Structures Algébriques - 3MA262

2025-2026

Pierre-Vincent Koseleff

29 janvier 2026

Table des matières

Introduction

Le but de ce cours est de proposer une première approche des structures algébriques de base. On se concentrera sur le cas commutatif, même si parfois nous aborderons des notions plus générales.
Le fil rouge sera la structure quotient. Nous commençons par décrire l'anneau euclidien $\mathbf{Z}$. Les sous-groupes de $\mathbf{Z}$, qui sont dans ce cas également des idéaux, sont monogènes. Les quotients $\mathbf{Z}/n\mathbf{Z}$ sont les premiers exemples de groupe quotient et d'anneau quotient. Ce sont aussi les modèles de groupes cycliques. L'anneau $\mathbf{Z}/p\mathbf{Z}$ est un corps si et seulement si p est un nombre premier. Nous abordons dans cette partie l'algorithme d'Euclide et quelques applications.
Lorsque H est un sous-groupe de G, l'ensemble G/H est un groupe lorsque H est distingué dans G, ce qui

est le cas lorsque G est abélien. Nous abordons les théorèmes d'isomorphisme, outil essentiel pour étudier la structure des groupes.
Nous abordons également la notion d'anneau (commutatif), et en particulier les notions d'anneaux factoriels, principaux et euclidiens. Nous démontrons les théorèmes d'isomorphisme, en particulier, le théorème chinois.
Lorsque K est un corps, l'anneau $K[X]$ est naturellement un anneau euclidien. L'algèbre $K[X]/(P)$ est un corps lorsque P est irréductible. De cette manière, nous construisons des corps finis comme des extensions algébriques de $\mathbf{Z}/p\mathbf{Z}$ et nous examinons plus généralement les extensions finies des corps finis $\mathbf{Z}/p\mathbf{Z}$ ou du corps $\mathbf{Q}$ des nombres rationnels.
Les lecteurs intéressés pourront lire avec intérêt les parties abordées dans ce cours et également traitées dans les ouvrages suivants (liste non exhaustive) : [1, 3, 5].

1 Espace quotient

Nous présentons tout d'abord la notion d'espace obtenu par passage au quotient. Des espaces aussi usuels que l'anneau $\mathbf{Z}/n\mathbf{Z}$, les espaces L^p, le groupe $\mathbf{R}/2\pi\mathbf{Z}$, le corps $\mathbf{C} \simeq \mathbf{R}[X]/(X^2+1)$, par exemple, reposent sur cette construction.

1.1 Quotient

Les deux notions importantes, indispensables à la manipulation des quotients, sont la *surjection canonique* et la *propriété universelle*.

Relation d'équivalence

Soit E un ensemble.

Définition 1.1. *Une relation d'équivalence $\mathscr{R}$ sur un ensemble* E *est une relation binaire sur* E *qui est à la fois* réflexive*,* symétrique *et* transitive*.*

On dit que $\mathscr{R}$ est réflexive si pour tout x de E, on a $x\mathscr{R}x$. On dit que $\mathscr{R}$ est symétrique si pour tous x, y de E, on a $x\mathscr{R}y$ si et seulement si $y\mathscr{R}x$. On dit que $\mathscr{R}$ est transitive si pour tout x, y, z de E, on a

$$\Big[(x\mathscr{R}y)\text{et}(y\mathscr{R}z)\Big] \Longrightarrow (x\mathscr{R}z).$$

Exemple 1.2. *Dans E un espace vectoriel normé, on peut définir la relation $x\mathscr{R}y \Leftrightarrow \|x\| = \|y\|$.*
Si $f \in \mathrm{F}^{\mathrm{E}}$ est une application de E *vers* F*, on peut définir $x\mathscr{R}y : f(x) = f(y)$. Deux éléments de E sont équivalents si ils ont la même image par f. C'est le cas dans l'exemple précédent.*
Dans l'anneau $\mathbf{Z}$, on peut définir $a \sim b \Leftrightarrow a = \pm b$.
Dans l'ensemble $\mathbf{N}\times\mathbf{N}$, on définit $(a,b) \sim (c,d) \Leftrightarrow a+d = b+c$.
Dans l'ensemble $\mathbf{Z}\times\mathbf{Z}^*$, on définit $(a,b) \sim (a',b') \Leftrightarrow ab' = a'b$.
Dans l'ensemble $\mathbf{R}^{n+1} - \{0\}$, on définit $x \sim y$ par $\exists\lambda \neq 0; x = \lambda y$.

Définition 1.3. *Si $\mathscr{R}$ est une relation d'équivalence, la* classe d'équivalence *(pour la relation $\mathscr{R}$) de a, notée $\pi(a)$ ou $\overline{a}$, ou* $\mathrm{cl}\,(a)$ *est*

$$\pi(a) = \{x \in \mathrm{E} \mid x\mathscr{R}a\}.$$

La classe d'équivalence $\pi(a)$ de a contient toujours a. $\pi(a) = \pi(b)$ si et seulement si $b \in \pi(a)$. Les classes d'équivalence de E (pour la relation d'équivalence $\mathscr{R}$) forment donc une partition de E.

Les deux outils fondamentaux pour étudier les espaces quotients sont

1. la surjection canonique, pour la manipulation des éléments du quotient,
2. la propriété universelle, pour créer des applications partant d'un quotient.

