Structures Algébriques - 3MA262

2023-2024

Pierre-Vincent Koseleff

4 mars 2024

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 $\mathbf{Z}/p\mathbf{Z}$.

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 $\mathscr{R}$ 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 $\mathbf{Z} \times \mathbf{Z}^*$, on définit $(a,b) \sim (a',b') \Leftrightarrow ab' = a'b$.
Dans l'ensemble $\mathbf{R}^{n+1}$, 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*

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

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 $E/\mathscr{R}$, l'ensemble quotient de E par $\mathscr{R}$, c'est l'ensemble des classes d'équivalence de E, c'est un sous-ensemble de $\mathscr{P}(E)$. 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

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

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

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 $[\![1,n]\!]$. Si $u \in \mathrm{Bij}(A,A')$ et $v \in \mathrm{Bij}(B,B')$ alors B^A et $B'^{A'}$ sont en bijection par l'application :

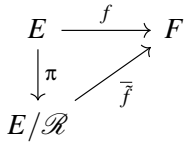
$$\begin{array}{ccc} B^A & \to & B'^{A'} \\ f & \mapsto & v\circ f\circ u^{-1}. \end{array}$$

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 $[\![1,m]\!]$.
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 $[\![1,m]\!]$.
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 $|I(n,m)| = m(m-1)\cdots(m-n+1)$..

On conclut aussi que le nombre de bijections de $I(n,n)$ est $n!$.
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 $|\mathcal{P}_k([\![1,n]\!])| = \binom{n}{k}$.

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.
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 (H est en fait la classe de l'élément neutre, voir ? ? ?).
2. Si E est un anneau, les relations d'équivalence compatibles avec les deux lois sont de la forme $x - y \in \mathrm{I}$ avec I idéal de E (ici aussi, I est la classe de 0, voir [RDO1, 3.2.2]).
3. Le cas des espaces vectoriels. Les «bonnes relations» sont de la forme $x - y \in \mathrm{F}$ avec F sous-espace vectoriel de E.

Dans cette partie, nous examinons l'algorithme d'Euclide du point de vue de l'effectivité, c'est-à-dire, nous envisageons les méthodes pour calculer le pgcd de deux éléments, ainsi qu'une relation de Bézout.
Nous commençons par décrire la situation dans l'anneau $\mathbf{Z}$ des entiers relatifs, puis rappelons quelques notions essentiels de la théorie des anneaux commutatifs pour finir par examiner le cas de $A[X]$ lorsque A est un anneau ou un corps.

2 L'anneau des entiers relatifs

$(\mathbf{Z}, +, \times)$ 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

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

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 $0 \leq r < |b|$, on notera $r = a \pmod b$ 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 $\mathcal{D}(a-kb) \cap \mathcal{D}(b) \subset \mathcal{D}((a-kb) - (-kb)) \cap \mathcal{D}(b) = \mathcal{D}(a) \cap \mathcal{D}(b)$. □

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 $d = \text{pgcd}(a,b) = r_n$ le pgcd de a et b.

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

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* $\text{pgcd}(a,b)$ *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 $|a|, |b| \leq n$. Nous verrons ultérieurement que nous pouvons donner une estimation plus fine de la complexité de cet algorithme en considérant la façon de représenter les entiers.

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. $|u_n|\leq\dfrac{b}{2d}$, $|v_n|\leq\dfrac{a}{2d}$.

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 $k\geq1$, 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 $q_n\geq2$ et $|u_n|\leq\frac{1}{2}|u_{n+1}|$.

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.

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. 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 $a \equiv b \pmod n$ 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.*

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 $au \equiv 1 \pmod n$, 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 $\{1 \le i \le n-1; (i,n) = 1\}$. 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 $\{\frac{1}{1}, \ldots, \frac{n}{n}\} = \{\frac{a}{d}; (a,d) = 1, 0 < a < d | n\}$, (voir le cours de L. Zapponi [10]), 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 $a^{\varphi(n)} \equiv 1 \pmod n$.*

et le théorème de Fermat :

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

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

2.4 Théorème Chinois

Le « théorème chinois » (Chinese Remainder Theorem) apparaît pour la première fois dans un traité appelé Sun Tzu Suan Ching ou Jiuzhang Suhanshu (date estimée : entre 280 et 473). Voir [2, 8].
Il s'énonce ainsi, sous forme d'énigme, souvent associée aux généraux préoccupés par le comptage de leur troupe : *Soit des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?*
La résolution proposée : *Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute-lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.*
On peut cependant remarquer que :

- 70 a pour reste 1 dans la division par 3 et pour reste 0 dans les divisions par 5 et 7 ;
- 21 a pour reste 1 dans la division par 5 et pour reste 0 dans les divisions par 3 et 7 ;
- 15 a pour reste 1 dans la division par 7 et pour reste 0 dans les divisions par 3 et 5.

Le nombre $2\times 70+3\times 21+2\times 15$ a bien alors pour restes respectifs 2, 3 et 2 dans les divisions par 3, 5 et 7. Enfin, comme 105 a pour reste 0 dans les trois types de division, on peut l'ôter ou l'ajouter autant de fois que l'on veut sans changer les valeurs des restes. La plus petite valeur pour le nombre d'objets est alors de 23.

Il correspond à l'énoncé mathématique suivant :
Théorème 2.18. *Soit $n_1,\dots,n_r$ des entiers premiers entre-eux deux-à-deux. Posons $N=n_1\cdots n_r$. Soit $x_1,\dots,x_r$ des entiers. Il existe un unique entier x modulo N, tel que $x\equiv x_1 \pmod{n_1},\dots,x\equiv x_r\pmod{n_r}$.*
Preuve. L'unicité est une conséquence du Lemme de Gauss (2.7), puisque deux solutions x et x' vérifient $n_i|(x-x')$ et donc N divise leur différence. Pour ce qui est de l'existence, considérons $N_i=N/n_i$. Il existe u_i,v_i, tels que $u_in_i+v_iN_i=1$, d'après l'identité de Bézout. Posons $e_i=v_iN_i$, on en déduit alors que $e_i=\delta_{i,j}\pmod{n_j}$ et par suite, l'entier $x=x_1e_1+\cdots+x_re_r$ est une solution. CQFD

Nous verrons dans la suite que l'application $(x_1,\dots,x_r)\mapsto x_1e_1+\cdots+x_re_r\pmod N$ est un morphisme d'anneau. C'est en fait un isomorphisme.

3 Rappels - Théorie des groupes

Nous rappelons ici quelques propriétés des groupes, en particulier des groupes finis commutatifs. Nous renvoyons à [7] ou [5]
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 *cyclique* $\langle g \rangle = \{g^n, n \in \mathbf{Z}\}$.

3.1 Classes à gauche, classes à droite, sous-groupes distingués

Définition 3.7. *Soit G un groupe. Si $g \in G$ et $H \subset G$, on note $gH = \{gh, h \in G\}$ et $Hg = \{hg, h \in G\}$. Si H et K sont deux parties de G, on pose*

$$HK = \{hk, h \in H, k \in K\}.$$

Notons que $\alpha_g : h \mapsto gh$ (resp. $h \mapsto hg$) est une bijection de G de réciproque $\alpha_{g^{-1}} : h \mapsto g^{-1}h$ (resp. $h \mapsto hg^{-1}$).

Lemme 3.8. *Soit H et K deux sous-groupes de G. Alors HK est un sous-groupe de G si et seulement si $HK = KH$.*

Preuve. En effet, si $x = hk \in HK$, alors $x^{-1} = k^{-1}h^{-1} \in KH$. Mais $\varphi : x \mapsto x^{-1}$ est une bijection de G, et même une involution (puisque $\varphi \circ \varphi = \mathbb{1}$). Pour tout sous-groupe G' de G on a $\varphi(G') \subset G'$ et donc $\varphi^2(G') = G' \subset \varphi(G')$, c'est-à-dire $\varphi(G') = G'$. On a donc $\varphi(HK) = KH$ et $\varphi(KH) = HK$.
HK contient toujours l'élément neutre e. Si $HK = KH$ alors pour tout élément $x, y \in HK$, on a $xy^{-1} \in HKKH \subset HKH = H^2K \subset HK$ et donc HK est un groupe. Si HK est un groupe alors $HK = \varphi(HK) = KH$. CQFD

Remarquons que si H est un sous-groupe alors $H^2 = H$. Lorsque G est un groupe abélien, alors $HK = KH$ est toujours un sous-groupe de G.

Définition 3.9. *On dira que H est sous-groupe distingué de G (on dit aussi est distingué dans G, ou est normal dans G) lorsque pour tout $g \in G$, on a $gH = Hg$. On notera $H \lhd G$ pour indiquer que H est un sous-groupe distingué de G.*

Dire que H est distingué dans G revient à $gHg^{-1} = H$ pour tout g. Remarquons que l'ensemble gHg^{-1} est un sous-groupe de G.
Lorsque H et K sont des sous-groupes et H (ou K) est distingué, alors HK est un sous-groupe de G. En effet, si $h \in H$ distingué, alors $hk = k(k^{-1}hk) \in KH$ et $kh = (khk^{-1})k \in HK$ donc $HK = KH$.

Classes à gauche

Nous nous restreindrons plus tard aux groupes abéliens, pour lesquels il n'y a pas à distinguer les classes à gauche des classes à droites.
Considérons l'ensemble des gH, pour $g \in G$. Si $g_1H \cap g_2H \neq \emptyset$, alors il existe h_1 et h_2, tels que $g_1h_1 = g_2h_2$, donc $g_2 \in g_1H$ et $g_1H \subset g_2H^2 \subset g_2H$. Par conséquent $g_1H = g_2H$. On définit donc une relation d'équivalence

$$g_1 \sim_H g_2 \Leftrightarrow g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$$

dont les classes d'équivalence sont précisément les gH, pour $g \in G$. Deux classes sont donc disjointes ou égales. On note alors $G/H = \{gH, g \in G\}$, c'est l'ensemble des classes à gauche de G sur H. De la même façon, on définit les classes à droite de G sur H, c'est l'ensemble des Hg, pour $g \in G$.
Supposons à présent que G soit un groupe fini. La bijection $\alpha_g : h \mapsto gh$ fait que $|H| = |gH|$ pour tout g. Par conséquent les éléments de G/H, c'est-à-dire les gH, sont tous de même cardinal et sont disjoints. On a donc $G = H \cup g_2H \cup \cdots \cup g_mH$. Notant $m = [G : H] = |G/H|$, le cardinal de G/H, appelé *indice de H dans G*, on obtient

$$|G| = [G : H] \cdot |H|.$$

On obtient le théorème de Lagrange :
Théorème 3.10. *Le cardinal d'un sous-groupe H de G divise le cardinal de G.*

Groupe quotient

Lorsque H est un sous-groupe distingué, alors G/H peut être muni d'une structure de groupe, en posant

$$gH \cdot g'H = (gH)(g'H) = g(Hg')H = g(g'H)H = gg'H.$$

Si l'on raisonne en terme de classe d'équivalence, et en notant $\overline{g} = gH$, on a bien $\overline{g}\overline{g'} := \overline{gg'}$.
Remarque 3.11. *Il convient de vérifier que si $\overline{g} = \overline{g_1}$ et $\overline{g'} = \overline{g'_1}$, alors $\overline{gg'} = \overline{g_1g'_1}$.*
Il existe h et h' éléments de H, tels que $g_1 = gh$ et $g'_1 = g'h'$. Alors

$$g_1g'_1 = g(hg'h') = gg'(g'^{-1}hg')h' = gg'h''h,$$

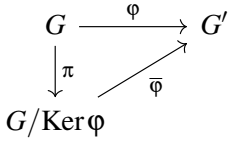
car H est distingué dans G. Ainsi $\overline{gg'} = \overline{g_1g'_1}$.
Réciproquement si pour tout g, g' on a $gH \cdot g'H = gg'H$ alors en particulier pour $g' = g^{-1}$ on a $gHg^{-1}H = H$ soit $gHg^{-1} \subset H$ et H est distingué dans G.
Exemple 3.12. *Dans le groupe $\mathbf{Z}/n\mathbf{Z}$, on a $\overline{a} + \overline{b} = \overline{a+b}$.*

