Algèbre linéaire MA122

Alexis Bouthier

Table des matières

Chapitre 1

Arithmétique de $\mathbb{Z}$ et des polynômes

1. Généralités sur les groupes

1.1. Groupes. Partant d'un ensemble, il s'agit de l'enrichir avec des structures supplémentaires, telles que des opérations.

Définition 1.1.1. Soit un ensemble E, une loi de composition interne (LCI) sur E est une fonction $* : E \times E \to E$. Cette loi est généralement notée entre deux éléments.

Exemple 1.1.2. Pour $(x, y) \in \mathbb{R}^2$, $(x, y) \mapsto x + y$ est une loi de composition interne. Si E est un ensemble non-vide et $\mathcal{P}(E)$ l'ensemble de ses parties, alors $(A, B) \mapsto A \cap B$ est une LCI sur $\mathcal{P}(E)$.

Définition 1.1.3. Soit $*$ une LCI sur E. On dit que $(E, *)$ est un monoïde si :

1. $\forall\ (x, y, z) \in E^3, (x * y) * z = x * (y * z)$ (Associativité).
2. $\exists\ e \in E, \forall\ x \in E, e * x = x * e = x$ (Existence d'un élément neutre).

Si pour toute paire $(x, y) \in E^2$, on a $x * y = y * x$, on dit que E est un monoïde commutatif ou abélien.

Remarque 1.1.4. L'utilité de l'associativité est qu'elle permet d'écrire $x * y * z$ sans se préoccuper du parenthésage. Toutes les lois de composition interne ne sont pas nécessairement associatives. La soustraction sur $\mathbb{R}$ est un exemple de loi non associative. $4 - (3 - 2) = 3 \neq (4 - 3) - 2 = -1$.

Exemple 1.1.5. $(\mathbb{N}, +)$ ou $(\mathbb{N}, \times)$ sont des monoïdes abéliens, $(M_n(\mathbb{R}), \times)$ est un monoïde non-commutatif.

Définition 1.1.6. Soit $*$ une LCI sur E. On dit que $(E, *)$ est un groupe si c'est un monoïde et qu'il vérifie :

$$\forall\ x \in E, \exists\ y \in E, xy = yx = e \text{(Existence d'un inverse).}$$

C'est un groupe abélien si de plus $(E, *)$ est un monoïde abélien.

Exemple 1.1.7. $(\mathbb{Z}, +)$ est un groupe abélien, $(GL_n(\mathbb{R}), \times)$ est un groupe non-commutatif.

Lemme 1.1.8. *Soit $(E, *)$ un ensemble avec une LCI, si elle admet un élément neutre, alors il est unique. De plus, si $(E, *)$ est un groupe, alors il y a unicité de l'inverse.*

Démonstration. En effet, si e et e' sont deux éléments neutres, on a $e * e' = e$ et $e * e' = e'$. Pour la deuxième assertion, soit $x \in E$, supposons qu'il admette deux inverses $y, y' \in E$. On a alors :

$$y = y(xy') = y'.$$

□

Ainsi, si $(E, *)$ est un groupe, pour tout $x \in E$, il résulte du lemme que l'on peut définir x^{-1}, l'inverse de x. On note immédiatement que pour toute paire $(x, y) \in E^2$:

$$(x * y)^{-1} = y^{-1} * x^{-1}$$

Dans la suite, on note la LCI de manière multiplicative, sauf mention explicite et l'élément neutre 1. Pour $n \in \mathbb{N}^*$, si l'on multiplie n fois x, on note x^n. Attention, en général :

$$(xy)^n \neq x^n y^n.$$

C'est vrai seulement si la loi est commutative (pensez aux matrices). En effet, on a :

$$x^2y^2 = xxyy \text{ et } (xy)^2 = xyxy.$$

1.2. Sous-groupes. On se donne dans la suite $(G, .)$ un groupe.

Définition 1.2.1. Une partie non-vide H de G est un sous- groupe si :

$$\forall\ (x, y) \in H^2, xy^{-1} \in H.$$

Remarques.

1.2.2. On remarque que comme H est non-vide, on a automatiquement $1 \in H$. En effet, il suffit de choisir $x \in H$ et par hypothèse, on a $1 = x.x^{-1} \in H$.

1.2.3. Dans les applications, pour montrer que quelque chose est un groupe, il est souvent plus commode de montrer que c'est un sous-groupe d'un groupe de « référence ».

Exemple 1.2.4. $(\mathbb{Q}^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$, $\mathbb{U}_n := \{z \in \mathbb{C} \mid z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

1.3. Morphismes de groupes. Soient $(A, .)$ et $(B, .)$ deux groupes.

Un morphisme de groupes est une fonction entre groupes $f : A \to B$ telle que :

$$f(1_A) = 1_B, f(xy) = f(x)f(y).$$

Remarque 1.3.1. On a automatiquement $f(x)f(x^{-1}) = f(xx^{-1}) = 1$ soit $f(x^{-1}) = f(x)^{-1}$.

Exemple 1.3.2. $z \mapsto |z|$ de $(\mathbb{C}^*, .) \to (\mathbb{R}^*, .)$ ou $x \mapsto e^x$ de $(\mathbb{R}, +)$ sur $(\mathbb{R}^*, .)$ sont des morphismes de groupes.

Vocabulaire usuel sur les morphismes :

Définition 1.3.3. Soit $f : G \to H$, un morphisme de groupes. On dit que :

1. f est un *endomorphisme* si $G = H$.
2. f est un *isomorphisme* si c'est un morphisme de groupes bijectif.
3. f est un *automorphisme* si c'est un endomorphisme bijectif.

Exemples.

1.3.4. $x \mapsto x^2$ est un endomorphisme de groupes de $(\mathbb{R}^*, \times)$.