Surjection canonique

On note $\mathrm{E}/\mathscr{R}$, l'ensemble quotient de E par $\mathscr{R}$, c'est l'ensemble des classes d'équivalence de E, c'est un sous-ensemble de $\mathscr{P}(\mathrm{E})$. On dispose à présent de l'application (surjective)

$$\pi : \begin{cases} \mathrm{E} \longrightarrow \mathrm{E}/\mathscr{R} \\ x \longmapsto \pi(x) \end{cases}.$$

On peut voir ainsi les classes d'équivalence comme les pré-images des éléments de $\mathrm{E}/\mathscr{R}$ par la *surjection canonique* π. Réciproquement, si $f \in \mathrm{F}^{\mathrm{E}}$ est une application de E vers F, alors la relation

$$x \sim y \Leftrightarrow f(x) = f(y)$$

est une relation d'équivalence. Ainsi $f^{-}(\{x\}) = \{y \in A \mid f(x) = f(y)\}$ est la classe d'équivalence de x.
On obtient ainsi une partition de E

$$\mathrm{E} = \underset{y \in F}{\cup} f^{-}(\{y\}).$$

Ainsi, lorsque E est un ensemble fini, on obtient

$$|E| = \sum_{y \in F} |f^{-}(\{y\})|.$$

Corollaire 1.4. *Soit f une application de de E vers F, ensembles finis.*

1. *Si f est injective, alors $|E| \leq |F|$.*
2. *Si f est surjective, alors $|E| \leq |F|$.*
3. *Si f est bijective, alors $|E| = |F|$.*

Mieux encore, on obtient le lemme des bergers, très utile en dénombrement

Lemme 1.5 (Lemme des bergers)**.** *Soit E et F des ensembles finis et $f \in F^E$.*
Si pour tout $y \in F$, $|\{x \in E \mid f(x) = y\}| = m$, alors $|E| = m \cdot |F|$.

Applications en dénombrement

On déduit du lemme des bergers précédent (1.5) de nombreux résultats de dénombrement.
Disons tout de suite que deux ensembles A et B sont de même cardinal si et seulement si il existe une bijection entre A et B. C'est une relation d'équivalence entre ensembles. A et B sont de même cardinal fini n si et seulement si A et B sont en bijection avec $[\![1,n]\!] = \{i \in \mathbf{Z} \mid 1 \leq i \leq n\}$. Si u et v sont des bijections, $u \in \mathrm{Bij}(A, A')$ et $v \in \mathrm{Bij}(B, B')$ alors B^A et $B'^{A'}$ sont en bijection par l'application :

$$\begin{array}{ccc} B^A & \to & B'^{A'} \\ f & \mapsto & v \circ f \circ u^{-1}. \end{array}$$

Ainsi, le nombre d'applications (resp. injectives, surjectives, bijectives) de A vers B est égal au nombre d'applications (resp. injectives, surjectives, bijectives) de $[\![1,n]\!]$ vers $[\![1,m]\!]$.

Nombre d'applications. Le nombre d'applications de $[\![1,n]\!]$ vers $[\![1,m]\!]$ est égal à m^n : c'est le nombre de m-uplets d'éléments de $[\![1,m]\!]$. En effet, à toute application f de $[\![1,n]\!]$ vers $[\![1,m]\!]$, on peut associer de façon unique le n-upplet $(f(1),\ldots,f(n))$ de $[\![1,m]\!]^n$.

Nombre d'injections. Soit $I(n,m)$ l'ensemble des injections $[\![1,n]\!]$ vers $[\![1,m]\!]$. Considérons l'application φ_n de $I(n,m)$ vers $I(n-1,m)$, qui à une injection f associe $\varphi_n(f) = g = f_{|[\![1,n-1]\!]}$.
On voit alors que $\varphi_n^{-}(\{g\})$ est l'ensemble des injections f, qui vérifie $f(1) = g(1), \ldots, f(n-1) = g(n-1)$ et $f(n) \in [\![1,m]\!] - \{g([\![1,n-1]\!])\}$. Il y a donc une bijection entre $\varphi_n^{-}(\{g\})$ et $[\![1,m]\!] - \{g([\![1,n-1]\!])\}$.
On a donc, en vertu du lemme des bergers (1.5), $I(n,m) = I(n-1,m) \cdot (m-n+1)$, lorsque $m \geq n$ et $I(n,m) = 0$ lorsque $m < n$. On conclut alors que $|I(n,m)| = m(m-1)\cdots(m-n+1) = \dfrac{m!}{(m-n)!}$.

Nombre de bijections. On conclut aussi que le nombre de bijections de $I(n,n)$ est $n!$.

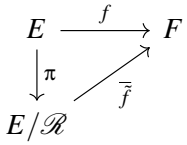
Nombre de parties. À toute injection $f \in I(k,n)$, on associe la partie (à k éléments) $f([\![1,k]\!]) \in \mathcal{P}_k([\![1,n]\!])$. Le nombre d'injections ayant même ensemble d'arrivée $A \in \mathcal{P}_k([\![1,n]\!])$ est précisément le nombre de bijections entre $[\![1,k]\!]$ et A, c'est-à-dire, $k!$. Ainsi $|\mathcal{P}_k([\![1,n]\!])| = \binom{n}{k}$. Le nombre de parties à k éléments de $[\![1,n]\!]$ est donc $\binom{n}{k}$.

1.2 Propriété universelle

La *propriété universelle* (appelée aussi *propriété de factorisation*) est l'outil fondamental pour créer des applications partant d'un quotient.

Théorème 1.6 (Propriété de factorisation)**.** *Soit* E *et* F *deux ensembles, $\mathscr{R}$ une relation d'équivalence sur* E *et* $f : \mathrm{E} \to \mathrm{F}$ *une application. Si f est compatible avec $\mathscr{R}$ (c'est-à-dire $x\mathscr{R}y \Longrightarrow f(x) = f(y)$), alors il existe une unique application $\tilde{f} : \mathrm{E}/\mathscr{R} \to \mathrm{F}$ vérifiant $\tilde{f} \circ \pi = f$.*

Cette propriété se résume sur le diagramme commutatif suivant, typique du passage au quotient :



On définit alors l'image par $\tilde{f}$ d'un élément de $\mathrm{E}/\mathscr{R}$ comme la valeur commune prise par f sur tous les éléments de cette classe d'équivalence. Notons que f et $\tilde{f}$ ont même ensemble image.

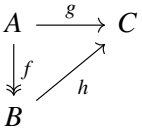
Corollaire 1.7. *$\tilde{f}$ est une application injective, si et seulement si $x\mathscr{R}y \Leftrightarrow f(x) = f(y)$. Dans ce cas là, $\tilde{f}$ est une une bijection entre $f(E)$ et $E/\mathscr{R}$.*

La relation d'équivalence $x \sim y : f(x) = f(y)$ vérifie que $x\mathscr{R}y \Longrightarrow x \sim y$. On dit que $\mathscr{R}$ est *plus fine* que $\sim$. En particulier il existe une application canonique entre $E/\mathscr{R}$ et $E/\sim$, lui-même en bijection avec $f(E)$.

