Agrégation : Anneaux, première partie

Cyril Demarche

31 janvier 2026

Dans ce chapitre, après quelques généralités sur les anneaux et les idéaux, nous étudions les anneaux euclidiens et les anneaux principaux. Au passage, nous revoyons les propriétés cruciales des anneaux $\mathbf{Z}$ et $K[X]$, qui seront fondamentales dans les chapitres d'arithmétique et d'algèbre linéaire, respectivement.

1 Généralités et premiers exemples

1.1 Anneaux

Commençons par définir le principal objet d'étude de ce chapitre.

Définition 1.1. Un anneau est un triplet $(A, +, \cdot)$ où A est un ensemble muni de deux lois de composition interne $A \times A \xrightarrow{\cdot} A$, notée $+$ et $\cdot$, vérifiant

1. $(A, +)$ est un groupe abélien.
2. la loi $\cdot$ est associative.
3. pour tous $x, y, z, t \in A$, $(x + y) \cdot (z + t) = x \cdot z + x \cdot t + y \cdot z + y \cdot t$.

Le dernier axiome est appelé "distributivité".

Exemples 1.2.
- $(\mathbf{Z}, +, \cdot)$ est un anneau.
- $(\mathrm{M}_n(K), +, \cdot)$ et $(\mathcal{L}(V), +, \circ)$ (où K est un corps et V est un espace vectoriel) sont des anneaux.
- $(2\mathbf{Z}, +, \cdot)$ est un anneau.
- l'ensemble des fonctions holomorphes sur $\mathbf{C}$, muni de l'addition et de la multiplication, est un anneau.
- si K est un corps (et même un anneau commutatif), $K[X]$ et $K[[X]]$ sont des anneaux.
- si $n \in \mathbf{N}$, l'ensemble $\mathbf{Z}/n\mathbf{Z}$ des entiers modulo n, muni de l'addition et de la multiplication des entiers modulo n, est un anneau.

Lemme 1.3. *Soit A un anneau. Alors $0 \cdot x = x \cdot 0 = 0$ pour tout $x \in A$. On dit que 0 est un élément absorbant.*

Démonstration. On a $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, donc en simplifiant par $0 \cdot x$, il reste $0 \cdot x = 0$. □

Cette définition est trop générale pour nous. Tous les anneaux que nous croiserons seront unitaires :

Définition 1.4. Soit A un anneau.

On dit que A est unitaire s'il existe un élément $1 \in A$ qui est un élément neutre pour la loi $\cdot$, i.e. tel que pour tout $x \in A$, $1 \cdot x = x \cdot 1 = x$.

À partir de maintenant, "anneau" signifie "anneau unitaire".

Rappelons qu'un tel élément est nécessairement unique. On l'appelle "élément unité" ou "unité" de A.

Définition 1.5. Un anneau A est dit commutatif si la loi $\cdot$ est commutative.

Définition 1.6. Soit A un anneau unitaire.

Un élément $x \in A$ est dit inversible s'il existe $y \in A$ (nécessairement unique) tel que $x \cdot y = y \cdot x = 1$. Dans ce cas, y est noté x^{-1}.

L'ensemble des éléments inversibles de A est noté $A^\times$.

Proposition 1.7. *L'ensemble $A^\times$ muni de la loi $\cdot$ est un groupe.*

Remarque 1.8. Attention, si A est unitaire non nul, $(A, \cdot)$ n'est jamais un groupe car 0 n'est pas inversible.

Exemples 1.9.
- $\mathbf{Z}^\times = \{\pm 1\}$.
- $A[X]^\times = A^\times$.
- $A[[X]]^\times = \{\sum_{n\geq 0} a_n X^n : a_0 \in A^\times\}$.
- $\mathrm{M}_n(K)^\times = \mathrm{GL}_n(K)$.
- $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$.
- $\mathbf{Z}[\sqrt{3}]^\times = \{a + b\sqrt{3} : (a, b) \in \mathbf{Z}^2 \text{ tels que } a^2 - 3b^2 = 1\} = \{\pm(2 + \sqrt{3})^k, k \in \mathbf{Z}\}$.

Définition 1.10. Un anneau non nul A est une algèbre à division (ou un corps gauche, ou corps non commutatif) si tout élément non nul est inversible.

Un anneau non nul A est un corps si A est commutatif et tout élément non nul est inversible.

Exemples 1.11.
- les anneaux $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, $\mathbf{Q}(X)$ sont des corps.
- la $\mathbf{R}$-algèbre des quaternions $\mathbf{H}$ est une algèbre à division.

Définition 1.12. Soit A un anneau. Un élément $x \in A$ est un diviseur de 0 (à gauche) si $x \neq 0$ s'il existe $y \neq 0$ tel que $x \cdot y = 0$.

Définition 1.13. Soit A un anneau commutatif.

On dit que A est intègre si A est non nul et A n'a pas de diviseur de 0, c'est-à-dire si pour tous $x, y \in A$, $x \cdot y = 0$ implique $x = 0$ ou $y = 0$.

Exemples 1.14.
- $\mathbf{Z}$, $K[X]$ sont des anneaux intègres.
- $\mathbf{Z}/4\mathbf{Z}$ et $\mathbf{Z}/6\mathbf{Z}$ ne sont pas des anneaux intègres.

Proposition 1.15. *Un anneau intègre fini est un corps.*

Démonstration. Soit A un tel anneau. Soit $x \in A$ non nul. L'application $A \to A$ définie par $y \mapsto x \cdot y$ est injective (car A est intègre), donc surjective (car A est fini), donc il existe $y \in A$ tel que $xy = 1$, donc x est inversible. □

Théorème 1.16. *Soit $n \geq 1$. Les assertions suivantes sont équivalentes :*

1. *l'anneau $\mathbf{Z}/n\mathbf{Z}$ est intègre.*

2. *l'anneau* $\mathbf{Z}/n\mathbf{Z}$ *est un corps.*
3. *l'entier* n *est premier.*

Démonstration. On donnera une preuve plus générale de cet énoncé un peu plus loin.
- La proposition 1.15 assure que 1 et 2 sont équivalents.
- Si n n'est pas premier, alors $n = kd$, avec $k, d \geq 2$, alors $\bar{k}, \bar{d} \neq \bar{0}$ dans $\mathbf{Z}/n\mathbf{Z}$, et $\bar{k}\bar{d} = \bar{0}$, donc $\mathbf{Z}/n\mathbf{Z}$ n'est pas intègre.
- Si n est premier et si $\bar{k}, \bar{d} \in \mathbf{Z}/n\mathbf{Z}$ tels que $\bar{k}\bar{d} = \bar{0}$ avec $\bar{k} \neq \bar{0}$. Alors n divise kd, et n ne divise pas k, donc n divise d (lemme d'Euclide), i.e. $\bar{d} = \bar{0}$, donc $\mathbf{Z}/n\mathbf{Z}$ est intègre.

