Algèbre et mathématiques discrètes

Jiang Zeng

Institut Camille Jordan, UCBL
Email : zeng@math.univ-lyon1.fr

4 novembre 2020

Table des matières

Chapitre 1

Introduction

Résumé

I. Ensembles. II. Cardinaux des ensembles finis. Combinatoire élémentaire. III. Ensembles infinis, dénombrables, exemples de $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

1.1 Ensembles

La notion d'ensemble joue un rôle fondamental en mathématiques modernes. Nous n'avons pas l'intention de présenter ici une théorie mathématique rigoureuse et complète. Il faudrait pour cela des prérequis de logique, un appareillage complexe, choisir entre différentes axiomatiques... Nous nous bornerons à une partie de la « théorie naïve des ensembles ».

Définition 1.1.1. *Un ensemble est une collection d'objets issus de notre perception ou de notre pensée, tous déterminés et distincts. Ces objets s'appellent* éléments de l'ensemble.

On utilise les lettres $a, b, c, \ldots$ pour désigner des éléments d'un ensemble, les lettres $A, B, C, \ldots$ pour désigner des ensembles. Si a est un élément de A on écrit $a \in A$ et $b \notin M$ signifie que b n'est pas un élément de M.

Certains ensembles particulièrement importants ont une notation symbolisée. Ainsi les symboles $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont utilisées pour représenter respectivement les ensembles des nombres naturels, entiers relatifs, rationnels, réels, complexes.

Définition 1.1.2. *Deux ensembles sont dits* égaux *s'ils contiennent exactement les mêmes éléments,* $A = B \iff \forall x (x \in A \iff x \in B)$.

On appelle **sous-ensemble** d'un ensemble E, un ensemble F tel que : $\forall x \in F$, $x \in E$, et on écrit $F \subset E$ ou $F \subseteq E$. L'ensemble vide et E lui-même sont des sous-ensebles de E.

L'ordre des éléments n'a donc aucune importance. Ainsi $\{2,3,5,7\} = \{3,5,7,2\}$. La relation d'égalité entre les ensembles est une relation d'équivalence. Une condition irréalisable du type $\{x \,|\, x < 6 \wedge x > 8\}$ induit la notion d'ensemble vide.

Définition 1.1.3. $\emptyset = \{x \mid x \neq x\}$.

Il est bien connu que considérer l'ensemble de tous les ensembles conduit au *paradoxe du Roussell*. Supposons que E est l'ensemble de tous les ensembles. On peut alors considérer l'ensemble $A = \{x \in E | x \notin x\}$. Alors $A \in A \Longleftrightarrow A \notin A$.

Si A et B sont deux ensembles, on définit leur union $A \cup B$ et leur intersection $A \cap B$ par

$$A \cup B = \{x \mid x \in A \vee x \in B\} \quad A \cap B = \{x \mid x \in A \wedge x \in B\}.$$

On définit la différence ensembliste

$$A \setminus B = \{x \in A \mid x \notin B\}.$$

On va maintenant définir le couple (a,b) : c'est l'ensemble

$$(a,b) = \{\{a\},\{a,b\}\}.$$

Cela permet d'obtenir l'équivalence :

$$(a,b) = (a',b') \Longleftrightarrow (a = a' \wedge b = b').$$

Ne pas confondre le couple avec l'ensemble (la paire) $\{a,b\}$; avec notre définition, le couple (a,a) désigne l'ensemble $\{\{a\}\}$. Le produit cartésien de deux ensembles est l'ensemble des couples :

$$A \times B = \{(a,b) \mid a \in A \wedge b \in B\}.$$

Définition 1.1.4. *Une relation binaire d'un ensemble A vers un ensemble B est un sous-ensemble de $A \times B$; on écrit $a\mathcal{R}b$ plutôt que $(a,b) \in \mathcal{R}$. Une application de A dans B est une relation f qui vérifie :*

$$\forall a \in A, \quad \exists! b \in B \quad \textit{tel que} \quad a\, f\, b.$$

On peut composer des relations, mais considérons seulement le cas des applications. Si $\mathcal{R}$ et $\mathcal{S}$ sont des applications, de A dans B, resp. de B dans C, alors $\mathcal{S} \circ \mathcal{R}$ est une application définie par :

$$z = \mathcal{S} \circ \mathcal{R}(x) \iff \exists y \in B \qquad y = \mathcal{R}(x) \quad \text{et} \quad z = \mathcal{S}(y).$$

C'est ce qu'on appelle « la loi rond ».

L'ensemble des applications d'un ensemble A dans un ensemble B est noté B^A. On peut alors définir les applications **injective, surjectives et bijectives**.

On appelle famille indexée par un ensemble I, une application de I dans un ensemble A. On note a_i l'omage de $i \in I$ et $(a_i)_{i\in I}$ la famille. Il est possible bien sûr que les a_i soient eux-même des ensembles. Si $(A_i)_{i\in I}$ est une famille d'ensemble, il existe un ensemble qui est la réunion des ensembles A_i ; on le note

$$A = \bigcup_{i\in I} A_i$$

et il est caractérisé par :

$$a \in A \iff \exists i \in I,\ a \in A_i.$$

Si I est de la forme $I = \{i_1, i_2\}$, on retrouve la réunion traditionnelle de deux ensembles. Si I est vide, la réunion est vide. Et si I est non vide, on peut définir l'intersection de la famille :

$$B = \bigcap_{i\in I} A_i$$

caractérisée par :

$$b \in B \iff \forall i \in I,\ b \in A_i.$$

Il y a un peu de subtilité dans ces définitions : l'intersection d'une famille vide $I = $ ne peut être définie sans contradiction, en fait cela dépend de l'ensemble de référence choisi : soit U l'ensemble de référence, i.e., U inclut tous les A_i $(i \in I)$, alors $B = \{x \in U \mid \forall i \in I,\ b \in A_i\}$, donc $B = U$ si $I = \emptyset$ (c'est lié à l'impossibilité d'accepter l'existence de l'ensemble de tous les ensembles) ; bien sûr, l'intersection peut être vide, par exemple quand l'un des A_i est vide, mais pas seulement dans ce cas...

De même qu'on a défini le produit cartésien de deux ensembles, définissons le produit d'une famille par :

$$\prod_{i\in I} A_i = \{f : I \to \bigcup_{i\in I} A_i \mid f(i) \in A_i\}.$$

Se donner un élément de ce produit, c'est finalement se donner une famille, indexée par I, de la forme $(a_i)_{i\in I}$ où $a_i \in A_i$ pour tout $i \in I$, et si I a deux éléments, on retrouve le produit cartésien habituel.

Définition 1.1.5. *Une relation binaire $\sim$ dans E est une relation d'équivalence si elle a les trois propriétés :*

1. $\forall x \in E,\ x \sim x$ *(réflexivité)*
2. $\forall (x, y) \in E \times E \qquad (x \sim y) \implies (y \sim x)$ *(symétrie)*
3. $\forall (x, y, z) \in E^3, \quad (x \sim y \text{ et } y \sim z) \implies (x \sim z)$ *(transitivité).*

Une relation d'équivalence dans E est associée à un regroupement en « classes » de E. Rapeplons : une famille $(E_i)_{i\in I}$ de sous-ensembles de E est une partition de E si :

— $\forall i \in I\ E_i \neq \emptyset$.
— $\bigcup_{i\in I} E_i = E$.
— $\forall i, j \in I,\ (i \neq j) \implies (E_i \cap E_j = \emptyset)$.
À tout $a \in E$, on définit la classe d'équivalence :

$$\bar{a} = \{b \in E \mid b\mathcal{R}a\}$$

et les classes d'équivalence forment une partition de E. On obtient alors la partition associée à une relation d'équivalence par :

$$E/\mathcal{R} = \{\bar{a} \mid a \in E\}.$$

L'ensemble $E/\mathcal{R}$ des classes d'équivalence est appelé l'ensemble quotient de E par $\mathcal{R}$. Cet ensemble est le résultat d'un « processus d'abstraction » : la proriété permettant de construire une classe d'équivalence peut être identifiée à cette classe, les éléments de celle-ci perdent leur originalité propre. Par exemple, la propriéte commune à deux entiers congrus modula 2 est leur « parité », celle commune à deux sous-ensembles équipotents leur « cardinal ».

1.2 Cardinal d'un ensemble fini

Commençons par admettre qu'on a défini l'ensemble des nombres entiers $\mathbb{N}$: cet ensemble contient un élément noté 0 et tout élément n a un successeur, noté $n+1$; deux éléments qui ont même successeur sont égaux, et 0 n'est pas un successeur. De plus, $\mathbb{N}$ a la propriété de récurrence, que l'on peut énoncer ainsi : pour tout $F \subset \mathbb{N}$, on a

$$\begin{cases} 0 \in F \\ \forall n \in F,\ (n \in F \implies n+1 \in F) \end{cases} \implies F = \mathbb{N}.$$

On peut alors définir dans $\mathbb{N}$ l'addition, la multiplication et la relation d'ordre habituellle, que l'on appelle **ordre naturel** et que l'on note $\leq$.

On dit que deux ensembles sont **équipotents** s'il existe une bijection de l'un vers l'autre, et on conviendra que le cardinal d'un ensemble est la « classe » de tous les ensembles qui sont en bijection avec lui. On definit les ensembles finis, infinis, dénombrables :
— On dit qu'un ensemble A est **fini** s'il existe un entier n tel que A soit en bijection avec $[\![1, n]\!] := [n] := \{1, \ldots, n\}$.
— Un ensemble est **infini** s'il n'est pas fini, et **dénombrable** s'il est en bijection avec $\mathbb{N}$.

Lemme 1.2.1. *Soient n et $m \in \mathbb{N}^*$. Il existe une injection de $[n]$ dans $[m]$ si et seulement si $n \leq m$.*

Démonstration. — Si $n \leq m$ alors $[n] \subset [m]$ et $i : [n] \to [m]$ est une injection.

— Réciproquement, pour montrer que nécessairement $n \leq m$ s'il existe une injection de $[n]$ dans $[m]$, on peut proceder par récurrence sur n. Pour $n = 1$, il n'y a rien à démontrer : $m \geq 1$ puisque $m \in \mathbb{N}^*$!
Soit $n \in \mathbb{N}^*$. Supposons que pour tout $n \in \mathbb{N}^*$ tel que'il existe une injection de $[n]$ dans $[m]$ on ait $n \leq m$. (Noter que cette hypothèse de récurrence porte sur n et non sur m !) On veut montrer que cette propriété est vraie pour $n+1$. S'il existe une injection $i : [n+1] \to [m]$, avec $m \in \mathbb{N}^*$, alors $m \geq 2$ (sinon on aurait $i(1) = i(n+1) = 1$ avec $1 \neq n+1$ et i ne serait pas injective).
  — Si $i(n+1) = m$ alors $i|_{[n]} : [n] \to [m-1]$ est encore une injection. Donc $n \leq m-1$ d'après l'hypothèse de récurrence, on a donc bien $n+1 \leq m$.
  — Si $i(n+1) \neq m$, soit φ la transposition entre m et $i(n+1)$ dans $[m]$. Alors $\varphi \circ i : [n+1] \to [m]$ est une injection car φ est bijective, et $\varphi \circ i(n+1) = m$. D'après le cas précédent, ceci implique $n+1 \leq m$.

□

Corollaire 1.2.1. *Les ensembles $[n]$ et $[m]$ sont équipotents ssi $n = m$.*

Par suite, pour tout ensemble fini non vide A il existe un unique $n \in \mathbb{N}^*$ tel que A soit équipotent à $[n]$. On appelle cet entier le *cardinal* de A, et on le note $\mathrm{card}(E)$ ou $\#(A)$ ou $|A|$. On pose de plus $\#(\emptyset) = 0$. Autrement dit, le cardinal de A est le nombre d'éléments de A ! Si A est non vide, on peut numéroté les éléments de A de 1 à $n = \#(A)$ en posant $a_k = \varphi(k)$ pour tout $k \in [n]$, où $\varphi : [n] \to A$ est une bijection. Ainsi $A = \{a_k \mid k \in [n]\}$.

Si A est un sous-enseble d'un ensemble E, on peut aussi écrire $\#(A)$ à l'aide de la *fonction caractéristique* ou *indicatrice* de A :

$$\chi_A : E \to \{0,1\} \quad x \mapsto \chi_A(x) = \begin{cases} 1 & \text{si } x \in A; \\ 0 & \text{si } x \notin A. \end{cases}$$

Si A est fini, alors $\#(A) = \sum_{x \in E} \chi_A(x)$.

Proposition 1.2.1 (Vérifications laissées en exercice)**.** *On suppose que les ensembles ci-dessous sont finis.*

1. *Si $A \subset E$ avec E fini, alors A est fini, $E \setminus A$ aussi et l'on a $\#(E \setminus A) = \#(E) - \#(A)$.*
2. *Si A et B sont deux ensembles finis disjoints, alors $\#(A \cup B) = \#(A) + \#(B)$. (Principe de somme)*
3. *Plus généralement, pour deux ensembles finis, on a $\#(A \cup B) = \#(A) + \#(B) - \#(A \cap B)$.*
4. *Et $\#(A \times B) = \#(A) \times \#(B)$. (Principe de produit)*
5. *Soit F^E l'ensemble des applications de E dans F. Alors : $\#(F^E) = \#(F)^{\#(E)}$.*

Proposition 1.2.2. *Si E est un ensemble fini alors l'ensemble de ses parties $\mathcal{P}(E)$ est fini et $\#(\mathcal{P}(E) = 2^{\#(E)}$.*

Démonstration. En écrivant $E = \{e_1, \ldots, e_n\}$ avec $n = \#(E)$ on peut définir l'application

$$\psi : \mathcal{P}(E) \to \{0,1\}^n \quad A \mapsto (\chi_A(e_1), \ldots, \chi_A(e_1)).$$

On vérifie que ψ est une bijection : $\forall(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$ il existe l'unique partition $A = \{e_i : i \in I\}$ telle que $\psi(A) = (\alpha_1, \ldots, \alpha_n)$, où $I = \{i \in [n] : \alpha_i = 1\}$. Or $\#(\{0,1\}^n) = 2^n$. □

Proposition 1.2.3. *Soit E et F deux ensembles finis de cardidaux respectifs n et p.*

1. *Le nombre d'applications injectives de F dans E est :*

$$A_n^p = \begin{cases} \frac{n!}{(n-p)!} = n(n-1)\cdots(n-p+1) & si \quad 1 \leq p \leq n, \\ 0 & si \quad p > n. \end{cases}$$

2. *En particulier, le nombre de bijections de E dans E est : $n!$.*
3. *Soit $\binom{n}{p}$ le nombre de parties à p éléments de E. Alors :*

$$\binom{n}{p} = \begin{cases} \frac{n!}{p!(n-p)!} & si \quad 0 \leq p \leq n, \\ 0 & si \quad p > n. \end{cases}$$

Démonstration.

1. Soit $E = \{e_1, \ldots, e_n\}$ et $F = \{f_1, \ldots, f_p\}$. On construit chaque injection de F dans E en choisissant les images de f_1 de n façons, $\ldots$, f_p de $n - p + 1$ façons successivement. Donc il y en a $n(n-1)\ldots(n-p+1) = n!/(n-p)!$ telles injections.
2. Si $E = F$, alors $p = n$ et chaque injection de E dans E est une bijection.
3. Si $f : F \to E$ est une injection, alors $f(F)$ est une partie à p éléments de E. On peut définir f en choisissant d'abord une p-partie A de E avec $\binom{n}{p}$ possibilités et puis définir une bijection de E dans A avec $p!$ possibilités. Il s'en suit que

$$A_n^p = \binom{n}{p} \times p! \Longrightarrow \binom{n}{p} = \frac{n!}{p!(n-p)!}$$

avec $p \leq n$.

□

À partir de la définition combinatoire, on pourra vérifier que les coefficients binomiaux $\binom{n}{k}$ satisfont la relation de récurrence :

$$\forall k > 0 \quad \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k} \tag{1.2.1}$$

avec les condidtions initiales

$$\binom{0}{0} = 1 \quad \text{et} \quad \forall k > n \quad \binom{n}{k} = 0. \tag{1.2.2}$$

Proposition 1.2.4 (Formule de binôme)**.** *Soit n un nombre naurel positif et x une variable. On a*

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Démonstration. En développant $(1+x)^n$ on a

$$(1+x)^n = \sum_{(\epsilon_1,\ldots,\epsilon_n)\in\{0,1\}^n} x^{\epsilon_1+\cdots+\epsilon_n}.$$

On définit une bijection φ de $\{0,1\}^n$ dans l'ensemble des parties de $[n]$:

$$(\epsilon_1,\ldots,\epsilon_n) \mapsto \pi = \{i \in [n] \mid \epsilon_i = 1 \quad \forall i \in [n]\}.$$

De plus π est un sous-ensemble de $[n]$ à k éléments ssi $\epsilon_1 + \cdots + \epsilon_n = k$. Il s'en suit que le nombre de n-uplets $(\epsilon_1,\ldots,\epsilon_n) \in \{0,1\}^n$ tels que $\epsilon_1 + \cdots + \epsilon_n = k$ est $\binom{n}{k}$. D'où la formule du binôme. □

En particulier, on en déduit de la preuve ci-dessus que le nombre de sous-ensembles d'un ensemble à n éléments est 2^n.

Proposition 1.2.5 (Lemme des bergers)**.** *Si un ensemble E possède une partition en p sous-ensembles contenant chacun r éléments, alors le cardinal de E est $p \times r$.*

Proposition 1.2.6 (Principe des tiroirs)**.** *Si E et F sont deux ensembles finis tels que $card(E) > card(F)$ et si $f : E \to F$ est une application de E dans F, alors il existe un élément de F qui admet au moins deux antécédents par f ; autrement dit il n'existe pas d'application injective de E dans F.*

Proposition 1.2.7 (Principe d'inclusion-exclusion)**.** *Soit E un ensemble fini et $A_1,\ldots,A_r \subset E$. Alors*

$$|A_1 \cup \cdots \cup A_r| = \sum_{i=1}^{r} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| + \cdots + (-1)^{r-1} |A_1 \cap \cdots \cap A_r|. \tag{1.2.3}$$

Démonstration. Pour chaque lment x de $A_1 \cup \cdots \cup A_r$ on va compter le nombre de fois qu'il est compt dans les deux membres de la formule ci-dessus. Il est clair que x est compt une fois gauche. Supposons que x appartient exactement l sous-ensembles $A_1, \ldots, A_l$ avec $l \leq r$. Alors, le nombre de fois qu'il est compt droite est

$$\binom{l}{1} - \binom{l}{2} + \cdots + (-1)^{l-1}\binom{l}{l} = 1 - (1-1)^l = 1.$$

Donc chaque lment de $A_1 \cup \cdots \cup A_r$ est compt exactement une fois dans les deux ct. □

En utilisant la fonction indicatrice on pourra réécrire la formule (1.2.3) sous la fome suivante :

$$\chi_{A_1 \cup \cdots \cup A_r}(x) = \sum_{i=1}^{r} \chi_{A_i}(x) - \sum_{i<j} \chi_{A_i \cap A_j}(x) + \sum_{i<j<k} \chi_{A_i \cap A_j \cap A_k}(x) + \cdots + (-1)^{l-1} \chi_{A_1 \cap \cdots \cap A_l}(x),$$

pour tout élément $x \in E$.