1.3.5. $x \mapsto e^x$ est une bijection de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$. On dit que ces groupes sont isomorphes.

aut-int

Exemple 1.3.6. Pour un groupe G et $x \in G$, $\phi_x : G \to G$ donné par $y \mapsto xyx^{-1}$ est un automorphisme de G. On appelle un tel automorphisme, un automorphisme intérieur. Si $x = 1$, on obtient l'automorphisme identité Id_G donné par $y \mapsto y$.

Exemple 1.3.7. Soit G un groupe, alors l'ensemble $\mathrm{Aut}(G)$ des automorphismes de G avec la composition des applications comme LCI est un groupe.

Démonstration. La loi de composition est clairement associative et pour tout $\sigma \in \mathrm{Aut}(G)$, on a $\mathrm{Id}_G \circ \sigma = \sigma \circ \mathrm{Id}_G = \sigma$. De plus comme σ est bijective, soit σ^{-1} son inverse, alors on a bien $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{Id}$. Il suffit donc de vérifier que σ^{-1} est aussi un morphisme de groupes. On a $\sigma(1) = 1$ donc $\sigma^{-1}(1) = 1$. Soit $(x, y) \in G^2$, alors $\sigma(\sigma^{-1}(x)\sigma^{-1}(y)) = \sigma(\sigma^{-1}(x))\sigma(\sigma^{-1}(y)) = xy = \sigma(\sigma^{-1}(xy))$, soit $\sigma^{-1}(x)\sigma^{-1}(y) = \sigma^{-1}(xy)$ par injectivité de σ. □

1.4. Image et noyau d'un morphisme. Soit $\phi : G \to H$ un morphisme de groupes.

Lemme 1.4.1. *Soient $G' \subset G$, $H' \subset H$ des sous-groupes, alors $\phi(G')$ et $\phi^{-1}(H')$ sont aussi des sous-groupes.*

Démonstration. $e \in G'$ comme G' est un sous-groupe et $\phi(e) = e' \in \phi(G')$. De plus, $\phi(x)\phi(y)^{-1} = \phi(xy^{-1})$ et $xy^{-1} \in G'$ donc $\phi(G')$ est un sous-groupe. On a l'équivalence :

$$x \in \phi^{-1}(H') \iff \phi(x) \in H'.$$

Comme $\phi(1) = 1 \in H'$, $1 \in \phi^{-1}(H')$. Si $x, y \in \phi^{-1}(H')$, alors $\phi(x)\phi(y)^{-1} \in H'$. Or $\phi(x)\phi(y)^{-1} = \phi(xy^{-1})$, donc on obtient $xy^{-1} \in \phi^{-1}(H')$, ce qui conclut. □

Définition 1.4.2. **1.** On définit l'image de ϕ, notée $\operatorname{Im}\phi$ par le sous-groupe $\phi(G) \subset H$. On a $\operatorname{Im}\phi = H$ si et seulement si ϕ est surjective.

2. On définit le noyau de ϕ, noté $\operatorname{Ker}\phi$, par le sous-groupe $\phi^{-1}(\{e\}) \subset G$.

Exemple 1.4.3.

$\phi : \mathbb{C} \to \mathbb{R}$, donné par $z \mapsto \operatorname{Re}(z)$ est surjectif, donc $\operatorname{Im}\phi = \mathbb{R}$. De plus, $\operatorname{Ker}\phi = i\mathbb{R}$.

$\phi : (\mathbb{R}, +) \to (\mathbb{U}, \times)$, donné par $x \mapsto e^{ix}$ est surjectif de noyau $2\pi\mathbb{Z}$.

Proposition 1.4.6. *Soit $\phi : G \to H$ un morphisme de groupes. Alors, ϕ est injectif si et seulement si* $\operatorname{Ker}\phi = \{1\}$.

Démonstration. Sens direct : soit $x \in G$ tel que $\phi(x) = 1$ alors $\phi(x) = \phi(1)$ et $x = 1$.

Sens réciproque : Si pour $(x, x') \in G^2$, on a $\phi(x) = \phi(x')$, alors $\phi(x)\phi(x')^{-1} = 1$, d'où $\phi(xx'^{-1}) = 1$. Comme $\operatorname{Ker}\phi = \{1\}$, on obtient $xx'^{-1} = 1$ et $x = x'$. □

Proposition 1.4.7. *Soit $\phi : G \to H$ un morphisme de groupes finis de même cardinal, alors on a l'équivalence :*

$$\phi \text{ injective} \iff \phi \text{ surjective} \iff \phi \text{ bijective.}$$

Démonstration. On montre (1) $\implies$ (2) $\implies$ (3) $\implies$ (1). Si ϕ est injective, $\operatorname{card}(G) = \operatorname{card}(\phi(G)) = \operatorname{card}(H)$ donc $\phi(G) = H$ et ϕ est surjective. Si ϕ est surjective, alors $\phi(G) = H$ et si ϕ n'est pas injective, on aurait $\operatorname{card}(H) = \operatorname{card}\phi(G) < \operatorname{card} G$, donc ϕ est injective donc bijective. La dernière assertion est triviale. □

fin **Lemme 1.4.8.** *Soit G un groupe fini, alors pour tout $x \in G$, il existe $n \in \mathbb{N}^*$, $x^n = 1$.*

Démonstration. En effet si tel n'est pas le cas alors on obtiendrait un morphisme de groupes injectif :

$$\mathbb{Z} \to G$$

donné par $k \mapsto x^k$. Or, G est fini, contradiction. □

1.5. Anneaux.

Définition 1.5.1. Soit $(A, +, .)$ un ensemble muni de deux LCI, on dit que A est un anneau si :

1. $(A, +)$ est un groupe abélien.

2. $(A, .)$ est un monoïde.