□

Définition 1.17. Soit A un anneau.
Un élément $a \in A$ est dit nilpotent s'il existe $n \geq 1$ tel que $a^n = 0$.

Définition 1.18. Soit A un anneau commutatif. On dit que A est réduit si A ne contient aucun élément nilpotent non nul.

Définition 1.19. Soit A un anneau commutatif. Un élément $a \in A$ est dit irréductible si $a \notin A^\times$ et pour tous $b, c \in A$ tels que $a = b \cdot c$, on a $a \in A^\times$ ou $b \in A^\times$.

Exemple 1.20. Dans $\mathbf{Z}$, les éléments irréductibles sont exactement les nombres premiers.
Dans $K[X]$, les éléments irréductibles sont exactement les polynômes irréductibles non constants.

1.2 Sous-anneaux

Intéressons-nous maintenant à la notion de sous-objet :

Définition 1.21. Soit A un anneau. Un sous-anneau de A est une partie B de A telle que
1. $(B, +)$ est un sous-groupe de $(A, +)$.
2. B est stable par $\cdot$ (et contient 1 si A est unitaire).

Exemples 1.22.
1. Pour tout anneau A, $\{0\}$ et A sont des sous-anneaux de A.
2. $\mathbf{Z}[i]$, $\mathbf{Z}[j]$, $\mathbf{Q}(i)$, $\mathbf{Q}[\sqrt{2}]$ sont des sous-anneaux de $\mathbf{C}$.

1.3 Morphismes

Maintenant que nous avons défini les objets (à savoir les anneaux), il s'agit de définir un moyen de comparer ces objets, à savoir les morphismes entre objets.

Définition 1.23. Soient A et B deux anneaux unitaires. Une application $\varphi : A \to B$ est un morphisme d'anneaux seulement si φ est un morphisme de groupes additifs, $\varphi(1_A) = 1_B$ et pour tous $x, y \in A$, $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

Définition 1.24. On dit qu'un morphisme d'anneaux $\varphi : A \to B$ est un
- isomorphisme si φ est une bijection.
- endomorphisme si $A = B$.
- automorphisme si $A = B$ et φ est un isomorphisme.

Proposition 1.25. *Soit $\varphi : A \to B$ un isomorphisme. Alors $\varphi^{-1} : H \to G$ est un morphisme d'anneaux.*

Définissons deux sous-anneaux naturellement associés à un morphisme d'anneaux :

Définition 1.26. Soit $\varphi : A \to B$ un morphisme d'anneaux.
Le noyau de φ, noté $\ker(\varphi)$, est $\varphi^{-1}(\{0_B\})$. L'image de φ, notée $\mathrm{im}\,(\varphi)$, est $\varphi(A)$.

Proposition 1.27. *Soit $\varphi : A \to B$ un morphisme d'anneaux.*
Alors $\ker(\varphi)$ *(resp.* $\mathrm{im}\,(\varphi)$*) est un sous-anneau de A (resp. B).*

1.4 Algèbre sur un anneau

Définition 1.28. Soit A un anneau commutatif. Une A-algèbre est un anneau B muni d'un morphisme d'anneaux $A \to B$ tel que l'image de A soit contenue dans le centre de B.

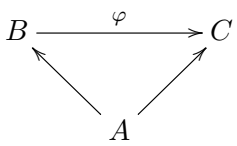
Intuitivement, c'est un mélange entre la notion d'anneau et celle d'espace vectoriel (sur l'anneau A).

En particuler, une A-algèbre commutative est exactement la donnée d'un anneau commutatif B et d'un morphisme d'anneaux $A \to B$.

Exemples 1.29.

1. A est naturellement une A-algèbre.
2. Tout anneau B est naturellement une $\mathbf{Z}$-algèbre.
3. Si $A = K$ est un corps, une K-algèbre est un K-espace vectoriel muni d'une structure d'anneau compatible à celle de K.
4. Si I est un ensemble, l'algèbre des polynômes $A[(X_i)_{i\in I}]$ est naturellement une A-algèbre commutative.
5. L'ensemble des matrices carrées $\mathrm{Mat}_n(A)$ est une A-algèbre, non commutative en général.
6. Si $K \subset L$ est un sous-corps d'un corps L (on parle d'extension de corps), alors L est une K-algèbre.
7. L'algèbre des quaternions de Hamilton, notée $\mathbf{H}$, est une $\mathbf{R}$-algèbre, non commutative, de dimenson 4.
8.

On dispose d'une notion naturelle de morphisme de A-algèbres : si B et C sont deux A-algèbres, un morphisme de A-algèbres $\varphi : B \to C$ est un morphisme d'anneaux tel que le diagramme évident



soit commutatif.

2 Idéaux d'un anneau

La notion de sous-anneau est trop faible pour pouvoir faire des quotients qui soient naturellement des anneaux. La bonne notion est celle d'idéal.

Définition 2.1. Soit A un anneau commutatif. Une partie $I \subset A$ est un idéal si
- I est un sous-groupe de $(A, +)$.
- Pour tout $a \in A$ et tout $x \in I$, on a $a \cdot x \in I$.

Exemples 2.2.
- $\{0\}$ et A sont des idéaux de A.
- Pour tout $a \in A$, l'ensemble $aA := \{a \cdot x, x \in A\}$ est un idéal de A, noté (a). Un tel idéal est dit principal.
- Si $n \in \mathbf{Z}$, $n\mathbf{Z}$ est un idéal de $\mathbf{Z}$.
- Dans l'anneau $K[X, Y]$, l'ensemble $\{XP + YQ, P, Q \in K[X, Y]\}$ est un idéal.