3.2 Morphismes

Définition 3.13. *Soit G et G' deux groupes. Une application $\varphi : G \to G'$ est un morphisme (de groupes) si et seulement si $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1}$, pour tout $x, y \in G$.*
Notons alors qu'on a nécessairement $\varphi(1_G) = 1_{G'}$ et $\varphi(xy) = \varphi(x)\varphi(y)$ pour tout $x, y \in G$.
L'ensemble des morphismes de groupes de G dans G' est noté $\mathrm{Hom}(G, G')$. Lorsque φ est bijectif, on dit que φ est un isomorphisme. La réciproque de φ est alors un morphisme de G' dans G. L'ensemble des isomorphismes de groupes de G dans G' est noté $\mathrm{Iso}(G, G')$. L'ensemble des isomorphismes de G dans G est noté $\mathrm{Aut}(G)$. C'est un groupe pour la composition.
Exemple 3.14 (Surjection canonique)**.** *Lorsque H est un sous-groupe distingué, alors la surjection canonique $\pi_H : x \in G \mapsto xH \in G/H$ est un morphisme puisque $(xH) \cdot (yH) = xyH$.*
Exemple 3.15 (Automorphisme intérieur)**.** *Considérons $\iota_g : h \mapsto ghg^{-1}$. ι_g est un automorphisme de G, appelé automorphisme intérieur. Et $g \mapsto \iota_g$ est un élément de $\mathrm{Hom}(G, \mathrm{Aut}(G))$. L'ensemble des automorphismes intérieurs de G est noté $\mathrm{Int}(G)$ et est isomorphe à G. $\mathrm{Int}(G)$ est distingué dans $\mathrm{Aut}(G)$.*
Un sous-groupe distingué est alors un sous-groupe stable par les automorphismes intérieurs. Deux éléments h et h' sont dits conjugués si et seulement si il existe $g \in G$, tels que $ghg^{-1} = h'$. La conjugaison est une relation d'équivalence dans G.

Soit φ un élément de $\mathrm{Hom}(G, G')$. Alors le *noyau de* φ, $\mathrm{Ker}\,\varphi = \{x \in G, \varphi(x) = 1_{G'}\}$ est un sous-groupe distingué de G. En effet, $1_G \in \mathrm{Ker}\,\varphi$ et si $x, y \in \mathrm{Ker}\,\varphi$, alors $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = 1_{G'}1_{G'} = 1_{G'}$, donc $xy^{-1} \in \mathrm{Ker}\,\varphi$. Par ailleurs, pour $g \in G$, on a $\varphi(gxg^{-1}) = \varphi(g)1_{G'}\varphi(g)^{-1} = 1'_G$. Enfin, notons que $\varphi \in \mathrm{Hom}(G, G')$ est injectif si et seulement si $\mathrm{Ker}\,\varphi = \{1_G\}$.
L'image de φ, $\varphi(G)$, noté aussi $\mathrm{Im}\,\varphi = \{\varphi(g), g \in G\}$ est un sous-groupe de G'. Si H est un sous-groupe de G alors $\varphi(H)$ est un sous groupe de G' et si H' est un sous-groupe de G', alors $\varphi^-(H') = \{g \in G, \varphi(g) \in H'\}$ est un sous-groupe de G.
Le noyau d'un morphisme est donc un sous-groupe distingué de G. Réciproquement, si H est distingué dans G, alors $\pi_H : G \mapsto G/H, g \mapsto gH$ est un morphisme surjectif de noyau $\mathrm{Ker}\,\pi_H = H$. On alors $G/H = G/\mathrm{Ker}\,\pi_H$.

Théorème 3.16 (Théorème de factorisation)**.** *Soit $\varphi \in \mathrm{Hom}(G,G')$ un morphisme de groupes de G dans G'. Alors $H = \mathrm{Ker}\,\varphi$ est un sous-groupe distingué et induit un unique isomorphisme $\overline{\varphi} \in \mathrm{Iso}(G/\mathrm{Ker}\,\varphi, \mathrm{Im}\,\varphi)$, tel que $\varphi = \overline{\varphi} \circ \pi$.*



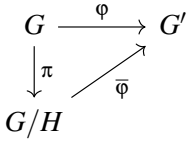
Preuve. Posons $\overline{\varphi}: \begin{array}{ccc} G/H & \to & \mathrm{Im}\,\varphi \\ gH & \mapsto & \varphi(g) \end{array}$. Si $gH = g'H$ alors $g^{-1}g' \in H$ et $\varphi(g^{-1}g') = 1_{G'}$ donc $\varphi(g) = \varphi(g')$.
Ainsi $\overline{\varphi}$ est bien défini et est un morphisme. $\overline{\varphi}$ est injectif car $H = \mathrm{Ker}\,\varphi$. CQFD
On déduit que si $\varphi \in \mathrm{Hom}(G,G')$ où G est fini, alors

$$|\mathrm{Ker}\,\varphi| \cdot |\mathrm{Im}\,\varphi| = |G|.$$

En particulier, lorsque G et G' sont des groupes finis de cardinal n et n', et $\varphi \in \mathrm{Hom}(G,G')$, le cardinal $|\mathrm{Im}\,\varphi|$ divise (n,n'). En particulier lorsque $(n,n') = 1$, il n'y a qu'un seul morphisme entre G et G', c'est le morphisme trivial $x \mapsto e_{G'}$.
Exemple 3.17. *Soit $\mathbf{F}_q$ un corps fini commutatif à q éléments (par exemple $K = \mathbf{Z}/p\mathbf{Z}$, où p est premier). Alors si $q \equiv 1 \pmod 2$, $\mathbf{F}_q^*$ a exactement $(q-1)/2$ carrés, sinon tous les éléments de $\mathbf{F}_q^*$ sont des carrés.*

3.3 Théorèmes d'isomorphismes

Nous avons vu que si φ est un morphisme alors $G/\mathrm{Ker}\,\varphi \simeq \mathrm{Im}\,\varphi$. On peut généraliser ce théorème 4.10 :
Théorème 3.18 (Propriété universelle du quotient)**.** *Soit G et G' deux groupes. Soit $\varphi \in \mathrm{Hom}(G,G')$. Il existe un (unique) morphisme $\overline{\varphi} \in \mathrm{Hom}(G/H,G')$ tel que $\varphi = \overline{\varphi} \circ \pi_H$ si et seulement si $H \subset \mathrm{Ker}\,\varphi$.*



Dans ce cas, on a $\mathrm{Ker}\,\overline{\varphi} = \mathrm{Ker}\,\varphi/H$.
Preuve. Si $\overline{\varphi}$ existe alors pour tout $h \in H$, on a $\varphi(h) = 1_{G'}$ dont $H \subset \mathrm{Ker}\,\varphi$. On doit donc avoir $\overline{\varphi}(gH) = \varphi(g)$ et $\overline{\varphi}$ est défini de façon unique. Réciproquement, si $H \subset \mathrm{Ker}\,\varphi$ alors $\overline{\varphi}(gH) := \varphi(g)$ définit bien un morphisme. $gH \in \mathrm{Ker}\,\overline{\varphi}$ ssi $g \in \mathrm{Ker}\,\varphi$. L'ensemble des $gH, g \in \mathrm{Ker}\,\varphi$ est précisement $\mathrm{Ker}\,\varphi/H$ car H est distingué dans G donc a fortiori dans $\mathrm{Ker}\,\varphi$. CQFD
Théorème 3.19. *Si H est un sous-groupe distingué de G, alors il y a une bijection entre les sous-groupes de G/H et les sous-groupes de G contenant H. De plus $K/H \lhd G/H$ si et seulement si $K \lhd G$. Alors $(G/H)/(K/H)$ et G/K sont isomorphes.*
Preuve. Soit K un sous-groupe de G contenant H. Alors H est distingué dans K. Notons π_H la projection $G \to G/H$. Alors $\pi(K) = K/H$ est un sous-groupe de G/H. Réciproquement si A est un sous-groupe de G/H alors $A' = \pi_H^-(A)$ est un sous-groupe de G contenant H et $\pi(A') = A'/H = A$.
Considérons π_K la projection canonique $G \to G/K$. Elle induit un morphisme surjectif $\overline{\pi_K}$ de G/H to G/K car $H \subset \mathrm{Ker}\,\pi_K = K$. Mais alors $\mathrm{Ker}\,\overline{\pi_K} = K/H$, d'où le résultat. CQFD
Exemple 3.20. *Il y a une bijection entre les sous groupes de $\mathbf{Z}/n\mathbf{Z}$ et les sous-groupes de $\mathbf{Z}$ contenant $n\mathbf{Z}$, qui sont les $d\mathbf{Z}$, pour $d|n$. Les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont donc les $\overline{d}\mathbf{Z}/n\mathbf{Z}$, où $d|n$.*

Revenons au théorème chinois 2.18. Si G_1 et G_2 sont des groupes, on peut munir l'ensemble $G = G_1 \times G_2$ d'une structure de groupe en posant $(g_1,g_2)\cdot(g_1',g_2') = (g_1g_1', g_2g_2')$. Ici, nous considérons le morphisme

$$\Psi: \begin{array}{ccc} \mathbf{Z} & \to & \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \\ x & \mapsto & (x \pmod n, x \pmod m) \end{array}$$

Il est immédiat $\mathrm{Ker}\,\Psi = n\mathbf{Z} \cap m\mathbf{Z} = N\mathbf{Z}$ où $N = \mathrm{ppcm}(n,m)$. Dans le cas où $(n,m) = 1$, alors $\mathrm{Ker}\,\psi = nm\mathbf{Z}$. Mais alors $\Psi(\mathbf{Z})$ est isomorphe à $\mathbf{Z}/nm\mathbf{Z}$ et par cardinalité. Nous déduisons

Théorème 3.21 (Théorème chinois)**.** *Soit n et m deux entiers premiers entre-eux. Alors les groupes* $\mathbf{Z}/nm\mathbf{Z}$ *et* $\mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$ *sont isomorphes.*

Remarque 3.22. *En général, si n et m sont des entiers, les ensembles* $\mathbf{Z}/nm\mathbf{Z}$ *et* $\mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$ *sont en bijection puisqu'ils ont le même cardinal. Ils ne sont isomorphes que si n et m sont premiers entre-eux (voir la suite du cours). Par exemple, les groupes additifs* $(\mathbf{Z}/2\mathbf{Z})^2$ *et* $\mathbf{Z}/4\mathbf{Z}$ *ne sont pas isomorphes car le premier n'a pas d'éléments d'ordre 4.*
Si n et m sont premiers entre-eux, le théorème chinois peut aussi se voir comme un isomorphisme de groupes entre $\mathbf{Z}^2 \;/\; (n\mathbf{Z}\times m\mathbf{Z})$ *et* $\mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$*. En effet le morphisme de groupe* $\psi : \mathbf{Z}^2 \to \mathbf{Z}/n\mathbf{Z}\times\mathbf{Z}/m\mathbf{Z}$*,* $(x,y)\mapsto (x\,(\mathrm{mod}\,n), y\,(\mathrm{mod}\,m))$ *est surjectif et a comme noyau* $n\mathbf{Z}\times m\mathbf{Z}$*.*

3.4 Ordre d'un élément, exposant d'un groupe

Soit G un groupe et $g\in G$. Considérons le morphisme φ_g de $(\mathbf{Z},+)$ vers $(G,\cdot)$, donné par $\varphi_g(n)=g^n$. $\mathrm{Ker}\,\varphi$ est un sous-groupe de $\mathbf{Z}$.