C'est un cas particulier de la propriété de factorisation :

Proposition 1.8 (Factorisation d'une application)**.** *Soit $f : A \to B$ surjective et $g : A \to C$. Supposons que $f(x) = f(x) \Longrightarrow g(x) = g(y)$, alors il existe une unique application $h : B \to C$ telle que $g = h \circ f$.*

Cette propriété se conçoit avec le diagramme



Preuve. Si h existe, alors nécessairement pour tout $z = f(x)$, on doit avoir $h(z) = g(x)$. Cette application est bien définie car f est surjective et si $z = f(x) = f(x')$ alors $g(x) = g(x')$, ne dépend que de z. C'est la seule façon de définir h et la fonction ainsi définie vérifie bien $g = h \circ f$. CQFD

Le travail de construction est fait une fois pour toutes dans la démonstration de la propriété universelle.

Morphisme canonique

L'important pour effectuer des calculs dans le quotient est que la surjection canonique π soit un morphisme. Pour certaines relations d'équivalence sur E, il est impossible d'imposer à π d'être un morphisme. La relation d'équivalence doit en fait vérifier certaines conditions : les notions de sous-groupe distingué et d'idéal apparaissent.

Soit E un ensemble muni de lois (internes ou externes) et d'une relation d'équivalence $\mathscr{R}$. On souhaite construire sur $\mathrm{E}/\mathscr{R}$ autant de lois que sur E telles que la surjection canonique $\pi : \mathrm{E} \to \mathrm{E}/\mathscr{R}$ soit un morphisme. La relation d'équivalence doit pour cela être compatible avec les lois.

1. Si E est un groupe, les relations d'équivalence compatibles avec la loi de groupe sont de la forme $xy^{-1} \in \mathrm{H}$ avec H un sous-groupe distingué de E

2. Si E est un anneau, les relations d'équivalence compatibles avec les deux lois sont de la forme $x-y \in$ I avec I idéal de E.
3. Le cas des espaces vectoriels. Les relations sont de la forme $x-y \in$ F avec F sous-espace vectoriel de E.

Exemple : le tore

Soit $\mathscr{R}$ la relation d'équivalence définie sur $\mathbf{R}$, par

$$x\mathscr{R}y \Longleftrightarrow x-y \in 2\pi\mathbf{Z}.$$

Le quotient $\mathbf{R}/2\pi\mathbf{Z}$ se note $\mathbf{T}$ (tore). Soit f une application de $\mathbf{R}$ dans F et π la surjection canonique de $\mathbf{R}$ sur $\mathbf{T}$. f est compatible avec la relation $\mathscr{R}$ signifie que f est 2π-périodique. Dans ce cas, le théorème 1.6 établit qu'il existe une unique application $\tilde{f}:\mathbf{T}\to F$ telle que $\tilde{f}\circ\pi = f$. Ainsi, l'ensemble $\mathcal{F}(\mathbf{T},F)$ des applications issues du tore s'identifie à l'ensemble $\mathcal{F}_{2\pi}(\mathbf{R},F)$ des applications 2π-périodiques. Voir [7].
Le tore $\mathbf{T}$ est un groupe (c'est un sous-groupe de $\mathbf{R}$). On montrera, dans la partie 3.2, que la surjection canonique π, dans ce cas, est un morphisme de groupe Ainsi, par exemple la fonction exponentielle, tout morphisme de $(\mathbf{Z},+)$ dans $(\mathbf{C}^*,\times)$, 2π-périodique donnera lieu à un morphisme de $\mathbf{T}$ vers $\mathbf{C}^*$.
En revanche $2\pi\mathbf{Z}$ n'est pas un idéal de $\mathbf{R}$ et il n'existe pas de structure d'anneau sur $\mathbf{T}$ telle que π soit un morphisme d'anneau, voir la partie 4.1.

2 L'anneau des entiers relatifs

Nous rappelons ici quelques propriétés de l'anneau des entiers relatifs, certaines seront (re)démontrées ultérieurement. $(\mathbf{Z},+,\times)$ est un *anneau commutatif, unitaire et intègre*. C'est un anneau euclidien :

Théorème. Division euclidienne.
Soit $(a,b)\in\mathbf{Z}\times\mathbf{Z}^*$, il existe un couple unique $(q,r)\in\mathbf{Z}^2$ tel que

$$a = bq+r,\ \textit{avec}\ 0\le r<|b|;$$

r est le reste*, q est le* quotient *de la division euclidienne de a par b.*

Par exemple, on a $17 = 3\cdot 5+2$, $17 = -3\cdot -5+2$, $-17 = -4\cdot 5+3$, $-17 = 4\cdot -5+3$.
Si $a = bq$ et on dit que b *divise* a dans $\mathbf{Z}$ ou que b est un *diviseur* de a. On écrit $b|a$. On dit aussi que a est un *multiple* de b. Si $a = bq+r$ avec $0\le r<|b|$, on notera $r = a\,(\mathrm{mod}\,b)$ le reste de la division (on dit a modulo b) et on notera $q = a\div b$.
$\mathbf{Z}$ n'est pas un corps : les seuls éléments non nuls qui ont un inverse pour la multiplication sont $+1,-1$, i.e. $U(\mathbf{Z}) = \{-1,+1\}$.
Un diviseur de a distinct de 1, -1, a et $-a$ - s'il en existe - est appelé *diviseur propre* de a.
Un *nombre premier* p est un entier >1 dont les seuls diviseurs positifs sont 1 et p (autrement dit, un nombre premier n'a pas de diviseur propre). On notera $\mathcal{P}$ l'ensemble des nombres premiers.

Théorème fondamental de l'arithmétique - Tout entier relatif $n\in\mathbf{Z}^*$ s'écrit de manière unique sous la forme

$$n = \varepsilon\prod_{p\in\mathcal{P}} p^{n_p},\ \text{où}\ n_p\in\mathbf{N}^*,\ \varepsilon = \pm 1.$$

Ce dernier résultat a un inconvénient majeur : on ne connaît pas d'algorithme "rapide" pour factoriser un entier relatif. Cet inconvénient se révèle aussi un avantage, et il est à la base des méthodes de cryptographie à clé publique.