Définition 2.3. Soit A un anneau commutatif. Pour toute partie $P \subset A$, on note (P) l'idéal engendré par la partie P, i.e. le plus petit idéal (pour l'inclusion) contenant P.

Concrètement, (P) peut être décrit comme l'intersection de tous les idéaux de A contenant P (une intersection d'idéaux est un idéal), ou alors comme l'ensemble des combinaisons linéaires $\sum_{i=1}^{n} a_i p_i$, avec $a_i \in A$ et $p_i \in P$.

Par exemple, dans $K[X, Y]$, $(X, Y) = \{XP + YQ, P, Q \in K[X, Y]\}$.

Lemme 2.4. *Soit A un anneau commutatif et I un idéal de A.*
- *Si I contient un élément inversible de A, alors $I = A$.*
- *On suppose A intègre. Soient $a, b \in A$. Alors $(a) = (b)$ si et seulement s'il existe $u \in A^\times$ tels que $b = u \cdot a$. On dit alors que a et b sont associés.*

Démonstration.
- Si $a \in I$ est inversible, alors $a^{-1}a \in I$, donc $1 \in I$, donc pour tout $a \in A$, $a = a \cdot 1 \in I$. Donc $I = A$.
- Si $a = u \cdot b$, alors clairement $(b) \subset (a)$. Comme u est inversible, on a $b = u^{-1} \cdot a$, donc $(a) \subset (b)$. Donc finalement $(a) = (b)$.

  Réciproquement, supposons que $(b) = (a)$. Alors a divise b et b divise a, donc il existe $u, v \in A$ tels que $a = bv$ et $b = au$. Donc $a = auv$, donc $a(uv - 1) = 0$. Puisque A est intègre, on a donc $a = 0$ ou $uv = 1$. Dans le premier cas, on a aussi $b = 0$, donc $a = b$. Dans le second cas, on a $b = ua$ et $uv = 1$, donc $u \in A^\times$. □

Proposition 2.5. *Soit $f : A \to B$ un morphisme d'anneaux commutatifs.*
Alors $\ker(f)$ *est un idéal de A.*

Démonstration. Vérification facile. □

Théorème 2.6. *Les idéaux (resp. les sous-groupes) de* $\mathbf{Z}$ *sont exactement les $n\mathbf{Z}$, avec $n \in \mathbf{N}$.*

Démonstration. cf chapitre précédent. Il suffit seulement de vérifier en plus que tout sous-groupe de $\mathbf{Z}$ est un idéal (cela résulte de la définition de la multiplication dans $\mathbf{Z}$ à partir de l'addition). □

Définition 2.7. Soit A un anneau commutatif.

Considérons l'unique morphisme d'anneaux $\varphi : \mathbf{Z} \to A$, défini par $\varphi(n) = n1_A := 1_A + \cdots + 1_A$ (n fois) si $n \geq 0$. Le noyau de φ est un idéal de $\mathbf{Z}$, de la forme $n\mathbf{Z}$ pour un certain $n \in \mathbf{N}$ unique. Cet entier n est appelé la caratéristique de A.

Autrement dit, c'est le plus petit entier (s'il existe) $n \geq 1$ tel que $n1_A = 0_A$. Si un tel entier n'existe pas, la caractéristique de A est nulle.

La notion d'idéal est cruciale pour parler de quotients d'anneaux commutatifs.

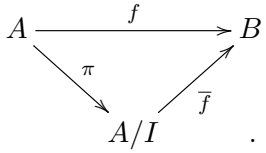
Proposition 2.8. *Soit A un anneau commutatif et I un idéal de A.*

Alors il existe une unique structure d'anneau sur l'ensemble A/I de sorte que le morphisme canonique $\pi : A \to A/I$ soit un morphisme d'anneaux.

Démonstration. La structure d'anneau recherchée est unique, car π est surjective et on doit avoir, pour tout $a, b \in A$, $\pi(a) + \pi(b) = \pi(a + b)$ et $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$.

Pour l'existence, il faut vérifier que ces formules sont bien définies. Pour l'addition, il s'agit du quotient d'un groupe abélien par un sous-groupe, donc la vérification a été faite dans le chapitre précédent. Vérifions la multiplication. Pour que la formule $\pi(a) \cdot \pi(b) = \pi(a \cdot b)$ soit une définition d'une multiplication sur A/I, il faut et il suffit que pour tous $a, b \in A$, et $i, j \in I$, on ait $\pi(a \cdot b) = \pi((a + i) \cdot (b + j))$. Or $(a+i)\cdot(b+j) = a\cdot b+a\cdot j+b\cdot i+i\cdot j$, donc il suffit de montrer que $a\cdot j+b\cdot i+i\cdot j \in I = \ker \pi$. Ceci résulte de la définition d'un idéal (et on voit que l'on a vraiment besoin de la stabilité de I par multiplication par tout élément de A et pas seulement par un élément de I). □

Théorème 2.9. *Soit $f : A \to B$ un morphisme d'anneaux commutatifs et I un idéal de A. L'idéal I est contenu dans* $\ker(f)$ *si et seulement s'il existe un unique morphisme $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi$, autrement dit le diagramme suivant*



Démonstration. La propriété universelle du quotient par un sous-groupe assure l'existe d'un unique morphisme de groupes additifs $\overline{f} : A/I \to B$ tel que $f = \overline{f} \circ \pi$. Montrons que $\overline{f}$ est un morphisme d'anneaux. Soient $\bar{a}, \bar{b} \in A/I$, et $a, b \in A$ tels que $\pi(a) = \bar{a}$ et $\pi(b) = \bar{b}$. Alors par définition de la multiplication sur A/I, on a $\pi(a \cdot b) = \bar{a} \cdot \bar{b}$, donc $\overline{f}(\bar{a} \cdot \bar{b}) = f(a \cdot b) = f(a) \cdot f(b) = \overline{f}(\bar{a}) \cdot \overline{f}(\bar{b})$. □

Corollaire 2.10. *Soit $f : A \to B$ un morphisme d'anneaux commutatifs. Alors f induit un isomorphisme d'anneaux*

$$\overline{f} : A/\ker(f) \xrightarrow{\sim} \operatorname{im}(f).$$

Démonstration. Preuve identique au résultat analogue de théorie des groupes. □

Définition 2.11. Soit A un anneau commutatif, I et J deux idéaux de A. On définit les idéaux suivants :

— $I + J := \{i + j : (i, j) \in I \times J\}$ est l'idéal engendré par I et J.