Définition 3.23 (Ordre d'un élément)**.** *Si* $\mathrm{Ker}\,\varphi=\{0\}$*, on dit que g est d'ordre infini. Si* $\mathrm{Ker}\,\varphi = m\mathbf{Z}$*,* $m>0$*, on dit que* $\mathrm{ord}\,(g)=m$*, l'ordre de g est fini égal à m.*

$\varphi_g(\mathbf{Z})=\langle g\rangle$ est un sous-groupe de G, C'est le groupe *engendré* par g. C'est le plus petit sous-groupe de G contenant g. Lorsque $\mathrm{ord}\,(g)=m$ alors $\langle g\rangle$ est un groupe *cyclique* et on a $\langle g\rangle=\{1,g,\ldots,g^{m-1}\}\simeq\mathbf{Z}/m\mathbf{Z}$.
De plus, on a l'équivalence $g^k=e\Leftrightarrow \mathrm{ord}\,(g)|k$.

Définition 3.24. *Un groupe fini G est cyclique si il existe un élément g de G d'ordre* $n=|G|$*. On a alors* $G=\langle g\rangle$*.*

Exemple 3.25. *Le groupe* $(\mathbf{Z}/n\mathbf{Z},+)$ *est cyclique, pour tout n. Le groupe* $(\mathbf{Z}/8\mathbf{Z})^*$ *n'est pas cyclique. En effet tout élément de* $(\mathbf{Z}/8\mathbf{Z})^*$ *vérifie* $x^2=1$*.*

Lemme 3.26. *Si g est d'ordre fini, on a* $\mathrm{ord}\,(g^d)=\dfrac{\mathrm{ord}\,(g)}{(d,\mathrm{ord}\,(g))}$.

Preuve. Écrivons $e=g^{d^k}=g^{kd}$ si et seulement si $\mathrm{ord}\,(g)|kd$, ie $\dfrac{\mathrm{ord}\,(g)}{(d,\mathrm{ord}\,(g))}\Big|\dfrac{d}{(d,\mathrm{ord}\,(g))}k$, ie $\dfrac{\mathrm{ord}\,(g)}{(d,\mathrm{ord}\,(g))}|k$, par le lemme de Gauss.

Exercice 3.27. *Soit G commutatif et* a,b *des éléments de G. Si a et b sont d'ordre n et m et* $(n,m)=1$ *alors* $\mathrm{ord}\,(ab)=nm$*.*

Preuve. On a $|\langle a\rangle|=n$ et $|\langle b\rangle|=m$. Supposons que $(ab)^k=e$, alors

$$a^k=b^{-k}\in\langle a\rangle\cap\langle b\rangle=\{e\}.$$

Donc $a^k=b^k=e$ et $n|k$ et $m|k$ donc $nm|k$. On déduit que $nm=\mathrm{ord}\,(ab)$. CQFD

Remarque 3.28. *Lorsque G n'est pas commutatif, il n'y a pas de raison que le produit de deux éléments d'ordres finis soit d'ordre fini. Par exemple, si a et b sont des symétries orthogonales, alors ab est une rotation, pas nécessairement d'ordre fini.*

En supposant à présent que G est commutatif, il est faux de dire que $\mathrm{ord}\,(ab)=\mathrm{ppcm}\,(\mathrm{ord}\,(a),\mathrm{ord}\,(b))$. On a seulement que $\mathrm{ppcm}\,(\mathrm{ord}\,(a),\mathrm{ord}\,(b))|\mathrm{ord}\,(ab)$, penser à $b=a^{-1}$. Néanmoins

Exercice 3.29. *Il existe* $a'\in\langle a\rangle$ *et* $b'\in\langle b\rangle$*, tels que* $\mathrm{ord}\,(a'b')=\mathrm{ppcm}\,(\mathrm{ord}\,(a),\mathrm{ord}\,(b))$.

Preuve. Si $(n,m)\neq 1$. Écrivons $n=\prod_{i=1}^{k}p_i^{\alpha_i}$ et $m=\prod_{i=1}^{k}p_i^{\beta_i}$. On alors $\mathrm{ppcm}\,(n,m)=\prod_{i=1}^{k}p_i^{\max\alpha_i,\beta_i}$. Posons $n'=\prod_{\alpha_i>\beta_i}p_i^{\alpha_i}$ et $m'=\prod_{\alpha_i\leq\beta_i}p_i^{\beta_i}$. Nous avons $n'|n$, $m'|m$, $(n',m')=1$ et $n'm'=\mathrm{ppcm}\,(n,m)$. Mais alors $a'=a^{n/n'}$ est d'ordre n' et $b'=b^{m/m'}$ est d'ordre m' et nous concluons que $a'b'$ est d'ordre $n'm'=\mathrm{ppcm}\,(n,m)$. CQFD

Définition 3.30 (Exposant de G)**.** *Soit G un ordre fini. On note* $w(G)$*, l'exposant de G, le* $\mathrm{ppcm}\,(\mathrm{ord}\,(g),g\in G)$.

Puisque $\mathrm{ord}\,(g)\mid|G|$, par le théorème de Lagrange, on obtient que $w(G)\mid|G|$.

Théorème 3.31. *Si G est commutatif, alors il existe* $g\in G$*,* $w(G)=\mathrm{ord}\,(g)$.

Preuve. On montre d'abord que l'ensemble $\{\text{ord}\,(g), g \in G\}$ est stable par ppcm. D'après l'exercice 3.29, si a et b sont dans G, il existe $c \in G$ d'ordre $\text{ppcm}\,(\text{ord}\,a, \text{ord}\,b)$. Soit $g \in G$ d'ordre N maximum. Si N n'est pas un multiple de tous les ordres des éléments de G alors il existe $a \in G$ d'ordre d tel que $d/(N,d) > 1$. Mais alors $\text{ppcm}\,(N,d) > N$ et il existe un élément de G d'ordre $> N$. Contradiction. Donc il existe $g \in G$ d'ordre $N = \text{ppcm}\,(\text{ord}\,(a), a \in G) = w(G)$. CQFD

Remarque 3.32. *Lorsque le groupe G est commutatif, alors G est cyclique si et seulement si $w(G) = |G|$.*
Si le groupe n'est pas commutatif, l'exposant n'est pas nécessairement atteint. Par exemple, $w(\Sigma_3) = 6$ mais il n'y a pas d'élément d'ordre 6. l

Théorème 3.33. *Soit G un groupe cyclique d'ordre n. Pour tout diviseur d de n il y a exactement $\varphi(d)$ éléments d'ordre d.*

Preuve. On a $G = \langle g \rangle$. Un élément de G s'écrit $x = g^k$ où $k \in [\![0, n-1]\!]$. g^k est d'ordre $d = n/(n,k)$. Posons alors $k = k'(n,k) = k'n/d$, où $k' \in [\![0, d-1]\!]$ et $(k', d) = 1$. Les éléments de G d'ordre d sont exactement les $\left(g^{n/d}\right)^{k'}$ où $(k', d) = 1$. Il y en a exactement $\varphi(d)$. CQFD

On retrouve ainsi la formule d'Euler : $\sum_{d|n} \varphi(d) = n$.

Théorème 3.34 (Caractérisation des groupes cycliques)**.** *Soit G un groupe commutatif fini. G est cyclique si et seulement si pour tout d divisant n, il y a au plus d éléments de G satisfaisant $g^d = e$.*

Preuve. Soit d un diviseur de n. Posons $H_d = \{x \in G \mid \text{ord}\,(x) = d\}$ et G_d le sous-groupe de G : $\{x \in G \mid x^d = 1\}$, Si $H_d \neq \emptyset$, alors G a un élément g d'ordre d et G_d contient le groupe cyclique $\langle g \rangle$. Par cardinalité $G_d = \langle g \rangle$. Les éléments de H_d sont les éléments d'ordre d de $\langle g \rangle$, il y en a $\varphi(d)$. On obtient donc que $|H_d| = \varphi(d)$ ou $|H_d| = 0$. Les H_d formant une partition de G, on conclut en utilisant la formuler d'Euler que pour tout d divisant n, il y a exactement $\varphi(d)$ éléments d'ordre d. CQFD

On déduit aussi que tout sous-groupe d'un groupe cyclique est cyclique et que G_d est l'unique sous-groupe de G d'ordre d.

Exercice 3.35. *Soit G_1 et G_2 deux groupes commutatifs. Alors $w(G_1 \times G_2) = \text{ppcm}\,(w(G_1), w(G_2))$. En déduire que $G_1 \times G_2$ est cyclique si et seulement si G_1 et G_2 sont cycliques de cardinaux premiers entre-eux.*

3.5 Théorème de structure des groupes abéliens finis

Du théorème chinois et de la décomposition de tout entier en produits de facteurs irréductibles, nous déduisons

Corollaire 3.36. *Soit a et b deux entiers relatifs, $d = \text{pgcd}(a,b)$ et $N = \text{ppcm}\,(a,b)$. Alors*

$$\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z} \simeq \mathbf{Z}/d\mathbf{Z} \times \mathbf{Z}/N\mathbf{Z}.$$

Preuve. Il suffit de considérer, ce que nous essayons de nous interdire, les décompositions

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}, \quad m = \prod_{i=1}^{r} p_i^{\beta_i}.$$

Alors $d = \prod_{i=1}^{r} p_i^{\min(\alpha_i,\beta_i)}$, $N = \prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)}$, et $\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z} \times \mathbf{Z}/p_i^{\beta_i}\mathbf{Z} \simeq \mathbf{Z}/p_i^{\min(\alpha_i,\beta_i)}\mathbf{Z} \times \mathbf{Z}/p_i^{\max(\alpha_i,\beta_i)}\mathbf{Z}$. CQFD

L'intérêt du groupe produit $d\mathbf{Z} \times N\mathbf{Z}$ réside dans le fait que $d|N$. Cette présentation est unique, comme l'indique le théorème suivant.

Théorème 3.37. *Soit $(a,b) \in \mathbf{Z}^2$ tel que $a|b$ et $(c,d) \in \mathbf{Z}^2$ tels que $c|d$. Si $\mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z} \simeq \mathbf{Z}/c\mathbf{Z} \times \mathbf{Z}/d\mathbf{Z}$, alors $b = \pm d$ et $a = \pm c$.*

Preuve. On peut supposer que a, b, c et d sont des entiers naturels, quitte à les changer en leur opposé, car $n\mathbf{Z} = (\pm n)\mathbf{Z}$. Considérons l'exposant de $G = \mathbf{Z}/a\mathbf{Z} \times \mathbf{Z}/b\mathbf{Z}$: $w(G) = \min\{k \in \mathbf{Z}, k > 0; \forall x \in G, k \cdot x = 0\}$. Il est clair que $w(G) = b$. Mais deux groupes isomorphes ont le même exposant, donc $b = d$. Par suite, par cardinalité, on a $a = c$. CQFD

Ce théorème se généralise en le théorème de Kronecker :

Théorème 3.38 (Théorème de structure des groupes abéliens)**.** *Soit G un groupe abélien fini. Il existe $d_1|d_2|\cdots|d_r$ des entiers naturels non nuls tels que $G \simeq \mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$. En outre la suite $(d_1, \ldots, d_r)$ est unique.*

On peut démontrer ce théorème de plusieurs façons, par exemple en utilisant la structure du groupe dual $\hat{G} = \mathrm{Hom}(G, \mathbf{C}^*)$, ou en étudiant les sous-groupes (on devrait dire les sous $\mathbf{Z}$-modules) de $\mathbf{Z}^n$. Nous ne démontrons pas ce théorème ici, le lecteur pourra consulter par exemple [5].
Par la suite nous étudierons (sans avoir besoin d'utiliser le théorème de structure des groupes abéliens finis) à quelle condition le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique.