3. $\forall\ (x, y, z) \in A^3$, on a $x.(y + z) = x.y + x.z$ et $(x + y).z = x.z + y.z$ (distributivité) .

Enfin, A est un anneau commutatif, si $(A, .)$ est un monoïde commutatif.

Exemple 1.5.2. $(\mathbb{Z}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs, $(M_n(\mathbb{R}), +, \times)$ est un anneau non-commutatif. Si A et A' sont deux anneaux alors le produit direct de $A \times A'$ est aussi un anneau en faisant les opérations composantes par composantes. Pour un anneau A, on a l'anneau des polynômes à coefficients dans A :

$$A[X] = \{\sum_{d=0}^{n} a_d X^d, n \in \mathbb{N}, a_i \in A\},$$

avec l'addition et la multiplication habituelle des polynômes. Plus généralement on dispose de l'anneau $A[X_1, \ldots, X_r]$ en r indéterminées, qui consiste en les expressions de la forme $\sum_{\underline{i} \in \mathbb{N}^r} a_{\underline{i}} X_1^{i_1} \ldots X_r^{i_r}$ avec les $a_{\underline{i}}$ presque tous nuls. On vérifie en développant que

$$(A[X])[Y] = A[X, Y] = A[Y][X],$$

(admis ou laissé en exercice).

Définition 1.5.3. Un sous-anneau B de A vérifie :

— $(B, +)$ est un sous-groupe de $(A, +)$.

— $(B, \times)$ est un sous-monoïde de $(A, \times)$.

1.6. Groupes des inversibles et Corps. Soit un anneau $(A, +, \times)$. Tout élément $x \in A$ n'est pas nécessairement inversible.

inv-ring **Lemme 1.6.1.** *Soit $(A^\times, \times)$ l'ensemble des éléments inversibles pour $\times$, alors c'est un groupe. On l'appelle le groupe des inversibles.*

Démonstration. $(A^\times, \times)$ est un sous-monoïde de $(A, \times)$ et par définition tout élément est inversible. □

Exemple 1.6.2. $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q}^*$.

Définition 1.6.3. Soit un anneau A, on dit que c'est un corps s'il est non-réduit à $\{0\}$ et si tout élément non-nul est inversible. Un sous-corps est un sous-anneau qui est un corps.

Remarque 1.6.4. Dans ce cours, on ne considèrera que des corps commutatifs, i.e. tels que A soit un anneau commutatif.

Exemple 1.6.5. Les ensembles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps.

1.7. Espaces vectoriels. On rappelle la définition suivante.

Définition 1.7.1. Soit $\mathbb{K}$ un corps. On appelle $\mathbb{K}$-espace vectoriel un ensemble E, muni d'une LCI + telle que :

(i) $(E, +)$ est un groupe abélien.

(ii) Il existe une application $. : \mathbb{K} \times E \to E$, appelée loi externe telle que :

(a) $\forall\ x \in E, 1.x = x.$

(b) $\forall\ (\lambda, \mu) \in \mathbb{K}^2, x \in E, (\lambda.\mu).x = \lambda.(\mu.x).$

(c) $\forall\ (\lambda, \mu) \in \mathbb{K}^2, (x, y) \in E^2, (\lambda + \mu).(x + y) = \lambda.x + \mu.x + \lambda.y + \mu.y.$

Remarques.

1.7.2. Nous n'allons pas refaire toutes les définitions qui sont déjà connues. On a surtout rappelé celle-ci pour bien mettre l'accent que l'on travaille avec $\mathbb{K}$ un corps arbitraire et pas seulement $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1.7.3. Ces données peuvent être rassemblées en une seule. Si l'on note $\mathrm{End}(E)$ l'anneau des endomorphismes de groupes abéliens de E, muni de l'adddition et de la composition des endomorphismes, alors la donnée d'une structure de $\mathbb{K}$-espace vectoriel revient à la donnée d'un morphisme d'anneaux $\phi : A \to \mathrm{End}(M)$, donné par $a \mapsto \phi_a$ où $\phi_a : E \to E$ est donnée par $x \mapsto a.x$.

On a ensuite les notions usuelles de sous-epaces vectoriels, morphisme d'espaces vectoriels, qui sont précisément les applications linéaires, et de noyau et d'image d'applications linéaires.

1.8. Morphismes d'anneaux et de corps. Un morphisme d'anneaux est une fonction entre anneaux $f : A \to B$ telle que :

— $f : (A, +) \to (B, +)$ est un morphisme de groupes.

— $f : (A, \times) \to (B, \times)$ est un morphisme de monoïdes.

Un morphisme de corps est un morphisme d'anneaux entre corps.

Exemple 1.8.1. Le morphisme $\mathrm{ev} : \mathcal{F}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ donné par $f \mapsto f(0)$ est un morphisme d'anneaux. La conjugaison complexe $(\bar{-}) : \mathbb{C} \to \mathbb{C}$ est un automorphisme de coprs, i.e. un morphisme de corps bijectif.

Définition 1.8.2. (i) Soit $\phi : A \to B$ un morphisme d'anneaux, on définit le noyau et l'image de ϕ :

$$\mathrm{Ker}(\phi) = \phi^{-1}(0), \quad \mathrm{Im}(\phi) = \phi(A) \subset B.$$

(ii) Soit un anneau A, $(I, +) \subset (A, +)$ un sous-groupe abélien, on dit que I est un idéal si pour tout $a \in A$, on a $aI = \{ax, x \in I\} \subset I$.

Remarques.