— $IJ := \{\sum_{k=0}^{r} i_k j_k, r \in \mathbf{N}, i_k \in I, j_k \in J\}$ est l'idéal engendré par les produits d'un élément de I et d'un élément de J.

Proposition 2.12 (Théorème chinois, version générale)**.** *Soit A un anneau commutatif, I et J deux idéaux de A tels que $I + J = A$.*

Alors $I \cap J = IJ$ et le morphisme naturel $A \to A/I \times A/J$ induit un isomomrphismes d'anneaux

$$A/IJ = A/(I \cap J) \xrightarrow{\sim} A/I \times A/J\,.$$

Démonstration. Notons $\pi : A \to A/I \times A/J$. Un élément $a \in A$ est dans $\ker \pi$ si et seulement si $a \in I$ et $a \in J$, donc $\ker \pi = I \cap J$. En général, on a l'inclusion d'idéaux $IJ \subset I \cap J$.

Puisque $I + J = A$, il existe $i \in I$ et $j \in J$ tels que $i + j = 1$ (analogue d'une relation de Bézout). Donc pour tout $x \in I \cap J$, on a $x = 1 \cdot x = (i + j) \cdot x = i \cdot x + j \cdot x$, donc $x \in IJ$. Donc on a bien $IJ = I \cap J = \ker \pi$.

Donc en passant au quotient, π induit un morphisme injectif $\bar{\pi} : A/IJ \to A/I \times A/J$. Montrons pour finie que $\bar{\pi}$ est surjectif. Soit $(\bar{a}, \bar{b}) \in A/I \times A/J$, et on choisit a (resp. b) dans A des représentants de $\bar{a}$ et $\bar{b}$. Alors $\pi(ib + ja) = (\overline{ja}, \overline{ib})$. Comme $i + j = 1$, on a $\bar{j} = 1$ dans A/I et $\bar{i} = 1$ dans A/J. Donc finalement $\pi(ib + ja) = (\bar{a}, \bar{b})$, ce qui assure que π est surjective. Donc $\bar{\pi}$ est bien un isomorphisme $A/IJ \xrightarrow{\bar{\pi}} A/I \times A/J$. □

Définition 2.13. Un idéal I d'un anneau commutatif A est dit

— premier si l'anneau quotient A/I est intègre.

— maximal si l'anneau quotient A/I est un corps.

En particulier, tout idéal maximal est premier.

Exemple 2.14. Soit $n \geq 1$. Le théorème **??** assure que dans $\mathbf{Z}$, l'idéal $I = (n)$ est premier si et seulement si (n) est maximal si et seulement si n est un nombre premier.

Proposition 2.15. *Soit I un idéal de A.*

— *l'idéal I est premier si et seulement si pour tout $a, b \in A$, si $a \cdot b \in I$, alors $a \in I$ ou $b \in I$.*

— *l'idéal I est maximal si et seulement si I est maximal (pour l'inclusion) parmi les idéaux de A distincts de A.*

Démonstration. □

Proposition 2.16. *Soit A un anneau commutatif intègre et $p \in A$.*

Si (p) est premier, alors p est irréductible.

Démonstration. On suppose (p) premier. Soient $x, y \in A$ tels que $p = xy$. Alors $xy \in (p)$, donc comme (p) est premier, x ou y est dans (p), par exemple x. Alors p divise x, donc $x = pz$ pour un $z \in A$. Donc $p = pzy$, donc puisque A est intègre, $zy = 1$, donc y est inversible. Donc p est irréductible. □

Remarque 2.17. La réciproque de cet énoncé est fausse en général. Par exemple, dans l'anneau $A = \mathbf{Z}[i\sqrt{5}]$, on a les égalités suivantes :

$$(1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}) = 6 = 2 \cdot 3\,.$$

En particulier, l'élément 2 est irréductible, car si on a $a+ib\sqrt{5}$ divise 2, alors en calculant les modules au carré, on en déduit que a^2+5b^2 divise 4, donc $a^2+5b^2 \in \{1,2,4\}$, donc $b=0$, et $a=\pm 1, \pm 2$. Donc $a+ib\sqrt{5} = \pm 1, \pm 2$, ce qui assure que 2 est irrédutible dans A. En revanche, $(1+i\sqrt{5})\cdot(1-i\sqrt{5}) = 6$ est dans l'idéal (2), mais $(1 \pm i\sqrt{5}) \notin (2)$ de façon évidente. Donc (2) n'est pas premier. De façon équivalente, le quotient $A/(2)$ s'identifie à $\left(\mathbf{Z}[X]/(X^2+5)\right)/(2) \cong \mathbf{F}_2[X]/(X^2+1) \cong \mathbf{F}_2[X]/((X+1)^2)$ qui n'est pas intègre, car $X+1$ est nilpotent. Donc (2) n'est pas premier.

3 Anneaux principaux et euclidiens

3.1 Généralités

Les anneaux principaux et euclidiens sont les anneaux idéaux pour faire de l'arithmétique. Ils sont cruciaux en théorie des nombres, mais aussi en algèbre linéaire.

Définition 3.1. Soit A un anneau commutatif.

On dit que A est principal si A est intègre et tout idéal de A est principal.

Exemples 3.2.
— $\mathbf{Z}$ est principal.
— $K[X]$ est principal.
— $\mathbf{Z}[X]$, $K[X,Y]$, $\mathbf{Z}[i\sqrt{3}]$, $\mathbf{Z}[\sqrt{5}]$, $\mathbf{Z}[i\sqrt{5}]$ ne sont pas principaux.

Dans les deux cas, la preuve repose sur la division euclidienne.