4 Propriétés arithmétiques des anneaux

Dans cette partie, nous précisons à nouveau le vocabulaire et les propriétés de base des anneaux que nous allons considérer.

Définition 4.1. *$(A,+,\cdot)$ est un anneau unitaire si et seulement si*

1. *$(A,+)$ est un groupe commutatif d'élément neutre 0_A.*
2. *La multiplication $\cdot$ est associative, distributive à gauche et à droite sur l'addition, et possède un élément neutre 1_A.*

A est un anneau commutatif lorsque la multiplication $\cdot$ est commutative.
Par exemple, $(\mathbf{Z},+,.)$ est un anneau commutatif (la loi $\cdot$ est commutative). Par exemple $(\mathcal{P}(E),\Delta,\cap)$ est un anneau commutatif. $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$ sont des anneaux commutatifs
Il existe de nombreux anneaux entre $\mathbf{Z}$ et $\mathbf{Q}$, par exemple l'ensemble $\mathbb{D}$ des nombres décimaux. Il existe de nombreux autres anneaux, par exemple l'anneau $A[X]$ des polynômes à coefficients dans A. Il existe des anneaux non-commutatifs, par exemple l'ensemble des endomorphismes $\mathcal{L}(E)$ d'un espace vectoriel, mais nous nous restreindrons dans ce cours aux anneaux commutatifs.

Inversibles, diviseurs de 0

Un élément non nul a est un *diviseur de* 0 si et seulement si il existe un élément non nul b de A, tel que $ab = 0$.
A est un anneau *intègre* si et seulement si $a \cdot b = 0 \Rightarrow a = 0$ ou $b = 0$. A est donc intègre si et seulement si A n'admet pas de diviseur de 0 ;
Un élément $a \in A$ est une *unité* ou inversible si il existe donc $a' \in A$, tel que $aa' = a'a = 1_A$. L'ensemble de inversibles de A est noté $U(A)$. C'est un groupe, puisque $(ab)^{-1} = b^{-1}a^{-1}$.
Un anneau A est un corps si et seulement si $U(A) = A - \{0\}$. Un corps est donc un anneau intègre. Remarquons, que lorsque A est fini, alors A est un corps si A est intègre.
Deux éléments a et b sont *associés* si et seulement si $\mathcal{D}(a) = \mathcal{D}(b)$. Lorsque A est intègre, a et b sont associés si et seulement si il existe $u \in U(A)$, tel que $b = ua$. On écrira $a \sim b$.

4.1 Sous-anneaux, idéaux, morphismes

Définition 4.2. *Un sous-anneau B de A est un anneau inclus dans A.*
B est un sous-anneau de A si et seulement si $(B,+)$ est un sous-groupe de $(A,+)$ et, B est stable par multiplication, et contient l'élément neutre 1_A.
L'intersection de sous-anneaux de A est un sous-anneau de A.
Si $P \subset A$, le sous-anneau de A engendré par P est le plus petit anneau contenant P. C'est l'intersection des sous-anneaux de A contenant B.
B étant un sous-anneau de A, on peut considérer le groupe quotient A/B. Pour que A/B ait une structure d'anneau, il faudrait que la multiplication soit compatible avec la relation d'équivalence $x \sim y \Leftrightarrow y - x \in B$.
Pour cela, nous considérons les idéaux plutôt que les sous-anneaux.

Définition 4.3. *Soit $(A,+,*)$ un anneau commutatif. Un sous-ensemble I de A est un* idéal de l'anneau *A si*

— *I est un sous-groupe de $(A,+)$,*
— *pour tout $x \in A$, pour tout $a \in I, x*a \in I$.

Soit I un idéal de A. On définit la relation d'équivalence $a\mathscr{R}b$ par

$$a\mathscr{R}b \Leftrightarrow b - a \in I.$$

Les classes d'équivalence sont les $\overline{a} = a + I, a \in I$. L'ensemble des classes d'équivalence

Théorème 4.4. *A/I a une structure d'anneau unitaire en définissant*

$$\overline{a}+\overline{b}=\overline{a+b}, \quad \overline{a}\cdot\overline{b}=\overline{a\cdot b}.$$

Preuve. On sait déjà que $(A/I,+)$ est un groupe commutatif. Pour $x\in A/I$, considérons $m_x : A\to A/I, y\mapsto xy+I$. m_x est clairement un morphisme de groupe de $(A,+)$ vers $(A/I,+)$. $\mathrm{Ker}\,(m_x)$ contient I, puisque $xI\subset I$, ainsi, le morphisme se factorise de façon unique en un morphisme $\tilde{m}_x\in \mathrm{Hom}\,(A/I,A/I)$. On a donc défini une loi de composition (notée $\cdot$) de $A/I\times A/I\to A/I$ qui vérifie $(x+I)\cdot(y+I)=\tilde{m}_x(y+I)=xy+I$. CQFD

Exemple 4.5. *$(0)=\{0\}$ et $A=(1)$ sont des idéaux* triviaux *de A. Remarquons que $I=A$ si et seulement si $1_A\in I$.*
Un idéal propre *de A est un idéal non trivial de A.*
Si $a\in A$, l'ensemble $(a)=aA=\{ax, x\in A\}$, est un idéal de A. On dit que (a) est principal.
Le sous-groupe $(n)=n\mathbf{Z}$ de $\mathbf{Z}$ est un idéal de $\mathbf{Z}$. $(\mathbf{Z}/n\mathbf{Z},+,\cdot)$ est un anneau.
Remarquons qu'un anneau A est un corps si et seulement si A n'a pas d'idéaux propres. En effet si A n'a pas d'idéal propre et $a\in A$ est différent de 0, alors $(a)=aA=\{ax, x\in A\}$ est un idéal de A. C'est donc A et il existe $x\in A$, tel que $1_A=ax$. Réciproquement si A est un corps et I un idéal non nul de A, alors I contient un élément x non nul et donc $x\cdot x^{-1}=1_A\in I$ donc $I=A$.

Définition 4.6 (Homomorphisme d'anneaux)**.** *Soit A et B deux anneaux (unitaires et commutatifs). Un* homomorphisme d'anneaux *$\varphi : A\to B$ est une application, telle que $\varphi(1_A)=1_B$, et pour tous $a,b\in A$*

$$\varphi(a-b)=\varphi(a)-\varphi(b), \quad \varphi(ab)=\varphi(a)\varphi(b).$$

On vérifie que $\mathrm{Ker}\,\varphi=\{x\in A, \varphi(x)=0_B\}$ est un idéal de A. On vérifie également que $\mathrm{Im}\,\varphi=\varphi(A)$ est un sous-anneau de B. Lorsque φ est bijectif, on dit que φ est un isomorphisme (d'anneaux).

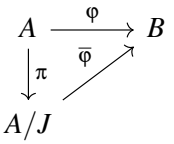
Exemple 4.7 (Surjection canonique)**.** *Lorsque I est un idéal, alors la surjection canonique $\pi_I : x\in A\mapsto x+I\in A/I$ est un homomorphisme d'anneau surjectif.*

Proposition 4.8 (Propriété universelle de $\mathbf{Z}$)**.** *Soit A un anneau unitaire. Il existe un unique morphisme $\varphi\in \mathrm{Hom}\,(\mathbf{Z},A)$. Il est défini par $\varphi(n)=n\cdot 1_A=1_A+\cdots+1_A$. On notera alors n au lieu $n\cdot 1_A$.*

Définition 4.9 (Caractéristique d'un anneau)**.** *Considérant le morphisme précédent. $\mathrm{Ker}\,\varphi$ est un idéal de $\mathbf{Z}$. On appelle $\mathrm{car}\,(A)$ la caractéristique de A, l'unique entier positif tel que $\mathrm{Ker}\,\varphi=n\mathbf{Z}$.*
Lorsque A est intègre, $\mathrm{car}A$ est nulle, ou un nombre premier. Par exemple, la caractéristique de $\mathbf{Z}/p\mathbf{Z}$ est p.

Si I est un idéal de A, alors $\pi : A\to A/I$, $a\mapsto\overline{a}$, est un homorphisme d'anneaux, surjectif. On l'appelle la *projection canonique*. Un idéal est donc toujours le noyau d'un morphisme.

Théorème 4.10 (Premier théorème d'isomorphisme)**.** *Soit $\varphi : A\to B$ un homomorphisme d'anneaux. Soit $J\subset\mathrm{Ker}\,\varphi$ un idéal de A et $\pi : a\to A/J$ la projection canonique. Alors*



1. *Il existe un unique homomorphisme $\overline{\varphi} : A/J\to B$, tel que $\varphi=\overline{\varphi}\circ\pi$.* On dit que φ se factorise par A/J.
2. *$\overline{\varphi}$ est injectif si et seulement si $I=J$.*
3. *$\overline{\varphi}$ est surjectif si et seulement si φ est surjectif.*
4. *En particulier* $\mathrm{Im}\,\varphi\simeq A/\mathrm{Ker}\,\varphi$.

Preuve. Si $\overline{\varphi}$ existe, alors $\varphi(a)=\overline{\varphi}(\overline{a})$. Vérifions que $\overline{\varphi}$ est bien défini. En effet, si $\overline{a}=\overline{b}$, alors $(b-a)=x\in J\subset I$ et $\varphi(b)=\varphi(a)+\varphi(x)=\varphi(a)$. On vérifie ensuite que $\overline{\varphi}$ est un homomorphisme. $\overline{\varphi}(\overline{x})=0$ si et seulement si $\varphi(x)=0$, c'est-à-dire, $x\in I$. Par construction $\mathrm{Im}\,\overline{\varphi}=\mathrm{Im}\,\varphi$. CQFD

Les idéaux de l'anneau quotient A/I sont en bijection avec les idéaux de A contenant I. Plus précisément

Théorème 4.11 (Second théorème d'isomorphisme)**.** *Soit A un anneau, I un idéal de A et J un idéal de A contenant I. Alors J/I est un idéal de A/I, et il y a un isomorphisme :*

$$(A/I)\,/\,(J/I)\simeq A/J.$$

Preuve. Considérons le diagramme suivant :

$$\begin{array}{ccc} A & \xrightarrow{\pi_J} & A/J \\ \downarrow{\scriptstyle \pi_I} & \nearrow{\scriptstyle \overline{\pi}} & \\ A/I & & \end{array}$$

où $\pi_J = \overline{\pi} \circ \pi_I$, puisque $I \subset J = \mathrm{Ker}\,\pi_J$. $\overline{\pi}$ est surjectif car π_J est surjectif. Le noyau de $\overline{\pi}$ est précisément J/I. Ainsi

$$(A/I)\,/\,(J/I) = (A/I)\,/\mathrm{Ker}\,\overline{\pi} \simeq \mathrm{Im}\,\overline{\pi} = A/J$$

CQFD

Exemple 4.12. *Les idéaux de* $\mathbf{Z}/n\mathbf{Z}$ *sont les* $d\mathbf{Z}/n\mathbf{Z}$ *où* d *divise* n *et on a* $(\mathbf{Z}/n\mathbf{Z})/(d\mathbf{Z}/n\mathbf{Z}) \simeq \mathbf{Z}/d\mathbf{Z}$.