Définition. Soit A un anneau, on note $\mathcal{D}(a) = \{d\in A; d\mid n\}$, l'ensemble des diviseurs de a.

Le résultat suivant sert de point de départ à l'algorithme d'Euclide.

Lemme. *Pour tout $a,b \in A$ et tout $k \in A$, on a $\mathcal{D}(a)\cap\mathcal{D}(b) = \mathcal{D}(a-kb)\cap\mathcal{D}(b)$.*

Preuve. Si d divise a et b, alors $a = d\cdot a'$ et $b = d\cdot b'$ donc $a-kb = d(a'-b')$ et d est un multiple de d. Donc $\mathcal{D}(a)\cap\mathcal{D}(b) \subset \mathcal{D}(a-kb)\cap\mathcal{D}(b)$. Mais $\mathcal{D}(a-kb)\cap\mathcal{D}(b) \subset \mathcal{D}((a-kb)-(-kb))\cap\mathcal{D}(b) = \mathcal{D}(a)\cap\mathcal{D}(b)$. CQFD

On considère l'*algorithme d'Euclide* suivant, pour définir l'ensemble des diviseurs communs de a et b. Partons de $r_0 = a$, $r_1 = b$. On définit par récurrence $r_{i+1} = 0$ si $r_i = 0$, sinon $r_{i+1} = r_{i-1} \pmod{r_i}$.

Proposition 2.1. *La suite $(r_i)_{i\geq 2}$ est décroissante puis nulle.*

Preuve. Soit $r_2 = 0$ et l'algorithme s'arrête. Sinon, tant que $r_i > 0$ on a $r_i < r_{i-1} < r_2 - (i-2)$. On déduit que pour $i > r_2$, on a nécessairement $r_i = 0$. Soit n le plus grand indice tel que $r_n \neq 0$. La suite $(r_i)_{i\geq 2}$ est strictement décroissante pour $i \leq n+1$ puis nulle. CQFD

À chaque étape, on a $\mathcal{D}(r_i)\cap\mathcal{D}(r_{i+1}) = \mathcal{D}(r_{i-1})\cap\mathcal{D}(r_i)$, donc $\mathcal{D}(a)\cap\mathcal{D}(b) = \mathcal{D}(r_n)\cap\mathcal{D}(r_{n+1}) = \mathcal{D}(r_n)$.

$$\star^{\star}\star$$

Les diviseurs communs de a et de b sont donc exactement les diviseurs de r_n. On appelle $d = \mathrm{pgcd}(a,b) = r_n$ le pgcd de a et b.

Exemple 2.2. $\mathrm{pgcd}(415,175) = \mathrm{pgcd}(175,65) = \mathrm{pgcd}(65,45) = \mathrm{pgcd}(45,20) = \mathrm{pgcd}(20,5) = \mathrm{pgcd}(5,0) = 5$.

Proposition 2.3. *Soit a et b deux entiers non nuls tel que a ne divise pas b et réciproquement. Le plus grand commun diviseur (pgcd, gcd en anglais) de a et b est le dernier reste non nul de l'algorithme d'Euclide. On le note* $\mathrm{pgcd}(a,b)$ *ou* (a,b) *ou* $a\wedge b$. *On a donc $\mathcal{D}(a)\cap\mathcal{D}(b) = \mathcal{D}(d)$: tout diviseur commun de a et de b est un diviseur de d.*

$$(\delta|a \text{ et } \delta|b) \Longleftrightarrow \delta|d.$$

A priori le pgcd de a et de b n'est pas unique. Si d et d' vérifient $\mathcal{D}(d) = \mathcal{D}(d')$ alors il existe u inversible dans $\mathbf{Z}$, tel que $d = ud'$. Ici les inversibles de $\mathbf{Z}$ sont ± 1.

On peut borner le nombre d'étapes dans l'algorithme d'Euclide :

Théorème 2.4 (Théorème de Lamé)**.** *Considérons la suite de Fibonacci, définie par $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$. Soit a et b deux entiers naturels tels que $0 < b < a$. et $d = (a,b)$. Si l'algorithme d'Euclide s'arrête au bout de n pas, alors on a :*

$$a \geq dF_{n+2}, \quad b \geq dF_{n+1}.$$

Preuve. On raisonne par récurrence sur n. Si $n = 1$, alors $b|a$ et $b = d = dF_2$ et $a \geq b = dF_1$. Soit $n > 1$ et supposons que l'algorithme s'arrête au bout de $n+1$ pas. Appliquant la récurrence à $(b, r_2 = a - qb)$, on obtient $b \geq dF_{n+2}, r_2 \geq dF_{n+1}$. Mais $a = r_2 + qb \geq r_2 + b \geq d(F_{n+1} + F_{n+2}) = dF_{n+3}$. CQFD

Suite de Fibonacci

La suite de Fibonacci est une suite récurrente linéaire d'ordre 2. Elle vérifie l'équation (linéaire)

$$F_{n+2} = F_{n+1} + F_n, n \geq 0$$

dans $\mathbf{R}^{\mathbf{N}}$. D'après le cours de seconde année, l'ensemble des suites réelles vérifiant cette équation forme un sous-espace vectoriel de dimension 2. Une base de ce sous-espace est donnée par les suites géométriques $(r^n)_{n\geq 0}$ où r est solution de l'équation caractéristique : $r^2 = r+1$. On obtient le nombre d'or $r = \varphi = \frac{1}{2}(1+\sqrt{5})$ et $r = -\dfrac{1}{\varphi}$. On déduit ensuite que $F_n = \dfrac{1}{\sqrt{5}}\left(\varphi^n + (-\frac{1}{\varphi})^n\right)$. Remarquons enfin par récurrence que $\varphi^n = \varphi F_n + F_{n-1}$ pour tout n.