Proposition 3.3. *Soit A un anneau principal et $p \in A$. Les assertions suivantes sont équivalentes :*
— *p est irréductible.*
— *(p) est premier.*
— *(p) est maximal.*

Démonstration.
— On suppose p irréductible. Puisque p n'est pas inversible, (p) n'est pas égal à A. Soit I un idéal de A contenant (p). Puisque A est principal, il existe $a \in A$ tel que $I = (a)$. Comme $(p) \subset (a)$, l'élément a divise p. Puisque p est irréductible, soit a est inversible, soit $a = up$, avec $u \in A^\times$. Donc $I = (a)$ est égal à A ou à (p), ce qui assure que (p) est maximal.
— L'affirmation "maximal" implique "premier" est évidente.
— L'affirmation "premier" implique "irréductible" est vraie en général, et démontrée en proposition 2.16.

□

Corollaire 3.4 (lemme d'Euclide)**.** *Pour tout $p \in A$ irréductible, pour tous $a, b \in A$, si p divise ab, alors p divise a ou p divise b.*

Démonstration. C'est eaxctement l'affirmation "irréductible" implique "premier". □

Définition 3.5. Soit A un anneau commutatif. On dit que A est euclidien si A est intègre et il existe une application (appelée stathme) $\varphi : A \setminus \{0\} \to \mathbf{N}$ telle que pour tout $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que

$$\begin{cases} a = b \cdot q + r \\ r = 0 \text{ ou } \varphi(r) < \varphi(b)\,. \end{cases}$$

Exemples 3.6. — $\mathbf{Z}$ est euclidien avec $\varphi(n) := |n|$.
— $\mathbf{Z}[i]$ est euclidien $\varphi = |\cdot|^2$.
— $K[X]$ est euclidien avec $\varphi(P) := \deg(P)$.

Démonstration. — Pour $\mathbf{Z}$, soient $a, b \in \mathbf{Z}$ avec $b \neq 0$. Si $b > 0$, notons $q \in \mathbf{Z}$ l'entier maximal tel que $q \leq \frac{a}{b}$ (i.e. q est la partie entière de $\frac{a}{b}$). Alors $r := a - bq$ convient. Si $b < 0$, on note $q \in \mathbf{Z}$ l'entier minimal tel que $q \geq \frac{a}{b}$ (i.e. q est la partie entière supérieure de $\frac{a}{b}$). Alors $r := a - bq$ convient. Notez que l'on n'a pas besoin de distinguer ces deux cas en fait (puisqu'on n'exige pas que le reste soit positif).
— Pour $\mathbf{Z}[i]$, pour tout $a, b \in \mathbf{Z}$ avec $b \neq 0$, on considère $\frac{a}{b} \in \mathbf{Q}[i]$. il existe $q \in \mathbf{Z}[i]$ tel que $|\frac{a}{b} - q| \leq \frac{\sqrt{2}}{2}$ (faire un dessin). On en déduit que $|a - bq|^2 \leq \frac{|b|^2}{2}$, donc en posant $r := a - bq$, on a le résultat souhaité.
— Pour tout $A = \sum_{i=0}^{n} a_i X^i, B = \sum_{j=0}^{m} b_j X^j \in K[X]$, avec $B \neq 0$ (donc on peut supposer $b_m \neq 0$), on a $\deg(A) < \deg(B)$ ou ($\deg(A) > \deg(B)$ et $\deg(A - B\frac{a_n}{b_m} X^{n-m}) < \deg(A)$). Dans le premier cas, on pose $Q = 0$ et $R = A$. Dans le second, on sait par récurrence sur le degré qu'il existe Q', R' tels que $A - B\frac{a_n}{b_m} X^{n-m} = BQ' + R'$ avec $\deg(R') < \deg(B)$. Alors $A = B(\frac{a_n}{b_m} X^{n-m} + Q') + R'$, donc $Q = \frac{a_n}{b_m} X^{n-m} + Q'$ et $R = R'$ conviennent.

□

Remarque 3.7. Soit S un anneau commutatif. L'algorithme de division euclidienne des polynômes dans $K[X]$ s'adapte dans $S[X]$, pourvu que le coefficient dominant du diviseur soit inversible dans R. Plus précisément :

Pour tout $A, B \in S[X]$, si le coefficient dominant de B est inversible dans S, alors il existe un unique couple (Q, R) dans $S[X]$ tel que $A = BQ + R$ et $\deg(R) < \deg(B)$.

En particulier, si un polynôme $P \in S[X]$ s'annule en un élément $\alpha \in S$, alors on a une factorisation $P = (X - \alpha)Q$ dans $S[X]$, avec $\deg Q = \deg P - 1$.

Une conséquence utile de cette dernière remarque :

Proposition 3.8. *Soit A un anneau commutatif et $P \in A[X]$. Pour tout $a \in A$, on a $P(a) = 0$ si et seulement si $X - a$ divise P dans $A[X]$.*

Démonstration. Soit $a \in A$. Si $X - a$ divise P, alors clairement $P(a) = 0$. Montrons maintenant la réciproque. Notons $P = (X - a)Q + R$ la division euclidienne (au sens généralisé de la dernière remarque) dans $A[X]$, avec R polynôme constant. Alors $P(a) = 0$ si et seulement si $R(a) = 0$ si et seulement si $R = 0$ si et seulement si $X - a$ divise P. □

Proposition 3.9. *Soit A un anneau commutatif intègre. Soit $P \in A[X]$ un polynôme de degré d.*

Alors P a au plus d racines distinctes dans A.

Démonstration. Soient $a_1, \ldots, a_r \in A$ des racines distinctes de P. Par la proposition précédente, il existe $P_1 \in A[X]$ tel que $P = (X - a_1)P_1$. Montrons que $a_2, \ldots, a_r$ sont racines de P_1. Pour tout $i \geq 2$, on a $0 = P(a_i) = (a_i - a_1)P_1(a_i)$. Or $a_i \neq a_1$ et A est intègre, donc $P_1(a_i) = 0$. Donc par récurrence, il existe $Q \in A[X]$ tel que $P = (X - a_1) \ldots (X - a_r)Q$. En calculant les degrés, on a $d = r + \deg(Q)$, donc $r \leq d$, ce qui conclut la preuve. □

Théorème 3.10. *Un anneau euclidien est principal.*

Démonstration. Soit I un idéal de A, non nul. Il existe un élément $a \in I \setminus \{0\}$ de valuation minimale. Soit alors $\alpha \in I$. On effectue la division euclidienne de α par a : il existe $(q, r) \in A^2$ tels que $\alpha = aq + r$ avec $r = 0$ ou $\varphi(r) < \varphi(a)$. Dans le second cas, on a $r = \alpha - q$, donc $r \in I$, et $\varphi(r) < \varphi(a)$, donc $r = 0$. Dans tous les cas, $r = 0$, donc $\alpha = aq$, donc $I \subset (a)$. L'inclusion réciproque est évidente. □

Exemples 3.11. Les anneaux $\mathbf{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ et $\mathbf{R}[X, Y]/(X^2 + Y^2 + 1)$ sont principaux non euclidiens.