Proposition 1.2.8. *Soit E et F deux ensembles de caldinaux finis respectifs n et p. Alors le nombre de surjections de E dans F est donné par*

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

Démonstration. On suppose que $E = [n]$ et $F = [p]$. Alors le nombre d'applications de F^E est p^n. Pour tout $i \in [p]$ soit $A_i = \{f \in F^E \mid i \notin f([n])\}$. Alors f est une surjection de E vers F ssi $f \notin \bigcup_{i=1}^{p} A_i$, à savoir $f \in F^E \setminus (A_1 \cup \cdots \cup A_p)$. Donc le nombre de surjections de E vers F est

$$|F^E| - |A_1 \cup \cdots \cup A_p|$$

Pour tout sous-ensemble $\{i_1, \ldots, i_k\}$ à k éléments de $[p]$ avec $k \geq 1$, l'intersection $A_{i_1} \cap \cdots \cap A_k$ est l'ensemble des applications de E vers $F \setminus \{i_1, \ldots, i_k\}$, dont le cardinal est $(p-k)^n$. La formule s'ensuit par la fomule d'inclusion-exclusion (1.2.3). □

Soit $S(n,k)$ le nombre de partitions d'un ensemble à n éléments en k sous-ensembles. On appelle $S(n,k)$ $(1 \leq k \leq n)$ les nombres de Stirling de second espèce.

Proposition 1.2.9. *On a*

$$S(n,p) = \frac{1}{p!} \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^n.$$

Démonstration. Soit $\mathcal{F}$ l'ensemble des application surjective de $E := [n]$ vers $F = [p]$. Pour toute application surjective $f : E \to F$ l'ensemble $\pi_f = \{f^{-1}(1), \ldots, f^{-1}(p)\}$ est une partition de E en p parties. On dit que deux applications de $\mathcal{F}$ ont une relation $\mathcal{R}$ ssi elles donnent la même partition. Il est clair que $\mathcal{R}$ est une relation d'équivalence de $\mathcal{F}$ et deux surjections f et g de E dans F ont la relation $\mathcal{R}$ ssi il existe une permutation σ de $[p]$ telle que $g = \sigma \circ f$. Donc, pour toute application $f \in \mathcal{F}$ le cardinal de la classe d'équivalence de f est $\#(\bar{f}) = p!$ car $\bar{f} = \{\sigma \circ f \mid \sigma \text{ est une permutation de } [p]\}$.

Comme il y a une bijection entre l'ensemble quotient $\mathcal{F}/\mathcal{R}$ et l'ensemble de partitions en p parties de E. Ceci implique que $\#(\mathcal{F}/\mathcal{R}) = S(n,k)$ et par suite

$$\#(\mathcal{F}) = \sum_{\bar{f} \in \mathcal{F}/\mathcal{R}} \#(\bar{f}) = p!S(n,k). \qquad \text{(Lemme des bergers)}$$

On déduit la formule pour les nombres de Stirling d'après la Proposition 1.2.8. □

À partir de la définition combinatoire, on pourra vérifier que les nombres de Stirling $S(n,k)$ vérifient la relation de récurrence :

$$\forall k > 0 \quad S(n+1,k) = S(n,k-1) + kS(n,k) \tag{1.2.4}$$

avec les condidtions initiales

$$S(0,0) = 1 \quad \text{et} \quad \forall n > 0 \quad S(n,0) = S(0,n) = 0. \tag{1.2.5}$$

Les premières valeurs de $S(n,k)$ sont comme suit :

$$\begin{array}{cccccc} 1 & & & & & \\ 1 & 1 & & & & \\ 1 & 3 & 1 & & & \\ 1 & 7 & 6 & 1 & & \\ 1 & 15 & 25 & 10 & 1 & \\ 1 & 31 & 90 & 65 & 15 & 1 \end{array}$$

1.3 Ensembles dénombrables

Définition 1.3.1. *Un ensemble est dit dénombrable s'il est équipotent à* $\mathbb{N}$.

Autre dit, en posant $a_k = \varphi(k)$ pour tout $k \in \mathbb{N}$ où $\varphi : \mathbb{N} \to A$ est une bijection, on peut écrire $A = \{a_k : k \in \mathbb{N}\}$, les a_k étant deux à deux distincts. On qu'un ensemble est au plus dénombrable, c'est-à-dire fini si la suite $(b_n)_{n\in\mathbb{N}})$ ne prend qu'un nombre fini de valeurs ou dénombrable.

Examples d'ensembles dénombrables :

— $\mathbb{N}^*$ (bien qu'il semble avoir "un élément de moins" que $\mathbb{N}$), car

$$\varphi : \mathbb{N}^* \to \mathbb{N} \quad n \mapsto n-1 \quad \text{est une bijection.}$$

— Plus généralement, quelque soit $n \in \mathbb{N}$, l'ensemble $\mathbb{N} \setminus [n]$ est dénombrable, car

$$\varphi : \mathbb{N} \setminus [n] \to \mathbb{N} \quad k \mapsto k-n-1 \quad \text{est une bijection.}$$

— Plus étaonnant, bien qu'apparemment "deux fois plus gros" que $\mathbb{N}$, l'ensemble $\mathbb{Z}$ est dénombrable, car

$$\varphi : \mathbb{N} \setminus [n] \to \mathbb{Z} \quad n \mapsto \begin{cases} -\frac{n}{2} & \text{si } n \text{ est pair} \\ \frac{n+1}{2} & \text{si } n \text{ est impair} \end{cases}$$

est une bijection.

Exemples d'ensembles non dénombrables :

Théorème 1.3.1. *Soit E un ensemble. Alors il n'existe pas de bijection entre E et $\mathcal{P}(E)$.*

Corollaire 1.3.1. *L'ensemble $\mathcal{P}(\mathbb{N})$ est non dénombrable.*

Démonstration. Supposons qu'il existe une bijection $f : E \to \mathcal{P}(E)$. On considère l'ensemble $A = \{x \in E : x \notin f(x)\}$. Soit $x_0 = f^{-1}(A)$. Alors $x_0 \in A \iff x_0 \notin A$. C'est absurde. □

Remarque 1.3.1. *Dès qu'un ensemble admet un sous-ensemble non dénombrable il est non dénombrable. On le justifiera plus loin.*

Exemple 1.3.1. *L'ensemble $]0,1[$ de $\mathbb{R}$ n'est pas dénombrable. On considère l'ensemble A des nombres $x \in]0,1[$ dont l'écriture décimale ne contienne des chiffres 1 et 8. Supposons par l'absurde qu'il existe une numérotation de tous les nombres de A . Nous pouvons alors écrire ces nombres dans l'ordre de la numérotation $(a_k)_{k\in\mathbb{N}}$. Soit $a_n = 0, a_{n,1}a_{n,2}\dots a_{n,n}\dots$ avec $a_{n,k} = 1$ ou 8.*

$$\begin{aligned}
a_0 &= 0, a_{0,0}\, a_{0,1}\, a_{0,2}\, \dots\, a_{1,n}\dots \\
a_1 &= 0, a_{1,0}\, a_{1,1}\, a_{1,2}\, \dots\, a_{1,n}\dots \\
a_2 &= 0, a_{2,0}\, a_{2,1}\, a_{2,2}\, \dots\, a_{2,n}\dots \\
\dots &= \dots \\
a_n &= 0, a_{n,1}\, a_{n,2}\, a_{n,3}\, \dots\, a_{n,n}\dots
\end{aligned}$$

On considère le nombre

$$b = 0, \bar{a}_{0,0}\bar{a}_{1,1}\bar{a}_{2,2}\bar{a}_{3,3}\ldots\bar{a}_{n,n}\ldots$$

o $\bar{a}_{n,k} = 9 - a_{n,k}$. *Alors* $b \neq a_n$ *pour tout* $n \in \mathbb{N}$ *car* $\bar{a}_{n,n} \neq a_{n,n}$ *pour tout* $n \in \mathbb{N}$.

Proposition 1.3.1. *Le produit cartésien* $\mathbb{N}^2$ *est dénombrable !*

Démonstration. On donne deux preuves.

1) L'idée est de "balayer" le quadrant $\mathbb{N}^2$ par les doites l_n : $x + y = n$ pour $n \in \mathbb{N}$ et puis "parcourir" chaque droite l_n de $(n, 0)$ vers $(0, n)$ dans la direction "nord-ouest". Intuitivement on parcourt chaque point de $\mathbb{N}^2$ une et une seule fois.

On pose $(p_0, q_0) = (0, 0)$, $(p_1, q_1) = (1, 0)$, $(p_2, q_2) = (0, 1)$, et par récurrence :

$$\begin{cases} p_{n+1} = p_n - 1, & q_{n+1} = q_n + 1 \quad \text{si} \quad p_n \neq 0; \\ p_{n+1} = q_n + 1, & q_{n+1} = 0 \quad \text{si} \quad p_n = 0. \end{cases}$$

On peut vérifier que le numéro du point $(p, q) \in \mathbb{N}^2$ est donné par

$$f(p, q) = \sum_{i=0}^{p+q} i + q = \binom{p + q + 1}{2} + q.$$

car $f(p, q) = f(p + q, 0) + q$ et $f(p + q, 0) = f(p + q - 1, 0) + p + q$ avec $f(0, 0) = 0$.

2) Tout entier $n \in \mathbb{N}^*$ s'écrit de façon unique comme $n = 2^a(2b + 1)$ avec $(a, b) \in \mathbb{N}^2$. Par exemple, on a $28 = 2^2(2 \times 3 + 1)$. Donc $\mathbb{N}^2$ est équipotent à $\mathbb{N}^*$. □

Plus généralement on a

Proposition 1.3.2. *Tout produit fini d'ensembles dénombrables est dénombrable.*

Démonstration. Soit A et B deux ensembles dénombrables. Alors si $\varphi : A \to \mathbb{N}$ et $\psi : B \to \mathbb{N}$ sont des bijections, alors $f : A \times B \to \mathbb{N}^2 \quad (a, b) \mapsto (\varphi(a), \psi(b))$ est une bijection. Donc $A \times B$ est équipotent à $\mathbb{N}^2$ d'après la proposition prédédente.

On montre ensuite par récurrence immédiate sur $n \in \mathbb{N}^*$ que si des ensembles $A_1, \ldots, A_n$ sont dénombrables alors $\prod_{k=1}^{n} A_k$ aussi. □

Attention :

Un "produit infini d'ensemble" dénombrables ne l'est pas nécessairement. Par exemple, $[\![0, 9]\!]^{\mathbb{N}}$ est l'ensemble des suites d'entiers compris entre 0 et 9. Il contient l'ensemble des suites $(p_n)_{n\in\mathbb{N}}$ telles que pour tout $N \in \mathbb{N}$ il existe $n \geq N$ pour lequel $p_n \neq 9$. Celui-ci est équipotent à $[0, 1[$ via les développements décimaux propres, dont on a montré qu'il n'était pas dénombrable.

Ensembles au plus dénombrables

Définition 1.3.2. *Un ensembles est dit au plus dénombrable s'il est fini ou dénombrable.*

C'est le cas de toute partie de $\mathbb{N}$ par exemple. On rappelle que toute partie non vide de $\mathbb{N}$ admet un plus petit élément.

Proposition 1.3.3. *Si A est une partie non vide de $\mathbb{N}$, elle est finie si majorée, et dénombrable sinon.*

Démonstration. Soit $A \subset \mathbb{N}$, $A \neq \emptyset$. On définit par récurrence la suite (a_k) d'entiers et la suite A_k de parties de $\mathbb{N}$ par $a_0 = \min A$, $A_0 = \{a_0\}$, et pour tout $n \in \mathbb{N}$, tant que $A \setminus A_n \neq \emptyset$, $a_{n+1} = \min(A \setminus A_n)$, $A_{n+1} = \{a_{n+1}\} \cup A_n$. Si l'on atteint $N \in \mathbb{N}$ tel que $A = A_N$, alors $[\![0, N]\!] \to A\ n \mapsto a_n$ est une bijection strictement croissante, $a_N = \max A$ et $\#(A) = N + 1$.

Si pour tout $n \in \mathbb{N}$, $A \setminus A_n \neq \emptyset$, alors $\underset{n \mapsto a_n}{\mathbb{N} \to A}$ est une bijection (s'il existe un $a \in A$ tel $a \neq a_k$ alors il existe un $k \in \mathbb{N}$ tel que $a_k < a < a_{k+1}$ c'est absurde !) strictement croissante, et A n'est pas majorée sinon elle aurait un plus grand élément a_N, et on ne pouvait pas avoir $a_{N+1} > a_N$. □

Corollaire 1.3.2. *Etant donné un ensemble A,*

1. *s'il existe une injection de A dans $\mathbb{N}$, alors A est au plus dénombrable.*
2. *s'il existe une surjection de $\mathbb{N}$ dans A, alors A est au plus dénombrable.*

Démonstration. 1) si $i : A \to \mathbb{N}$ est injective, alors $i(A)$ est une partie de $\mathbb{N}$, donc au plus dénombrable, et i définit une bijection de A sur $i(A)$, donc A est fini si $i(A)$ est finie, et dénombrable si $i(A)$ l'est.

2) si $s : \mathbb{N} \to A$ est surjective, on peut définir $i : A \to \mathbb{N}$ par $i(a) = \min s^{-1}(a)$, puisque quelque soit $a \in A$, $s^{-1}(a)$ est une partie non vide de $\mathbb{N}$ du fait que s est surjective. De plus, $s(i(a) = a$ pour tout a. Donc i est injective, et A est au plus dénombrable d'après 1). □

Proposition 1.3.4. *Si $(A_n)_{n \in \mathbb{N}}$ est une famille d'ensembles au plus dénombrable alors $\bigcup_{n \in \mathbb{N}} A_n$ est au plus dénombrable.*

Démonstration. Pour tout $n \in \mathbb{N}$, on peut écrire $A_n = \{a_{n,k} : k \in \mathbb{N}\}$, de sorte que $\bigcup_{n \in \mathbb{N}} A_n = \{a_{n,k} : k \in \mathbb{N}, n \in \mathbb{N}\}$. Ainsi on a une surjection

$$\begin{aligned} \mathbb{N}^2 &\to \bigcup_{n \in \mathbb{N}} A_n \\ (n, k) &\mapsto a_{n,k} \end{aligned}$$

Comme $\mathbb{N}^2$ est dénombrable, on en déduit qu'il existe une surjection de $\mathbb{N}$ dans $\bigcup_{n \in \mathbb{N}} A_n$, qui est donc au plus dénombrable. □

Exemple 1.3.2. *L'ensemble* $\mathbb{Q} = \bigcup_{n\in\mathbb{N}^*} \{\frac{m}{n} : m \in \mathbb{Z}\}$. *Quel que soit* $n \in \mathbb{N}^*$, $\{\frac{m}{n} : m \in \mathbb{Z}\}$ *est équipotent à* $\mathbb{Z}$, *qui est dénombrable. Donc* $\mathbb{Q}$ *est au plus dénombrable. Comme il n'est pas fini puisqu'il contient* $\mathbb{Z}$, *il est dénombrable.*

L'hypothèse du continu

Une question naturelle s'impose : existe-t-il un infini intermédiaire entre le dénombrable (cardinal de $\mathbb{N}$) et le continu (cardinal de $\mathbb{R}$) ? Pour être précis, existe-t-il un ensemble infini qui ne peut pas être mis en bijection avec $\mathbb{N}$ et $\mathbb{R}$ mais qui peut s'injecter dans $\mathbb{R}$?

La réponse n'est ni oui, ni non ! Kurt Gödel et Paul COHEN ontt démontré qu'il était impossible de répondre à cette question dans le cadre des axiomes de la théorie des ensembles. Autrements dit, on peut décider qu'un tel ensembles existe ou bien décider qu'il n'existe pas ; dans les deux cas, cela ne conduira pas à des contradictions de la théorie. On dit que cette question est indécidable.

Chapitre 2

L'arithmétique

Résumé

I. Divisibilité. Rappels sur le groupe $(\mathbb{Z}, +)$ et anneaux $(\mathbb{Z}, +, x)$. Division euclidienne. L'axiome de bon ordre de $\mathbb{N}$. Tout sous-groupe de $\mathbb{Z}$ peut s'ecrire $a\mathbb{Z}$ $(a \geq 0)$. II. Pgcd et Ppcm. Identité de Bézout. Interpretation en termes d'ideaux de l'anneau $\mathbb{Z}$. $\text{pgcd}(a, b) \cdot \text{ppcm}(a, b) = |ab|$. Entiers premiers entre eux ; théorème de Bézout. III. Nombres premiers. Tout entier > 1 admet un diviseur premier et s'il est composé il admet un diviseur premier majoré par $\sqrt{n}$. Il y a une infinité de nombres premiers. Lemme de Gauss. Lemme d'Euclide. Théorème fondamental de l'arithmetique. IV. Algorithme d'Euclide et algorithme de Bezout. Résolution d'equation diophantienne $ax + by = c$.

2.1 Divisibilité

2.1.1 L'anneau $\mathbb{Z}$

Rappelons que l'ensemble des entiers relatifs $\mathbb{Z}$ est constitué des éléments ordonnés :

$$\ldots, -2, -1, 0, 1, 2, \ldots.$$

$\mathbb{Z}$ est muni de deux lois de composition : l'addition $+ : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ et multiplication $\cdot : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ vérifiant :

$$\begin{array}{lll} a + b = b + a & a \cdot b = b \cdot a & \\ a + 0 = 0 + a = a & a \cdot 1 = 1 \cdot a = a & a \cdot (b + c) = a \cdot b + a \cdot c \\ a + (b + c) = (a + b) + c & a \cdot (b \cdot c) = (a \cdot b) \cdot c & \end{array}$$

Tout $a \in \mathbb{Z}$ est *symétrisable*, i.e. $\exists b \in \mathbb{Z}$ t.q. $a + b = 0$. Par contre, le seul élément *inversible* a dans $\mathbb{Z}$ est 1 ou -1, i.e. $\exists b \in \mathbb{Z}$ t.q. $a \cdot b = 1$. On dit que $(\mathbb{Z}, +)$ a une structure de groupe additif ou abélien et $(\mathbb{Z}, +, \cdot)$ une structure d'anneau commutatif unitaire.

Exercice 2.1.1. . *Montrer que* $0 \cdot a = 0$ *dans* $\mathbb{Z}$.

Définition 2.1.1. *On dit que* $a \leq b$ *si* $b - a \geq 0$ *et* $a < b$ *si* $b - a > 0$.