Corollaire 2.5. *Soit $0 \leq b < a$. L'algorithme d'Euclide calcule (a,b) en $n = \log_\varphi b + 1$ étapes.*

Preuve. On a $\varphi^{n+1} = \varphi F_{n+1} + F_n$ et $b \geq dF_{n+1} \geq F_{n+1}$ donc $n+1 = \log_\varphi(\varphi F_{n+1} + F_n) \leq \log_\varphi(\varphi F_{n+1} + F_{n+1}) = \log_\varphi(\varphi^2 F_{n+1}) \leq 2 + \log_\varphi b$. CQFD

On dira que l'algorithme d'Euclide a une *complexité arithmétique* $O(\log n)$, si $|a|, |b| \leq n$.

2.1 Identité de Bézout

Reprenons l'exemple précédent du calcul de $(415,175)$. En effectuant des opérations élémentaires sur les lignes $(L_0) : 415 = 1\cdot 415 + 0\cdot 175$ et $(L_1) : 175 = 0\cdot 415 + 1\cdot 175$, on obtient

$$\begin{array}{rrcrcr}
(L_0) & 415 & = & 1\cdot 415 & + & 0\cdot 175 \\
(L_1) & 175 & = & 0\cdot 415 & + & 1\cdot 175 \\
(L_2 = L_0 - 2L_1) & 65 & = & 1\cdot 415 & - & 2\cdot 175 \\
(L_3 = L_1 - 2L_2) & 45 & = & -2\cdot 415 & + & 5\cdot 175 \\
(L_4 = L_2 - 2L_3) & 20 & = & 3\cdot 415 & - & 7\cdot 175 \\
(L_5 = L_3 - 2L_4) & 5 & = & -8\cdot 415 & + & 19\cdot 175 \\
(L_6 = L_4 - 4L_5) & 0 & = & 35\cdot 415 & - & 83\cdot 175
\end{array}$$

Cet algorithme s'appelle *Algorithme d'Euclide étendu*. Il permet de démontrer :

Théorème 2.6 (Bézout)**.** *Soit $(a,b) \in \mathbf{Z}^2$, non nuls et $d = (a,b)$. Alors il existe $(u,v) \in \mathbf{Z}^2$, $au+bv = d$.*

Preuve. $r_0 = a$, $r_1 = b$, étant définis, on construit q_i et r_{i+1} comme le quotient et le reste de la division euclidienne de r_{i-1} par r_i : $r_{i+1} = r_{i-1} - q_i r_i$. En ayant posé $u_0 = 1$, $u_1 = 0$, $v_0 = 0$, $v_1 = 1$, on définit ensuite, $u_{i+1} = u_{i-1} - q_i u_i$ et $v_{i+1} = v_{i-1} - q_i v_i$. On a alors, par récurrence,

$$r_i = u_i a + v_i b, i = 0, \ldots, n+1.$$

En particulier $r_n = u_n a + v_n b, \quad r_{n+1} = 0 = u_{n+1} a + v_{n+1} b.$ CQFD

L'algorithme d'Euclide étendu fournit donc une identité de Bézout (rang n) et une solution de l'équation homogène $ax+by = 0$, dans $\mathbf{Z}^2$ (rang $n+1$).

Utilisant l'identité de Bézout, on déduit le lemme de Gauss.

Lemme 2.7 (Lemme de Gauss)**.** *Soit a, b et c trois entiers relatifs tels que a divise bc. Si $(a,b) = 1$ alors $a|c$.*

Preuve. On écrit $au+bv = 1$. On déduit que a divise $bc \times v$ donc $a \times uc + b \times vc = c$ CQFD

Corollaire 2.8. *Soit a, b deux entiers divisant c. Si $(a,b) = 1$ alors ab divise c.*

Preuve. Si $c = \lambda a = \mu b$ alors a divise μ d'après le Lemme de Gauss 2.7 et ab divise c. CQFD

Corollaire 2.9. *Soit a et b deux entiers. Alors pour tout entier k, on a $(k\cdot a, k\cdot b) = k\cdot(a,b)$. En particulier $a/(a,b)$ et $b/(a,b)$ sont premiers entre-eux (on dit étrangers).*

Preuve. Posons $d = (a,b) = au+bv$. Si δ divise ka et kb alors $ka = \delta a'$ et $kb = \delta b'$. Alors on obtient $kd = \delta(a'u+b'v)$ et $\delta \mid kd$. Réciproquement, si $\delta \mid kd$, alors δ divise ka et kb et donc (ka,kb). CQFD

On peut alors définir le ppcm de deux entiers.

Définition 2.10. *Soit a et b deux entiers, et d leur pgcd. $N = \dfrac{ab}{d}$ est le* ppcm(a,b). *On a*

$$(a|n \text{ et } b|n) \Longleftrightarrow (N|n)$$

Preuve. $N = \dfrac{a}{d}b = \dfrac{b}{d}a$ est un multiple commun de a et de b. Si a et b divisent simultanément n, alors a/d et b/d divisent n/d et, par conséquent (Lemme de Gauss 2.7) leur produit N/d divise n/d donc N divise n. L'ensemble des multiples communs de a et de b est l'ensemble des multiples de N. CQFD

2.2 Résolution de l'équation diophantienne linéaire : $ax+by = c$

Commençons par remarquer que

Théorème 2.11. *Soit a, b et c des entiers relatifs. L'équation $ax+by = c$ a (au moins) une solution si et seulement si $d = \text{pgcd}(a,b)|c$.*

Preuve. Si une solution particulière (x_0,y_0) existe, nous constatons que ax_0+by_0 est un multiple de d et donc d doit diviser c Réciproquement, si $c = \lambda d$ et (u,v) sont des coefficients de Bézout vérifiant $ua+vb = d$, alors $(x_0,y_0) = \lambda(u,v)$ est une solution particulière. CQFD

Comme pour toute équation affine, toute solution de l'équation $ax+by = c$ est la somme d'une solution particulière (x_0,y_0), si elle existe, et d'une solution de l'équation homogène : $ax+by = 0$.

Si (x,y) est solution de l'équation homogène $ax+by=0$ alors elle est aussi solution de $\frac{a}{d}x+\frac{b}{d}y=0$. Mais alors $\frac{a}{d}$ divise $\frac{b}{d}\cdot y$, donc $\frac{a}{d}$ divise y, d'après le corollaire du Lemme de Gauss 2.9. Donc $y=k\frac{a}{d}$ et par suite $(x,y)=k(-\frac{b}{d},\frac{a}{d})$ où $k\in\mathbf{Z}$.