Théorème Chinois dans le cas de Z

Lorsque A et B sont des anneaux unitaires, alors $A \times B$ est un anneau en considérant les lois de composition :

$$((a,b)+(a',b') = (a+a',b+b'), \quad (a,b)\cdot(a',b') = (aa',bb').$$

L'élément neutre de $A \times B$ est $(1_A, 1_B)$ et $U(A \times B) = U(A) \times U(B)$.
Soit n et m des entiers premiers entre-eux. Le morphisme (de groupe) $\Phi : \mathbf{Z} \mapsto \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ est en fait un morphisme d'anneau. $\mathrm{Ker}\,\Phi = nm\mathbf{Z}$, si bien que $\mathbf{Z}/nm\mathbf{Z} \simeq \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$. On déduit alors
Théorème 4.13 (Théorème Chinois)**.** *Lorsque* n *et* m *sont premiers entre-eux, l'anneau* $\mathbf{Z}/nm\mathbf{Z}$ *est isomorphe à* $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$.
Considérons la relation de Bézout $un + vm = 1$. Soit $x, y \in \mathbf{Z}^2$ et considérons $z = uny + vmx$. Alors $z \equiv x \,(\mathrm{mod}\, n)$ et $z \equiv y \,(\mathrm{mod}\, m)$. Si bien que $\Phi(z) = (x \,(\mathrm{mod}\, n), y \,(\mathrm{mod}\, m))$. En d'autre termes, le morphisme réciproque Φ^{-1} est donné par $(x,y) \mapsto vmx + unx \,(\mathrm{mod}\, nm)$.
Par ailleurs, les inversibles de $\mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ sont les éléments de $(\mathbf{Z}/n\mathbf{Z})^* \times (\mathbf{Z}/m\mathbf{Z})^*$. On déduit alors que si $(n,m) = 1$, alors $\varphi(nm) = \varphi(n)\varphi(m)$. Partant de $\varphi(p^n) = p^n(1 - \frac{1}{p})$, on déduit que

$$\varphi(n) = n \prod_{p|n} (1 - \tfrac{1}{p}).$$

4.2 L'anneau des polynômes A[X]

A étant un anneau commutatif unitaire, on considère l'ensemble $A^{(\mathbf{N})}$ des suites presque nulles d'éléments de A. Pour deux éléments $a = (a_i)_{i\in\mathbf{N}}$ et $b = (b_i)_{i\in\mathbf{N}}$, on pose

$$a + b = (a_i + b_i)_{i\in\mathbf{N}}, \quad a \cdot b = (\sum_{i+j=k} a_i b_j)_{k\in\mathbf{N}}.$$

En posant $0 = (0_A, \ldots), 1 = (1_A, 0, \ldots)$ et $X = (0, 1_A, 0, \ldots)$, on constate que tout élément a de $A^{(\mathbf{N})}$ s'écrit de façon unique $a = a_0 + a_1 X + \cdots a_n X^n$. On désigne donc par $A[X]$ l'anneau des polynômes à coefficients dans l'anneau A, en l'indéterminée X. $A[X]$ est un anneau commutatif et unitaire. Lorsque $A = \mathbf{K}$ est un corps, $A[X]$ est un $\mathbf{K}$-espace vectoriel, dont une base de $(X^i)_{i\in\mathbf{N}}$. Nous étudions $\mathbf{K}[X]$ dans la partie **??**. Lorsque A n'est pas nécessairement un corps, on dit que $A[X]$ est une A-algèbre, ie tout élément est une combinaison linéaire finie des $(X^i)_{i\in\mathbf{N}}$, à coefficients dans A.

Soit $P = a_0 + a_1 X + \cdots + a_n X^n$ un polynôme non nul de $\mathbf{K}[X]$: si $a_n \neq 0$, on dit que P est de *degré n* (on note $\deg P$) et a_n s'appelle le *coefficient dominant* de P; si P est de degré n et $a_n = 1$, on dit que P est *unitaire*. Si $P = 0$, on convient que P est de degré $-\infty$. De cette façon on a $\deg P \cdot Q = \deg P + \deg Q$ car le coefficient dominant de $P \cdot Q$ est le produit de leurs coefficients dominants.

Seuls les polynômes constants non nuls ont un inverse (pour la multiplication) dans l'anneau $A[X]$, c'est-à-dire, $U(A[X]) = U(A)$.

Définition 4.14 (Propriété universelle des polynômes)**.** *Soit φ un homomorphisme d'anneaux entre un anneau A commutatif et un anneau B. Soit b un élément de B. Il existe un unique homomorphisme d'anneau $\tilde{\varphi}_b \in \mathrm{Hom}(A[X],B)$, tel que $\varphi(X) = b$ et $\varphi_b(a) = \varphi(a)$, pour tout $a \in A$.*
En particulier si $\varphi \in \mathrm{Hom}(A,B)$, il existe un unique morphisme $\tilde{\varphi} \in \mathrm{Hom}(A[X],B[X])$, tel que $\tilde{\varphi}_{|A} = \varphi$.
Lorsque $A = \mathbf{Z}$, le sous-anneau obtenu $\varphi_b(\mathbf{Z}[X])$ est $\mathbf{Z}[b]$, le sous-anneau de B engendré par b
Définition 4.15 (Morphisme d'évaluation)**.** *Lorsque $A \subset B$, on obtient le morphisme d'évaluation $P \in B[X] \mapsto P(b)$.*
Preuve. On vérifie que dans ce cas, si $P = a_0 + a_1X + \cdots + a_nX^n$, on a

$$\varphi_b(P) = P(b) = a_0 + a_1 \cdot b + \cdots + a_nb^n.$$

CQFD

Notons que $\mathrm{Ker}\,\varphi_b = \{P \in A[X] \mid P(b) = 0\}$ est un idéal de $A[X]$.

Définition 4.16 (Sous-anneau engendré par un élément)**.** *Soit A un anneau commutatif et a un élément de A. Le sous-anneau $\mathbf{Z}[a]$ est le sous-anneau engendré par a.*
$\mathbf{Z}[a]$ est le plus petit sous-anneau de A contenant a.
Exemple 4.17 (Entiers de Gauss)**.** *Considérons $\mathbf{Z}[i] = \{P(i), P \in \mathbf{Z}[X]\}$. Alors $\mathbf{Z}[i] = \{a+ib, a,b, \in \mathbf{Z}\}$. Le noyau de $P \mapsto P(i)$ est l'ensemble des polynômes multiples de X^2+1 (démonstration à suivre). On a donc $\mathbf{Z}[i] \simeq \mathbf{Z}[X]/\langle X^2+1\rangle$.*

Lorsque $P(b) = 0$, on dit que b est une racine de P, dans B.
Lemme 4.18. *a est une racine de P si et seulement si $P(a) = 0$ si et seulement si $(X-a)$ divise P dans $A[X]$.*
Preuve. On a, pour tout $k \in \mathbf{N}$:

$$X^k - a^k = (X-a)(X^{k-1} + aX^{k-2} + \cdots + a^{k-2}X + a^{k-1}).$$

On déduit alors que $X-a$ divise $X^k - a^k$, dans l'anneau $A[X]$, pour tout k, et par suite $X-a$ divise $P(X) - P(a)$.
On en déduit que $P(a) = 0 \Leftrightarrow (X-a)|P$. CQFD

Théorème 4.19 (Nombre de racines)**.** *Soit A un anneau commutatif et intègre et $P \in A[X]$ de degré n. P a au plus n racines distinctes dans A.*
Preuve. Démontrons le résultat par récurrence sur le degré de P. Soit $P \in A[X]$, de degré n. Si P a une racine $a \in A$, alors $P = (X-a)Q$ où $\deg Q = n-1$. Soit b une racine distincte de a, alors $P(b) = (b-a)Q(b) = 0$ donc $Q(b) = 0$, car A est intègre. P a donc au plus $(n-1)$ racines distinctes de a et donc au plus n racines distinctes.
CQFD

Remarque 4.20. *Ce résultat est faux si A n'est pas intègre :*
dans l'anneau $\mathbf{Z}/8\mathbf{Z}[X]$, le polynôme X^2-1 a 4 racines : $\{\pm 1, \pm 3\}$.

Ce résultat est faux si A n'est pas commutatif :
par exemple, dans le corps des quaternions $\mathbb{H}$, le polynôme X^4-1 a au moins 8 racines : c'est le groupe $\mathbb{H}_8$.
On déduit un résultat important :
Théorème 4.21. *Soit K un corps fini commutatif, alors K^* est cyclique.*
Preuve. Dans K^*, l'équation $x^n = 1$ a au plus n solutions. D'après la caractérisation des groupes cycliques (Théorème 3.34), K^* est cyclique. CQFD
Exercice 4.22. *Montrer que n est premier si et seulement si il existe un élément d'ordre $n-1$ dans $(\mathbf{Z}/n\mathbf{Z})^*$.*
Démontrons un résultat plus précis.
Théorème 4.23. *Soit p un nombre premier impair. Alors $(\mathbf{Z}/p^n\mathbf{Z})^*$ est cyclique.*
$(\mathbf{Z}/2^n\mathbf{Z})^* \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{n-2}\mathbf{Z}$, *si $n \geq 2$.*
Preuve. Voir par exemple la démonstration dans [2]. Commençons par remarquer que pour p premier, et $1 \leq k \leq p-1$, on a $p|\binom{p}{k}$. En effet, en notant que $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$, on déduit que p divise $k\binom{p}{k}$. Mais p premier doit diviser k ou $\binom{p}{k}$, donc p divise $\binom{p}{k}$.
Nous montrons ensuite par récurrence que $(1+p)^{p^k} \simeq 1 + p^{p^{k+1}} \pmod{p^{k+2}}$, si bien que $a = (1+p)$ est d'ordre p^{n-1} dans $(\mathbf{Z}/p^n\mathbf{Z})^*$.

D'autre part, puisque $p^n\mathbf{Z} \subset p\mathbf{Z}$, il existe un morphisme surjectif φ de $\mathbf{Z}/p^n\mathbf{Z}$ dans $\mathbf{Z}/p\mathbf{Z}$. Soit $b \in \mathbf{Z}/p^n\mathbf{Z}$ tel que $\varphi(b)$ engendre $(\mathbf{Z}/p\mathbf{Z})^*$. Alors b est d'ordre m et $\varphi(b)^m = 1$ donc $m = \lambda p$. On déduit que $b' = b^\lambda$ est d'ordre $p-1$. Ainsi ab' est d'ordre $(p-1)p^{n-1}$ et $\mathbf{Z}/p^n\mathbf{Z}^*$ est cyclique.

Dans le cas où $p = 2$, on montre que $5^{2^k} = 1 + 2^{k+1} \pmod{2^{k+2}}$. Ainsi 5 est d'ordre 2^{n-2} dans $(\mathbf{Z}/2^n\mathbf{Z})^*$. Le groupe $\langle 5 \rangle$ correspond aux éléments $x \equiv 1 \pmod 4$ de $(\mathbf{Z}/2^n\mathbf{Z})^*$. Tout élément de $(\mathbf{Z}/2^n\mathbf{Z})^*$ s'écrit alors $\pm 5^k$ si bien que

$$(\mathbf{Z}/2^n\mathbf{Z})^* = \{-1,1\} \cdot \langle 5 \rangle \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2^{n-2}\mathbf{Z}.$$

CQFD

Corollaire 4.24. *Le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique si et seulement si $n = 2,4$ ou $n = p^k$ ou $2p^k$ si p est un nombre premier impair.*

Preuve. Supposons que $n = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ où les p_i sont des nombres premiers impairs et les α_i sont des entiers strictement positifs. On a alors

$$(\mathbf{Z}/n\mathbf{Z})^* \simeq (\mathbf{Z}/2^\alpha\mathbf{Z})^* \times (\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z})^* \times \cdots \times (\mathbf{Z}/p_k^{\alpha_k}\mathbf{Z})^*$$

$(\mathbf{Z}/n\mathbf{Z})^*$ est cyclique si et seulement si tous les groupes $\mathbf{Z}/2^\alpha\mathbf{Z}^*$, $\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z}^*, \ldots, \mathbf{Z}/p_k^{\alpha_k}\mathbf{Z}^*$ sont cycliques et de cardinaux premiers entre-eux deux-à-deux. On doit donc avoir $k \leq 1$. Si $k = 0$, on doit avoir $\alpha \leq 2$, sinon si $k = 1$ on doit avoir $\alpha \leq 1$. CQFD

4.3 Opérations sur les idéaux

On note $(a) = a \cdot A$, l'*idéal engendré* par $a \in A$. On dira que (a) est *principal* ou *monogène* si les groupes $(A,+)$ et $(aA,+)$ sont isomorphes. Notons que $(a) \subset (b) \Leftrightarrow \mathcal{D}(b) \subset \mathcal{D}(a)$. En particulier $(a) = (b)$ si et seulement si $\mathcal{D}(a) = \mathcal{D}(b)$ c'est-à-dire, $a \sim b$.