On note $\mathbb{N} = \{0, 1, 2, \ldots\}$ *l'ensemble des entiers positifs.*

Théorème 2.1.1. *Les trois propriétés sur les nombres naturels sont équivalentes :*
a) (1er principe de récurrence) Soit A *une partie de* $\mathbb{N}$ *et* $n_0 \in \mathbb{N}$. *Si* $n_0 \in A$ *et pour tout* $n \geq n_0$, $n \in A \Longrightarrow n + 1 \in A$, *alors* $A = \mathbb{N} \cap [n_0, +\infty[$.
b) (2e principe de récurrence) Soit A *une partie de* $\mathbb{N}$. *Si* $n_0 \in A$ *et pour tout* $n \geq n_0$, $n_0, n_0 + 1, \ldots n \in A \Longrightarrow n + 1 \in A$, *alors* $A = \mathbb{N} \cap [n_0, +\infty[$.
c) (Axiome de bon ordre) Toute partie non vide A *de* $\mathbb{N}$ *possède un plus petit élément.*

Preuve. Nous allons montrer que *a)* $\Longrightarrow$ *b)*, *b)* $\Longrightarrow$ *c)* et *c)* $\Longrightarrow$ *a)* .

a) $\Longrightarrow$ b). Soit $B = \{n \geq n_0 | n_0, n_0 + 1, \ldots, n \in A\}$. Alors $n_0 \in B$. Pour tout entier $n \geq n_0$, l'hypothèse de b) entraîne que $n \in B \Longrightarrow n + 1 \in B$. D'où, d'après l'hypothèse de a), $B = \mathbb{N} \cap [n_0, +\infty[$. Comme $B \subset A \subset \mathbb{N} \cap [n_0, +\infty[$ on en déduit que $A = B = \mathbb{N} \cap [n_0, +\infty[$.
b) $\Longrightarrow$ c) Supposons que $A \subset \mathbb{N}$ n'a pas de minimum. On pose $B = \{n \in \mathbb{N} | n \notin A\}$. On a $0 \in B$ car sinon 0 serait le minimum. De même, $\forall n \in \mathbb{N}$, le fait que $0, 1, \ldots, n \in B$ entraîne que $n + 1 \in B$ (car sinon $n + 1$ serait le minimum de A). Le 2e principe de récurrence implique que $B = \mathbb{N}$, par conséquent le complémentaire de B dans $\mathbb{N}$ est vide, c'est-à-dire que $A = \emptyset$. C'est absurde.
c) $\Longrightarrow$ a) Soit $B = \{n \geq n_0 | n \notin A\}$. Il suffit de montrer que $B = \emptyset$. Supposons le contraire. Alors il existe un plus petit élément m_0 dans B. Comme $n_0 \in A$ on a $m_0 > n_0$. Donc $m_0 - 1 \geq n_0$ et $m_0 - 1 \in A$. Or l'hypothèse de a) impose que $m_0 - 1 \in A \Longrightarrow m_0 \in A$, c'est absurde. Donc $B = \emptyset$. □

2.1.2 Division euclidienne

Théorème 2.1.2 (Division euclidienne)**.** *Etant donnés deux entiers relatifs* a *et* b $(b > 0)$*, il existe un couple unique d'entiers* (q, r) *tel que*

$$a = bq + r \qquad et \qquad 0 \leq r < b.$$

NB. a*—le dividende,* b*—le diviseur,* q*—le quotient et* r *le reste de la division de* a *par* b.

Preuve. (Existence) Soit $A = \{a - bk | k \in \mathbb{Z}\}$. Alors A contient des entiers positifs (si $a \geq 0$, alors $a = a - b0 \geq 0$, si $a < 0$, alors $a - ba = (-a)(b - 1) \geq 0$). Soit r le plus petit entier positif de A et q la valeur de k correspondant à $r = a - bq$. Donc $r \geq 0$ et $r - b = a - (q + 1)b < 0$ car r est le plus petit !
(Unicité) Supposons qu'on a aussi $a = bq' + r'$ avec $0 \leq r' < b$ alors $b(q - q') = r' - r$. Si $q \neq q'$ alors $|r' - r| \geq b$. C'est absurde car $0 \leq r, r' < b$. □

Exemple 2.1.1. $8 = 3 \times 2 + 2$ *et* $-8 = 3 \times (-3) + 1$.

Définition 2.1.2. *Soit A une partie non vide de $\mathbb{Z}$. Si A est stable par addition et passage à l'opposé, on dit que A est un sous-groupe (additif) de $\mathbb{Z}$.*

Exemple 2.1.2. *Quel que soit $a \in \mathbb{Z}$, l'ensemble $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$; réciproquement :*

Proposition 2.1.1. *Soit A un sous-groupe de $\mathbb{Z}$, alors il existe un $a \in \mathbb{N}$ tel que $A = a\mathbb{Z}$.*

Preuve. Si $A = \{0\}$, alors $A = 0\mathbb{Z}$. Supposons $A \neq \{0\}$, alors A contient des entiers > 0. Soit a le plus petit entier > 0 de $A \cup \mathbb{N}^*$. De $a \in A$, on tire : $a\mathbb{Z} \subset A$. Soit $x \in A$; la division euclidienne de x par $a > 0$ permet d'écrire :

$$x = aq + r \qquad \text{et} \qquad 0 \leq r < a.$$

Donc $r = x - aq \in A$ (car A est un ss-gp de $\mathbb{Z}$). Sachant $r < a$, la seule possibilité est : $r = 0$, c'est-à-dire $x = aq \in a\mathbb{Z}$. Donc l'inclusion $A \subset a\mathbb{Z}$ est démontrée. Les deux inclusions entraînent alors $A = a\mathbb{Z}$. □

Définition 2.1.3. *Soient a et b deux entiers. On dit que a divise b ou a est un diviseur de b ou b est un multiple de a, s'il existe un entier c tel que $b = ac$.*

Proposition 2.1.2. *On a*
— $a|b$ *et* $b \neq 0 \Longrightarrow |a| \leq |b|$.
— $d|a$ *et* $d|b \Longrightarrow \forall \lambda,\ \mu \in \mathbb{Z}, d|\lambda a + \mu b$
— *Soit* $a, b \in \mathbb{Z}$, $a|b$ *et* $b|a \Longrightarrow a = \pm b$.

Remarque 2.1.1. *La divisibilité est une relation d'ordre partiel dans $\mathbb{Z}$: $a \prec b$ si $a \mid b$. Il est clair qu'on ne pourra pas toujours comparer deux entiers selon cet ordre.*

2.2 P.G.C.D et P.P.C.M.

Théorème 2.2.1 (PGCD)**.** *Soient a et b deux entiers non tous nuls. Il existe un diviseur commun $d > 0$ de a et b tel que tout diviseur commun à a et b divise d. Un tel entier d est unique et est appelé le PGCD de a et b. De plus, il existe des entiers u et v tels que*

$$d = au + bv. \qquad \text{(Identité de Bézout)}$$

Preuve. L'ensemble

$$a\mathbb{Z} + b\mathbb{Z} = \{am + bn | m, n \in \mathbb{Z}\} \neq 0\mathbb{Z}$$

est un ss-gp de $\mathbb{Z}$. Il existe un entier unique $d > 0$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Or $a = a \cdot 1 + b \cdot 0 \in d\mathbb{Z}$ et $b = a \cdot 0 + b \cdot 1 \in d\mathbb{Z}$, donc il existe a' et b' tq

$$a = da' \qquad b = db' \qquad (a', b' \in \mathbb{Z})$$

et d est un diviseur commun de a et b. Pour $d = d \cdot 1 \in d\mathbb{Z}$, il existe u et v tels que

$$d = au + bv.$$

Si $c|a$ et $c|b$, il existe un $c \in \mathbb{Z}$ tel que

$$a = ca', \qquad b = cb' \qquad (a', b' \in \mathbb{Z}).$$

Il s'ensuit que $d = au + bv = c(a'u + b'v)$, i.e. c divise d, et $d \geq c$. Donc $d = (a, b)$. □

Remarque 2.2.1. *Dans l'identité de Bézout, le couple (u, v) n'est pas unique. Par exemple, si $a = 8$ et $b = 6$, alors $d = 2$. On a*

$$8 \cdot 1 - 6 \cdot 1 = 2, \quad 8 \cdot (-2) + 6 \cdot 3 = 2, \quad 8 \cdot 4 + 6 \cdot (-5) = 2, \ldots$$

Théorème 2.2.2 (Bézout)**.** *Deux entiers a et b sont premiers entre eux ssi il existe un couple d'entiers (u, v) tel que $au + bv = 1$.*

Preuve. L'identité de Bézout prouve que la condition est bien nécessaire. Réciproquement, si $au + bv = 1$ alors tout diviseur commun à a et b est un diviseur de 1, ce qui implique que le $pgcd(a, b) = 1$. □

Lemme 2.2.1 (Gauss)**.** *Soit a, b et c des entiers.*
— *Si $a|bc$ et si a est premier avec b, alors $a|c$.*
— *Si $a|c$, $b|c$ et $(a, b) = 1$, alors $ab|c$.*

Démonstration. (1) Comme $pgcd(a, b) = 1$, il existe des entiers u et v tels que $au + bv = 1$. Donc $acu + bcv = c$. Comme $a|acv$ et $a|bcv$, on en dédeuit que a divise $c = acu + bcv$.

(2) En écrivant $au + bv = 1$, $c = aa' = bb'$ on a $c = ab(b'u + a'v)$, d'où ab| c. □

Théorème 2.2.3 (p.p.c.m.)**.** *Soient a et b deux entiers non nuls, d leur p.g.c.d. Il existe un multiple commun $m > 0$ à a et b tel que tout multiple commun de a et b est un multiple de m. Cet entier m est unique et appelé le PPCM (plus petit commun multiple) de a et b. De plus, $m = |ab|/d$.*

Preuve. En effet, l'ensemble des multiples communs à a et b est $a\mathbb{Z} \cap b\mathbb{Z}$, qui est un un ss-gp de $\mathbb{Z}$ (exercice !). Donc il existe un entier unique $m \geq 0$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

Il est évident que $ab/d \in a\mathbb{Z} \cap b\mathbb{Z}$. Donc m divise ab/d. Le thm de Bezout entraîne qu'il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = d \Longrightarrow \frac{a}{d}u + \frac{b}{d}v = 1$$

Comme m est un multiple commun à a et b. En écrivant $m = am_1 = bm_2$ avec $m_1, m_2 \in \mathbb{Z}$, on obtient

$$m = \frac{am}{d}u + \frac{bm}{d}v = \frac{ab}{d}(m_2u + m_1v).$$

Ce qui montre que ab/d divise m. D'où $m = |ab|/d$. □

2.3 Nombres premiers

Définition 2.3.1. *Un entier $p \geq 2$ est dit premier si ses seuls diviseurs positifs sont 1 et lui-même. Un entier $n \geq 2$ est dit composé s'il n'est pas premier.*

Proposition 2.3.1. *Tout nombre entier $n \geq 2$ admet au moins un diviseur premier. De plus, si n est un nombre composé, il admet un diviseur premier $p \leq \sqrt{n}$.*

Preuve. Si $n \geq 2$ est premier, alors n est un diviseur premier de n. Sinon, l'ensemble $\{1 < d < n \mid d|n\}$, qui n'est pas vide, admet un minimum p, qui est premier (car sinon, p a un diviseur $< p$ qui divise n, contradiction). De plus n/p est un diviseur de n, donc $n/p \geq p$ et $p \leq \sqrt{n}$. □

Théorème 2.3.1 (Euclide)**.** *Il y a une infinité de nombres premiers.*

Preuve. Par absurde. Supposons qu'il n'y a qu'un nombre fini de nombres premiers : $p_1, p_2, \ldots, p_m$. Posons $N = p_1p_2 \ldots p_m + 1$. Alors N a un diviseur premier p_i, ce qui implque que $p_i|1$. C'est absurde. □

Remarque 2.3.1. *Pour tout nombre réel $x > 0$, si l'on note $\pi(x)$ le nombre des nombres premiers $\leq x$, alors $\pi(x) \sim x/\log(x)$.*

Lemme 2.3.1 (Euclide)**.** *Si p premier divise un produit alors il divise un des facteurs, ie. si $p|a_1a_2 \ldots a_n$, alors $p|a_i$ pour un certain i.*

Preuve. Par récurrence sur n et le thm de Gauss. (Exercice) Pour $n = 2$, $p|a_1a_2$. Si $(p, a_1) = 1$ alors Gauss $\Longrightarrow p|a_2$. Supposons vrai jusqu'à $n - 1$. Si $p|a_1a_2 \ldots a_n$ alors $p|a_1 \ldots a_{n-1}$ et H.R. implique que $p|a_i$ ou $p|a_n$. □

Exemple 2.3.1. *Soit p un nombre premier. Alors p divise le coefficient binomial $\binom{p}{k}$ pour $1 < k < p$. En effet, on a $p! = k!(p-k)!\binom{p}{k}$. Donc p divise le produit $k!(p-k)!\binom{p}{k}$ et $p \nmid k!(p-k)!$, donc p divise $\binom{p}{k}$ par le lemme d'Euclide.*

Théorème 2.3.2 (Thm. fondamental de l'arithmétique)**.** *Tout entier > 1 se factorise d'une manière unique comme un produit de nombres premiers.*

Preuve. (Existence) On s'appuie sur un raisonnement par récurrence.
Si $n = 2$, c'est clair.
H.R. : Tout entier de $[2, n]$ se factorise comme un produit de nombres premiers.
Si $n+1$ est premier, il n'y à rien à démontrer, sinon, $n+1$ admet un diviseur $p \in]1, n+1[$ d'où $n+1 = pq$, où p, q sont dans $[2, n]$, donc chacun égal à un produit de de nombres premiers. Il en est de même de $n+1$. L'existence est donc prouvée par récurrence.

Montrons maintenant l'unicité de la factorisation. Supposons que l'on ait

$$n = p_1^{a_1} \dots p_r^{a_r} = p_1^{b_1} \dots p_s^{b_r}$$

où les a_i et b_j sont ≥ 0, les p_i sont des nbres premiers distincts, et $a_i \neq b_i$ pour au moins un indice i.

Supposons, par exemple, cet indice égal à 1, $a_1 > b_1$, alors après division par $p_1^{b_1}$ on arrive à

$$p_1^{a_1 - b_1} \dots p_r^{a_r} = p_2^{b_2} \dots p_r^{b_r}.$$

Donc p_1 doit être égal à l'un des $p_2, \dots, p_r$. C'est absurde. Ceci montre que $a_i = b_i$ pour tout $i = 1, \dots, r$. □

Remarque *: Contre-exemple pour factorisation unique.*

$$E = 2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}.$$

On appelle "nombre premier" tout nombre de E qui n'est pas produit de deux nombres pairs. On a

$$\begin{aligned} 840 &= (2 \times 3) \times (2 \times 5) \times (2 \times 7) \\ &= (2 \times 1) \times (2 \times 7) \times (2 \times 15) \\ &= (2 \times 1) \times (2 \times 5) \times (2 \times 21) \end{aligned}$$

Proposition 2.3.2. *Si les décompositions en facteurs premiers de deux entiers positifs a et b s'écrivent*

$$a = p_1^{a_1} \dots p_r^{a_r} \qquad b = q_1^{b_1} \dots q_r^{b_r}$$

où $a_i \geq 0$ et $b_i \geq 0$. Alors

$$pgcd(a,b) = p_1^{\min(a_1,b_1)} \cdots p_r^{\min(a_r,b_r)}, \tag{2.3.1}$$
$$ppcm(a,b) = p_1^{\max(a_1,b_1)} \cdots p_r^{\max(a_r,b_r)}. \tag{2.3.2}$$

Il s'en suit que $ab = pgcd(a,b) \cdot ppcm(a,b)$.

Exemple 2.3.2. *: Le coefficient binomial $\binom{n}{k}$ est défini par*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \qquad 0 \leq k \leq n.$$

Comment peu-on vérifier de façon arithmétique que c'est un entier ? Pour tout nombre premier p la valuation p-adique de $n!$ est

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

D'où la valuation p-adique de $\binom{n}{k}$ est

$$\sum_{i \geq 0} \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor - \left\lfloor \frac{n-k}{p^i} \right\rfloor \right)$$

Le résultat suit donc de l'identité évidente :

$$\lfloor \alpha + \beta \rfloor - \lfloor \alpha \rfloor - \lfloor \beta \rfloor = 0 \quad or \quad 1$$

quelques soient les nombres réels α et β.

2.4 L'algorithme d'Euclide

Lemme 2.4.1. *Soient a, b, c trois entiers tels que $a = bq + c$ avec $q \in \mathbb{Z}$. Alors $pgcd(a,b) = pgcd(b,c)$.*

Preuve. Il suffit de remarquer que tout diviseur commun à a et b est aussi un diviseur commun à b et c et vice versa. □

Soient a et b deux entiers positifs tels que $a \geq b > 0$. On effectue les divisions euclidiennes successivement :

$$\begin{aligned}
a &= bq_1 + r_1 \qquad 0 < r_1 < b \\
b &= r_1 q_2 + r_2 \qquad 0 < r_2 < b \\
r_1 &= r_2 q_3 + r_3 \qquad 0 < r_3 < b \\
&\cdots \\
r_{k-2} &= r_{k-1} q_k + r_k \qquad 0 < r_k < r_{k-1} \\
&\cdots \\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \qquad 0 < r_{n-1} < r_{n-2} \\
r_{n-2} &= r_{n-1} q_n \qquad r_n = 0.
\end{aligned}$$

La suite des restes $r_1, r_2, \ldots, r_k, \ldots$ est une suite d'entiers positifs ou nuls strictement décroissante, donc nécessairement il existe un entier n tel que $r_n = 0$.

D'après le lemme, on a

$$pgcd(a, b) = pgcd(b, r_1) = \cdots = pgcd(r_{j-1}, r_j) = r_j.$$

Le pgcd de a et b est le dernier reste non nul.

Exemple 2.4.1. *$a = 198$ et $b = 75$. On déroule l'algorithme comme suit :*

$$\begin{aligned}
198 &= 75 \times 2 + 48 \\
75 &= 48 \times 1 + 27 \\
48 &= 27 \times 1 + 21 \\
27 &= 21 \times 1 + 6 \\
21 &= 6 \times 3 + 3 \\
6 &= 3 \times 2 \qquad \Longrightarrow pgcd(a, b) = 3.
\end{aligned}$$

L'algorithme d'Euclide-Bézout ou d'Euclide étendu

De l'algorithme d'Euclide ci-dessus on peut aussi déduire un couple (u, v) satisfaisant l'identité de Bézout : $d = au + bv$. Le sous-groupe de $\mathbb{Z}$

$$H = \{am + bn \mid m, n \in \mathbb{Z}\}$$

contient les nombres $r_1 = a - bq_1$, $r_2 = b - r_1q_2$, ... *Si* $r_1, \ldots, r_{k-1}, r_k$ *sont des éléments de* H, *de la forme*

$$r_k = au_k + bv_k \qquad (k \geq 1)$$

alors, de la relation

$$r_{k+1} = r_{k-1} - q_{k+1}r_k$$

on déduit

$$\begin{aligned} r_{k+1} &= au_{k-1} + v_{k-1} - q_{k+1}(au_k + bv_k) \\ &= a(u_{k-1} - q_{k+1}u_k) + b(v_{k-1} - q_{k+1}v_k), \end{aligned}$$

d'où les relations de récurrence

$$\begin{aligned} u_{k+1} &= u_{k-1} - q_{k+1}u_k \\ v_{k+1} &= v_{k-1} - q_{k+1}v_k. \qquad (k \geq 2) \end{aligned}$$

Les coefficients u *et* v *cherchés sont* u_{n-1} *et* v_{n-1}. *Pour que*

$$u_1 = 1 = u_{-1} - q_1u_0, \quad v_1 = -q_1 = v_{-1} - q_1v_0,$$

on convient que

$$u_{-1} = 1, \quad u_0 = 0, \quad v_{-1} = 0, \quad v_0 = 1.$$

Pour l'exemple ci-dessus on a

k	r_k	q_k	u_k	v_k
-1	198	*	1	0
0	75	*	0	1
1	48	2	1	-2
2	27	1	-1	3
3	21	1	2	-5
4	6	1	-3	8
5	3	3	11	-29
6	0	2	-25	66

c'est-à-dire

$$\begin{aligned} 3 &= 21 - 6 \times 3 \\ &= 21 - (27 - 21) \times 3 \\ &= 21 \times 4 - 27 \times 3 \\ &= (48 - 27) \times 4 - 27 \times 3 \\ &= 48 \times 4 - 27 \times 7 \\ &= 48 \times 4 - (75 - 48) \times 7 \\ &= (198 - 75 \times 2) \times 11 - 75 \times 7 \\ &= 11a + (-29)b. \end{aligned}$$

Définition 2.4.1. *On dit que deux entiers non nuls sont premiers entre eux si leur pgcd est égal à 1.*

Théorème 2.4.1. *L'équation diophantienne $ax + by = c$ a des solutions dans $\mathbb{Z}^2$ ssi $d = pgcd(a, b)$ divise c. Si (x_0, y_0) est une solution, alors toute solution (x, y) peut s'exprimer comme suit :*

$$x = x_0 - bt/d, \qquad y = y_0 + at/d \qquad t \in \mathbb{Z}.$$

Preuve. D'abord on a

$$\{ax + by | x, y \in \mathbb{Z}\} = d\mathbb{Z}.$$

Donc l'équation a des solutions entières ssi $c \in d\mathbb{Z}$, i.e. $d|c$.