1.8.5. Si I est un idéal et $1 \in I$, alors $I = A$, car $a = a.1$ pour $a \in A$.

1.8.6. Si $a \in A$, $aA = \{ax, x \in A\}$ est idéal de A. On le note (a).

Définition 1.8.7. Un anneau est dit principal s'il est intègre et tout idéal $I \subset A$ est de la forme $I = (a)$ pour $a \in A$. On verra que $\mathbb{Z}$ et $\mathbb{K}[X]$ pour $\mathbb{K}$ un corps sont aussi principaux (cf. 2.1.2, 4.2.1).

Remarque 1.8.8. Un corps $\mathbb{K}$ est principal. En effet, si $I \neq 0$, alors soit $x \in I$ non-nul, alors $1 = xx^{-1} \in I$, donc $I = A$.

Lemme 1.8.9. *Soit $\phi : A \to B$ un morphisme d'anneaux, alors* $\mathrm{Ker}(\phi)$ *est un idéal et* $\mathrm{Im}(\phi)$ *est un sous-anneau.*

Démonstration. Comme ϕ est un morphisme de groupes abéliens, alors $\mathrm{Ker}(\phi)$ est un sous-groupe abélien et de plus si $a \in A$, $x \in \mathrm{Ker}(\phi)$, on a $\phi(ax) = \phi(a)\phi(x) = 0$, donc $ax \in \mathrm{Ker}(\phi)$ et $\mathrm{Ker}(\phi)$ un idéal. Pour la deuxième assertion, on sait déjà que $(\mathrm{Im}(\phi), +)$ est un sous-groupe abélien et $(\mathrm{Im}(\phi), \times)$ est un sous-monoïde, donc $\mathrm{Im}(\phi)$ est un sous-anneau. □

root **Exemple 1.8.10.** Soit $\mathbb{K}$ un corps, $\phi : \mathbb{K}[X] \to \mathbb{K}$ donné par $P \mapsto P(0)$, alors $\mathrm{Ker}(\phi) = (X)$. En effet, on a clairement $(X) \subset \mathbb{K}[X]$. De plus, si $P(0) = 0$, alors en écrivant $P = \sum a_i X^i$, si $P(0) = 0$, alors $a_0 = 0$ et $X | P$.

1.9. Anneaux quotients. Soit un anneau commutatif A, $I \subset A$ un idéal, on considère la relation de congruence modulo I :

$$a = b \mod I \iff a - b \in I.$$

quot1 **Proposition 1.9.1.** *La relation de congruence modulo I est une relation d'équivalence. On note A/I l'ensemble des classes d'équivalence, il admet une structure d'anneau donnée par :*

$$\bar{a} + \bar{b} = \overline{a+b} \mod I, \bar{a}.\bar{b} = \overline{ab} \mod I,$$

telle que la projection $p : A \to A/I$ est un morphisme d'anneaux de noyau $\mathrm{Ker}(p) = I$.

Démonstration. La symétrie et la réflexivité sont évidentes, pour la transitivité si $a = b \mod I$ et $b = c \mod I$, alors $c - a = (c - b) + (b - a) \in I$. Passons à la structure d'anneau, il faut s'assurer que la définition ne dépend pas du choix du représentant, soit si :

$$a = a' \mod I, b = b' \mod I, \quad \text{alors} \quad a + b = a' + b' \mod I, ab = a'b' \mod I.$$

On a donc $(a - a'), (b - b') \in I$ d'où comme $(I, +)$ est un groupe abélien :

$$(a + b) - (a' + b') \in I, \quad \text{soit} \quad a + b = a' + b' \mod I.$$

De plus, comme I est un idéal :

$$ab - a'b' = a(b - b') + b'(a - a') \in I, \quad \text{soit} \quad ab = a'b' \mod I.$$

On obtient donc que le produit et la somme sont bien définis et on vérifie immédiatement à partir des propriétés d'anneau de A que A/I l'est aussi et que :

$$p : A \to A/I$$

est un morphisme d'anneaux. De plus si $x = 0 \mod I$, alors $x \in I$, donc $\mathrm{Ker}(p) = I$. □

Les deux exemples fondamentaux pour la suite de ce cours d'anneaux quotients sont les suivants :

Exemple 1.9.2. $n\mathbb{Z} \subset \mathbb{Z}$ est un idéal et on note $\mathbb{Z}/n\mathbb{Z}$ l'anneau quotient. Dans ce cas la relation de congruence modulo I se récrit comme :

$$a = b\ [n] \Longleftrightarrow n|b - a.$$

Le deuxième vient des polynômes :

Exemple 1.9.3. Soit un anneau A, $P \in A[X]$ et $I = (P)$, alors on peut former l'anneau quotient $A[X]/(P)$. La relation de congruence est donnée par :

$$R = Q \mod (P), \quad \text{si} \quad P|R - Q.$$

Un cas particulièrement intéressant est pour construire les complexes, sur lequel on reviendra plus tard quand on étudiera les polynômes :

$$\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$$

donnée par $P \mapsto P(i)$. (On peut également prendre le membre de gauche comme la construction des nombres complexes.)

uquot **Proposition 1.9.4** (Propriété universelle du quotient)**.** *Soit $\phi : A \to B$ un morphisme d'anneaux tel que $I \subset \mathrm{Ker}(\phi)$, alors il existe une unique application $\bar{\phi} : A/I \to B$ telle que $\phi = \bar{\phi} \circ p$ avec $p : A \twoheadrightarrow A/I$.*

Démonstration. En effet si $\bar{x} \in A/I$, on choisit $x \in A$ qui relève et on pose

$$\bar{\phi}(\bar{x}) = \phi(x).$$

Il s'agit de voir que cela ne dépend pas du choix du relèvement, or si $x' \in A$ est un autre relèvement, alors $x - x' \in I$ de telle sorte que :

$$\phi(x) = \phi(x' + (x - x')) = \phi(x'),$$

puisque que $I \subset \mathrm{Ker}(\phi)$. Le fait que $\bar{\phi}$ soit un morphisme d'anneaux se déduit alors de la définition de l'addition et du produit sur A/I et du fait que ϕ est un morphisme. □

2. Arithmétique de $\mathbb{Z}$

2.1. Sous-groupes de $\mathbb{Z}$.

eucl **Proposition 2.1.1.** *[Division euclidienne] Soit $(a, b) \in \mathbb{N} \times \mathbb{N}^\times$, alors il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que :*

$$a = bq + r$$

avec $r < b$.