Un idéal I est dit *premier* si $I \neq A$ et $xy \in A \Rightarrow x \in A$ ou $y \in A$. Un idéal I est donc premier si et seulement si A/I est intègre.

Un idéal I est dit *maximal* si I est propre et si pour tout idéal J contenant I, on a $J = A$. Un idéal I est maximal si et seulement si A/I est un corps. En effet, les idéaux de A/I sont les J/I où J est un idéal de A contenant I.

Une intersection d'idéaux est un idéal. L'idéal engendré par une partie $S \subset A$ est le plus petit idéal de A contenant S. C'est l'intersection des idéaux contenant S.
La somme $I + J = \{x+y, (x,y) \in I \times J\}$ est un idéal de A.

Théorème 4.25 (Troisième théorème d'isomorphisme)**.** *Soit A un anneau commutatif et I et J des idéaux de A. Alors $A/(I+J) \simeq (A/I)/(I+J/I) \simeq (A/I)/(J/I)$*

Preuve. Ici $I+J$ est un idéal contenant I. Le groupe quotient $(I+J)/I$ est un idéal de A/I. On a aussi $(I+J)/I = J/I = \{\pi_I(x), x \in J\}$ CQFD

Le produit IJ des deux idéaux I et J est l'idéal engendré par les produits xy d'éléments de I et J. IJ est un idéal et on a $IJ \subset I \cap J$.

Définition 4.26. *Deux idéaux I et J sont dits premiers entre-eux si et seulement si $I + J = A$.*

Lemme 4.27. *Si $I + J = A$, alors $IJ = I \cap J$. Si $I + J = A$ et $I + J' = A$ alors $I + JJ' = A$ et pour tout $n, m > 0$, $I^n + J^m = A$.*

Preuve. Il suffit de montrer que $I \cap J \subset IJ$. Soit $(i,j) \in I \times J$, tels que $1_A = i + j$. Si $z \in I \cap J$ alors $z = z(i+j) = iz + zj \in IJ$
Si de plus $I + J' = A$, alors il existe $(i', j') \in I \times J'$, tels que $i + j = i' + j' = 1_A$. Mais alors

$$1 = (i+j)(i'+j') = \underbrace{ii' + i'j + ij'}_{\in I} + \underbrace{jj'}_{\in JJ'}$$

et $A = I + JJ'$. CQFD

Théorème 4.28 (Théorème Chinois)**.** *Soit $I_1, \ldots, I_n$ des idéaux de A, premiers entre-eux deux à deux. Alors l'application $\varphi : A/I_1 \cdots I_n \to A/I_1 \times \cdots \times A/I_n$ est un isomorphisme d'anneaux.*

On montre par récurrence sur $1 \leq k \leq n-1$ que $I_n + I_1 \cdots I_k = A$ et donc que I_n et $I_1 \cdots I_{n-1}$ sont premiers entre-eux.

Il suffit alors de montrer que $A/IJ \simeq A/I \times A/J$ si $I+J=A$. Posons $\varphi : A \to A/I \times A/J, \varphi(x) = (x+I, x+J)$. φ est un homomorphisme de noyau $\operatorname{Ker}\varphi = I \cap J = IJ$. Puisque $I+J=A$ alors $1 = i+j$ où $i \in I$ et $j \in J$. Mais alors $\varphi(jx+iy) = (x+I, y+J)$ donc φ est surjective. Finalement il existe un isomorphisme $\overline{\varphi}$ entre A/IJ et $A/I \times A/J$, d'après le théorème d'isomorphisme 4.10. CQFD

4.4 Anneaux principaux

On dira que a est *irréductible* si et seulement si $(a = bc \Rightarrow a \sim b$ ou $a \sim c)$. a est donc irréductible si et seulement si (a) est un idéal maximal parmi les idéaux principaux.
On dira que p est *premier* si et seulement si $(p|bc) \Rightarrow p|b$ ou $p|c$. L'idéal (p) est donc premier si et seulement si p est premier.

Lemme 4.29. *Lorsque p est premier alors p est irréductible.*

Preuve. Si p est premier et $p = bc$, alors p divise b (ou c). Dans ce cas, b divise p et $b \sim p$. CQFD

Si l'idéal (p) est maximal alors p est irréductible. La réciproque est fausse puisque $\langle X \rangle \subset \langle 2, X \rangle \neq \mathbf{Z}[X]$ et pourtant X est irréductible dans $\mathbf{Z}[X]$, pour une question de degré.

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

Proposition 4.30. *Soit a et b des éléments d'un anneau A principal. a et b ont un pgcd d et un ppcm N. On a*

$$(a)+(b) = (d), \quad (a)\cdot(b) = (ab), \quad (a)\cap(b) = (N).$$

Du plus il existe un couple $(u,v) \in A^2$ tel que $d = au + bv$.

Preuve. Si A est principal alors l'idéal $(a)+(b)$ est principal et $(a)+(b) = (d)$. On déduit que $\delta \in \mathcal{D}(a) \cap \mathcal{D}(b) \Leftrightarrow (a)+(b) \subset (\delta) \Leftrightarrow \delta \in \mathcal{D}(d)$. d est donc un diviseur de a et de b et tout diviseur commun de a et de b est un diviseur de d. Autrement dit, d est un $\operatorname{pgcd}(a,b)$. Le pgcd est donc défini à une unité près. Comme $d \in (a)+(b)$ alors on déduit l'identité de Bézout : il existe $u, v \in A$, tels que $d = au + bv$.

L'idéal $(a)\cdot(b)$ est engendré par les produits de multiples de a et de b. On a donc $(a)\cdot(b) = (ab)$.

Lorsque A est principal, l'idéal $(a)\cap(b) = (N)$ est formé des multiples communs de a et de b. On déduit que $a, b \in \mathcal{D}(\delta) \Leftrightarrow N \in \mathcal{D}(\delta)$. N est un ppcm de a et de b. CQFD

Lorsque A est principal, les notions d'idéal premier et maximal coïncident.

Lemme 4.31. *Si A est principal, alors p est irréductible si et seulement si p est premier.*

Preuve. On sait qu'un premier p est irréductible (lemme 4.29). Si A est principal et $p \in A$ est irréductible. Supposons que $p|bc$, donc $bc = px$. L'idéal (b,p) est principal engendré par un élément q. On a $p = \lambda q$ donc $\lambda \sim p$ et q est une unité ou $q \sim p$ et λ est une unité. Si q est une unité, alors $(b,p) = (b)+(p) = A$ et on peut écrire une relation de Bézout : $bu + pv = 1$. Mais alors $c = bcu + pcv = p(xu + cv)$ donc p divise c. Si λ est un unité, alors $(b,p) = (q) = (p)$ donc p divise b. CQFD

Lemme 4.32 (Lemme de Gauss)**.** *Soit A un anneau principal. Alors $(a,b) = 1$ et $a|bc$ implique $a|c$.*

Corollaire 4.33. *Soit a, b deux entiers divisant c. Si $(a,b) = 1$ alors ab divise c.*

Les démonstrations sont similaires au cas où $A = \mathbf{Z}$, Lemme 2.7 et Corollaire 2.8.

4.5 Anneaux euclidiens

On dira que A est euclidien si il existe un algorithme (ou un stathme) euclidien $N : A - \{0\} \to \mathbf{N}$, tel que pour tout $a \in A$ et $b \in A - \{0\}$, on a $a = bq + r$ avec $r = 0$ ou $N(r) < N(b)$.

Exemple 4.34. $\mathbf{Z}$ *est euclidien avec $N(x) = |x|$.* $\mathbf{K}[X]$ *est euclidien avec $N(P) = \deg P$ (voir théorème 4.36).*
Un corps $\mathbf{K}$ *est un anneau euclidien, en considérant le stathme $d(a) = 0$ si $a \in K^*$ et $d(0) = -\infty$. L'anneau* $\mathbf{Z}[i]$ *est un anneau euclidien mais* $\mathbf{Z}[i\sqrt{3}]$ *n'est pas euclidien.*

Théorème 4.35. *Si A est euclidien alors A est principal.*

Preuve. Soit I un idéal de A. Si $I \neq \{0\}$, $N(I-\{0\})$ est une partie de $\mathbf{N}$ non vide donc admet un plus petit élément n_0. Soit $b \in I$, tel que $N(b) = n_0$. Alors si $a \in I$, effectuons la division euclidienne $a = bq + r$. $r \in I$ vérifie $N(r) < N(b)$ donc $r = 0$. On déduit que $b|a$ et $I \subset (b) \subset I$. CQFD

Algorithme d'Euclide

Lorsque A est euclidien, on calculera le pgcd de a et de b par l'algorithme d'Euclide. On définit $r_0 = a$ et $r_1 = b$ puis r_{i+1} comme le reste de la division euclidienne de r_{i-1} par r_i si r_i est nul et $r_{i+1} = r_i = 0$ sinon. Alors la suite $N(r_i)$ étant strictement décroissante pour $i \geq 2$, on déduit qu'il existe un dernier reste non nul $r_n = d$ dans cette suite et on a $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(d)$.
De manière similaire, on calculera des coefficients de Bézout en utilisant l'algorithme d'Euclide étendu :

Partant de

$$r_0 = a, \quad u_0 = 1, \quad v_0 = 0, \quad r_1 = b, \quad u_1 = 0, \quad v_1 = 1.$$

Tant que $r_i \neq 0$, on calcule (q_i, r_{i+1}) en effectuant la division euclidienne $r_{i-1} = r_i q_i + r_{i+1}$ et on pose

$$\text{Si } r_i \neq 0 : r_{i+1} = r_{i-1} - q_i r_i, \quad u_{i+1} = u_{i-1} - q_i u_i, \quad v_{i+1} = v_{i-1} - q_i v_i,$$

Alors, à chaque étape, on a $r_i = u_i a + v_i b$, et en particulier il existe $u, v \in A^2$ tels que $au + bv = d$.
On a alors $(a,b) = (d)$ et d est un pgcd de a et de b. Lorsque $d \in U(A)$, on dira que a et b sont étrangers ou premiers entre-eux.