Si l'équation a une solution (x_0, y_0) on vérifie facilement que (x, y) donné par la formule ci-dessus est une solution. Inversement, si (x, y) est une solution, alors

$$ax + by = ax_0 + by_0 = c \Longrightarrow a(x - x_0) = -b(y - y_0).$$

Donc

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0).$$

Comme a/d et b/d sont premiers entre eux, Thm. Gauss implique que

$$y - y_0 = \frac{a}{d}t \qquad \text{pour un } t \in \mathbb{Z}$$

et puis $x - x_0 = -\frac{b}{d}t$. □

Exemple 2.4.1. *Résoudre $15x + 10y = 3$. Comme $pgcd(15, 10) = 5$ et $5 \nmid 3$, l'équation n'a pas de solution entière.*

Exemple 2.4.2. *Résoudre $169x + 121y = 1$. On sait que $(58, -81)$ est une solution. Donc la solution générale est*

$$x = 58 - 121t, \qquad y = -81 + 169t \qquad t \in \mathbb{Z}.$$

Chapitre 3

Congruences

Résumé

Congruences dans Z. L' "anneau " Z/nZ .Resolution des equations lineaires modulo n .Algorithme d'inversion. Petit theoreme de Fermat. Theoreme de Wilson. Theoreme des restes chinois. Indicateur d' Euler. Theoreme d' Euler. Application a la cryptographie a clefs publiques.

3.1 L'anneau $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 1$ fixé. On dit que a est congru à b modulo n si n divise $a - b$ et on écrit $a \equiv b \pmod{n}$, i.e.

$$a \equiv b \pmod{n} \iff n|(a-b).$$

On vérifie que c'est une relation d'équivalence, i.e. elle est
— *réflexive : $\forall x \in \mathbb{Z}$, $x \equiv x$,*
— *symétrique : $\forall x, y \in \mathbb{Z}$, $x \equiv y \iff y \equiv x$,*
— *transitive : $\forall x, y, z \in \mathbb{Z}$, si $x \equiv y$ et $y \equiv z$, alors $x \equiv z$.*
Soit $\bar{a}$ la classe d'équivalence de a, i.e., l'ensemble des entiers congrus à a modulo n :

$$\bar{a} = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\} = \{a + kn \mid k \in \mathbb{Z}\}.$$

On sait que toute relation déquivalence sur un ensemble induit une partition de cet ensemble en classes d'équivalence. Comme tout entier peut s'écrire sous la forme $a + kn$ avec $0 \leq a < n$ et $k \in \mathbb{Z}$, on en déduit qu'il existe n classes d'équivalence et on note l'ensemble quotient par $\mathbb{Z}/n\mathbb{Z}$, i.e.

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \quad \bar{1}, \quad \ldots, \quad \overline{n-1}\}.$$

Par exemple, l'heure est comptée dans $\mathbb{Z}/24\mathbb{Z}$ ou dans $\mathbb{Z}/12\mathbb{Z}$.

Remarque 3.1.1. *La relation de congruence $\equiv$ est plus faible que la relation d'égalité $=$. En effet,*

$$a = b \Longleftrightarrow a \equiv b \pmod{n} \quad \forall n \geq 1.$$

On pourrait utiliser des congruences pour tester l'égalité. Votre numéro de sécurité sociale est formé du numéro d'inscription (NIR) à 13 chiffres et d'une clé de contrôle à 2 chiffres :

$$\textit{Clé NIR} = 97 - (\textit{NIR} \pmod{97})$$

Exemple : 1 53 12 45 007 231 60.

Proposition 3.1.1. *Soit n un entier ≥ 1. Si*

$$a \equiv b, \qquad c \equiv d \pmod{n}$$

avec a, b, c, $d \in \mathbb{Z}$, alors

$$a + c \equiv b + d, \qquad ac \equiv bd \pmod{n}.$$

Démonstration. En effet, si $n \mid a - b$ et $n \mid c - d$, il divise leur somme $(a - b) + (c - d) = (a + c) - (b + d)$. De même, si n divise $(a - b)c$ et $b(c - d)$, alors il divise leur somme $ac - bd$. □

Ce résultat signifie que la relation de congruence est compatible avec l'addition et multiplication de l'anneau $\mathbb{Z}$. Autrement dit,

$$a \in \bar{k},\ b \in \bar{l} \Longrightarrow a + b \in \overline{k + l},\ ab \in \overline{kl}.$$

Ceci nous permet de définir deux lois de composition $+$ et $\cdot$ dans $\mathbb{Z}/n\mathbb{Z}$:

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

On vérifie sans peine que $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ a une structure d'anneau :

$$\begin{gathered} \bar{a} + \bar{b} = \bar{b} + \bar{a}, \qquad \bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a} \\ (\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b}, +\bar{c}) \qquad (\bar{a} \cdot \bar{b}) \cdot \bar{c} = \bar{a} \cdot (\bar{b} \cdot \bar{c}) \\ \bar{0} + \bar{a} = \bar{a}, \qquad \bar{1} \cdot \bar{a} = \bar{a}. \end{gathered}$$

De plus

$$\forall \bar{a} \in \mathbb{Z}/n\mathbb{Z}, \qquad \exists - \bar{a} = \overline{-a} \quad \textit{tel que} \quad \bar{a} + (-\bar{a}) = \bar{0}.$$

Exemple 3.1.1. *Les tables d'addition et de multiplication de $\mathbb{Z}/n\mathbb{Z}$ pour $n = 3$ et $n = 4$. On note que $2 \cdot 2 = 0$ dans $\mathbb{Z}/4\mathbb{Z}$.*

Exercice 3.1.1. *Construire les tables d'addition et de multiplication de $\mathbb{Z}/n\mathbb{Z}$ pour $n = 6$ et $n = 5$.*

Définition 3.1.1. *Un élément $\bar{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est dit inversible si $\exists \bar{b} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\bar{a} \cdot \bar{b} = \bar{1}$.*

Si $\bar{a}$ est inversible, alors son inverse est unique. En effet, si $\bar{a} \cdot \bar{b}' = \bar{1}$. Alors $\bar{b}' = (\bar{b} \cdot \bar{a}) \cdot \bar{b}' = \bar{b} \cdot (\bar{a} \cdot \bar{b}') = \bar{b}$.

Proposition 3.1.2. *Soit n un entier ≥ 2. L'ensemble des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour la multiplication, noté $(\mathbb{Z}/n\mathbb{Z})^*$.*

Démonstration. Il suffit de remarquer que :
a) si $\bar{a}$ est inversible, alors son inverse $\bar{a}^{-1}$ est aussis inversible, d'inverse $\bar{a}$,
b) si $\bar{a}$ et $\bar{b}$ sont inversibles, d'inverses $\bar{a}^{-1}$ et $\bar{b}^{-1}$, alors $\overline{ab}$ est inversible, d'inverse $\bar{b}^{-1}\bar{a}^{-1}$.

□

Exemple 3.1.1. $(\mathbb{Z}/6\mathbb{Z})^* = \{\bar{1}, \bar{5}\}$ *et* $(\mathbb{Z}/5\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$.

Proposition 3.1.3. *Soit $n \geq 2$. Alors $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ est inversible ssi a est premier avec n.*

Preuve. L'équation $\bar{a} \cdot \bar{b} = \bar{1}$ équivaut à $ab - nk = 1$ pour un certain $k \in \mathbb{Z}$. La dernière a des solutions entières ssi $pgcd(a, n) = 1$. □

Corollaire 3.1.1. *Soit p un nombre premier. Alors tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible.*

Remarque 3.1.2. *On dit que $\mathbb{Z}/p\mathbb{Z}$ est un corps. Notons que dans un corps le produit de deux éléments non nuls n'est pas nul, autrement dit $ab = 0 \Longrightarrow a = 0$ ou $b = 0$ car si $a \neq 0$ alors a^{-1} existe, donc $b = a^{-1}(ab) = a^{-1}0 = 0$.*

Définition 3.1.2. *Soit $n \geq 2$. On appelle indicatrice d'Euler, et on note $\varphi(n)$, le nombre d'entiers positifs $< n$ qui sont premiers avec n.*

Par convention, on pose $\varphi(1) = 1$. On a, par exemple, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$ et $\varphi(p) = p - 1$ où p est premier.

Théorème 3.1.1 (Euler)**.** *Soit n un entier ≥ 2 et a un entier premier avec n. Alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Preuve. Soient $t_1, t_2, \ldots, t_{\varphi(n}$ les entiers premiers positifs $< n$ premiers avec n. On note s_i le reste de la division de at_i par n pour $i = 1, 2, \ldots, \varphi(n)$. Alors $s_1, \ldots, s_{\varphi(n)}$ est une permutation de $t_1, \ldots, t_{\varphi(n)}$. Il suffit de vérifier que $s_i \neq s_j$ pour $i \neq j$. Supposons le contraire, alors $at_i = at_j \pmod{n}$. Comme a est premier avec n, le théorème de Gauss implique que $t_i \equiv t_j \pmod{n}$. C'est absurde. D'où

$$(at_1) \ldots (at_{\varphi(n)}) \equiv s_1 \ldots s_{\varphi(n)} \pmod{n},$$

i.e.

$$a^{\varphi(n)}t_1 \dots t_{\varphi(n)} \equiv t_1 \dots t_{\varphi(n)} \pmod{n},$$

Comme $t_1 \dots t_{\varphi(n)}$ est premier avec n, le thm. de Gauss implique que $a^{\varphi(n)} = 1 \pmod{n}$. □

Corollaire 3.1.2 (Fermat)**.** *Soit p un nombre premier et $pgcd(a,p) = 1$, alors $a^{p-1} \equiv 1 \pmod{p}$.*

2eme preuve. On montre l'identité équivalente $a^n \equiv a \pmod{p}$ par récurrence sur a. Si $a = 1$ c'est évident. Supposons $a^p \equiv a \pmod{p}$. On a

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

Or $p \mid \binom{p}{k}$ pour $1 < k < p$, d'où $(a+1)^p \equiv 1 + a \pmod{p}$ par l'hypothèse de récurrence. □

Théorème 3.1.2 (Wilson)**.** *Si p est un nombre premier, alors*

$$(p-1)! \equiv -1 \pmod{p}.$$

1ère Preuve. On considère le polynôme $p(x) = x^{p-1} - \bar{1}$ sur le corps $\mathbb{Z}/n\mathbb{Z}$. Le petit thm. de Fermat montre que $\bar{1}, \bar{2}, \dots, \overline{p-1}$ sont des racines de $p(x)$. Donc

$$p(x) = (x - \bar{1})(x - \bar{2}) \dots (x - \overline{p-1}).$$

En identifiant le terme constant de $p(x)$ on obtient $\overline{(p-1)!} = -\bar{1}$, ce qui équivaut au thm. de Wilson. □

2ème Preuve. Tout élément non nul $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ admet un unique inverse $\bar{a}^{-1}$. On remarque que $\bar{a} \neq \bar{b}$ implique que $\bar{a}^{-1} \neq \bar{b}^{-1}$, car sinon, $\bar{a}^{-1} = \bar{b}^{-1}$ alors

$$\bar{b} = \bar{a}\bar{b}\bar{a}^{-1} = \bar{a}\bar{b}\bar{b}^{-1} = \bar{a}.$$

De plus $\bar{1}^{-1} = \bar{1}$ et $\overline{p-1} = \overline{p-1}$. Soit $A_p = \{2, \dots, p-2\}$. Alors pour tout $a \in A_p$ il existe un $b \in A_p$ tel que $\bar{a} \cdot \bar{b} = \bar{1}$. Montrons que $a \neq b$. Sinon, $\bar{a}^2 = \bar{1}$. Ceci équivaut à $p \mid (a-1)(a+1)$. Comme p est premier, on a $p \mid (a-1)$ ou $p \mid (a+1)$, c'est absurde car $a \leq p-2$. En résumé, on peut coupler les entiers de A_p deux à deux tel que la classe de leur produit dans $\mathbb{Z}/p\mathbb{Z}$ soit égale à $\bar{1}$. On en déduit donc

$$\overline{(p-1)!} = \overline{(p-1)} \prod_{a \in A_p} \bar{a} = \overline{(p-1)} = \overline{-1}.$$

□

Remarque 3.1.3. *L'inverse du théorème de Wilson est aussi vrai : si $(n-1)! \equiv -1 \pmod{n}$ alors n est premier. En effet, si n était composé, alors $n = pq$ avec $1 < p, q < n$. Donc $n = pq \mid [(n-1)!]^2 \implies [(n-1)!]^2 \equiv 0 \pmod{n}$. Ceci contredit le fait que $(n-1)! \equiv -1 \pmod{n}$.*

3.2 Système d'équations diophantiennes

Proposition 3.2.1. *Soient a, b, d des entiers et r, s des entiers positifs. Alors*
— $a \equiv b \pmod{r}$ *et* $a \equiv b \pmod{s} \Longrightarrow a \equiv b \pmod{[r,s]}$,
— $ad \equiv bd \pmod{r}$ *et* $d \neq 0 \Longrightarrow a \equiv b \pmod{r/(r,d)}$.

Considérons l'équation de congruence $ax \equiv b \pmod{n}$.

Lemme 3.2.1. *On a*

$$ax \equiv b \pmod{n} \quad \textit{dans} \quad \mathbb{Z} \Longleftrightarrow \bar{a}\bar{x} = \bar{b} \quad \textit{dans} \quad \mathbb{Z}/n\mathbb{Z}.$$

Preuve. En effet

$$ax \equiv b \pmod{n} \Longleftrightarrow ax = b + nk \quad (k \in \mathbb{Z}) \Longleftrightarrow \overline{a} \cdot \bar{x} = \overline{b}.$$

□

Proposition 3.2.2. *L'équation $ax \equiv b \pmod{n}$ a des solutions entières ssi $pgcd(a,n) \mid b$.*

Preuve. Résoudre $ax \equiv b \pmod{n}$ dans $\mathbb{Z}$ équivaut à résoudre $ax + ny = b$ dans $\mathbb{Z}^2$. □

Supposons que $pgcd(a,n) \mid b$. Soit $d = pgcd(a,n)$. Alors l'équation du départ devient

$$(a/d)x \equiv (b/d) \pmod{n/d} \Longleftrightarrow \overline{(a/d)}\bar{x} = \overline{(b/d)} \qquad \mathbb{Z}/(n/d)\mathbb{Z}.$$

D'où $\bar{x} = \overline{(a/d)}^{-1}\overline{(b/d)}$ dans $\mathbb{Z}/(n/d)\mathbb{Z}$.

Comment calculer a tq $ab \equiv 1 \pmod{n}$ où $(a,n) = 1$. i) par l'algorithme étendu d'Euclide, $ab + nk = 1$. ii) par le théorème d'Euler : $a \cdot a^{\varphi(n)-1} \equiv 1 \pmod{n}$.

Considérons le système d'équations de congruence

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ \cdots &\equiv \cdots \\ a_r x &\equiv b_r \pmod{m_r} \end{aligned}$$

D'après ce qui précède, ce système équivaut à résoudre plusieurs systèmes de type suivants :

$$x \equiv b_1 \pmod{m_1} \quad \cdots \quad x \equiv b_r \pmod{m_r} \qquad (S)$$

Lemme 3.2.2. *Soient $m_1, \ldots, m_r$ des entiers > 0 deux à deux premiers entre eux. Si $m_i \mid n$ pour $i = 1, \ldots, r$ alors $m_1 \cdots m_r \mid n$.*

Preuve. Par récurrence sur r et *Gauss*. Pour $r = 1$ il n'y a rien à démontrer.
H.R. vrai pour $r - 1$.
Comme m_r divise $n = m_1 \cdots m_{r-1} q$ et m_r est premier avec $m_1 \cdots m_{r-1}$, donc Gauss implique que $m_r \mid q$, i.e. $q = m_r q'$. □

Lemme 3.2.3. *Si $m_1, \ldots, m_r$ sont tous premiers avec m, alors $(m_1 \cdots m_r, n) = 1$.*

Preuve. Bézout : $m_i u_i + n v_i = 1$. On les multiplie : $m_1 \cdots m_r u_1 \cdots u_r + nV = 1$. Le thm de Bézout permet de conclure. □

Théorème 3.2.1 (Thm. du reste chinois)**.** *Soient $m_1, \ldots, m_r$ des entiers > 0 deux à deux premiers entre eux. Alors le système (S) a des solutions et deux solutions diffèrent d'un multiple de $m_1 \ldots m_r$.*

Preuve. Soit $M = m_1 \ldots m_r$, $m_i' = M/m_i$ $(1 \leq i \leq r)$. Par Lemme 1, M et m_i' sont premiers entre eux. Il existe donc un entier c_i tel que $m_i' c_i \equiv 1 \pmod{m_i}$ pour $i = 1, \ldots, r$. On vérifie que

$$x_0 = \sum_{i=1}^{r} b_i c_i m_i'$$

est une solution. En effet, m_j' est un multiple de m_i pour $j \neq i$, donc

$$x \equiv b_i m_i' c_i \equiv b_i \pmod{m_i}.$$

Si x' est aussi une solution. Alors $x_0 \equiv x' \pmod{m_i}$ pour $i = 1, \ldots, r$. Comme $m_1, \ldots, m_r$ sont deux à deux premiers entre eux, le Lemme 2 entraîne que $x \equiv x' \pmod{m_1 \ldots m_r}$. □

La preuve montre que la solution générale du système (S) est

$$x \equiv \sum_{i=1}^{r} b_i c_i m_i' \pmod{M}.$$

Exemple 3.2.1. *Considérons le système*

$$x \equiv c_1 \pmod{10}, \quad x \equiv c_2 \pmod{11}, x \equiv c_3 \pmod{13}.$$

On est amené à résoudre les équations :

$$143 z_1 \equiv 1 \pmod{10}, \quad 130 z_2 \equiv 1 \pmod{11}, 110 z_3 \equiv 1 \pmod{13}.$$

et elles ont les solutions : $z_1 = 7, \quad z_2 = 5, \quad z_3 = 11$. Donc

$$\begin{aligned} x &\equiv 143 \cdot 7 c_1 + 130 \cdot 5 c_2 + 10 \cdot 11 c_3 \\ &\equiv 1001 c_1 + 650 c_2 + 1210 c_3 \pmod{1430}. \end{aligned}$$

Proposition 3.2.3. *Si m et n sont deux entiers premiers entre eux, alors $\varphi(mn) = \varphi(m)\,\varphi(n)$.*

Preuve. Le thm du reste chinois signifie que l'application

$$\begin{aligned} \phi : \mathbb{Z}/mn\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x + mn\mathbb{Z} &\mapsto (x + m\mathbb{Z},\ x + n\mathbb{Z}) \end{aligned}$$

est bijective. L'élément $x + mn\mathbb{Z}$ est inversible dans $\mathbb{Z}/mn\mathbb{Z}$ ssi $(x,\, mn) = 1$, ce qui équivaut à $(x,\, m) = 1$ et $(x,\, n) = 1$, à savoir que $x + m\mathbb{Z}$ et $x + n\mathbb{Z}$ sont inversibles dans $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ respectivement. Par restriction on déduit une bijection $\bar{\phi}$ de $(\mathbb{Z}/mn\mathbb{Z})^*$ sur $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. Par conséquent ils ont le même cardinal : $\varphi(mn) = \varphi(m)\,\varphi(n)$. □

Proposition 3.2.4. *Soit p un nombre premier et $n > 0$. Alors*

$$\varphi(p^n) = (p-1)p^{n-1}.$$

Preuve. Les nombres $\leq p^n$ qui ne sont pas premiers avec p^n sont précisément kp avec $k = 1, 2, \ldots, p^{n-1}$. D'où $\varphi(p^n) = p^n - p^{n-1}$. □

3.3 Application à la cryptographie

La cryptographie (du grec kruptos*, caché, et* graphein*, écriture) est la science du codage et du déchiffrement des messages codés. L'arithmétique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo n fournit des systèmes de codage.*

On identifie l'alphabet avec l'ensemble $\mathbb{Z}/26\mathbb{Z}$ en remplaçant chaque lettre par son rang dans l'alphabet, mais dans la pratique on devrait prendre $\mathbb{Z}/n\mathbb{Z}$ avec $n \geq 26$ à cause de virgule, d'espace, ...