Les anneaux euclidiens ont d'excellentes propriétés arithmétiques, que nous allons explorer maintenant. On commence par rappeler la définition suivante :

Définition 3.12. Soit A un anneau commutatif et $a, b \in A$.

Un pgcd de a et b est un élément $d \in A$ tel que $d|a$ et $d|b$, et pour tout $k \in A$ divisant a et b, on a $k|d$.

Cette définition ce généralise sans difficultés au pgcd d'une famille quelconque d'éléments de A.

Proposition 3.13. *Soit A un anneau principal.*

Pour toute famille $(a_i)_{i\in I}$ d'élements de A, il existe un pgcd de cette famille, unique à multiplication près par un inversible. On note "le" pgcd de cette famille par $\mathrm{pgcd}((a_i))$.

Plus précisément, un élément $d \in A$ est un pgcd des (a_i) si et seulement si on a l'égalité d'idéaux $(d) = (a_i, i \in I)$.

Démonstration. Soit $d \in A$ tel que $(d) = (a_i, i \in I)$. Montrons que d est un pgcd des a_i.

Soit $k \in A$ tel que k divise a_i pour tout $i \in I$. Alors $(k) \subset (a_i, i \in I) = (d)$, donc d divise k. Cela assure que d est un pgcd des a_i. □

Théorème 3.14 (Bézout)**.** *Soit A un anneau principal et $(a_i)_{i\in I}$ des éléments de A. Si d est un pgcd des (a_i), alors il existe une famille $(u_i)_{i\in I}$ à support fini, telle que*

$$d = \sum_{i\in I} u_i a_i \,.$$

Plus concrètement, pour tout $a, b \in A$, il existe $u, v \in A$ tels que

$$\mathrm{pgcd}(a, b) = au + bv \,.$$

Démonstration. C'est évident. □

Corollaire 3.15 (Lemme de Gauss)**.** *Soit A un anneau principal.*

Pour tout $a, b, c \in A$, si a divise bc et $(a, b) = 1$, alors a divise c.

Démonstration. Par Bézout, il existe $u, v \in A$ tels que $au + bv = 1$. On multiplie par c pour obtenir $acu + bcv = c$. Or a divise acu et bcv par hypothèse, donc a divise c. □

Corollaire 3.16 (Théorème chinois dans un anneau principal)**.** *Soit A un anneau principal, et $a, b \in A$ deux éléments premiers entre eux (i.e. tels que* $\mathrm{pgcd}(a, b) = 1$*).*

Alors le morphisme naturel

$$A/(ab) \xrightarrow{\sim} A/(a) \times A/(b)$$

est un isomorphisme d'anneaux, dont on peut expliciter la réciproque à l'aide d'une relation de Bézout entre a et b : si $au + bv = 1$, l'antécédent de $(\bar{x}, \bar{y}) \in A/(a) \times A/(b)$ par ce morphisme est la classe de $auy + bvx$ dans $A/(ab)$.

Par récurrence, on peut étendre ce résultat à $a_1, \ldots, a_n$ deux-à-deux premiers entre eux.

Démonstration. Il s'agit seulement d'adapter la preuve du théorème chinois général (voir proposition 2.12) dans ce contexte. □

Exemples 3.17. On utilisera souvent le théorème chinois dans $\mathbf{Z}$ ou dans $K[X]$.

1. si $m, n \in \mathbf{Z}$ sont premiers entre eux, on a un isomorphisme d'anneaux $\mathbf{Z}/(mn)\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$ dont on peut expliciter la réciproque à l'aide d'une relation de Bézout entre m et n.
2. si $P, Q \in K[X]$ sont premiers entre eux, on a un isomorphisme d'anneaux $K[X]/(PQ) \xrightarrow{\sim} K[X]/(P) \times K[X]/(Q)$ dont on peut expliciter la réciproque à l'aide d'une relation de Bézout entre P et Q.

3.2 Indicatrice d'Euler

On étudie quelques propriétés classiques de l'anneau $\mathbf{Z}/n\mathbf{Z}$, en lien également avec la structure de groupe de $\mathbf{Z}/n\mathbf{Z}$.

Théorème 3.18. *Soit $n \geq 1$ et $k \in \mathbf{Z}$. On note $\overline{k}$ la classe de k dans $\mathbf{Z}/n\mathbf{Z}$. Les assertions suivantes sont équivalentes :*

1. *$\overline{k}$ est un générateur du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$.*
2. *il existe $d \in \mathbf{Z}$ tel que $\overline{dk} = 1$ dans $\mathbf{Z}/n\mathbf{Z}$ (on dit que $\overline{k}$ est inversible dans l'anneau $\mathbf{Z}/n\mathbf{Z}$).*
3. *k et n sont premiers entre eux.*

Démonstration.
— On suppose que $\overline{k}$ est un générateur du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$. Alors il existe $d \in \mathbf{Z}$ tel que $d\overline{k} = 1$, donc $\overline{d}\overline{k} = 1$, donc $\overline{k}$ est inversible.
— On suppose que $\overline{k}$ est inversible. Alors il existe $d \in \mathbf{Z}$ tel que $\overline{dk} = 1$ dans $\mathbf{Z}/n\mathbf{Z}$. Donc il existe $a \in \mathbf{Z}$ tel que $dk = 1 + an$ dans $\mathbf{Z}$. Donc $dk - an = 1$, donc k et n sont premiers entre eux.
— On suppose k et n premiers entre eux. Par Bézout, il existe $u, v \in \mathbf{Z}$ tels que $uk + vn = 1$. Donc $u\overline{k} = 1$ dans $\mathbf{Z}/n\mathbf{Z}$, donc $1 \in \langle \overline{k} \rangle$. Or 1 est clairement générateur de $\mathbf{Z}/n\mathbf{Z}$, donc $\overline{k}$ aussi.