Démonstration. **Unicité :**

Si $bq + r = bq' + r'$, alors $b(q - q') = r - r'$, or $0 \leqslant r, r' \leqslant b - 1$ d'où :

$$-(b-1) \leqslant r - r' \leqslant b - 1$$

et $b|(r - r')$ donc $r - r' = 0$ et $r = r'$.

Existence : Par récurrence sur a, b étant fixé. Si $a = 0$ et $a = 0.b$. Sinon par récurrence, on a $a = bq + r$ avec $r \leqslant b - 1$, soit $a + 1 = bq + r + 1$. Si $r + 1 < b$, on prend le couple $(q, r + 1)$, sinon $r + 1 = b$ et on a alors $a + 1 = b(q + 1)$, donc $(q + 1, 0)$ marche. □

sgZ **Proposition 2.1.2.** *Soit G un sous-groupe de $(\mathbb{Z}, +)$, alors il existe un unique élément $n \in \mathbb{N}$ tel que $G = n\mathbb{Z}$. Ce sont également les idéaux de $\mathbb{Z}$. En particulier, $\mathbb{Z}$ est principal.*

Démonstration. Si $G = \{0\}$, c'est clair. Sinon, soit $n = \min(G \cap \mathbb{N}^*)$. Le minimum est bien défini car, soit $x \in G\backslash\{0\}$ qui est non-vide par hypothèse alors comme G est un groupe $\{x, -x\} \in G$, de telle sorte que $G \cap \mathbb{N}^*$ est non-vide donc admet un plus petit élément. Comme G est un groupe, on a clairement $n\mathbb{Z} \subset G$, montrons la réciproque. Soit $x \in G$, à nouveau quitte à changer x en $-x$, on peut supposer que $x \in \mathbb{N}$ et on effectue la division euclidienne 2.1.1 de x par n, il existe donc un couple (q, r) tel que :

$$x = bn + r, 0 \leqslant r < n, \quad \text{soit} \quad r = x - bn \in G \cap \mathbb{N}$$

et donc par minimalité de n, $r = 0$ et $G = n\mathbb{Z}$.

Montrons l'unicité. Si $n\mathbb{Z} = m\mathbb{Z}$ avec $n, m \neq 0$, alors $n = km$ et $m = ln$ avec $k, l \in \mathbb{N}^*$, soit $n = kln$ d'où $kl = 1$ et $k = l = 1$. Comme les $n\mathbb{Z}$ sont clairement des idéaux, on en déduit que tous les idéaux de $\mathbb{Z}$ sont de cette forme puisque qu'en particulier les idéaux sont des sous-groupes abéliens. □

2.2. PGCD.

Lemme 2.2.1. *Soient $a, b \in \mathbb{Z}$, alors $a\mathbb{Z} + b\mathbb{Z} = \{ak + bl, k, l \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$, il existe donc un unique $m \in \mathbb{N}$ tel que :*

$$a\mathbb{Z} + b\mathbb{Z} = m\mathbb{Z}.$$

On dit que m est le pgcd de a et b, noté $a \wedge b$.

Démonstration. En vertu de sgZ 2.1.2, il suffit de montrer que $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. On remarque alors que c'est l'image du morphisme de groupes :

$$\mathbb{Z}^2 \to \mathbb{Z}$$

donné par $(x, y) \mapsto ax + by$. □

Remarque 2.2.2. On notera que même si a et b sont des entiers relatifs, le pgcd est toujours un entier positif.

gcd2 **Lemme 2.2.3.** *Soient $a, b \in \mathbb{N}$, on note $d = a \wedge b$.*

1. *On a $d|a$ et $d|b$.*
2. *Il existe un couple $(u, v) \in \mathbb{Z}^2$ tel que $d = au + bv$. On appelle une telle relation, une relation de Bezout.*
3. *Si $m|a$ et $m|b$, alors $m|d$.*
4. *$\lambda a \wedge \lambda b = |\lambda| d$.*

Démonstration. (i) On a $a, b \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donc il existe $k, l \in \mathbb{Z}$ tels que $a = kd$ et $b = ld$.

(ii) On a $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, d'où l'existence de $(u, v) \in \mathbb{Z}^2$ tel que $d = au + bv$.

(iii) Si $d = au + bv$ est une relation de Bezout, si $m|a$, $m|b$, alors $m|au + bv = d$ et $m|d$. Ce qui justifie l'appelation de plus grand diviseur commun.

(iv) $\lambda a\mathbb{Z} + \lambda b\mathbb{Z} = |\lambda|(a\mathbb{Z} + b\mathbb{Z}) = |\lambda| d\mathbb{Z}$ et on conclut par unicité du pgcd. □

2.3. Entiers premiers entre eux.

Définition 2.3.1. On dit que $a, b \in \mathbb{N}$ sont premiers entre eux si $a \wedge b = 1$.

Théorème 2.3.2. (i) *Si $a|bc$ et $a \wedge b = 1$, alors $a|c$ (Lemme de Gauss).*

(ii) *Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge bc = 1$.*

Démonstration. (i) On écrit une relation de Bezout, $au + bv = 1$, soit $auc + bvc = c$ et donc comme $a|bc$, on trouve $a|c$.