3.3.1 Alphabet de Jule César ou codage par décalage

Le premier système authentique de cryptographie est celui de Jules César. Chaque lettre était remplacée par celle située trois positions plus loin dans l'alphabet : c'est ainsi que le mot BONJOUR devient DRQNRWS. En terme de l'anneau, c'est le codage par l'addition : $a \mapsto a+2$, decodage par sousstraction : $a \mapsto a - 2$

$$a \longrightarrow a + 2 \longrightarrow a + 2 - 2 = a$$

3.3.2 Codage par multiplication

Ceci consiste à la multiplication de chaque entier par un entier inversible modulo 26. Il y a $\varphi(26) = 12$ *entiers inversibles modulo 26. Choisisson, par exemple, 7, appelé la clé de codage. Alors le codage du mot* $2-15-14-11-10-15-21-18$*, qui signifie BONJOUR, est donné par*

$$14-1-20-25-18-1-17-22.$$

Pour le déchiffrer on multiplie chaque nombre par 15, qui est l'inverse de 7 modulo 26. Le nombre 15 est la clé de déchiffrement. Illustration

$$a \mapsto 7a \mapsto 15(7a) = a \qquad (\text{mod } 26).$$

Le déchifrement des codages ci-dessus (permutation de alphabet) est assez facile à trouver.

3.3.3 Codage par élevation à une puissance

Soit $\varphi(n)$ *l'indicatrice d'Euler de* n *et soit* h *un entier premier avec* $\varphi(n)$*. Il existe alors un entier* k *tel que*

$$hk \equiv 1 \pmod{\varphi(n)}.$$

D'après le thm d'Euler, pour tout $a \in (\mathbb{Z}/n\mathbb{Z})^*$ *on a*

$$a \longrightarrow a^h \longrightarrow (a^h)^k = a^{1+m\varphi(n)} = a.$$

Par exemple, soit à coder le message BONJOUR. On remplace chaque lettre par son rang dans l'alphabet. On obtient : $2\,15\,14\,1110\,15\,21\,18$*. Choisissons* $n = 43$*. Nous avons* $\varphi(n) = 42$*. Elevons chacun des nombres à la puissance* $h = 5$ *modulo 43. On obtient*

$$32-38-23-16-25-38-4-19$$

3.3.4 Système RSA

Le problème avec les exemples ci-dessus est que le codage et le déchiffrement peuvent être facilement déduites de quelques messages. Il suffit en effet de connaître la fréquence d'apparition des lettres dans un texte d'une langue donnée. A partir d'un échantillon de messages suffisant le décryptage est rapide.

Le système RSA fournit une solution à ce problème. On commence par compliquer le cryptage en procédant comme suit. Au lieu de remplacer une lettre par une autre on peut remplacer une suite, disonbs de k *lettres ou symboles successifs (éventuellement des blancs) par un autre symbole. Cela veut dire construire une application de* A^k*, où* A *est notre alphabet usuel auquel*

on a adjoint un certain nombre de symboles (virgule, point, blanc, ...) vers un autre ensemble B. On donnera un exemple plus loin.

Dans cette section on va donner une brève introduction à la cryptographie. *Plus précisément, on va donner une description rapide et très simplifiée du système* RSA *(pour Rivest, Shamir et Adleman).*

On commence On considère deux personnes appelées Alice et Bob par exemple, souhaitant communiquer entres elles en toute confidentialité. Ils choisissent chacun une paire de nombres premiers garnds, *p_x et q_x pour Alice et p_y et q_y pour Bob. On pose $n_x = p_x q_x$ et $n_y = p_y q_y$. Puis Alice choisit également un entier c_x premier avec*

$$\varphi(n_x) = (p_x - 1)(q_x - 1)$$

et Bob un entier c_y premier avec

$$\varphi(n_y) = (p_y - 1)(q_y - 1)$$

La classe de congruence de l'entier c_x admet un inverse d_x dans le groupe multiplicatif $(\mathbb{Z}/n_x\mathbb{Z})^* \sim \mathbb{Z}/\varphi(n_x)\mathbb{Z}$. Cette classe est facile à calculer rapidement dans la mesure où l'on connaiît la valeur de $\varphi(n_x)$. De même la classe de congruence de l'entier c_y admet un inverse d_y dans le groupe multiplicatif $(\mathbb{Z}/n_y\mathbb{Z})^* \sim \mathbb{Z}/\varphi(n_y)\mathbb{Z}$, elle est rapide à calculer dans la mesure où l'on connaît la valeur de $\varphi(n_y)$. Nous ne rentrerons pas dans les détails mais ce calcul, en temps, est court.

Mais si on ne connaît que les valeurs n_x et n_y, respectivement n_y et c_y, le calcul devient très difficile, c'est-à-dire très long en temps. La seule façon connue de procéder en général est de chercher la décomposition en nombres premiers de n_x et n_y, puis d'en déduire les valeurs de la fonction d'Euler.

La décomposition en nombres premiers est facile théoriquement, on divise successivement par tous les nombres premiers, par contre, elle est extrêmement longue du point de vue du temps de calcul, au point de devenir inaccessible dès que les nombres en jeu sont très grands. Pratiquement le calcul de d_x, respectivement d_y est impossible à partir de n_x et c_x, respectivement de n_y et c_y.

Les messages sont alors codés de la façon suivante. D'abord les lettres des alphabets B introduit plus haut sont identifiées à des classes de congruences inversibles modulo n_x d'une part, à des classes de congruences modulo n_y d'autre part. On entend par là que l'on se donne une application injective de

$$\alpha \ : \ B \longrightarrow (\mathbb{Z}/n_x\mathbb{Z})^*$$

et une application injective

$$\beta \ : \ B \longrightarrow (\mathbb{Z}/n_y\mathbb{Z})^*$$

Ces identifications sont publiques et connues des correspondants.

On ne considère donc maintenant que des suites de symboles qui sont des classes de congruences.

Les clés n_x, c_x et n_y, c_y sont publiques. Les valeurs de p_x, q_x, d_x et p_y, q_y, d_y par contre sont secrètes et ne sont connues que de Alice, respectivement de Bob. Bient entendu les valeurs de $\varphi(n_x)$ et $\varphi(n_y)$ sont aussi secrètes.

Supposons alors que Alice veuille coder un message destiné à Bob et que ce message soit exprimé comme une suite de symboles appartenant à $(\mathbb{Z}/n_x\mathbb{Z})^*$. Il applique à cette suite de symboles, soit $(a_1, a_2, \ldots, a_k, \ldots)$ la transformation :

$$(a_1, a_2, \ldots, a_k, \ldots) \mapsto (a_1^{c_y}, a_2^{c_y}, \ldots, a_k^{c_y}, \ldots)$$

puis il envoie le message. Le calcul effectif n'est pas prohibitif en temps.

Quand Bob reçoit le message il applique la transformation inverse :

$$(b_1, b_2, \ldots, b_k, \ldots) \mapsto (b_1^{d_y}, b_2^{d_y}, \ldots, b_k^{d_y}, \ldots)$$

Ce qu'il est seul à pouvoir faire dans la mesure où il est le seul à connaître d_y. Ceci restitue le message émis.

Décrivons maintenant le processus sur un exemple. Supposons que l'on veuille transmettre le mot cryptage. *On commence par le diviser en parquets de 2 lettres successives. On obtient donc la suite* cr, yp, ta, ge. *Choisissons $p_y = 19, \qquad q_y = 43$. On a $n_y = 817$ et $\varphi(n_y) = 756$.*

Supposons avoir choisi une application β de A^2 dans $(\mathbb{Z}/817\mathbb{Z})^*$. C'est possible, il suffit de comparer les cardinaux. Supposons avoir

$$\beta(cr) = 2, \quad \beta(yp) = 11, \quad \beta(ta) = 3, \quad \beta(ge) = 8.$$

Bob choisit maintenant $c_y = 11$ et à l'aide de l'algorithme d'Euclide, trouve $d_y = 275$. Alice connaît la valeur de c_y et donc aplique la transformation suivante

$$(2,\ 11,\ 3,\ 8) \mapsto (2^{11},\ 11^{11},\ 3^{11},\ 8^{11}) \equiv (414,\ 64,\ 675,\ 677) \pmod{817},$$

et transmet. Bob applique alors la transformation suivante :

$$(414,\ 64,\ 675,\ 677) \mapsto (414^{275},\ 64^{275},\ 675^{275},\ 677^{275}) \equiv (2, 11, 3, 8) \pmod{817}.$$

Il est le seul à pouvoir la faire, étant le seul à connaître d_y.

Chapitre 4

Groupes

Résumé

Groupes. Generalités.Exemples. Sous-groupes. Morphismes. Image et noyau d'un morphisme. Isomorphismes. Produit direct. Automorphismes. Conjugaisons. Centre. Ordre d'un groupe. Groupe symetrique. Théorème de Cayley. Groupes monogènes et groupes cycliques.

4.1 Définitions, généralités, exemples

Définition 4.1.1. *Un groupe est un ensemble G muni d'une loi de composition interne $*$, i.e., une application $* : G \times G \longrightarrow G$ qui satisfait aux conditions suivantes :*
i) la loi $*$ est associative,
ii) il existe un élément neutre e, i.e., $e * a = a * e = a$ pour tout $a \in G$,
iii) tout élément est symétrisable, i.e., $\forall a \in G$, $\exists a' \in G$ tel que $a * a' = a' * a = e$.
Le groupe $(G, *)$ est dit abélien *ou* commutatif *si la loi $*$ est commutative, i.e., $a * b = b * a$, $\forall a, b \in G$.*

Remarque 4.1.1. *Le couple $(G, *)$ avec i) est dit un* semi-groupe *et $(G, *)$ avec i) et ii) est appelé* monoïde*. Dans un groupe, l'élément neutre e est unique. En effet, si e' est aussi un élément neutre, alors $e' = e * e' = e$ par définition. L'inverse de chaque élément a est aussi unique : si $a'a = aa' = e$ alors $a^{-1} = e * a^{-1} = a'aa^{-1} = a'e = a'$.*
Notation *On note en général la loi de composition multiplicativement : $ab := a * b$ et addidivement si elle est commutative : $a + b := a * b$.*
Les éléments neutres sont respectivement donc 1 *et* 0*. L'élément inverse de a est aussi noté*

respectivement a^{-1} *et* $-a$. *Par suite, pour tout* $n \in \mathbb{N}$,

$$\begin{aligned} x^n &= \underbrace{x * \cdots * x}_{n} \qquad x^{-n} = \underbrace{x^{-1} * \cdots * x^{-1}}_{n} \\ nx &= \underbrace{x + \cdots + x}_{n} \qquad (-n)x = \underbrace{(-x) + \cdots + (-x)}_{n}. \end{aligned}$$

Exemples 4.1.1. — $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\{-1, 1\}, \cdot)$, $(\mathbb{Q}_+^*, \cdot)$ *et* $(\mathbb{Z}/n\mathbb{Z}, +)$ *sont tous des groupes abéliens.*

— *L'ensembles des éléments inversibles* $((\mathbb{Z}/n\mathbb{Z})^*, \times)$ *est un groupe multiplicatif abélien.*

— *L'ensemble des matrices inversibles d'ordre* n, *à coefficients réels* $GL(n, \mathbb{R})$ *muni du produit de matrices, est un groupe non commutatif si* $n \geq 2$.

— *L'ensemble* $\mathfrak{S}_n$ *des bijections de* $\{1, \ldots, n\}$ *muni de la composition d'applications est un groupe non abélien si* $n \geq 2$. *Par exemple, si*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad et \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

alors que

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \quad et \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Remarque 4.1.2. *Soit* $a \in G$. *Alors* $f_a : G \to G$ *définie par* $f_a(x) = ax$ $(\forall x \in G)$ *est une bijection.*

On peut caractériser un groupe par sa table de multiplication lorsque le cardinal est petit. Il est clair qu'il n'y a qu'un seul groupe d'ordre 1 : $(\{e\}, \cdot\})$. *Les groupes d'ordre 2 et 3 sont les suivants :*

$*$	e	a
e	e	a
a	a	e

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Il y a essentiellement deux groupes d'ordre 4 (qui sont isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *et* $\mathbb{Z}/4\mathbb{Z}$). *Soit* $G = \{e, a, b, c\}$ *un groupe. On distingue deux cas :* $a^2 = e$ *(ou* $b^2 = e$ *ou* $c^2 = e$*) :*

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	**e**	**a**
c	c	b	**a**	**e**

ou

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	**a**	**e**
c	c	b	**e**	**a**

et $a^2 \neq e$ (ou $b^2 \neq e$, ou $c^2 \neq e$), soit $a^2 = b$, alors

$*$	e	a	b	c
e	e	a	b	c
a	a	$\boldsymbol{b}$	c	e
b	b	c	e	a
c	c	e	a	b

On voit que les deux derniers groupes $\{e, b, b^2, b^3\}$ et $\{e, a, a^2, a^3\}$ sont isomorphes. Ils sont tous abéliens. Je vous laisse le soin de vérifier l'associativité.

4.2 Sous-groupes et morphismes

Soit $(G, *)$ un groupe et H, K deux parties de G. On définit

$$\begin{aligned} H \cdot K &= \{xy \mid x \in H,\, y \in K\}, \\ H^{-1} &= \{x^{-1} \mid x \in H\}. \end{aligned}$$

Définition 4.2.1. *Une partie non vide H de G est un sous-groupe de G si (i) $H \cdot H \subset H$ (ii) $H^{-1} \in H$.*

On note $H \leq G$ si H est un sous-groupe de G. Autrement dit, le sous-ensemble H a une structure de groupe par rapport à la loi $*$. Comme $H \neq \emptyset$, $\exists\, a \in H$ et donc l'élément neutre $e = aa^{-1} \in H$.

Proposition 4.2.1. *Soit H un sous-ensemble non vide de G. Alors H est un sous-groupe de G ssi $H \cdot H^{-1} \subset H$.*

Preuve. Exercice. □

Exemple 4.2.1. — *Tout groupe G a au moins deux ss-gr : G et $\{e\}$, qui sont appelés sous-groupes triviaux. Tt sous-groupe $\neq G$ est appelé sous-groupe propre de G.*
— *Soit G un groupe. Alors $Z(G) = \{x \in G : xy = yx\ \forall y \in G\}$ est un sous-groupe de G, qui est appelé le centre de G.*

Proposition 4.2.2. *Soit $(H_i)_{i \in I}$ une famille de sous-groupes de G, alors $\cap_{i \in I} H_i$ est un sous-groupe de G.*

Preuve. Exercice. □

Proposition 4.2.3. *Etant donnée une famille de groupes $(G_1, \ldots, G_n)$, le produit cartésien $G_1 \times \cdots \times G_n$ muni de la loi de composition interne :*

$$((x_1, \ldots, x_i, \ldots, x_n), (y_1, \ldots, y_i, \ldots, y_n)) \mapsto (x_1 y_1, \ldots, x_i y_i, \ldots, x_n y_n)$$

a une structure de groupe.

Preuve. Exercice. □

Définition 4.2.2. *Ce groupe s'appelle le produit direct des groupes $G_1, \ldots, G_n$.*

Les groupes sont importants tant pour eux mêmes que pour les relations qu'ils ont entre eux. Celles-ci s'expriment par les applications d'un groupe dans un autre, compatible aux lois à la source, et au but, plus précisément :

Définition 4.2.3. *On appelle* (homo)morphisme *de $(G, \cdot)$ dans $(G, *)$ une application $\phi : G \longrightarrow G'$ telle que*

$$\forall (x, y) \in G^2, \qquad \phi(x \cdot y) = \phi(x) * \phi(y).$$

De plus, ϕ est un
— *Isomorphisme $\Longleftrightarrow$ Homomorphisme bijectif*
— *Endomorphisme $\Longleftrightarrow$ Homomorphisme + $G = G'$*
— *Automorphisme $\Longleftrightarrow$ Endomorphisme bijectif*
— *Epimorphisme $\Longleftrightarrow$ Homomorphisme surjectif.*
On dit que deux groupes sont isomorphes s'il existe un isomorphisme entre eux.

Remarque *(i) $\phi(e)$ est l'élément neutre e' de G'. En effet, $e' * \phi(e) = \phi(e) = \phi(ee) = \phi(e) * \phi(e)$, d'où $e' = \phi(e)$.*
(ii) $\phi(x)^{-1} = \phi(x^{-1})$ car $\phi(x^{-1})\phi(x) = \phi(xx^{-1}) = \phi(e) = e'$.

Définition 4.2.4. *Soit $\phi : G \longrightarrow G'$ un morphisme de groupes. Son image et noyau sont définis par* $\mathrm{Im}(\phi) = \{\phi(x) \mid x \in G\}$ *et* $\mathrm{Ker}(\phi) = \{x \in G \mid \phi(x) = e'\}$.

Proposition 4.2.4. *Un morphisme de groupes $\phi : G \to G'$ est injectif ssi* $\mathrm{Ker}(\phi) = \{e\}$.

Preuve. En effet, $\phi(x) = \phi(x') \Longrightarrow \phi(xx'^{-1}) = e' \Longrightarrow xx'^{-1} = e \Longrightarrow x = x'$. La réciproque est claire. □

Les définitions ci-dessus donnent de nouveaux moyens de construire des groupes.