□

Définition 3.19. Soit $n \geq 2$.

On note $\varphi(n)$ le nombre d'entiers $1 \leq k < n$ tels que k est premier avec n. La fonction φ est appelée l'indicatrice d'Euler.

Grâce au théorème précédent, on a donc $\varphi(n) = |(\mathbf{Z}/n\mathbf{Z})^\times|$.

Corollaire 3.20. *Le groupe $\mathbf{Z}/n\mathbf{Z}$ (et donc tout groupe cyclique d'ordre n) admet exactement $\varphi(n)$ générateurs.*

Corollaire 3.21. *Soit $n \geq 1$.*
Alors $n = \sum_{d|n} \varphi(d)$.

Démonstration. On partitionne $\mathbf{Z}/n\mathbf{Z}$ selon l'ordre des éléments. Par le théorème de Lagrange, $\mathbf{Z}/n\mathbf{Z}$ est la réunion disjointe des G_d, pour d divisant n, où G_d est l'ensemble (ce n'est pas un sous-groupe) des éléments d'ordre d dans $\mathbf{Z}/n\mathbf{Z}$.

Donc $|\mathbf{Z}/n\mathbf{Z}| = \sum_{d|n} |G_d|$. Or pour tout d divisant n, le groupe $\mathbf{Z}/n\mathbf{Z}$ admet un unique sous-groupe (cyclique) de cardinal d, qui contient G_d. Donc $|G_d|$ est égal au nombre de générateurs de $\mathbf{Z}/d\mathbf{Z}$, qui vaut $\varphi(d)$ par la théorème précédent.

Donc finalement $n = \sum_{d|n} \varphi(d)$. □

Une conséquence importante de cette égalité est le résultat suivant :

Théorème 3.22. *Soit K un corps (ou même un anneau intègre) et $G < K^\times$ un sous-groupe fini.*
Alors G est cyclique.
En particulier, le groupe des inversibles d'un corps fini est cyclique.

Démonstration. Notons $n := |G|$, et pour tout d divisant n, G_d l'ensemble des éléments d'ordre d dans G.

Soit d divisant n et $x \in G_d$. Alors x est racine de $X^d - 1$, comme tout élément de $\langle x \rangle$. On a donc d racines distinctes de $X^d - 1$ dans $\langle x \rangle$. Or le polynôme $X^d - 1$ a au plus d racines dans K, donc ses racines sont exactement les éléments de $\langle x \rangle \cong \mathbf{Z}/d\mathbf{Z}$. En particulier, les éléments de G_d sont exactement les générateurs de $\langle x \rangle$, au nombre de $\varphi(d)$ par le corollaire 3.20. FInalement, pour tout d divisant n, soit G_d est vide, soit $|G_d| = \varphi(d)$. Finalement, dans tous les cas, $|G_d| \leq \varphi(d)$, donc

$$n = |G| = \sum_{d|n} |G_d| \leq \sum_{d|n} \varphi(d) = n\,,$$

ce qui assure que pour tout $d|n$, $|\varphi(d)| = \varphi(d)$, donc en particulier $|G_n| = \varphi(n) \geq 1$, donc G est cyclique. □

Poursuivons avec les propriétés de l'indicatrice d'Euler :

Corollaire 3.23. *La fonction indicatrice d'Euler est multiplicative, au sens suivant : si $m, n \in \mathbf{N}$ sont deux entiers premiers entre eux, alors $\varphi(mn) = \varphi(m)\varphi(n)$.*

Démonstration. Le lemme chinois assure que l'on a un isomorphisme d'anneaux $\mathbf{Z}/mn\mathbf{Z} \xrightarrow{\sim} \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$, donc un isomorphisme de groupes d'inversibles $(\mathbf{Z}/mn\mathbf{Z})^\times \xrightarrow{\sim} (\mathbf{Z}/m\mathbf{Z})^\times \times (\mathbf{Z}/n\mathbf{Z})^\times$. Donc en calculant les cardinaux, $\varphi(mn) = \varphi(m)\varphi(n)$. □

En particulier, pour connaître la fonction φ, il suffit de connaître $\varphi(p^k)$, pour $k \geq 1$ et p premier.

Corollaire 3.24. — *Pour tout p premier et $k \geq 1$, $\varphi(p^k) = p^{k-1}(p-1)$.*

— *pour tout $n \geq 1$, si $n = \prod_{i=1}^{r} p_i^{k_i}$ est la décomposition de n en facteurs premiers, alors*

$$\varphi(n) = \prod_{i=1}^{r} p_i^{k_i - 1}(p_i - 1)\,,$$

ou autrement dit

$$\frac{\varphi(n)}{n} = \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)\,.$$

Démonstration. Il suffit de compter les entiers premiers à p entre 1 et p^k (ce qui revient à calculer le nombre de multiples de p) pour calculer $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. □

Plus précisément, on peut montrer :

Théorème 3.25. *Soit p un nombre premier et $k \geq 1$. Alors on a les isomorphismes suivants :*

— *si $p \geq 3$, $(\mathbf{Z}/p^k\mathbf{Z})^\times \cong \mathbf{Z}/p^{k-1}(p-1)\mathbf{Z}$, i.e. $(\mathbf{Z}/p^k\mathbf{Z})^\times$ est cyclique d'ordre $p^{k-1}(p-1)$.*

— *si $p = 2$, $(\mathbf{Z}/2\mathbf{Z})^\times \cong \{1\}$, et si $k \geq 2$, $(\mathbf{Z}/2^k\mathbf{Z})^\times \cong \mathbf{Z}/2^{k-2}\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.*

Démonstration. Voir le livre de Perrin par exemple. □

3.3 Algorithme d'Euclide

Dans un anneau principal, cet énoncé est essentiellement théorique, puisque le calcul du pgcd et celui d'une relation de Bézout ne sont pas effectifs a priori (ce sont seulement des résultats d'existence, on ne dispose pas d'algorithme efficace ou évident pour faire ces calculs explicitement). Dans le cas d'un anneau euclidien, la situation est nettement meilleur d'un point de vue algorithmique.