(ii) On écrit deux relations de Bezout, $au + bv = 1$ et $aw + ct = 1$, on a alors :

$$(au + bv)(aw + ct) = a(u(aw + ct) + bvw) + bc(tv) = 1.$$

□

Corollaire 2.3.5. *Si $a \wedge b = 1$, alors $a^m \wedge b^n = 1$ pour tout $m, n \in \mathbb{N}$.*

2.4. Algorithme d'Euclide.

Lemme 2.4.1 (Lemme d'Euclide)**.** *On a $a \wedge (b + \lambda a) = a \wedge b$.*

Démonstration. On a $a\mathbb{Z} + (b + \lambda a)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} + \lambda a\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. □

Application : On se sert du lemme d'Euclide pour calculer le pgcd, sans avoir à connaître les facteurs premiers de a et b, ce qui peut être difficile à déterminer pour des grands nombres.

En changeant a en $-a$, on peut supposer $a, b \geqslant 0$.

— Si $b = 0$, alors $a \wedge b = a$.

— Si $b \neq 0$, on fait la division euclidienne de a par b et on a $a = bq + r_0$ avec $r_0 \leqslant b-1$ et $a \wedge b = (bq + r_0) \wedge b = r_0 \wedge b$. On fait alors la division euclidienne de b par r_0 et on trouve $b = q_1 r_0 + r_1$. En itérant, on a donc une suite d'entiers strictement décroissante (r_k) jusqu'à trouver un n tel que $r_n = 0$ et on a alors :

$$a \wedge b = r_{n-2} \wedge r_{n-1} = r_{n-1},$$

où la dernière égalité vient du fait que $r_n = 0$.

Exemple 2.4.2. On a $155 \wedge 4 = (4.38 + 1) \wedge 4 = 1 \wedge 4 = 1$.

Application pour calculer une relation de Bezout : Calculons $153 \wedge 35$, on a alors :

$$153 = 4.35 + 13, 35 = 2.13 + 9, 13 = 9 + 4, 9 = 2.4 + 1.$$

Ici c'est plus rapide d'utiliser la décomposition en nombres premiers pour trouver le pgcd, mais on va voir que c'est tout de même commode pour trouver une relation de Bezout. Pour trouver une relation de Bezout, il suffit de « remonter » l'algorithme d'Euclide. On écrit alors :

$$13 = 153 - 4.35, 9 = 35 - 2.13 = 35 - 2.(153 - 4.35) = 9.35 - 2.153,$$
$$4 = 13 - 9 = (153 - 4.35) - (9.35 - 2.153) = 3 * 153 - 2.35,$$
$$1 = 9 - 2.4 = (9.35 - 2.153) - 2.(3 * 153 - 2.35) = 13.35 - 8.153.$$

2.5. Nombres premiers.

Définition 2.5.1. Un entier $p \in \mathbb{N}^*$ est premier s'il admet exactement deux diviseurs, 1 et lui-même.

Remarque 2.5.2. En particulier, 1 n'est pas premier.

prime

Lemme 2.5.3. *Soit p premier, soit r non-divisible par p, alors $r \wedge p = 1$. En particulier, pour tout $d \in [\![1, p-1]\!]$, $d \wedge p = 1$ et si $r \wedge p \neq 1$, on a $p|r$.*

Démonstration. Soit $d = r \wedge p$, alors $d|p$, donc $d = 1$ ou $d = p$. Si $d = p$, alors comme $d|r$, r serait un multiple de p, ce qui n'est pas, donc $d = 1$. □

Théorème 2.5.4 (Euclide)**.** *Il y a une infinité de nombres premiers.*

Démonstration. Par l'absurde, s'il y en a un nombre fini $p_1, \ldots, p_n$, soit $N = p_1 \ldots p_n + 1$, alors N ne peut être premier, il est donc divisible par un des p_i, mais cela forcerait alors par définition de N, $p_i|1$, une contradiction. □

On note $\mathcal{P}$ l'ensemble des nombres premiers.

decomp **Théorème 2.5.5.** *[Décomposition en nombres premiers] On a :*

$$\forall\ n \in \mathbb{N}^*, \exists!(\alpha_p)_{p\in\mathcal{P}}, n = \prod_{p\in\mathcal{P}} p^{\alpha_p},$$

où la famille (α_p) est nulle sauf pour une nombre fini de premiers.

Démonstration. Montrons l'existence par récurrence sur n. Si $n = 1$, on prend $(\alpha_p) = 0$. Supposons le résultat vrai pour tout $k \leqslant n$, montrons le résultat pour $n+1$. Si $n+1$ est premier, il n'y a rien à montrer, sinon $n+1 = ab$ avec $a, b \leqslant n$. On écrit alors :

$$a = \prod_{p\in\mathcal{P}} p^{a_p}, b = \prod_{p\in\mathcal{P}} p^{b_p}, \quad \text{soit} \quad n+1 = \prod_{p\in\mathcal{P}} p^{a_p+b_p}.$$

Pour l'unicité, on a :

$$\prod_{p\in\mathcal{P}} p^{a_p} = \prod_{p\in\mathcal{P}} p^{b_p}.$$

Soit $p_0 \in \mathcal{P}$, par symétrie, on peut supposer que $a_{p_0} \leqslant b_{p_0}$ et on divise par $p^{a_{p_0}}$, on obtient :

$$G := \prod_{p\neq p_0\in\mathcal{P}} p^{a_p} = p_0^{b_{p_0}-a_{p_0}}\Big(\prod_{p\neq p_0\in\mathcal{P}} p^{b_p}\Big),$$

Si $p \neq p_0$, on a $p \wedge p_0 = 1$, soit $p_0 \wedge G = 1$ donc $a_{p_0} = b_{p_0}$ et l'unicité en découle. □

Remarque 2.5.6. Pour $n \in \mathbb{N}^*$ et un premier p, on note alors $v_p(n)$ la puissance maximale de p qui divise n, on l'appelle la valuation p-adique.

p-ad **Proposition 2.5.7.** (i) *On a $v_p(ab) = v_p(a) + v_p(b)$.*

(ii) *On a $a|b \iff \forall\ p \in \mathcal{P}, v_p(a) \leqslant v_p(b)$.*

(iii) *Si $c = a \wedge b$, alors $c = \prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$*

Démonstration. (i) On a :

$$a = \prod_{p\in\mathcal{P}} p^{v_p(a)}, b = \prod_{p\in\mathcal{P}} p^{v_p(b)},$$

il suffit alors de multiplier et d'identifier les valuations p-adiques par unicité.