Écriture matricielle dans l'algorithme d'Euclide

Posons $U_i=\begin{pmatrix}0 & 1\\ 1 & -q_i\end{pmatrix}$, on peut alors écrire

$$\begin{pmatrix} r_i & u_i & v_i\\ r_{i+1} & u_{i+1} & v_{i+1}\end{pmatrix}=U_i\begin{pmatrix} r_{i-1} & u_{i-1} & v_{i-1}\\ r_i & u_i & v_i\end{pmatrix}=U_i\cdot U_{i-1}\cdots U_1\cdot\begin{pmatrix} a & 1 & 0\\ b & 0 & 1\end{pmatrix}$$

On en déduit en particulier :

1. Dans l'algorithme d'Euclide étendu, on a à chaque étape $\begin{vmatrix} u_i & v_i\\ u_{i+1} & v_{i+1}\end{vmatrix}=(-1)^i$.
2. $u_{n+1}=\dfrac{b}{d}(-1)^{n+1}$, $v_{n+1}=\dfrac{a}{d}(-1)^n$.
3. $|u_n|\le\dfrac{b}{2d}$, $|v_n|\le\dfrac{a}{2d}$.

Preuve.

1. On a en effet $\begin{pmatrix} u_i & v_i\\ u_{i+1} & v_{i+1}\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & -q_i\end{pmatrix}\cdot\begin{pmatrix} u_{i-1} & v_{i-1}\\ u_i & v_i\end{pmatrix}$, d'où le résultat en considérant le déterminant.
2. On a aussi $\begin{vmatrix} r_{i-1} & u_{i-1}\\ r_i & u_i\end{vmatrix}=(-1)^{i-1}\begin{vmatrix} r_0 & u_0\\ r_1 & u_1\end{vmatrix}$, soit lorsque $i=n+1$: $du_{n+1}=(-1)^n\cdot(-b)$. On fait de même avec v_{n+1}.
3. De $u_{k+1}=u_{k-1}-q_ku_k$, on déduit que la suite u_k est de signe alterné, pour $k\ge1$, puis $|u_{k+1}|=|u_{k-1}|+|q_ku_k|>|u_k|$. Mais $q_n\neq1$ car $r_{n-1}=q_nr_n>r_n$ donc $q_n\ge2$ et $|u_n|\le\frac{1}{2}|u_{n+1}|$.

L'algorithme d'Euclide étendu fournit donc une identité de Bézout et une solution de l'équation homogène (dans $\mathbf{Z}^2$) : $ax+by=0$. Il est remarquable, que la solution obtenue par l'algorithme d'Euclide étendu engendre l'ensemble des solutions de l'équation homogène et que la solution particulière soit une solution particulière minimale (les coefficients u et v sont les plus petits possibles).

2.3 L'anneau quotient $\mathbf{Z}/n\mathbf{Z}$

Tout sous-groupe de $(\mathbf{Z},+)$, appelé aussi *idéal* de l'anneau $\mathbf{Z}$ (voire sous $\mathbf{Z}$-module de $\mathbf{Z}$), est de la forme $n\mathbf{Z}$, car $\mathbf{Z}$ est euclidien (voir aussi une démonstration dans l'exemple 3.5). On dit que $\mathbf{Z}$ est un anneau *principal*.

Exercice 2.12. *En terme d'idéaux, si a et b sont des entiers relatifs et d et N sont leur pgcd et leur ppcm, on a $a\mathbf{Z}\cap b\mathbf{Z}=N\mathbf{Z}$, $a\mathbf{Z}+b\mathbf{Z}=d\mathbf{Z}$.*

Soit $n>1$ un entier. Dans $\mathbf{Z}$, on définit la relation d'équivalence notée $\equiv$

$$(a,b)\in\mathbf{Z}^2, a\equiv b\iff b-a\in n\mathbf{Z}.$$

On note alors $a\equiv b\,(\mathrm{mod}\,n)$ et on dit que *a est congru à b modulo n*. Si $a\in\mathbf{Z}$, la classe de a pour la relation d'équivalence $\equiv$ est le sous-ensemble de $\mathbf{Z}$ suivant

$$\overline{a}=\{a+nk, k\in\mathbf{Z}\}=a+n\mathbf{Z}.$$

L'ensemble des classes d'équivalence est noté $\mathbf{Z}/n\mathbf{Z}$. L'ensemble $\mathbf{Z}/n\mathbf{Z}$ contient exactement n éléments distincts :

$$\mathbf{Z}/n\mathbf{Z}=\{\overline{0},\overline{1},\ldots,\overline{n-1}\}.$$

Par abus de notation on notera souvent de la même façon (quand il n'y a pas d'ambiguïté) un élément de $\mathbf{Z}$ et sa classe. Donc on pourra écrire

$$\mathbf{Z}/n\mathbf{Z}=\{0,1,\ldots,n-1\}.$$

On définit deux lois internes dans $\mathbf{Z}/n\mathbf{Z}$ (déduites de celles de $\mathbf{Z}$ et compatibles avec la relation d'équivalence $\equiv$) :

$$\overline{a}+\overline{b}:=\overline{a+b},\quad \overline{a}\times\overline{b}:=\overline{ab}.$$

Proposition 2.13. *$(\mathbf{Z}/n\mathbf{Z},+,\times)$ est un anneau commutatif unitaire.*

Groupe des inversibles

L'ensemble des inversibles de $\mathbf{Z}/n\mathbf{Z}$ forme un groupe multiplicatif. Par exemple, pour $n=8$. On remarque que si x est est pair alors $4\overline{x}=\overline{0}$. Ainsi si $\overline{x}$ était inversible, on aurait $\overline{x}\overline{x'}=\overline{1}$ et donc $\overline{4}=(4\overline{x})\cdot\overline{x'}=\overline{0}$ ce qui est impossible. Les inversibles de $\mathbf{Z}/8\mathbf{Z}$ sont donc impairs. On remarque que $(2k+1)(2k+1)\equiv 1\,(\mathrm{mod}\,8)$ ainsi tout élément impair de $\mathbf{Z}/8\mathbf{Z}$ est inversible et vérifie $x^2=1$.

