $xyz = 0$.

a) Préliminaires : On pose $\lambda := 1 - j$.

i) Montrer que $A = \{a + bj,\ a\, b \in \mathbf{Z}\}$, puis que A est euclidien et déterminer ses unités.

ii) Montrer que λ est irréductible dans A et que l'on a $3 = u\lambda^2$, avec $u \in A^\times$.

iii) Vérifier que pour $u \in A^\times$, on a $u \equiv \pm 1[\lambda^2] \implies u = \pm 1$.

iv) Déterminer l'anneau quotient $A/(\lambda)$ et en déduire que tout élément de A est congru à $-1, 0$, ou 1 modulo λ.
En déduire que si $a \in A$ n'est pas divisible par λ, alors $a^3 \equiv \pm 1[\lambda^4]$.

Soit (x, y, z) une solution primitive dans A. On distingue deux cas :

b) Si $\lambda \nmid xyz$: En utilisant **a)iv)**, montrer qu'on aurait $\pm 1 \pm 1 \pm 1 \equiv 0[\lambda^4]$ et conclure.

c) Si $\lambda \mid xyz$: on considère plus généralement l'équation $x^3 + y^3 = uz^3$, avec $u \in A^\times$.

i) Montrer que quitte à permuter x, y, z, on peut supposer que $\lambda | z$ et $\lambda \nmid xy$ et que la valuation $k := v_\lambda(z)$ est minimale.

ii) Montrer que $\lambda^2 | z$.
[**Indication:** Utiliser **a)iv)**.]

iii) De la factorisation $uz^3 = (x + y)(x + jy)(x + j^2y)$, montrer que λ^2 doit diviser l'un des facteurs de droite et qu'on peut supposer que c'est $x + y$.
Montrer qu'alors $\text{pgcd}(x + y, x + jy) = \text{pgcd}(x + y, x + j^2y) = \text{pgcd}(x + jy, x + j^2y) = \lambda$

iv) En déduire, comme à l'ex ***49***, qu'il existe des éléments $X, Y, Z \in A$ globalement premiers entre eux et des unités $u_1, u_2, u_3 \in A^\times$ telles que l'on ait :

$$x + y = u_1 X^3 \lambda^{3k-2}, \qquad x + jy = u_2 Y^3 \lambda \qquad x + j^2 y = u_3 Z^3 \lambda.$$

v) En déduire des unités $u_4, u_5 \in A^\times$ telles que l'on ait : $Y^3 + u_4 Z^3 = u_5(\lambda^{k-1} X)^3$.
[**Indication:** Considérer $0 = (x + y) + j(x + jy) + j^2(x + j^2 y)$.]

vi) En remarquant qu'alors $u_4 \equiv \pm 1[\lambda^2]$ et en utilisant **a)iii)**, conclure.