Proposition 4.2.5. *Soit $\phi : G \to G'$ un morphisme de groupes. Alors* $\mathrm{Im}(\phi)$ *est un sous-groupe de G' et* $\mathrm{Ker}(\phi)$ *est un sous-groupe de G.*

Preuve. En effet, $Im(\phi) \neq \emptyset$, car $\phi(e) \in Im(\phi)$, et $\phi(x)\phi(y)^{-1} = \phi(xy^{-1}) \in Im(\phi)$. Le résultat suit.
Comme $e \in \mathrm{Ker}(\phi)$ on a $\mathrm{Ker}(\phi) \neq \emptyset$. Si $x, y \in \mathrm{Ker}(\phi)$, alors $\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} = e'e' = e'$. Il en résulte que $xy^{-1} \in \mathrm{Ker}(\phi)$. □

Exemple 4.2.1. *Soit $u : \mathbb{Z} \to \mathbb{Z}$ un endomorphisme de $(\mathbb{Z}, +)$. Soit $u(1) = n$. Alors $u(2) = u(1) + u(1) = 2n$ et $\forall x \in \mathbb{Z}_+$ on a $u(x) = xu(1) = nx$ et $u(-x) = -u(x) = -nx$. Donc $u(x) = nx$ pour tout $x \in \mathbb{Z}$ et $\mathrm{Im}(u) = n\mathbb{Z}$. Il est clair que u est un automorphisme ssi $n = \pm 1$.*

Exemple 4.2.2. *L'application $p : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ définie par $a \mapsto \bar{a}$ est un epimorphisme de groupes, de limage $\mathbb{Z}/n\mathbb{Z}$ et de noyau $n\mathbb{Z}$.*

Exemple 4.2.3. *On considère l'application $f := \exp : (\mathbb{R}, +) \to (\mathbb{R}_+, \times)$, $x \mapsto \exp(x)$. Alors f est un isomorphisme de groupes : $f(x+y) = f(x) \cdot f(y)$ avec l'inverse $g := \ln : (\mathbb{R}_+, \times) \to (\mathbb{R}, +)$, $g(x) = \ln(x)$.*

Exemple 4.2.4. *L'application $\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ définie par*

$$\bar{a} := a + mn\mathbb{Z} \mapsto (\dot{a} := a + m\mathbb{Z}, \ddot{a} := a + n\mathbb{Z})$$

est un isomophisme de groupes additifs ssi m et n sont 1^{res} entre eux.

En effet, si m et n sont 1^{res} entre eux, alors le théorème chinois implique que φ est bijective. Réciproquement, si $\mathrm{pgcd}(m, n) = d > 1$, alors $\overline{mn/d} \mapsto (\dot{0}, \ddot{0})$ et $\mathrm{Ker}\,\varphi \neq \{\bar{0}\}$. Donc φ n'est pas injective.

Exercice 4.2.1. *Étudier le morphisme φ pour $(m, n) = (2, 2)$ et $(2, 3)$ en donnant la correspondance explicite.*

Soit $Aut(G)$ l'ensemble des automorphismes du groupe G. Muni de la loi de composition d'applications $Aut(G)$ est un groupe. Il n'est pas facile de déterminer $Aut(G)$. Mais on peut en trouver facilement un sous-groupe.

A tout $x \in G$ on associe l'application $i_x : G \longrightarrow G$ définie par $g \mapsto xgx^{-1}$.

Proposition 4.2.6. *L'application i_x est un automorphisme de G, i.e., $i_x \in Aut(G)$.*

Preuve. Pour tous $a, b \in G$, on a $i_x(ab) = x(ab)x^{-1} = xax^{-1}xbx^{-1} = i_x(a)i_x(b)$, donc i_x est un endomorphisme. D'ailleurs, pour tout $g \in G$ il existe $g' = x^{-1}gx \in G$ tel que $i_x(g') = g$ donc i_x est surjective. Enfin, $i_x(a) = i_x(b)$ ssi $a = b$. Donc $i_x \in Aut(G)$. □

Définition 4.2.5. *On appelle i_x un automorphisme intérieur de G. L'ensemble des automorphismes intérieurs de G sera noté $Int(G)$.*

On a donc un morphisme $\phi : G \longrightarrow Aut(G)$ défini par $x \mapsto i_x$. En effet, $\forall x, y \in G$, on a

$$\forall g \in G, \qquad i_x \circ i_y(g) = i_x(i_y(g)) = i_{xy}(g).$$

Donc $i_x \circ i_y = i_{xy}$.

On a $\mathrm{Im}(\phi) = Int(G)$. D'autre part, un élément $x \in G$ appartient au noyau $Ker(\phi)$ ssi $i_x = Id$, i.e., $xgx^{-1} = g$ soit $xg = gx$ pour tout $g \in G$. Donc le noyau est l'ensemble des éléments qui commutent avec tout élément de G. Cet ensemble s'appelle le centre de G, noté $Z(G)$, c'est-à-dire

$$Z(G) = \{g \in G : gx = xg \ \forall x \in G\}.$$

Définition 4.2.6. *Deux éléments de x, y de G sont dits conjugués s'il existe $g \in G$ tel que $i_g(x) = y$. L'ensemble des éléments conjugués à $x \in G$ s'appelle sa classe de conjuguaison, i.e., $C_x = \{gxg^{-1} \mid g \in G\}$.*

Cette notion n'est pas intéressante pour un groupe abélien car si G est abélien, $C_x = \{x\}$ pour tout $x \in G$.

Proposition 4.2.7. *La relation de conjugaison dans un groupe G est une relation d'équivalence de G.*

Preuve. La réflexivité est claire car $i_e(x) = x$. Pour la symétrie, si $i_g(x) = y$ alors $i_{g^{-1}}(y) = x$. Enfin, pour la transitivité, si l'on a $i_g(x) = y$ et $i_{g'}(y) = z$, alors $i_{g'g}(x) = z$. □

Rappelons que l'ensemble des permutations ou bijections S_X d'un ensemble X muni de la composition des applications est un groupe, appelé le groupe symétrique de X. En particulier S_G est un groupe.

Pour tout $g \in G$ on définit l'application $\tau_g : G \longrightarrow G$ par $x \mapsto gx$, appelée translation à gauche.

Lemme 4.2.1. *L'application $\varphi : G \longrightarrow S_G$ définie par $g \mapsto \tau_g$ est donc un morphisme injectif, i.e.,*
(i) Pour tout $g \in G$, τ_g est une bijection de G.
(ii) Pour tous $g, g' \in G$, on a $\tau_g \circ \tau_{g'} = \tau_{gg'}$.
(iii) Pour tous $g, g' \in G$, $\tau_g = \tau_{g'}$ ssi $g = g'$.

Preuve. (i) $\forall y \in G$ il existe un unique $x = g^{-1}y$ tel que $\tau_g(x) = y$. Donc $\tau_g \in S_G$.
(ii) $g, g' \in G$ on a $\tau_g \circ \tau_{g'}(x) = \tau_g(g'x) = gg'(x) = \tau_{gg'}(x)$. Donc $\tau_g \circ \tau_{g'} = \tau_{gg'}$.
(iii) Si $gx = g'x$ pour tout $x \in G$, alors $g = g'$ pour $x = e$. □

Théorème 4.2.1 (Cayley)**.** *Tout groupe G est isomorphe à un sous-groupe de son groupe symétrique S_G.*

Démonstration. D'après le lemme, le groupe G est isomorphe à son image $\mathrm{Im}(\varphi)$, qui est un sous-groupe de S_G. □

Remarque 4.2.1. *Il s'agit d'établir un morphisme injectif de G dans S_G. On remarque que le morphisme $x \mapsto i_x$ n'est pas injective, car $i_x = i_y$ ssi $xy^{-1} \in Z(G)$.*

4.3 Groupes monogènes et groupes cycliques

Nous définissons maintenant la notion de système de générateurs pour un groupe.

Définition 4.3.1. *Etant donné un groupe G et un sous-ensemble P de G, on appelle le sous-groupe engendré par P l'intersectin de tous les sous-groupes de G contenant P, noté $\langle P \rangle$.*

En fait, on a

$$\langle P \rangle := \{x_1^{\epsilon_1} \dots x_n^{\epsilon_n} \mid n \in \mathbb{N},\ x_1, \dots, x_n \in P,\ \epsilon_i = \pm 1\}.$$

L'ensemble ainsi défini est un sous-groupe de G. Par définition tout sous-groupe de G contenant P contient ce sous-groupe.

Soit $P = \{x_1, x_2, \dots, x_n\}$ une famille finie d'éléments de G. On notera

$$\langle x_1, x_2, \dots, x_n \rangle .$$

le sous-groupe engendré par P. Les éléments x_i sont appelés les générateurs. L'ensemble $P = \{x_1, x_2, \dots, x_n\}$ est un système de générateurs. Il n'y a évidemment pas d'unicité des systèmes de générateurs.

Définition 4.3.2. *On dira que G est engendré par n éléments s'il existe n éléments $x_1, x_2, \dots, x_n$ dans G tel que $G =< x_1, x_2, \dots, x_n >$.*

Le cas des groupes engendrés par un élément mérite une attention particulière. On remarque que ces groupes sont tous commutatifs. En effet si x désigne le générateur, le sous-ensemble $\{x^n \mid n \in \mathbb{Z}\}$ du groupe est un sous-groupe qui s'identifie au groupe par hypothèse. Il est clair que x^m commute à x^n pour tous m et n.

Définition 4.3.3. *Un groupe est dit monogène s'il existe un système générateur réduit à un élément. Un groupe monogène fini est appelé un groupe cyclique.*

Par exemple, le groupe $\mathbb{Z}$ est monogène et $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Mais les groupes $\mathbb{Z}^n$, avec $n > 1$, ne sont pas monogènes.

Définition 4.3.4. *Soit G un groupe et soit x un élément de G. On appelle ordre de x, noté $o(x)$, s'il existe, le plus petit entier positif non nul tel que $x^n = e$. Si un tel entier n'existe pas on dit que l'élément est d'ordre infini. Un élément d'ordre fini est aussi dit de torsion.*

Par exemple dans $\mathbb{Z}/n\mathbb{Z}$ la classe de 1 est d'ordre n.
Dans le groupe multiplicatif U des nombres complexes de module 1, i.e., $U = \{z \in \mathbb{C} \mid |z| = 1\}$, qui est un sous-groupe du groupe multiplicatif $(\mathbb{C}^*, \cdot)$, l'élément $i = e^{i\pi}$ est d'ordre 4, l'élément $j = e^{i2\pi/3}$ est d'ordre 3, l'élément $-j$ est d'ordre 6, et l'élément ij est d'ordre 12.

Proposition 4.3.1. *Soient G un groupe et x un élément de G d'ordre n. Alors tout entier k non nul tel que $x^k = e$ est un multiple de n.*

Preuve. Soit k tel que $x^k = e$. Faisons la division euclidienne de k par n : $k = nq + r$, $0 \leq r < n$. On a donc $e = x^k = x^{qn+r} = (x^n)^q x^r = x^r$, donc $x^r = e$. Comme $0 \leq r < n$, par définition de n, on a $r = 0$. □

Définition 4.3.5. *Le cardinal d'un groupe G est aussi appelé son ordre. On le note $|G|$.*

Proposition 4.3.2. *Soit G un groupe monogène. Alors G est soit isomorphe à $\mathbb{Z}$ soit isomorphe à $\mathbb{Z}/m\mathbb{Z}$ pour un $m \in \mathbb{N}^*$ fixé.*

Preuve. Soit $G =< x >$. Considérons le morphisme de groupes :

$$\varphi : \mathbb{Z} \to G, \quad n \mapsto x^n.$$

C'est un épimorphisme car x est un générateur de G. Le noyau de φ est un sous-groupe de $\mathbb{Z}$. Il existe donc un $m \in \mathbb{N}$ tel que $Ker\varphi = m\mathbb{Z}$.

Si $m = 0$, alors ϕ est injective et donc un isomorphisme.

Si $m > 0$, alors l'ordre de x est m. Deux éléments ont même image ssi ils sont congrus modulo m. Donc le sous-groupe image, qui est le groupe G lui même, est de la forme

$$G = \{e, x, \ldots, x^{m-1}\},$$

qui est isomorphe à $\mathbb{Z}/m\mathbb{Z}$ par l'identification $\bar{k} \mapsto x^k$. □

Corollaire 4.3.1. *L'ordre d'un élément est égal au cardinal du sous-groupe qu'il engendre.*

Ceci résulte de la preuve précédente. En effet, si l'ordre de x est infini, alors $< x >$ est isomorphe à $\mathbb{Z}$. Si l'ordre de x est fini, soit n. Alors la démonstration précédente montre que le cardinal de $< x >$ est n.

On note $n \wedge m$ le pgcd de n et m.

Proposition 4.3.3. *Soit G un groupe cyclique d'ordre n et a un générateur de G. Pour tout $k \in \mathbb{Z}$, l'ordre de $a^k \in G$ est $o(a^k) = \frac{n}{n \wedge k}$. En particulier, $G =< a^k >$ ssi $n \wedge k = 1$.*

Preuve. Soit $k \in \mathbb{Z}$. Posons $d = n \wedge k$. On a $n = dn'$, $k = dk'$ avec $n' \wedge k' = 1$. Pour tout $m \in \mathbb{N}$ on a

$$(a^k)^m = e \Leftrightarrow a^{km} = e \Leftrightarrow n \mid km \Leftrightarrow n' \mid k'm \Leftrightarrow n' \mid m.$$

Ainsi $n' = n/ \wedge k$ est le plus petit entier non nul tel que $(a^k)^{n'} = e$. On a donc $n' = o(a^k)$ □

On note qu'il existe $\varphi(n)$ générateurs distincts dans G si $|G| = n$. Par exemple, on a $\varphi(6) = 2$ et $\mathbb{Z}/6\mathbb{Z} =< 1 >=< 5 >$.

Exemple 4.3.1. *Le groupe multiplicatif $U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$ des racines $n^{ièmes}$ de l'unité dans $\mathbb{C}$, est engendré par $\zeta = \exp(2i\pi/n)$. Il est cyclique d'ordre n. Les générateurs du groupe U_n, sont appelés les racines $n^{ièmes}$ primitives de l'unité. L'ensemble des générateurs de U_{18} est*

$$\{\zeta, \zeta^5, \zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{17}\}, \quad \zeta = \exp(2i\pi/18).$$

Proposition 4.3.4. *Soit G un groupe cyclique d'ordre n et a un générateur. Soit $x \in G$, et soit d un diviseur de n. Il existe $y \in G$ tel que $y^d = x$ ssi $x^{\frac{n}{d}} = e$.*

Preuve. Soit $x = a^k$, alors $x^{\frac{n}{d}} = a^{kn/d} = e$, donc $n \mid \frac{kn}{d} \Longrightarrow d \mid k$. On a donc

$$x = (a^{k/d})^d.$$

L'implication inverse est immédiate : $x = y^d \Longrightarrow x^{n/d} = y^n = e$. □

Théorème 4.3.1. *Soit $G =< g >$ un groupe cyclique d'ordre n.*

1. *Si H est un sous-groupe de G, alors $H =< g^d >$ pour certain $d \mid n$.*
2. *Si H est un sous-groupe de G avec $|H| = k$, alors $k \mid n$.*
3. *Si $k \mid n$, alors $< g^{n/k} >$ est l'unique sous-groupe de G d'ordre k.*

Preuve. (On construit d'abord un sous-groupe cyclique dordre d)

1. Si $H \leq G$ est un sous-groupe de G, alors l'application $\phi : \mathbb{Z} \to G$ défénie par $\phi(k) = a^k$ est un epimorphisme de $\mathbb{Z}$ sur G. Comme $\phi^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$, il existe un $m \in \mathbb{N}$ tel que $\phi^{-1}(H) = m\mathbb{Z}$. Donc $H = \phi(m\mathbb{Z}) =< g^m >$. Le résultat est clair si $|H| = 1$. Sinon, soit $d = \text{pgcd}(m, n)$. Comme $d \mid m$ on a $g^m = (g^d)^{m/d}$ donc $H \subset< g^d >$. Or $d = xm + yn$, où $x, y \in \mathbb{Z}$, on a
$$g^d = (g^m)^x \cdot (g^n)^y = (g^m)^x \in< g^m >= H.$$
Ceci prouve que $< g^d >\subset H$ et donc $H =< g^d >$.

2. D'après 1. soit $H =< g^d >$ avec $d|n$. Alors $k = |H| = o(g^d) = \frac{n}{d}$. Donc $k|n$.
3. Supposons que K est un sous-groupe de G d'ordre k. Par 1. soit $K =< g^m >$ où $m \mid n$. Alors $k = |K| = o(g^m) = n/m$. D'où $m = n/k$, et $K =< g^{n/k} >$.

□

Proposition 4.3.5. *Soit G un groupe cyclique d'ordre n et a un générateur. Alors le groupe $Aut(G)$ est isomorphe au groupe $(\mathbb{Z}/n\mathbb{Z})^*$.*

Preuve. Notons $End(G)$ l'ensemble des endomorphismes de G. On observe qu'un morphisme $f : G \longrightarrow G$ est déterminé par l'image de a. En effet $f(a^k) = (f(a))^k$ pour tout $k \in \mathbb{Z}$.

On définit l'application $\phi : End(G) \longrightarrow \mathbb{Z}/n\mathbb{Z}$ par $f \mapsto \bar{l}$ si $f(a) = a^l$. Montrons que $f \in Aut(G)$ ssi $\phi(f)$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Soit g l'automorphisme réciproque de f avec $g(a) = a^k$. On a $g \circ f(a) = g(a^l) = a^{kl} = a$, soit $\bar{k}\bar{l} = \bar{1}$. Ce qui veut dire que $\bar{l}$ est inversible. On a donc une bijection $\phi : Aut(G) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$. Vérifions que c'est un morphisme de groupes. Si $g \mapsto \bar{k}$ i.e. $g(a) = a^k$, alors

$$f \circ g(a) = f(g(a)) = f(a^k) = a^{kl} \Longrightarrow f \circ g \mapsto \overline{kl} = \bar{k}\bar{l}.$$

Ceci démontre en fait que l'application ϕ est un isomorphisme de groupes. La loi à gauche étant la composition des applications, celle à droite la multiplication. □

4.4 Classes modulo un sous-groupe, indices

Définition 4.4.1. *Soit G un groupe et $H \leq G$. Pour tout $x \in G$, l'ensemble $xH = \{xy \mid y \in H\}$ est appelé* classe à gauche *de x modulo H et l'ensemble $Hx = \{yx \mid y \in H\}$ est appelé* classe à droite *de x modulo H.*

Si G n'est pas abélien, on n'a pas $xH = Hx$ en général pour $x \in G$. Si $xH = Hx$ pour tout $x \in G$ on dit que H est un sous-groupe normal ou distingué de G.
— *Pour que $y \in xH$, il faut et il suffit que $x^{-1}y \in H$.*
— *Pour que $y \in Hx$, il faut et il suffit que $yx^{-1} \in H$.*

Nous avons défini dans G deux relations qui sont en général distinctes lorsque G n'est pas abélien. Le résultat suivant en précise la nature.

Proposition 4.4.1. *Soit $H \leq G$. On dit que deux éléments x et y de G ont une relation, notée $x \sim y$, si $x^{-1}y \in H$ (resp. $yx^{-1} \in H$). La relation $\sim$ est relation d'équivalence dans G.*

Démonstration. Faisons la démonstration pour la 1re relation (la seconde s'endéduit sans difficulté.) :

a) réflexivité : $x^{-1}x = e \in H$ (qui est un sous-groupe) ;
b) symétrie : supposons $x^{-1}y \in H$, alors $y^{-1}x = (y^{-1}x)^{-1} \in H$ (qui est un sous-groupe) ;
c) transitivité : supposons $x^{-1}y \in H$ et $y^{-1}z \in H$; alors $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$ (qui est un sous-groupe).