$K[X]$ est euclidien

Lorsque K est un corps, l'anneau $K[X]$ est euclidien.
Théorème 4.36 (Division euclidienne)**.** *Pour tout $(A,B) \in \mathbf{K}[X]^2$, $B \neq 0$, il existe un couple unique $(Q,R) \in \mathbf{K}[X]^2$ tel que*

$$A = BQ + R, \text{ avec } R = 0 \text{ ou } \deg R < \deg B.$$

Preuve. On peut toujours écrire $A = B \cdot 0 + A$. Parmi toutes les écritures de la forme $A = B \cdot Q + R$, considérons une où $\deg R$ est minimal. Remarquons que $\overline{R} = \overline{A} \pmod{B}$. Soit donc R, de degré minimal, tel que $A = B \cdot Q + R$ et supposons que $\deg R \geq \deg B$. Écrivons $B = b_m X^m + \cdots + b_0$ et $R = r_{m'} X^{m'} + \cdots + r_0$. b_m étant inversible, on peut écrire

$$A = B \cdot (Q - (b_m)^{-1} r_{m'} X^{m'-m}) + (R - (b_m)^{-1} r_{m'} X^{m'-m}) = B \cdot \widetilde{Q} + \widetilde{R},$$

où $\deg \widetilde{R} < \deg R$, d'où une contradiction. On a donc l'existence de (Q,R), tels que $A = BQ + R$ et $\deg R < \deg B$.
Supposons que $A = BQ + R = BQ' + R'$ avec $\deg R, \deg R' < m$. Alors B divise $R - R'$ donc $R = R'$. CQFD
Remarque 4.37. *Si $\mathbf{K}$ n'est plus un corps, il suffit que B ait un coefficient dominant inversible pour pouvoir effectuer la division euclidienne.*
On déduit de ce fait que $\mathbf{K}[X]$ est principal (théorème 4.35). Réciproquement
Théorème 4.38. *Soit A un anneau intègre commutatif, alors $A[X]$ est principal si et seulement si A est un corps.*
Preuve. Si A est un corps alors $A[X]$ est euclidien donc principal. Si $A[X]$ est principal, alors X est irréductible (car de degré 1) et premier (car $A[X]$ est principal). $\langle X \rangle$ est maximal car si $\langle X \rangle \subset \langle P \rangle$, alors P divise X et X n'est pas associé à P donc $P \in A^*$ et $\langle P \rangle = A[X]$. $\langle X \rangle$ est donc un idéal maximal et $A[X]/\langle X \rangle \simeq A$ est un corps. CQFD

4.6 Anneau factoriel

Nous avons vu que $\mathbf{Z}$ est un anneau factoriel.
Définition 4.39. *On dira que A est factoriel si tout élément admet une décomposition unique en produit d'irréductibles. Autrement dit, si $a \in A - \{0\}$, il existe $p_1, \ldots, p_r \in A$, irréductibles, tels que $a = p_1 \cdots p_r$. Si $a = p_1 \cdots p_r = q_1 \cdots q_s$, alors $r = s$ et il existe une permutation $\sigma \in \Sigma_s$, telle que $p_i = u_i q_{\sigma(i)}$, pour tout $1 \leq i \leq s$ et $u_i \in U(A)$.*

Théorème 4.40. *Si A est principal alors A est factoriel.*
Preuve. Supposons qu'il existe $a \in A$ qui n'admette pas de décomposition en produits d'irréductibles. Alors on peut écrire $a = a_1 b_1$ où ni a_1, ni b_1 ne soit une unité. Mais alors a_1 non plus ne se décompose pas et on obtient $a_1 = a_2 b_2$, etc. Au final on écrira $a = a_1 b_1$ et $a_i = a_{i+1} b_{i+1}$ où a_{i+1} est un diviseur propre de a_i et n'admet pas de décomposition. L'idéal $I = \bigcup_{i \geq 1} (a_i)$ est principal engendré par b. Donc $b \in (a_{i_0})$ et $(b) \subset (a_{i_0}) = (a_{i_0+1})$ ce qui fait que $b_{i_0+1} \in U(A)$ et une contradiction.
Si $p_1 \cdots p_r = q_1 \cdots q_s$. Démontrons le résultat par récurrence sur r. Si $p_1 = q_1 \cdots q_s$, alors p_1 irréductible divise un des q_i, par exemple q_1 et q_1 divise p_1 donc $p_1 \sim q_1$ et on a $u = q_2 \cdots q_s \in U(A)$ donc $s = 1$ et $p_1 = q_1$. Sinon, si $r > 1$, alors p_1 irréductible donc premier divise un des q_i, appelons le q_1. Mais alors, puisque q_1 est irréductible, on a $p_1 = u q_1 \sim q_1$ et $p_2 \cdots p_r = q_2 \cdots q_s$, quitte à changer q_2 en $u q_2$. On conclut par hypothèse de récurrence. CQFD

En résumé, nous avons donc vu que

$$A \text{ euclidien } \Rightarrow A \text{ principal } \Rightarrow A \text{ factoriel}$$

Notons que dans un anneau factoriel, les éléments irréductibles et premier coïncident.
Exemple 4.41. [L'anneau $\mathbf{Z}[i\sqrt{3}]$
On vérifie que $\mathbf{Z}[i\sqrt{3}] = \{a + ib\sqrt{3}, a, b, \in \mathbf{Z}\}$ *est un sous-anneau de* $\mathbf{C}$ *contenant* $i\sqrt{3}$.
L'application norme N *définie par* $N(z) = |z\bar{z}|$ *vérifie* $N(zz') = N(z)N(z')$.
On vérifie que z est inversible dans $\mathbf{Z}[i\sqrt{3}]$ *si et seulement si* $N(z) = 1$. *Dans ce cas, on a* $z^{-1} = \bar{z}$. *Les inversibles* $z = a + ib$ *vérifient donc* $a^2 + 3b^2 = 1$ *On déduit que* $(\mathbf{Z}[i\sqrt{3}])^* = \{-1, 1\}$.
Nous remarquons alors qu'il n'y a pas d'élément de norme 2 *car* $a^2 + 3b^2 = 2$ *n'a pas de solution dans* $\mathbf{Z}^2$. *(car* $\sqrt{2}$*) est irrationnel).*
On remarque que $4 = 2 \cdot 2 = (1 + i\sqrt{3}) \cdot (1 - i\sqrt{3})$. *Les éléments* 2 *et* $1 \pm i\sqrt{3}$ *sont irréductibles car ils sont de norme 4, et ne sont pas associés, car ils ne sont pas opposé ni égaux. Ainsi* $1 + i\sqrt{3}$ *est irréductible mais n'est pas premier, car il divise* 2×2 *sans diviser* 2.
$\mathbf{Z}[i\sqrt{3}]$ *est donc un exemple d'anneau non factoriel.* $1 + i\sqrt{3}$ *est un exemple d'élément irréductible non premier.*

Lorsque A est factoriel on peut définir un pgcd et un ppcm de deux éléments a et b de A. Si $a = p_1 \cdots p_s$ et $b = q_1 \cdots q_s$, on peut écrire, en considérant pour chaque des p irréductibles associés, intervenant dans la décomposition de a et de b, un représentant unique $\widetilde{p}$, que $a = \varepsilon \widetilde{p_1}^{n_1} \cdots \widetilde{p_k}^{n_k}$ et $b = \varepsilon' \widetilde{p_1}^{m_1} \cdots \widetilde{p_k}^{m_k}$. Alors $d = \widetilde{p_1}^{\min(n_1,m_1)} \cdots \widetilde{p_k}^{\min(n_k,m_k)}$ est un pgcd de a et de b. On a bien sûr $(a,b) \subset (d)$, mais si de plus A est principal alors $(a,b) = (d)$. En revanche, dans l'anneau $\mathbf{Z}[X]$, l'idéal $(2,X)$ n'est pas principal et est différent de A tandis que $\text{pgcd}(2,X) = 1$. $N = \widetilde{p_1}^{\max(n_1,m_1)} \cdots \widetilde{p_k}^{\max(n_k,m_k)}$ est un ppcm de a et de b. Néanmoins, lorsque l'anneau n'est pas principal, il n'est pas toujours possible d'avoir une relation de Bézout entre deux éléments étrangers.

Corps des fractions

Si A est un anneau intègre commutatif, nous définissons le corps de fractions de la façon suivante.
Sur $A \times A - \{0\}$, on définit la relation d'équivalence

$$(a,b) \simeq (a',b') \Leftrightarrow ab' = a'b$$

$\text{Frac}(A)$ est l'ensemble des classes d'équivalences. On notera $\pi((a,b)) = \frac{a}{b}$ la classe d'équivalence de (a,b). On vérifie que si on définit

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

alors $\text{Frac}(A)$ est appelé le corps des fractions de A. En identifiant $a \in A$ et $\dfrac{a}{1_A}$, $\text{Frac}(A)$ est un corps contenant A.
Lorsque A est factoriel, alors tout élément de $K = \text{Frac}(A)$ se décompose de façon unique $z = \varepsilon p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ ou les α_i sont des entiers relatifs non nuls.

L'anneau $\mathbf{Z}[i]$

L'ensemble des $\{a+bi, a,b \in \mathbf{Z}\}$ est un sous-anneau de $\mathbf{C}$ contenant i. C'est donc $\mathbf{Z}[i]$. Le corps des fractions de $\mathbf{Z}[i]$ contient $\mathbf{Z}$ donc $\mathbf{Q}$et contient i donc contient $\mathbf{Q}[i]$. En utilisant le fait que $z^{-1} = \dfrac{\overline{z}}{|z|^2}$, on déduit que $\mathbf{Q}[i] = \{a+ib, a,b, \in \mathbf{Q}\}$ est le corps de fractions de $\mathbf{Z}[i]$.

$\mathbf{Z}[i]$ est euclidien

Soit $a = x_1 + iy_1$ et $b = x_2 + iy_2 \neq 0$, deux éléments de $\mathbf{Z}[i]$. Alors

$$\frac{a}{b} = \frac{x_1+iy_1}{x_2+iy_2} = \frac{1}{x_2^2+y_2^2}\Big[(x_1x_2+y_1y_2)+i(x_2y_1-x_1y_2)\Big] = x+iy \in \mathbf{Q}[i]$$

x et y étant rationnels, il existe des entiers n et m tels que $|n-x| \leq \frac{1}{2}$ et $|m-y| \leq \frac{1}{2}$, ainsi

$$|a/b-(n+im)|^2 = (n-x)^2+(m-y)^2 \leq \tfrac{1}{2}.$$

Posons $q = n+im$, il vient $|a-bq| \leq \frac{1}{\sqrt{2}}|b| < |b|$. Ainsi $\mathbf{Z}[i]$ est euclidien pour le stathme $z \mapsto |z|$.

5 L'algèbre $\mathbf{K}[X]$

Lorsque $\mathbf{K}$ est un corps commutatif, $\mathbf{K}[X]$ est une $\mathbf{K}$-algèbre, c'est-à-dire, est un anneau commutatif unitaire et intègre, et un $\mathbf{K}$-espace vectoriel.

$\mathbf{K}[X]$ est un anneau euclidien, d'après le théorème 4.36, donc principal et factoriel.

Un polynôme non nul P de degré ≥ 1 est dit *irréductible*, s'il n'a pas de diviseur propre. Les polynômes unitaires irréductibles sont, pour $\mathbf{K}[X]$, l'*analogue* des nombres premiers pour $\mathbf{Z}$. Un polynôme irréductible est associé à un unique polynôme irréductible unitaire.

Tout élément s'écrit de façon unique (aux unités près) comme le produit de facteurs irréductibles

Théorème 5.1. *Soit $P \in \mathbf{K}[X]$, $P \neq 0$, alors P s'écrit de façon unique (à l'ordre près)*

$$P = \lambda P_1^{n_1} \dots P_r^{n_r}$$

où $\lambda \in K^*$, les P_i sont unitaires et irréductibles, distincts deux à deux, et $n_i \in \mathbf{N}^*$.