(ii) Si $b = ac$, alors pour tout $p \in \mathcal{P}$, $v_p(b) = v_p(a) + v_p(c)$ ce qui donne le sens direct. Pour la réciproque, on a :

$$b = a \times \prod_{p\in\mathcal{P}} p^{v_p(b)-v_p(a)}.$$

(iii) Soit $D = \prod_{p\in\mathcal{P}} p^{\min(v_p(a),v_p(b))}$, par construction, on a $D|a$ et $D|b$ donc $D|c$. Réciproquement si $c|a, b$ alors $v_p(c) \leqslant v_p(a), v_p(b)$, ce qui conclut. □

Définition 2.5.11. Pour $a, b \in \mathbb{N}$, on définit le plus petit commun multiple par :

$$ppcm(a,b) = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}.$$

ppcm2 **Proposition 2.5.12.** *Soient $a, b \in \mathbb{N}$, on a :*

(i) $(a \wedge b) ppcm(a,b) = ab$. *En particulier, si $a \wedge b = 1$, on a $ppcm(a,b) = ab$.*

(ii) *Si $m|a$, $n|a$, alors $ppcm(m,n)|a$.*

Démonstration. (i) est immédiat à partir de p-ad 2.5.7(iii) et du fait que

$$\forall\ p \in \mathcal{P}, \min(v_p(a), v_p(b)) + \max(v_p(a), v_p(b)) = v_p(a) + v_p(b).$$

(ii) Les deux conditions et p-ad 2.5.7(ii) donnent que pour tout $p \in \mathcal{P}$, $v_p(m), v_p(n) \leqslant v_p(a)$ et en passant au max, on en déduit que $ppcm(m,n)|a$. □

3. Les anneaux $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$, rappelons que a et b sont congrus modulo n si :

$$a = b\ [n] \iff n|b-a.$$

On a vu que $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif.

cong **Lemme 3.0.1.** *On a* $\text{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

Démonstration. On a une application :

$$\phi : \{0, \dots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$$

donnée par $k \mapsto \bar{k}$, la classe d'équivalence correspondante. Montrons que c'est une bijection. Si $\bar{k} = \bar{m}$, alors $n|m-k$ et on a :

$$-(n-1) \leqslant m-k \leqslant n-1, \quad \text{soit} \quad k = m.$$

Montrons la surjectivité, si $x \in \mathbb{N}$, on écrit la division euclidienne par n, soit $x = bn + r$ avec $0 \leqslant r < n$, soit $x = r\ [n]$. Enfin, si $x \in \mathbb{Z}_{<0}$, alors l'argument ci-dessus donne que $x = -r\ [n]$ avec $0 \leqslant r < n$ et on a alors :

$$x = n - r\ [n], \quad \text{et} \quad n - r \in [\![0, n-1]\!].$$

□

Exemple 3.0.2. $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\} = \{2\bar{5}0, 2\bar{5}1\}$.

3.1. Quand $\mathbb{Z}/n\mathbb{Z}$ est-il un corps ?

Définition 3.1.1. Un anneau est intègre si pour tout $x, y \in A$ non-nuls, on a $xy \neq 0$.

Exemple 3.1.2. (i) Un corps est un anneau intègre.

(ii) $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre, car $2.3 = 0$ [6].

pfiel **Proposition 3.1.5.** *Soit $n \in \mathbb{N}^*$, les assertions suivantes sont équivalentes :*

(i) *$\mathbb{Z}/n\mathbb{Z}$ est un corps.*

(ii) *$\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.*

(iii) *n est premier.*

Démonstration. $(i) \Longrightarrow (ii)$ est clair. Montrons $(ii) \Longrightarrow (iii)$ par contraposée si n non premier, alors $n = dr$ avec $0 < d, r < n$ et donc $dr = 0$ $[n]$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. Il reste $(iii) \Longrightarrow (i)$, soit $0 < r < n$, comme n est premier, alors $r \wedge n = 1$ par 2.5.3 prime, on écrit alors une relation de Bezout $ru + dn = 1$ et en réduisant modulo n, on trouve :

$$ru = 1 \ [n]$$

et r est inversible donc $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

3.2. Arithmétique et congruences.

On note $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

3.2.1. *Le petit théorème de Fermat.*

fermat **Théorème 3.2.2.** *Soit $x \in \mathbb{F}_p$, alors $x^p = x$ $[p]$.*

Démonstration. On procède par récurrence sur $k \in \mathbb{N}$, si $k = 0, 1$, c'est clair.