□

Définition 4.4.2. *La relation $x^{-1}y \in H$ est appelée congruence à gauche modulo H. La relation $y^{-1}x \in H$ est appelée congruence à droite modulo H.*

Proposition 4.4.2. *Soit G un groupe et $H \leq G$. Pour tout $x \in G$, la classe xH (resp. Hx) est en bijection avec H.*

Preuve. Tout élément $x \in G$ étant inversible, l'application de H sur xH : $y \mapsto xy$ est une bijection □

Théorème 4.4.1 (Lagrange)**.** *Soit G un groupe fini et $H \leq G$. Alors l'ordre de H divise l'ordre de G.*

Preuve. D'après la prop. précédente, la relation de congruence modulo H partage G en classes d'équivalence $G/H = \{x_1H, \ldots, x_rH\}$. Comme chaque classe xH est en bijection avec H, on en déduit que $|G| = \sum_{i=1}^{r} |x_iH| = r|H|$. □

Définition 4.4.3. *Le cardinal de G/H est appelé l'indice de H dans G. On le note $[G : H]$.*

Corollaire 4.4.1. *Soit G un groupe fini d'ordre n. Alors l'ordre de tout élément de G divise n.*

Preuve. Soit $x \in G$. L'ordre de x est l'ordre du sous-groupe $< x >$ et donc divise n. □

Corollaire 4.4.2. *Tout groupe fini dont l'ordre est premier est cyclique.*

Preuve. Soit $x \in G$ distinct de l'élément neutre (ça existe car $o(G) \geq 2$). D'après le corollaire précédent, $o(x)$ divise $o(G)$. Ce dernier étant premier, on a $o(x) = o(G)$. D'où $G =< x >$. □

4.5 Sous-groupes distingués, groupes quotients

Définition 4.5.1. *Soit G un groupe, H un sous-groupe de G ; on dit que H est distingué ou normal si $xH = Hx^{-1}$ pour tout $x \in G$. On note $H \triangleleft G$.*

Cela signifie que modulo H les classes à gauche sont identiques aux classes à droite ; la condition peut aussi s'écrire $H = xHx^{-1}$, ce qui signifie : le sous-groupe H est globalement invariant par tout automorphisme intérieur de G.

Remarque. *L'inclusion $xHx^{-1} \subset H$, pour tout $x \in H$, suffit pour vérifier que H est normal dans G (car $H = y(y^{-1}Hy)y^{-1} \subset yHy^{-1}$).*

Exemples *: Les sous-groupes $\{1\}$ et G sont normaux dans G, s'il n'y en a pas d'autre on dit que G est simple.*

Théorème 4.5.1. *Soit φ un morphisme de G dans G'.*
1) Pour tout sous-groupe H' normal dans G', alors $\varphi^{-1}(H')$ est normal dans G.
2) Si φ est surjectif, pour tout sous-groupe H de G, alors $\varphi(H)$ est normal dans G'.

Preuve. 1) Soit $x \in \varphi^{-1}(H')$ et $y \in G$. On a $\varphi(yxy^{-1}) = \varphi(y)\varphi(x)\varphi(y)^{-1} \in H'$. D'où $yxy^{-1} \in \varphi^{-1}(H')$ et puis

$$y\varphi^{-1}(H')y^{-1} \subset \varphi^{-1}(H').$$

2) Soit $x' = \varphi(x) \in \varphi(H)$ et $y' \in G' = \varphi(G)$, alors
$y'x'y'^{-1} = \varphi(y)\varphi(x)\varphi(y)^{-1} = \varphi(yxy^{-1}) \in \varphi(H)$.
D'où $y'\varphi(H)y'^{-1} \subset \varphi(H)$. □

Voici un critère pour qu'un sous-groupe soit distingué.

Proposition 4.5.1. *Soit $H \leq G$. Si $[G : H] = 2$, alors $H \triangleleft G$.*

Preuve. Soit $a \in G$. Si $a \in H$, on a $Ha = H = aH$. Si $a \notin H$, l'indice de H étant 2, la partition de G en classes à gauche (resp. à droite) est $G = H \cup Ha$ (resp. $G = H \cup aH$). On a donc $Ha = H^c = aH$. Donc H est distingué. □

Définition 4.5.2. *Une relation d'équivalence $\mathcal{R}$ de G est dite compatible avec la structure du groupe G si*

$$a\mathcal{R}b,\ a'\mathcal{R}b' \Longrightarrow aa'\,\mathcal{R}\,bb'.$$

Une relation d'équivalence $\mathcal{R}$ sur un ensemble E induit une partition de G, qui est l'ensemble des classes d'équivalence, notée $E/\mathcal{R}$. Si G est muni d'une loi de composition interne $*$, et la relation d'équivalence $\mathcal{R}$ est compatible avec l'opération $*$ sur G, alors on peut définir une loi de composition interne sur $G/\mathcal{R}$.

Proposition 4.5.2. *Si la relation d'équivalence $\mathcal{R}$ est compatible avec la loi de composition interne $*$ de G, en posant $\bar{x} \cdot \bar{y} = \overline{x * y}$ on définit une loi de composition interne sur $G/\mathcal{R}$. Si $*$ est associative (resp. commutative, avec élément neutre), l'opération quotient $\cdot$ possède cette propriété sur $G/\mathcal{R}$. Si $x \in G$ est inversible, $\bar{x}$ est inversible dans G/R. Son inverse est la classe de x^{-1}.*

Preuve. Soit $(a, b) \in G/R \times G/R$. Il existe $(x, y) \in G \times G$ tel que $(a, b) = (\bar{x}, \bar{y})$. Si on considère d'autres représentants $x' \in E$ et $y' \in G$ des calsses a et b, on a xRx' et yRy'. Par l'hypothèse on a $\overline{x * y} = \overline{x' * y'}$. Ainsi, $\overline{x * y}$ ne dépend que de a et b et non des représentants x et y choisis. Il existe donc une application bien définie de $E/R \times E/R$ dans E/R telle que pour tout $x \in E$ et pour tout $y \in E$ l'image de $(\bar{x}, \bar{y})$ soit $\overline{x * y}$. Cela démontre la première assertion.
Si $*$ est associative sur E, il en est de même pour l'opération quotient car :

$$(\bar{x} \cdot \bar{y}) \cdot \bar{z} = (\overline{x * y} \cdot \bar{z} = \overline{(x * y) * \bar{z}} = \overline{x * (y * \bar{z})} = \bar{x} \cdot \overline{y * \bar{z}} = \bar{x} \cdot (\bar{y} \cdot \bar{z}).$$

Si $*$ est commutative on a $\bar{x}\cdot\bar{y}=\overline{x*y}=\overline{y*x}=\bar{y}\cdot\bar{x}$ et $(E/R,\cdot)$ est commutatif.
Si $e\in E$ est élément neutre pour $*$, pour tout $\bar{x}\in E/R$ on a $\bar{e}\cdot\bar{x}=\overline{e*x}=\bar{x}$ et de même $\bar{x}\cdot\bar{e}=\bar{x}$ donc $\bar{e}$ est neure dans E/R.
Si $x\in E$ a un inverse y, de la relation $x*y=y*x=e$ on déduit $\bar{x}\cdot\bar{y}=\bar{y}\cdot\bar{x}=\bar{e}$ donc $\bar{x}$ a pour inverse $\bar{y}$ dans E/R. □

Soit $\bar{a}=\{b\in G : a\mathcal{R}b\}$. Si $\mathcal{R}$ est compatible avec la structure de G, on peut alors définir une loi sur $G/\mathcal{R}=\{\bar{a}:a\in G\}$: $(\bar{a},\bar{b})\mapsto\overline{ab}$. Revenons maintenant à la question : quand est-ce que la relation de congruence modulo H est compatible avec la loi de composition du groupe G ?

Proposition 4.5.3. *Soient G un groupe et $H\leq G$. Les deux conditions suivantes sont équivalentes :*
(i) $y\in xH$ (resp. $y\in Hx$) est compatible avec la loi de composition de G.
(ii) H est distingué (donc les deux congruences sont identiques).

Preuve. (i)$\Longrightarrow$ (ii) Pour tout $y\in H$ et $x\in G$, comme $x\in xH$ et $x^{-1}\in x^{-1}H$ on a $xyx^{-1}\in xex^{-1}H=H$, donc $xHx^{-1}\subset H$.
(ii)$\Longrightarrow$ (i) Supposons que $x\in yH$ et $x'\in y'H$. Alors $xx'=yhy'h'=yy'h_1h'\in yy'H$, où $hy'=y'h_1$ avec $h_1\in H$ car H est distingué. Donc la relation $x\in yH$ est compatible avec la loi de G. □

D'après les deux propositions précédentes, on a

Proposition 4.5.4. *Soit $H\triangleleft G$ et $\bar{x}:=xH$ la classe de congruence de $x\in G$ modulo H. Alors, l'ensemble quotient G/H, muni de la loi de composition $\bar{x}*\bar{y}=\overline{xy}$ a une structure de groupe. De plus, l'application canonique $\varphi : x\mapsto\bar{x}$ est un épimorphisme de G vers G/H tel que $\operatorname{Ker}\varphi=H$.*

Exemple 4.5.1. *Soit $H=n\mathbb{Z}$ avec $n\in\mathbb{N}$. Alors $H\triangleleft\mathbb{Z}$. On retrouve le groupe qutotient $(\mathbb{Z}/n\mathbb{Z},+)$.*

4.6 Groupes symétriques

Soit E un ensemble fini ayant n éléments. Quitte à renuméroter les éléments, on peut supposer que $E=\{1,\dots,n\}$. Les bijections de E sur E sont appelées les permutations de E. Le groupe des permutations de E est le groupe symétrique. *Pour définir un élément σ de $\mathfrak{S}_n$, le plus simple est de donner le tableau de ses valeurs :*

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(n) & \cdots & \sigma(n)\end{pmatrix}$$

On utilise aussi la notation linéaire $\sigma=\sigma(1)\sigma(2)\dots\sigma(n)$.

Définition 4.6.1. *Soit $n \geq 2$ un entier. Pour toute permutation $\sigma \in \mathfrak{S}_n$, on appelle nombre d'inversions de σ l'entier :*

$$inv(\sigma) = \#\{(i,j) \in \{1,\ldots,n\}^2; i < j \text{ et } \sigma(i) > \sigma(j)\}.$$

On appelle signature de σ l'entier valant $+1$ ou -1 défini par :

$$\varepsilon(\sigma) = (-1)^{inv(\sigma)}.$$

Proposition 4.6.1. *Soit $\sigma \in \mathfrak{S}_n$. On a*

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Démonstration. Comme σ est une bijection de $\{1,\ldots,n\}$ sur lui même, l'application qui à tout doublon $\{i,j\}$ à $\{\sigma(i),\sigma(j)\}$ est aussi une bijection de l'ensemble des sous-ensembles à deux éléments de $\{1,\ldots,n\}$ sur lui même. Dans le produit $\prod_{1\leq i<j\leq n} \frac{\sigma(i)-\sigma(j)}{i-j}$ tous les facteurs du dénominateur se retrouvent donc une fois et une seule au numérateur, éventuellement changé de signe lorsque $i < j$ et $\sigma(i) > (j)$, ce qui donne exactement $\epsilon(\sigma)$. □

Théorème 4.6.1. *Soient σ et τ deux permutations de $\mathfrak{S}_n$; alors on a*

$$\varepsilon(\sigma\tau) = \epsilon(\sigma)\varepsilon(\tau).$$

Autrement dit, l'application ε $: \mathfrak{S}_n \to \{-1,+1\}$ est un morphisme de groues.

Démonstration. On a

$$\varepsilon(\sigma\tau) = \left(\prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)}\right)\left(\prod_{i<j} \frac{\tau(i) - \tau(j)}{i - j}\right).$$

Le fractur $\prod_{i<j} \frac{\tau(i)-\tau(j)}{i-j}$ est égal par définition à $\epsilon(\tau)$, il reste à montrer que le facteur $\prod_{i<j} \frac{\sigma\tau(i)-\sigma\tau(j)}{\tau(i)-\tau(j)}$ est égal à $\varepsilon(\sigma)$. Pour cela, on note que l'application qui à tout doublon $\{i,j\}$ associe le doublon $\{i',j'\}$, où $i' = \tau(i)$ et $j' = \tau(j)$, est une bijection de l'ensemble des parties à deux éléments sur lui-même et que par ailleurs on a les égalités

$$\frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} = \frac{\tau(i') - \tau(j')}{i' - j'} = \frac{\tau(j') - \tau(i')}{j' - i'}.$$

On a donc

$$\prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} = \prod_{i'<j'} \frac{\sigma(i') - \sigma(j')}{i' - j'}.$$

□

Remarque 4.6.1. *Soit $n \geq 2$ un entier. Le noyau* $\ker(\varepsilon)$ *est un sous-groupe de $\mathfrak{S}_n$ appelé le groupe alterné, noté A_n. Il est clair que le cardinal de A_n est $n!/2$.*

Définition 4.6.2. — *Le* support *de $\sigma \in \mathfrak{S}_n$ est l'ensemble des éléments $k \in [n]$ tels que $\sigma(k) \neq k$.*

— *Un élément c de $\mathfrak{S}_n$ est un cycle, s'il permute circulairement certains éléments $i_1, i_2, \ldots, i_k$ de $[n]$ et fixe les autrees éléments de $[n]$:*

$$c(i_1) = i_2, \quad c(i_2) = i_3, \quad \ldots, \quad c(i_{k-1}) = i_k, \quad c(i_k) = i_1.$$

On dit que c est un k-cycle, noté $(i_1, i_2, \ldots, i_k)$.

La partie $\{i_1, i_2, \ldots, i_k\}$ de E est le support de ce cycle. Le cardinal du support s'appelle la longueur *du cycle. Cette notation de c n'est pas unique, puisqu'on peut commencer par n'importe quel élément de son support.*

Proposition 4.6.2. *L'ordre d'un k-cycle c de $\mathfrak{S}_n$ est donc la longueur k du cycle.*

Démonstration. Soit $c = (i_1, \ldots, i_k)$. Alors $c^k(i_p) = i_p$ pour $1 \leq p \leq k$ et k est le plus petit entier strictement positif tel que $c^k = e$. □

Deux cycles c, c' sont dits disjoints *si leurs supports sont des parties disjointes de E. Dans ce cas on a $cc' = c'c$.*

Définition 4.6.3. *Un 2-cycle de support $\{i, j\}$ est appelé* transposition *et noté (i, j). Si i et j sont deux entiers consécutifs on dit que c'est une transposition simple.*

Il est clair qie les $n-1$ transpositions de $\mathfrak{S}_n$ sont $t_i = (i, i+1)$, où $i = 1, \ldots, n-1$.

Proposition 4.6.3. *Toute permutation $\sigma \in \mathfrak{S}_n$ avec $\sigma \neq e$ peut s'écrire de manière unique comme un produit $\sigma = c_1 c_2 \cdots c_p$ de cycles disjoints. L'ordre de σ est le* ppcm *des ordres de $c_1, \ldots, c_p$.*

Preuve. Soit S le support de σ. On raisonne par récurrence sur le cardinal n de S. Si $|S| = 2$, alors $\sigma = (1, 2)$. H.R. le résultat est vrai pour tout support de cardinal $s < n$. Soit $a \in S$ on considère l'ensemble $\{a^k\}_{k \in \mathbb{N}^*}$. Par le rpincipe des tiroirs $\exists l > k$ tels que $a^k = a^l \Longrightarrow a^{k-l+1} = a$. Soit m le plus petit entier > 1 tel que $a^j = a$, alors $C_1 = (a, \sigma(a), \ldots, a^{m-1}(a))$ est un m-cycle. On en déduit que $\sigma \circ C_1^{-1}$ est une permutation de support $S' = S \setminus \{a, \ldots, \sigma^{m-1}(a)\}$. Comme le cardinal de S' est plus petit que r, l'H.R. implique qu'il existe des cycles deux à deux disjoints $C_2, \ldots, C_p$ tels que $\sigma \circ C_1^{-1} = C_2 \ldots C_p$.

On démontre l'unicité par récurrence sur le nombre de cycles p : Soit $\sigma = C'_1 \dots C'_q$ une autre décomposition de σ en cycles disjoints et soit i un élément du support de C_1. Quitte à renuméroter, on suppose que i appartient au support de C'_1. Alors

$$\sigma^r(i) = {C_1}^r(i) = {C'_1}^r(i)$$

pour tout $r \in \mathbb{N}$. Il s'en suit que $C_1 = C'_1$. De $C_1 \dots C_p = C'_1 \dots C'_q$ on déduit que $C_2 \dots C_p = C'_2 \dots C'_q$. Le résultat suit par récurrence.

Puisque les cycles disjoints commutent, on a $\sigma^n = {C_1}^n \dots {C_p}^n$ pour tout $n \in \mathbb{N}$. Les supports étant disjoints, $\sigma^n = e$ ssi ${C_1}^n = \dots = {C_p}^n = e$, i.e. si n est un multiple commun des ordres de $C_1, \dots, C_p$. Le plus petit tel entier strictement positif est donc le ppcm des ordres de $C_1, \dots, C_p$. □

Proposition 4.6.4. *Soit $C = (a_1, \dots, a_k)$ un k-cycle de $\mathfrak{S}_n$. Alors la signature de σ est $\varepsilon(\sigma) = (-1)^{k-1}$.*

Démonstration. Le nombre d'inversions d'une transposition $\tau = (i, j)$ où $i < j$ est égal à

$$\#\{(j,k) : i \leq k < j\} + \#\{(k,i) : i < k \leq j\} = 2(j-i) - 1.$$

Donc la signature de τ est -1. En écrivant C en produit de transpositions $(a_1, a_2)(a_2, a_3) \dots (a_{k-1}, a_k)$ on a le résultat. □

Remarque 4.6.2. *Si $\sigma = C_1 \dots C_r$ est la décomposition en cycles de $\sigma \neq e$, alors on obtient une la formule suivante pour la signature*

$$\varepsilon(\sigma) = (-1)^{l(C_1)+\dots+l(C_r)-r}, \tag{4.6.1}$$

où $l(C_i)$ est la longueur du cycle C_i ($1 \leq i \leq r$). On pourra vérifier (exercice !) que l'exposant s'écrit aussi sous la forme plus compact $n - cyc(\sigma)$ où $cyc(\sigma)$ est le nombre de cycles de longueur ≥ 2 plus le nombre de points fixes de σ.

Exemple 4.6.1. *Soit*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 1 & 9 & 4 & 6 & 3 & 8 & 2 \end{pmatrix} \in \mathfrak{S}_9.$$

Le support de σ est $\{1, 2, 3, 4, 5, 7, 9\}$.

- *Partant du plus petit élément 1, on a $\sigma(1) = 7$, $\sigma(7) = 3$, $\sigma(3) = 1$ d'où le 1er cycle $c_1 = (1, 7, 3)$.*
- *L'entier 2 étant le plus petit élément parmi les éléments restants dans le support, on a $\sigma(2) = 5$, $\sigma(5) = 4$, $\sigma(4) = 9$, $\sigma(9) = 2$ d'où un deuxième cycle $c_2 = (2, 5, 4, 9)$. On a donc $\sigma = c_1 c_2$.*

L'ordre de σ *est* $\mathrm{ppcm}(3,4) = 12$.

Proposition 4.6.5. *Le conjugué d'un* k*-cycle est un* k*-cycle. Deux* k*-cycles quelconques sont conjugués.*

Démonstration. Soit $c = (\alpha_1, \ldots, \alpha_k)$ un k-cycle. Pour tout $\varphi \in \mathfrak{S}_n$, la permutation $c' = \varphi \circ c \circ \varphi^{-1}$ est le k-cycle $(\varphi(\alpha_1), \ldots, \varphi(\alpha_k))$ car $c'(\varphi(i)) = \varphi(i)$ pour tout $i \notin Support(c)$ et $c'(\varphi(\alpha_i)) = \varphi(\alpha_{i+1})$ pour $i = 1, \ldots k$ avec $\alpha_{k+1} = \alpha_1$.