Algorithme d'Euclide (étendu)

Soit A et B deux polynômes non nuls, $\deg A \geq \deg B$. On cherche leurs diviseurs communs (et donc leur PGCD). On pose $R_0 = A, R_1 = B$ et on fait les divisions euclidiennes successives

$$\begin{array}{rcll} A & = & BQ_1+R_2, & \deg R_2 < \deg B \\ B & = & R_2Q_2+R_3, & \deg R_3 < \deg R_2 \\ R_2 & = & R_3Q_3+R_4, & \deg R_4 < \deg R_3 \\ & \vdots & & \vdots \\ R_{n-1} & = & R_nQ_n+0 & \end{array}$$

La suite des restes (R_k) étant une suite de polynômes dont les degrés forment une suite strictement décroissante, on obtient un reste nul au bout d'un nombre fini de divisions.
Les diviseurs communs de A et de B sont les diviseurs communs de R_k et R_{k+1} donc l'ensemble des diviseurs du dernier reste non nul : R_n. Le PGCD de A et B est donc le dernier reste non nul R_n rendu unitaire. On déduit alors

Proposition 5.2. *Soit A et B deux polynômes non nuls. A et B ont un* pgcd *D et on a : $D|A, D|B$ et tout diviseur commun de A et de B est un diviseur de D.*

De la même façon que pour le calcul de pgcd de deux entiers relatifs, nous définissons l'algorithme d'Euclide étendu : soit $R_0 = A$, $R_1 = B$, posons $U_0 = 1$, $U_1 = 0$, $V_0 = 0$, $V_0 = 1$.
Nous calculons successivement $Q_i = R_{i-1} \div R_i$, puis $R_{i+1} := R_{i-1} \pmod{R_i} = R_{i-1} - R_i Q_i$. En posant $U_{i+1} = U_{i-1} - U_i Q_i, V_{i+1} = V_{i-1} - V_i Q_i$, nous obtenons à chaque étape $R_i = U_i A + V_i B$.

Théorème 5.3 (Identité de Bézout)**.** *Soit $(P,Q) \in \mathbf{K}[X]^2$, non nuls. Alors $P \wedge Q = D$ existe et*

$$\text{il existe } (U,V) \in \mathbf{K}[X]^2,\ PU + QV = D\,.$$

On déduit des propriétés générales des anneaux euclidiens et de la définition des polynômes irréductibles (qui sont également premiers) :

Corollaire 5.4.

1. $(P \wedge Q) | D \iff$ *il existe* $(U,V) \in \mathbf{K}[X]^2,\ PU + QV = D\,.$
2. *Lemme de Gauss :* $A|BC$ *et* $A \wedge B = 1 \Rightarrow A|C\,.$
3. *Si P est irréductible et* $P|AB$*, alors* $P|A$ *ou* $P|B$*.*
4. *si* $A \wedge B = 1$ *et si* $A|C$ *et* $B|C$*, alors* $AB|C$*.*

5.1 Quotient de $\mathbf{K}[X]$

Soit $P \in \mathbf{K}[X]$. $\langle P \rangle = P\mathbf{K}[X] = \{PQ,\ Q \in \mathbf{K}[X]\}$ est un idéal de $\mathbf{K}[X]$ et réciproquement, tout idéal est engendré par un polynôme unitaire. Les idéaux de $\mathbf{K}[X]$ sont aussi des sous $\mathbf{K}$-espaces vectoriels de $\mathbf{K}[X]$.
On notera $\overline{A} = A \pmod{P} = A + \langle P \rangle$, un élément de $\mathbf{K}[X]/\langle P \rangle$.

Proposition 5.5. $\mathbf{K}[X]/\langle P \rangle$ *est une K-algèbre*

Preuve. On sait que $\mathbf{K}[X]/\langle P \rangle$ est un anneau commutatif. $\langle P \rangle$ étant un sous-espace vectoriel de $\mathbf{K}[X]$, $\mathbf{K}[X]/\langle P \rangle$ a une structure d'espace vectoriel quotient. En effet, si F est un sous-espace vectoriel de E, E/F est un groupe additif.
Pour $\lambda \in \mathbf{K}$, on considère le morphisme $m_\lambda : x \in E \mapsto (\lambda.x) + F \in E/F$. m_λ est un morphisme de groupe et $\operatorname{Ker} m_\lambda$ contient F. On peut passer au quotient et on obtient un morphisme $\tilde{m}_\lambda \in \operatorname{Hom}(E/F)$. Ceci définit une multiplication externe $(\lambda, x+F) \mapsto \lambda.(x+F) = \tilde{m}_\lambda(x+F)$, qui vérifie tous les axiomes de la multiplication par un scalaire $\lambda \in K$ et confère à E/F une structure d'*espace vectoriel quotient*. □

On a alors, si $\deg P = m$,

$$\mathbf{K}[X]/\langle P \rangle = \{\overline{A},\ A \in \mathbf{K}[X]\} = \{\overline{A},\ A \in \mathbf{K}[X]\,;\, \deg A < m\}.$$

En notant $\alpha := \overline{X}$ dans $\mathbf{K}[X]/\langle P \rangle$, on a

$$\mathbf{K}[X]/\langle P \rangle = \{c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1},\ c_i \in \mathbf{K}\}\,.$$

On écrira $\mathbf{K}[X]/\langle P \rangle = \mathbf{K}[\alpha]$ avec la condition $P(\alpha) = 0$.

Proposition 5.6. $(\mathbf{K}[X]/\langle P \rangle, +, *, .{}_K)$ *est une* $\mathbf{K}$*-algèbre. Si* $\deg P = m$*, alors* $(1, \overline{X}, \cdots, \overline{X}^{m-1})$ *est une base.*
Preuve. Si $A \in \mathbf{K}[X]$, alors $\overline{A} = \overline{R}$, où $A = BQ + R$ et $\deg R < \deg P = m$ donc $\overline{A} \in \operatorname{Vect}(1, \alpha, \ldots, \alpha^{m-1})$. Si $a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} = 0$ alors le polynôme $A = a_0 + a_1 X + \cdots + a_{m-1}X^{m-1} \equiv 0 \pmod{P}$ donc P divise A et $A = 0$ car $\deg A < \deg P$. CQFD

Corollaire 5.7. *Soit* $\mathbf{K}$ *un corps fini ayant q éléments et* $P \in \mathbf{K}[X]$ *un polynôme unitaire de degré* $m \geq 1$*. Alors* $|\mathbf{K}[X]/\langle P \rangle| = q^m\,.$
Preuve. $\mathbf{K}[X]/\langle P \rangle \simeq \mathbf{K}^m$. CQFD
D'après l'identité de Bézout, les inversibles de $\mathbf{K}[X]/\langle P \rangle$ sont les $Q \pmod{P}$ tels que $(P,Q) = 1$.

Théorème 5.8. *Soit* $\mathbf{K}$ *un corps et* $P \in \mathbf{K}[X]$ *un polynôme unitaire de degré* ≥ 1*. Alors* $\mathbf{K}[X]/\langle P \rangle$ *est un corps si et seulement si P est irréductible dans* $\mathbf{K}[X]$*.*
Preuve. $P = P_1 P_2 \Leftrightarrow \overline{P_1 P_2} = \overline{O}$. CQFD

Corollaire 5.9. *Soit* $\mathbf{K}$ *un corps fini ayant q éléments et* $P \in \mathbf{K}[X]$ *un polynôme unitaire irréductible de degré* $m \geq 1$*. Alors* $\mathbf{K}[X]/\langle P \rangle$ *est un corps fini ayant* q^m *éléments.*

Exemple 5.10. *On pourra vérifier que*

$$\mathbf{F}_2[X]/\langle X^3+X+1\rangle = \{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\}$$

est un corps ayant 8 *éléments et que*

$$\mathbf{F}_3[X]/\langle X^2+1\rangle = \{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}$$

est un corps ayant 9 *éléments.*

En effet, le polynôme X^3+X+1 est irréductible dans $\mathbf{F}_2[X]$ car il n'a pas de racine et donc pas de facteur de degré 1. $\mathbf{F}_8 = \mathbf{F}_2[X]/\langle X^3+X+1\rangle$ est donc un corps à 8 éléments, de base $(1,x,x^2)$ ou $x=\overline{X}$. Notons que $x \in \mathbf{F}_8^*$ est donc d'ordre 7. On vérifie que $x^2=x^2$, $x^3=x+1$, $x^4=x^2+x$, $x^5=x^3+x^2=x^2+x+1$, $x^6=x^2+1$, $x^7=1$.

Le polynôme X^2+1 est irréductible dans $\mathbf{F}3[X]$. Ainsi $\mathbf{F}_9 = \mathbf{F}_3[X]/\langle X^2+1\rangle$ est un corps à 9 éléments, de base $(1,x)$. Remarquons que $x^2=-1$ donc $x^4=1$ et x est d'ordre 4. Mais $\mathbf{F}_9^*$ a exactement 2 éléments d'ordre 4 : x et x^3, 1 élément d'ordre 2 : x^2, un élément d'ordre 1 : 1. Tous les autres sont d'ordre 8. Par exemple $x+1$ est d'ordre 8, car $(x+1)^2=-x$, donc $(x+1)^4=x^2=-1$. D'ailleurs $x+1$ est annulé par $(X-1)^2+1=X^2+X+2$, également irréductible.

5.2 Théorème chinois pour les algèbres quotients $\mathbf{K}[X]/\langle P\rangle$

Lorsque P_1 et P_2 sont premiers entre-eux alors les idéaux (P_1) et (P_2) sont premiers entre-eux. On a

Théorème 5.11 (Théorème chinois)**.** *Soit* **K** *un corps et $P_1, P_2 \in \mathbf{K}[X]$ deux polynômes premiers entre eux. Alors l'application*

$$\begin{array}{rcl} \mathbf{K}[X]/\langle P_1P_2\rangle & \stackrel{\varphi}{\to} & \mathbf{K}[X]/\langle P_1\rangle \times \mathbf{K}[X]/\langle P_2\rangle \\ Q \pmod{P_1P_2} & \mapsto & [Q \pmod{P_1}, Q \pmod{P_2}] \end{array}$$

est un isomorphisme de **K***-algèbres (morphisme d'anneaux et application linéaire bijective).*

Un cas particulier très intéressant, lorsque $P_i = X-a_i, i=0,\ldots,n$.

$$\mathbf{K}_{\leq n}[X] \simeq \mathbf{K}[X] \,/\, \langle \prod_{i=1}^{n}(X-a_i)\rangle \simeq \prod_{i=1}^{n}\mathbf{K}[X]/(X-a_i).$$

On obtient l'isomorphisme $\begin{array}{rcl} \mathbf{K}_{\leq n}[X] & \to & \mathbf{K}^{n+1} \\ P & \mapsto & (P(a_0),\ldots,P(a_n)) \end{array}$ et sa réciproque $\begin{array}{rcl} \mathbf{K}^{n+1} & \to & \mathbf{K}_{\leq n}[X] \\ (y_0,\ldots,y_n) & \mapsto & \sum_{i=0}^{n} y_iL_i \end{array}$ où

les $L_i = \dfrac{\prod_{j\neq i}(X-a_j)}{\prod_{j\neq i}(a_i-a_j)}$ vérifient $L_i(a_j)=\delta_{i,j}$. Les L_i s'appellent les *polynômes d'interpolation de Lagrange*.

Un cas particulier sera étudié lorsque $P = X^n-1 = \prod_{k=0}^{n-1}(X-w^i)$, donnant lieu à la transformation de Fourier.

Bibliographie

[1] A. Chambert-Loir. *Algèbre corporelle*. École polytechnique : Mathématiques. École Polytechnique, 2005.

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

[3] D. E. Knuth. *The Art of Computer Programming, volume 2*. Addison-Wesley, 1997.

[4] A. Kraus. *Arithmétique, 2M220*. L2 Mathématiques, UPMC, 2016. [PDF].

[5] L3 Mathématiques, Sorbonne Université. *ALGÈBRE 1 (ENS, PREMIÈRE ANNÉE)*, 2023. Site Web.

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

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

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

[9] P. Wassef. *Arithmétique : application aux codes correcteurs et à la cryptographie : cours et 122 exercices corrigés : licence de mathématiques*. Vuibert, 2008.

[10] L. Zapponi. *Cryptologie algébrique*. M1 Mathématiques, UPMC, 2024. Site Web.