Proposition 2.14. *L'ensemble $U(\mathbf{Z}/n\mathbf{Z})$ des inversibles de $\mathbf{Z}/n\mathbf{Z}$ est exactement l'ensemble des $i+n\mathbf{Z}$ tels que $(i,n)=1$.*

Preuve. $\overline{a}\in\mathbf{Z}/n\mathbf{Z}$ est inversible si et seulement si il existe $\overline{u}\in\mathbf{Z}/n\mathbf{Z}$ tel que $\overline{au}=1$. On obtient $au\equiv 1\,(\mathrm{mod}\,n)$, c'est-à-dire, qu'il existe $v\in\mathbf{Z}$ tel que $au-1=nv$. On déduit que $(a,n)=1$. La réciproque est immédiate.
CQFD

Cet ensemble est en bijection avec $\{1\leq i\leq n-1;(i,n)=1\}$. Le cardinal de $U(\mathbf{Z}/n\mathbf{Z})$ est noté $\varphi(n)$. La fonction $n\mapsto\varphi(n)$ est appelée *fonction caractéristique d'Euler*. En écrivant l'ensemble

$$\{\tfrac{1}{1},\ldots,\tfrac{n}{n}\}=\{\tfrac{a}{d};(a,d)=1,0<a<d|n\},$$

(voir [1]), on déduit la *formule d'Euler* :

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

Générateurs de $\mathbf{Z}/n\mathbf{Z}$

Le groupe $(\mathbf{Z}/n\mathbf{Z},+)$ est cyclique : il est engendré par $\overline{1}$. $U(\mathbf{Z}/n\mathbf{Z})$ est également l'ensemble des générateurs du groupe $(\mathbf{Z}/n\mathbf{Z},+)$. En effet, si $\overline{a}$ engendre $\mathbf{Z}/n\mathbf{Z}$ alors $\overline{1}=k\overline{a}=\overline{k\cdot a}$ et a est inversible modulo n, et d'ailleurs $\overline{k}$ est son inverse. L'identité de Bézout permet de déterminer si un entier m est inversible modulo n et le cas échéant de trouver son inverse.

Le corps $\mathbf{Z}/p\mathbf{Z}$

On remarque en particulier que $\mathbf{Z}/n\mathbf{Z}$ est un corps si et seulement si n est un nombre premier. Lorsque $n=p$ est un nombre premier, on note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

Théorème 2.15. *Pour tout a de $(\mathbf{Z}/n\mathbf{Z})^*$, on a $a^{\varphi}(n)=1$.*

Preuve. Considérons dans le groupe commutatif $G=(\mathbf{Z}/n\mathbf{Z})^*$, la translation $\tau_a : x\mapsto ax$. C'est une bijection d'inverse $\tau_{a^{-1}}$. Considérons le nombre $\alpha=\prod_{x\in(\mathbf{Z}/n\mathbf{Z})^*}x$. On a alors :

$$\alpha=\prod_{x\in(\mathbf{Z}/n\mathbf{Z})^*}x=\prod_{x\in(\mathbf{Z}/n\mathbf{Z})^*}ax=a^{\varphi(n)}\alpha.$$

Ainsi $a^{\varphi(n)}=1$. CQFD
On en déduit le

Théorème 2.16 (Théorème d'Euler)**.** *Soit n un entier naturel. Pour tout $a\in\mathbf{Z}$, si $(a,n)=1$ alors on a $a^{\varphi(n)}\equiv 1\,(\mathrm{mod}\,n)$.*

et le théorème de Fermat :

Corollaire 2.17 (Théorème de Fermat)**.** *Soit p un nombre premier. Pour tout $a\in\mathbf{Z}$, on a $a^p\equiv a\,(\mathrm{mod}\,p)$.*

Une conséquence du théorème de Fermat est que l'inverse de a dans $\mathbf{F}_p^*$ est a^{p-2}.

3 Rappels - Théorie des groupes

Nous rappelons ici quelques propriétés des groupes, en particulier des groupes finis commutatifs. Nous renvoyons à [5] ou [2]

Définition 3.1. *Soit G un ensemble et $*$ une loi de composition interne. $(G,*)$ est un groupe si et seulement si*

- *Il existe un élément neutre e dans G, tel que $g*e = e*g = g$, pour tout $g \in G$.*
- *Pour tout $a,b,c \in G$, on a $a*(b*c) = (a*b)*c$.* la loi est associative.
- *Pour tout $g \in G$, il existe $g' \in G$, tel que $g*g' = g'*g = e$.*
- *tout élément est inversible*

On note souvent la loi de composition par $+$ ou par $\cdot$, suivant qu'on préfère la notation additive ou multiplicative. Dans le cas de la notation additive, l'élément neutre est souvent noté 0, et l'inverse (on dira l'opposé), de g sera noté $-g$. Avec la notation multiplicative, on notera g^{-1}, l'inverse de g.

Lorsque la loi est commutative ($g*h = h*g$ pour tous $h,g \in G$), on dit que le groupe est *commutatif* ou *abélien*.

Remarque 3.2. *Le fait que la loi soit associative entraîne que l'élément neutre est unique. En effet si e et e' sont neutres, alors $e = e*e' = e'$. Si g' est un inverse (à gauche) et g'' un inverse à droite, alors on a $e = g'*g = g*g''$, donc $g'' = g'*(g*g'') = g'$.*

Exemple 3.3. *$(\mathbf{Z},+)$ est un groupe commutatif. $(\mathbf{Q},+)$, $(\mathbf{R},+)$, $(\mathbf{D},+)$, $(\mathbf{C},+)$ sont des groupes commutatifs. $(\mathbf{Q}^*,\cdot)$, $(\mathbf{R}^*,\cdot)$, $(\mathbf{C}^*,\cdot)$ sont des groupes commutatifs infinis.*
$\mathbf{U}_n = \{x \in \mathbf{C}^*, x^n = 1\}$ est un groupe commutatif abélien (c'est en fait un sous-groupe de $\mathbf{C}^*$).
$\mathrm{GL}_2(\mathbf{R})$ est un groupe non-commutatif. En effet les deux matrices de transvection $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ ne commutent pas.
Σ_3, le groupe des permutations de l'ensemble $\{1,2,3\}$ n'est pas commutatif. En effet, les deux transpositions (12) et (23) ne commutent pas, puisqu'on a $(12)(23) = (123)$ et $(23)(12) = (132) = (123)^2$.