Théorème 3.26 (Algorithme d'Euclide)**.** *Soit A un anneau euclidien et $(a, b) \in A^2$. L'algorithme suivant calcule un pgcd de a et b :*

1. *si $b = 0$, renvoyer a.*
2. *si $b \neq 0$, effectuer la division euclidienne de a par b, à savoir $a = bq + r$, et appliquer l'algorithme au couple (b, r).*

Démonstration. Évident. □

On peut également le formuler en terme de suite récurrente : on pose $r_0 := a$, $r_1 := b$, et pour tout $i \geq 1$, on écrit la division euclidienne de r_{i-1} par r_i : $r_{i-1} = r_i q_i + r_{i+1}$. L'algorithme s'arrête au premier entier n tel que $r_{n+1} = 0$, et le pgcd est r_n (le dernier reste non nul).

Théorème 3.27. *Si $\varphi(b) \leq \varphi(a)$, l'algorithme précédent calcule le pgcd de (a, b) en au plus $\varphi(b) + 1$ divisions euclidiennes dans A.*

Démonstration. C'est clair. □

Remarque 3.28. Dans $\mathbf{Z}$, un théorème plus précis dû à Lamé assure que si $b < F_{k+1}$, où (F_n) désigne la suite de Fibonacci, alors l'algorithme d'Euclide effectue au plus k divisions euclidiennes. Et c'est optimal car si $a = F_{k+2}$ et $b = F_{k+1}$, l'algorithme fait appel à exactement k divisions euclidiennes. On en déduit que l'algorithme d'Euclide pour deux entiers positifs (a, b) avec $a > b$ dans $\mathbf{Z}$, nécessite au maximum $\mathcal{O}(\log_\Phi(b))$ divisions euclidiennes, où Φ désigne le nombre d'or.

Théorème 3.29 (Algorithme d'Euclide étendu)**.** *Soit A un anneau euclidien et $(a, b) \in A^2$.*

L'algorithme suivant calcule un pgcd de a et b, ainsi qu'une relation de Bézout.

On pose $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$, $r_0 := a$, $r_1 := b$, et on définit par récurrence les suites (r_i), (q_i), (u_i) et (v_i) via

— *division euclidienne : $r_i = r_{i+1}q_{i+1} + r_{i+2}$.*

— *$u_{i+2} = u_i - q_{i+1}u_{i+1}$.*

— *$v_{i+2} = v_i - q_{i+1}v_{i+1}$.*

On s'arrête au premier entier n tel que $r_{n+1} = 0$. Alors une relation de Bézout est donnée par

$$au_n + bv_n = r_n\,.$$

Dans $\mathbf{Z}$ (resp. $K[X]$), cet algorithme fait au plus $\mathcal{O}(\log(b))$ (resp $\mathcal{O}(\deg b)$) appels récursifs.

Démonstration. Récurrence simple. □

3.4 Quotients d'anneaux principaux

Soit A un anneau principal. Nous avons vu plus haut que pour tout élément $p \in A$, on a l'équivalence entre "p est irréductible", "l'idéal (p) est premier", "l'idéal (p) est maximal", "$A/(p)$ est un corps".

L'exemple principal d'application de cette remarque est le suivant : si $P \in K[X]$ est un polynôme irréductible, le quotient $K[X]/(P)$ est un corps contenant K, et de dimension $\deg(P)$ comme K-espace vectoriel.

3.5 Factorisation en irréductibles

Proposition 3.30. *Soit A un anneau principal et K un ensemble non vide.*

Alors tout famille $(I_k)_{k\in K}$ d'idéaux de A admet un élément maximal.

Démonstration. On raisonne par l'absurde : supposons qu'un tel élément maximal n'existe pas. Il existe un idéal I_1 dans cette famille. Comme I_1 n'est pas maximal, il existe I_2 dans cette famille tel que $I_1 \subsetneqq I_2$. On poursuit et on construit par récurrence une suite infinie $I_k \subsetneqq I_{k+1}$ d'idéaux de A. On vérifie alors que $I := \bigcup_{k\geq 1} I_k$ est un idéal de A. Puisque A est principal, il existe $a \in I$ tel que $I = (a)$. Alors il existe $k \geq 1$ tel que $a \in I_k$, donc $I = (a) \subset I_k$, donc $I_{k+1} = I_k$, ce qui est contradictoire. □

Théorème 3.31. *Soit A un anneau principal. Pour tout $a \in A \setminus \{0\}$, il existe $u \in A^\times$ et $p_1, \ldots, p_n \in A$ irréductibles, tels que*

$$a = up_1 \ldots p_n\,.$$

De plus, cette décomposition est unique, à l'ordre près des facteurs et à multiplication près par des inversibles de A.

Démonstration. Montrons d'abord l'existence. Par l'absurde, si l'existence n'est pas vérifiée, l'ensemble E des éléments non nuls de A n'admettant pas de telle décomposition est non vide. Considérons la famille des idéaux (a), avec a décrivant E. Par la proposition précédente, cette famille admet un élément maximal (a_0) avec $a_O \in E$. En particulier, a_0 est non nul, non inversible, non irréductible, donc il existe une décomposition

$a_0 = b_0 c_0$, avec $b_0, c_0 \in A$ non inversibles. Puisque $(a_0) \subsetneq (b_0), (c_0)$, la maximalité de (a_0) assure que $b_0, c_0 \notin E$, donc b_0 et c_0 admettent une décomposition en irréductibles. En les concaténant, on voit donc que a_0 admet une décomposition en irréductibles, ce qui est contradictoire.

Montrons ensuite l'unicité, via le lemme d'Euclide : supposons que $up_1 \dots p_n = vq_1 \dots q_r$, avec des notations évidentes. Alors p_n divise $q_1 \dots q_r$, donc par le lemme d'Euclide, il existe i tel que p_n divise q_i. Quitte à permuter les q_j, on peut supposer que p_n divise q_r. Comme p_n et q_r sont irréductibles, ils sont associés. Donc $p_1 \dots p_{n-1}$ et $q_1 \dots q_{r-1}$ sont associés, et on conclut par récurrence sur le nombre de facteurs. □

Nous reviendrons plus tard (après l'algèbre linéaire) sur l'arithmétique des anneaux, avec notamment la notion d'anneau factoriel, puis celle d'extension de corps.