Montrons donc que :

$$(k+1)^p = k^p + 1 \ [p],$$

puisque par induction, on aura $k^p = k$ $[p]$. On applique alors le binôme de Newton pour obtenir :

$$(k+1)^p = \sum_{k=0}^{p} \binom{p}{k} k^l = k^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} k^l.$$

Pour conclure, il suffit d'établir le lemme suivant :

Lemme 3.2.3. *Pour tout $1 \leqslant k \leqslant p-1$, on a $p | \binom{p}{k}$.*

Démonstration. On a :

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\dots(p-k+1)}{k!},$$

soit $k!\binom{p}{k} = p(p-1)\dots(p-k+1) = 0\ [p]$, or $p \wedge k! = 1$, donc inversible modulo p et on trouve :

$$\binom{p}{k} = 0\ [p],$$

comme souhaité. □

□

3.2.4. *Théorème des restes chinois.*

Théorème 3.2.5. *Soient $m, n \in \mathbb{N}$ tels que $m \wedge n = 1$, alors l'application canonique :*

$$\phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

est un isomorphisme d'anneaux.

Démonstration. On a un morphisme d'anneaux $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ qui envoie $mn\mathbb{Z}$ sur 0 donc induit par passage au quotient un morphisme :

$$\phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Comme la source et le but ont même cardinal, il suffit de montrer l'injectivité, soit identifier $\mathrm{Ker}(\phi)$. Soit $x \in \mathrm{Ker}(\phi)$, alors $x = 0\ [n]$ et $x = 0\ [m]$, donc $m|x$ et $n|x$ et comme m et n sont premiers entre eux alors par lppcm2 2.5.12 $mn|x$ et $x = 0\ [mn]$ et ϕ injective. □

3.2.6. *Application : Groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.*

phid **Proposition 3.2.7.** *Soit $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff x \wedge n = 1$.*

Démonstration. On a :

$$x \wedge n = 1 \iff \exists (k,l) \in \mathbb{Z}^2, kx + ln = 1 \iff \bar{x} \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

□

On pose alors $\phi(n) := \mathrm{card}((\mathbb{Z}/n\mathbb{Z})^\times)$, on appelle la fonction $\phi : \mathbb{N} \to \mathbb{N}$ la fonction d'Euler.

phic **Proposition 3.2.8.** *Si $m \wedge n = 1$, alors $\phi(mn) = \phi(m)\phi(n)$. De plus, si p est premier et $k \in \mathbb{N}^*$, $\phi(p^k) = p^k - p^{k-1}$.*

Démonstration. Pour la première assertion, il suffit de passer aux inversibles dans le théorème des restes chinois et on obtient :

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

Calculons $\phi(p^k)$, il resulte de phid 3.2.7 que :

$$\phi(n) = \{k \in [\![0, n-1]\!], k \wedge n = 1\}.$$

Calculons le complémentaire de $(\mathbb{Z}/n\mathbb{Z})^\times$; pour $n = p^a$, dans ce cas si $k \wedge p^k \neq 1$, comme p est premier, on a $p|k$ par 2.5.3, en particulier le complémentaire consiste en les multiples de p dans $\mathbb{Z}/p^a\mathbb{Z}$, il y en p^{a-1} donc en passant au complémentaire, on obtient :

$$\phi(p^a) = p^a - p^{a-1}.$$

□

Corollaire 3.2.9. *Pour tout $n \in \mathbb{N}^*$, on a :*

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

Démonstration. En effet, on écrit $n = \prod_{p|n} p^{v_p(n)}$. La proposition précédente donne alors :

$$\phi(n) = \prod_{p|n} \phi(p^{v_p(n)}) = \prod_{p|n} p^{v_p(n)}(1 - \frac{1}{p}) = n \prod_{p|n} (1 - \frac{1}{p}).$$

□

Voyons un application au problème dit « de Sunzi » qui remonte à l'époque des Six Dynasties (220-589) en Chine.

Exemple 3.2.10. Supposons qu'on ait un nombre inconnus d'objets. S'ils sont comptés par 3, il en reste 2, s'ils sont comptés par 5, il en reste 3 et par 7, il en reste 2. Combien y-a-t-il d'objets au minimum ?

Il s'agit de chercher le plus petit n tel que $n = 2\ [3], n = 3\ [5], n = 2\ [7]$.

On se ramène à deux équations. On cherche d'abord une relation de Bezout entre 3 et 5 soit :

$$1 = 3a + 5b, \quad \text{soit} \quad 3a = 1\ [5], 5b = 1\ [3], \tag{3.2.10.1}$$

{beZ}

et on multiplie par les résidus respectifs modulo 5 et 3 pour se ramener à une équation modulo 15 par le théorème des restes chinois, soit 3.(3a)+2.(5b) modulo 15. Notez qu'en utilisant (3.2.10.1) :

$$3.(3a) + 2.(5b) = 3\ [5] \quad \text{et} \quad 3.(3a) + 2.(5b) = 2\ [3].$$

Ici on a par exemple $a = 2$, $c = -1$, d'où l'on se ramène à :

$$n = 18 - 10 = 8\ [15].$$

Maintenant on utilise l'équation $n = 2\ [7]$, une relation de Bezout est :

$$1 = 15c + 7d = 15.1 - 7.2$$

et on obtient $n = 2.15 - 8.14\ [105] = 23\ [105]$. Le plus tel entier est donc $n = 23$!.

On a la généralisation suivante du théorème de Fermat

Théorème 3.2.11. *Pour tout $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, on a $x^{\phi(n)} = 1\ [n]$. Si n est premier, on retrouve le petit théorème de Fermat via 3.2.8.*

DÉMONSTRATION. Soit $R = \{x_1, \ldots, x_{\phi(n)}\}$ un système de représentants de $(\mathbb{Z}/n\mathbb{Z})^\times$, Soit $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, alors la multiplication $x \mapsto ax$ est une bijection de $(\mathbb{Z}/n\mathbb{Z})^\times$, on a donc :

$$\prod_{i=1}^{\phi(n)} x_i = \prod_{i=1}^{\phi(n)} ax_i = a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i\ [n],$$

soit en simplifiant comme les x_i sont inversibles :

$$a^{\phi(n)} = 1\ [n].$$

□