Définition 3.4. *Une partie H de G est un sous-groupe de $(G,*)$ si $(H,*)$ est un groupe.*

Pour montrer que H est un sous-groupe de G, il suffit de montrer que H n'est pas vide (il doit contenir au moins l'élément neutre e) et que pour tous éléments a,b de H, on a $ab^{-1} \in H$.

Les sous-groupes $\{e\}$ et G sont appelés *sous-groupes triviaux* de G.

Exemple 3.5. *Si $n \in \mathbf{Z}$, $n\mathbf{Z}$ est un sous-groupe de $(\mathbf{Z},+)$. On montre également que tout sous-groupe de $(\mathbf{Z},+)$ est de cette forme. Soit $H \subset \mathbf{Z}$ un sous-groupe de $\mathbf{Z}$. Si $H \neq \{0\}$, alors $H^+ = H \cap \mathbf{Z}$ est une partie non vide de $\mathbf{N}^*$ donc admet un plus petit élément n. Si $m \in H$, écrivons $m = qn \cdot q + r$. Alors $q \cdot n \in \langle n \rangle = n\mathbf{Z} \subset H$ et donc $r = m - qn \in H$. Si $r \neq 0$ alors $0 < r < n$ ce qui contredit la minimalité de n dans H^+. Par conséquent $m \in n\mathbf{Z}$. On déduit donc que $H = n\mathbf{Z}$.*
Le groupe spécial linéaire $\mathrm{SL}_n(k)$ est un sous-groupe du groupe $(\mathrm{GL}_n(k),\cdot)$.
Si E est un k-espace vectoriel, alors $\mathrm{SL}(E)$ est un sous groupe de $(\mathrm{GL}(E),\circ)$
$\mathbf{U}_n = \{x \in \mathbf{C}, x^n = 1\}$ est un sous-groupe de $(\mathbf{C}^*,\cdot)$. $R^{+*} = \{x^2, x \in \mathbf{R}^*\}$ est un sous-groupe de $\mathbf{R}^*$. $\mathcal{A}_3 = \{\mathbb{1}, (123), (132)\} = \langle (123) \rangle$ est un sous-groupe de $(\Sigma_3,\circ)$.

Groupe engendré par une partie

Proposition 3.6. *Soit $(H_i)_{i\in I}$ une famille de sous-groupes de $(G,*)$. Alors $H = \bigcap_{i\in I}$ est un sous-groupe de G.*

Il ne faut pas croire que la réunion de deux sous-groupes soit un sous-groupe. Par exemple $3\mathbf{Z} \cup 5\mathbf{Z}$ ne contient pas $8 = 3+5$ donc n'est pas un sous-groupe de $\mathbf{Z}$.

Soit G un groupe et P une partie de G. Le *groupe engendré* par P, $\langle P \rangle$, est le plus petit sous-groupe de G contenant P. On a donc $\langle P \rangle = \bigcap_{P \subset H < G} H$.

Lorsque $P = \{g\} \subset G$, on obtient le groupe $\langle g \rangle = \{g^n, n \in \mathbf{Z}\}$. En effet, $\langle g \rangle$ contient g donc tous les g^n, $n \in \mathbf{Z}$. L'ensemble $H = \{g^n, n \in \mathbf{Z}\}$, contient l'élément neutre et si $a = g^n$ et $b = g^m$ alors $ab^{-1} = g^{n-m} \in H$. Ainsi H est un sous-groupe contenant g donc contient $\langle g \rangle$.

Considérons l'application $\Phi : \mathbf{Z} \mapsto \langle g \rangle, k \mapsto g^k$. Φ est surjective. Lorsque $\langle g \rangle$ est fini, Φ n'est pas injective et il existe $k > l$, tels que $g^k = g^l$, donc $g^{k-l} = e_G$. Ainsi $H = \{k \in \mathbf{Z}, g^k = e^G\}$ est un sous-groupe de $\mathbf{Z}$, différent de $\{0\}$ et il existe $n \in \mathbf{N}^*$, tel que $H = n\mathbf{Z}$. n est le plus petit entier naturel non nul tel que $g^n = e_G$. n est appelé l'*ordre* de g.

Examinons la relation d'équivalence $(k\mathscr{R}l \Leftrightarrow g^k = g^l)$, alors $\overline{k} = k + n\mathbf{Z}$. Ainsi l'ensemble quotient $\mathbf{Z}/\mathscr{R}$ est exactement $\mathbf{Z}/n\mathbf{Z}$ et est en bijection avec $\langle g \rangle$, d'après le corollaire 1.7.
Lorsque $\langle g \rangle$ est infini, on dira que $H = \langle g \rangle$ est un groupe *monogène*, en bijection avec $\mathbf{Z}$, car Φ est injective.
Lorsque $\langle g \rangle$ est fini, on dira que c'est un groupe *cyclique*.

Bibliographie

[1] M. Demazure. *Cours d'Algèbre*. Cassini, 2008.

[2] A. Ducros. *Algèbre 1, (ENS, première année)*. L3 Mathématiques, Sorbonne Université, 2023. Site Web.

[3] R. Goblot G. Auliac, J. Delcourt. *Mathématiques, algèbre et géométrie*. Ediscience, 2005.

[4] P. Naudin and Cl. Quitté. *Algorithmique algébrique*. Masson, 1992.

[5] J.-J. Risler and P. Boyer. *Algèbre pour la licence 3*. Dunod, 2006.

[6] V. Shoup. A computational introduction to number theory and algebra, 2008. [PDF].

[7] G. Peyré V. Beck, J. Malick. *Objectif Agrégation*. H-K, 2005.