Soient $c_1 = (\alpha_1, \ldots, \alpha_k)$ et $c_2 = (\beta_1, \ldots, \beta_k)$ deux k-cycles quelconques. Les compléments de supports de c_1 et c_2 ont même cardinal, il existe donc une bijection $\varphi : [n] \setminus support(c_1) \longrightarrow [n] \setminus support(c_2)$. On la prolonge en une permutation $\varphi \in S_n$ en définissant $\varphi(\alpha_i) = \beta_i$ pour $i = 1, \ldots, k$. On a alors $c_2 = \varphi c_1 \varphi^{-1}$, d'après ce qui précède. □

Corollaire 4.6.1. *Deux permutations* $\neq e$ *sont conjuguées ssi dans leurs décomposition canonique en cycles disjoints, appraissent le même nombre de* k*-cycles pour tout* k*,* $2 \leq k \leq n$*.*

Preuve. $\Longrightarrow$ Soit $\sigma' = \phi\sigma\phi^{-1}$ et soit $\sigma = c_1 \ldots c_t$ la décomposition canonique en cycles de τ. Alors

$$\sigma' = (\phi c_1 \phi^{-1}) \circ \cdots \circ (\phi c_t \phi^{-1}).$$

Comme les cycles conjugués ont le même longueur, la condition est nécessaire.

$\Longleftarrow$ Quitte à renuméroter les cycles on peut supposer que

$$\sigma = c_1 \ldots c_t, \qquad \sigma' = c'_1 \ldots c'_t$$

où $l(c_i) = l(c'_i)$. Comme les supports de σ et σ' ont le même cardinal, il existe une bijection $\phi : [n] \setminus support(\sigma) \longrightarrow [n] \setminus support(\sigma')$. Supposons que

$$c_i = (\alpha_{i1}, \ldots, \alpha_{il_1}), \qquad c'_i = (\beta_{i1}, \ldots, \beta_{il_1}) \qquad 1 \leq i \leq t.$$

On prolonge ϕ en une bijection de $[n]$ dans $[n]$ comme suit :

$$\phi(\alpha_{ij} = \beta_{ij} \qquad 1 \leq i \leq t, \quad 1 \leq j \leq l_i,$$

On a

$$\phi \circ \sigma \circ \phi^{-1} = (\phi \circ c_1 \circ \phi^{-1}) \circ \cdots \circ (\phi \circ c_p \circ \phi^{-1}) = \sigma'.$$

□

Chapitre 5

Anneaux, idéaux

Résumé. Anneaux unitaires. Produit fini d'anneaux, sous-anneau, morphisme et isomorphisme d'anneaux, anneau intègre, anneau euclidien. Corps, sous-corps. Idéaux dans un anneau commutatif, interprétation de la divisibilité en termes d'idéaux, idéaux de $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$.

5.1 Notion d'anneaux

Définition 5.1.1. *Un annneau A est un ensemble non vide muni de deux lois de composition internes, l'une notée comme une addidtion et l'autre comme une multiplication, vérifiant les propriétés suivantes :*

(1) A est un groupe abélien pour l'addition, (on note 0 son élément neutre),

(2) la multiplication est associative, c'est-à-dire :

$$x(yz) = (xy)z \quad \textit{pour tous} \quad x, y, x \in A,$$

(3) la multiplication est distributive sur l'addition à gauche et à droite, c'est-à-dire :

$$x(y+z) = xy + xz \quad \textit{et} \quad (x+y)z = xz + yz \quad \textit{pour tous} \quad x, y, x \in A.$$

On dit que l'anneau est commutatif *si de plus la multiplication est commutative, c'est-à-dire :*

$$xy = yx \quad \textit{pour tous} \quad x, y \in A.$$

On dit que A est unitaire *si de plus la multiplication ademt un élément neutre 1 :*

$$x \cdot 1 = 1 \cdot x = x \quad \textit{pour tout} \quad x \in A.$$

Exemple 5.1.1. PREMIERS EXEMPLES

(a) *L'ensemble $\mathbb{Z}$ des entiers est un anneau commutatif unitaire. Il en est de même de $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.*

(b) *L'ensemble des matrices carrées d'ordre $n \geq 2$ à coefficients réels est un anneau non-commutatif unitaire. Il en est de même de l'anneau des endomorphismes d'un espace vectoriel (pour la loi composition $\circ$).*

(c) *L'anneau nul est l'anneau $\{0\}$ formé d'un unique élément.*

(d) *Pour tout intervalle I de $\mathbb{R}$, l'ensemble $\mathcal{F}(I, \mathbb{R})$ des applications de I dans $\mathbb{R}$ est un anneau commutatif unitaire : $f + g : x \mapsto f(x) + g(x)$ et $fg : x \mapsto f(x)g(x)$ pour tous $f, g \in \mathcal{F}(I, \mathbb{R})$.*

(e) *Fixons un entier $n \geq 2$. L'ensemble $\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \ldots, \overline{n-1}\}$ muni de l'addition $\bar{x} + \bar{y} = \overline{x+y}$ et la multiplication $\bar{x} \cdot \bar{y} = \overline{xy}$ est un anneau commutatif unitaire.*

Exemple 5.1.2. SÉRIES FORMELLES *On fixe un anneau commutatif unitaire A. Notons $B = A^{\mathbb{N}}$ l'ensemble des suites d'éléments de A. On définit une addition et une multiplication dans B en posant, pour tous $f = (a_n)$ et $g = (b_n)$ dans B :*

$$f + g = (a_n + b_n) \quad et \quad fg = (c_n) \quad avec \quad c_n = \sum_{i+j=n} a_i b_j. \tag{5.1.1}$$

On peut montrer que B est un anneau commutatif unitaire pour ces opérations, avec $0_B = (0_A, 0_A, \ldots)$ et $1_B = (1_A, 0_A, 0_A, \ldots)$. On l'appelle l'anneau des séries formelles en une indéterminée à coefficients dans A.

On définit aussi le produit externe d'un élément $\alpha \in A$ par un élément $f = (a_n)$ en posant $\alpha f = (\alpha a_n)$. A noter que le produit externe $\alpha \cdot f$ n'est autre le produit interne de f par $(\alpha, 0_A, 0_A, \ldots)$. C'est pourquoi on convient de noter encore α l'élément $(\alpha, 0_A, 0_A, \ldots)$ de B. En particulier $0_B = 0_A$ et $1_B = 1_A$.

En posant $e_i = (0_A, \ldots, 0_A, 1_A, 0_A, \ldots)$, avec 1_A en $i+1$-ième position, pour tout $i \in \mathbb{N}$, tout élément de B s'écrit de façon unique $f = \sum_{n \in \mathbb{N}} a_n e_n$ avec $a_n \in A$. Il est clair que $e_n e_m = e_{n+m}$ pour tous $n, m \in \mathbb{N}$, et donc $e_n = e_1^n$ pour tout $n \in \mathbb{N}$. On note tradittionnellement $X = e_1$ et $B = A[[X]]$.

5.2 Sous-anneau

Définition 5.2.1. *Soit A un anneau. On appelle* sous-anneau *de A toute partie non-vide B de A qui vérifie les deux conditions suivantes :*

(1) *B est un sous-groupe du groupe additif A.*

(2) *B est stable par la multiplication de A, c'est-à-dire que l'on a : $xy \in A$ pour tous $x, y \in B$.*

Définition 5.2.2. *Soit A un anneau unitaire. On appelle B un sous-anneau unitaire de A qui contient 1_A.*

On note que $2\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}$, mais $1 \notin \mathbb{Z}$.

Remarque 5.2.1(a) *Si B est une sous-anneau de A, alors B est lui-même un anneau. De fait, dans la pratique, pour montrer qu'un ensemble donné est un anneau, on cherche souvent à montrer que c'est un sous-anneau d'un anneau déjà connu.*

(b) *Si B est un sous-anneau unitaire d'un anneau unitaire A, alors B est lui-même un anneau unitaire, et l'on a $1_B = 1_A$.*

(c) *Si l'anneau A est commutatif, alors tout sous-anneau de A est commutatif.*

Exemple 5.2.1. *Premiers exemples*

(a) *Si A est un anneau, alors $\{0\}$ et A sont des sous-anneaux de A.*

(b) *$\mathbb{Z}$ est un sous-anneau unitaire de $\mathbb{Q}$ (et de $\mathbb{R}$, et de $\mathbb{C}$). Pour tout $n \geq 2$, l'ensemble $n\mathbb{Z}$ est un sous-anneau non unitaire de $\mathbb{Z}$.*

(c) *Dans $\mathcal{F}(I, \mathbb{R})$ les fonctions continues forment un sous-anneau unitaire.*

Exemple 5.2.2. POLYNÔMES *Soit A un anneau commutatif unitaire. Notons $A[X]$ l'ensemble des suites d'éléments de A dont tous les termes sont nuls sauf un nombre fini d'entre eux, c'est-àdire, qui sont "à support fini". Il est clair que $A[X]$ muni des opérations dans* (5.1.1) *est un sous-anneau unitaire de l'anneau de séries formelles $A[[X]]$. Un élément de $A[X]$ est appelé un* polynôme *en une indéterminée à coefficients dans A.*

On retiendra que

(a) *L'anneau $A[X]$ contient A comme sous-anneau unitaire par identification α avec $(\alpha, 0_A, \ldots)$ pour tout $\alpha \in A$. Son neutre pour l'addition est 0_A. Son neutre pour la multiplication est 1_A.*

(b) *Pour tout élément non-nul P de $A[X]$, il existe un unique entier naturel n et un unique $(n+1)$-uplet $(a_0, a_1, \ldots, a_n)$ d'éléments de A tels que :*

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad et \quad a_n \neq 0.$$

L'entier n est appelé le degré de P, noté $\deg P$. L'élément non-nul a_n de A est applélé le coefficient dominant de P, noté $\operatorname{cd} P$. Par convention, on pose $\deg 0 = -\infty$ et $\operatorname{cd} 0 = 0$.

(c) *Deux polynômes $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{i=0}^{m} b_i X^i$ sont égaux ssi $n = m$ et $a_i = b_i$ pour tout $0 \leq i \leq n$. Un polynôme est nul ssi tous ses coefficents sont nuls.*

(d) *Si $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{i=0}^{m} b_i X^i$, on a :*

$$P + Q = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i \quad et \quad PQ = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) X^i.$$

(e) On en déduit que, pour P et Q dans $A[X]$, on a :

$$\deg(P+Q) \leq \max(\deg P, \deg Q) \quad et \quad \deg(PQ) \leq \deg P + \deg Q.$$

Exemple 5.2.1. Exemple des entiers de Gauss *On appelle entier de Gauss tout nombre complexe $a+ib$ avec $a, b \in \mathbb{Z}$. On note $\mathbb{Z}[i]$ leur ensemble :*

$$\mathbb{Z}[i] = \{a+ib : a, b \in \mathbb{Z}\},$$

qui est un anneau commutatif unitaire contenant $\mathbb{Z}$ comme sous-anneau.

En effet, quels que soient $x = a+ib$ et $x' = c+id$ avec $a, b, c, d \in \mathbb{Z}$, les complexes $x - x' = (a-c)+i(b-d)$ et $xx' = (ac-bd)+i(ad+bc)$ ont des parties réelles et imaginaires dans $\mathbb{Z}$, donc appartiennent à $\mathbb{Z}[i]$. Ceci prouve que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{C}$. L'application $N : \mathbb{Z}[i] \to \mathbb{N}$ définie par $N(a+ib) = a^2+b^2$ jouera dans l'étude de l'anneau $\mathbb{Z}[i]$ un rôle important. Comme $N(x) = x\bar{x} = [x|^2$ pour tout $x \in \mathbb{Z}[i]$, on a clairement $N(xx') = N(x)N(x')$ pour tous $x, x' \in \mathbb{Z}[i]$.

5.3 Groupe des unités

Définition 5.3.1. *Soit A un anneau commutatif unitaire. On appelle* unité *de A, ou élément inversible dans A, tout élément $x \in A$ tel qu'il existe un élément $y \in A$ vérifiant $xy = 1$.*

Proposition 5.3.1. *Soit A un anneau commutatif unitaire. L'ensemble des éléments inversibles de A est un groupe pour la multiplication, appelé groupe des unités de A, et noté $U(A)$.*

Démonstration. D'abord $1 \in U(A)$ donc $U(A)$ n'est pas vide. Soient x et y deux éléments de $U(A)$. Il existe x' et y' dans A tels que $xx' = 1 = yy'$. Donc $(xy)(y'x') = x(yy')x' = x1x' = xx' = 1$, ce qui prouve que $xy \in U(A)$. On a ainsi vérifié que la multiplication de A se restreint en une loi de composition interne de $U(A)$. Elle est associative, et admet comme neutre 1, qui appartient à $U(A)$. Il reste à vérifier que tout élément $x \in U(A)$ admet un inverse dans $U(A)$, ce qui est évident puisque l'inverse $x' = x^{-1}$ d'un élément $x \in U5A)$ est lui-même dans $U(A)$, d'inverse x. □

Exemple 5.3.1.

(a) $U(\mathbb{Z}) = \{-1, 1\}$.

(b) $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.
En effet, soient $x = a+ib$ et $y = c+id$ avec $a, b, c, d \in \mathbb{Z}$ tels que $xy = 1$. On a alors $1 = N(xy) = N(x)N(y)$ avec $N(x), N(y) \in \mathbb{N}^*$, d'où $N(x) = N(y) = 1$. Or $N(x) = 1$ équivaut à $a^2+b^2 = 1$ ce qui, dans $\mathbb{Z}$, se produit ssi (a, b) est l'un des quatre couples $(1, 0)$, $(-1, 0)$, $(0, 1)$ ou $(0, -1)$.

(c) Pour tout $n \geq 2$, on a $U(\mathbb{Z}/n\mathbb{Z}) = \{\bar{x} : 0 \leq x \leq n-1,$ et x premier avec $n\}$.

Remarquons que les éléments $\bar{x}$ qui sont inversibles dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont aussi ceux qui engendrent le groupe additif $\mathbb{Z}/n\mathbb{Z}$. En particulier le groupe $U(\mathbb{Z}/n\mathbb{Z})$ est fini d'ordre $\varphi(n)$, où φ est l'indicatrice d'Euler.

5.4 Corps

Définition 5.4.1. *On appelle* corps *commutatif tout anneau commutatif unitaire dans lequel tout élément non-nul est inversible.*

En notant, pour tout anneau A commutatif unitaire $A^* = A \setminus \{0\}$, on a donc :

$$(A \text{ corps}) \Longleftrightarrow (U(A) = A^*).$$

Définition 5.4.2. *Soit K un corps. On appelle* sous-corps *de K tout sous-anneau unitaire F de K tel que l'inverse de tout élément non-nul de F appartienne à F.*

Exemple 5.4.1.

(a) $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des corps : ils contiennent comme sous-anneau $\mathbb{Z}$ qui, lui, n'est pas un corps.

(b) $\mathbb{Q}(i) = \{p + iq; p, q \in \mathbb{Q}\}$ est un sous-corps de $\mathbb{C}$; il contient $\mathbb{Z}[i]$ comme sous-anneau qui, lui, n'est pas un corps.

Preuve. On vérifie aisément que $\mathbb{Q}(i)$ est un sous-anneau de $\mathbb{C}$; pour tout $x = p + iq \in \mathbb{Q}(i)$ non-nul, son inverse x^{-1} dans $\mathbb{C}$ est égal à $\frac{p}{p^2+q^2} + \frac{-q}{p^2+q^2}i$. Ce qui prouve que $\mathbb{Q}(i)$ est un sous-corps de $\mathbb{C}$. Il est clair que $\mathbb{Z}[i]$ est un sous-anneau de $\mathbb{Q}(i)$, et le fait que ce n'est pas un corps découle immédiatement de Exemple 5.3.1 (b). □

(c) Pour tout entier $n \geq 2$, ($\mathbb{Z}/n\mathbb{Z}$ est un corps) $\Longleftrightarrow$ (n est un nombre premier). et appartient donc à $\mathbb{Q}(i)$.

5.5 Intégrité

Définition 5.5.1. *Soit A un anneau commutatif. On dit que A est* intègre*, ou encore que A est un* domaine d'intégrité*, lorsqu'il est non-nul et vérifie la propriété suivante :*

$$\text{pour tous } x, y \in A,\ (xy = 0) \Longleftrightarrow (x = 0 \text{ or } y = 0).$$

Un élément x de A est appelé un diviseur de zéro *dans A lorsque $x \neq 0$ et lorsqu'il existe $y \neq 0$ dans A tel que $xy = 0$. En d'autres termes, A est intègre ssi il n'admet pas de diviseurs de zéro.*

Exemple 5.5.1.

(a) Tout corps est un anneau inègre.
Soit K un corps. Soient $x, y \in K$ tels que $xy = 0$. Si $x \neq 0$, alors x est inversible dans K par définition d'un corps. Donc $y = x^{-1}(xy) = x^{-1}0 = 0$. De même $y \neq 0$ implique $x = 0$.

(b) Tout sous-anneau d'un anneau intègre est intègre. En particulier, tout sous-anneau d'un corps est intègre. Par exemple, $\mathbb{Z}$ et $\mathbb{Z}$ sont intègres.

(c) Considérons les tables de multiplications des anneaux $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$. L'anneau $\mathbb{Z}/5\mathbb{Z}$ est un corps car 5 est un nombre premier. L'anneau $\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre car $\bar{2} \cdot \bar{3} = \bar{0}$ bien que $\bar{2} \neq \bar{0}$ et $\bar{3} \neq \bar{0}$.

Proposition 5.5.1. *Pour tout entier $n \geq 2$, les assertations suivantes sont équivalentes :*

(a) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre.

(b) n est un nombre premier.

(c) L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Preuve. On vérifie seulement l'implication $(a) \longrightarrow (b)$. Par contraposée, supposons que n n'est pas premier, il existe donc $k, m \in \mathbb{Z}$ tels que $n = km$ avec $1 < k < n$ et $1 < m < n$. On a alors $\bar{k} \cdot \bar{m} = \bar{0}$, bien que $\bar{k} \neq \bar{0}$ et $\bar{m} \neq \bar{0}$.

□

5.6 Morphismes d'anneaux

Définition 5.6.1. *Soient A et B deux anneaux commutatifs unitaires. On appelle* morphisme d'anneaux unitaires *de A dans B toute application $f : A \to B$ vérifiant les trois propriétes suivantes :*

$$(f(x+y) = f(x) + f(y), f(xy) = f(x)f(y) \text{ pour tous } x, y \in A) \text{ et } (f(1_A) = 1_B).$$

Proposition 5.6.1 (Propriétés)**.**

(I) Si $f : A \to B$ est un morphisme d'anneaux unitaires, alors l'image directe par f de tout sous-anneau unitaire de A est un sous-anneau unitaire de B, et l'image réciproque par f de tout sous-anneau unitaire de B est un sous-anneau unitaire de A.

(II) Si $f : A \to B$ et $g : B \to C$ sont des morphismes d'anneaux unitaires, alors $g \circ f : A \to C$ est un morphisme d'anneaus unitaires.

(III) $f : A \to B$ est un morphisme d'anneaux unitaires bijectif, alors sa bijection réciproque $f^{-1} : B \to A$ est un morphisme d'anneaux unitaires ; on dit dans ce cas que f est un isomorphisme, et que les deux anneaux A et B sont isomorphes.

Proposition et définition 5.6.1. *Soient A_1 et A_2 deux anneaux commutatifs unitaires.*

(i) Le produit cartésien $A_1 \times A_2$ est un anneau commutatif unitaire pour les lois définies par :

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2) \text{ et } (x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2),$$

pour tous $x_1, y_1 \in A_1$, $x_2, y_2 \in A_2$, et l'on a $1_{A_1 \times A_2} = (1_{A_1}, 1_{A_2})$. Cet anneau est appelé le produit direct de A_1 par A_2. On le note $A = A_1 \times A_2$.

(ii) L'application $p_1 : A \to A_1$ qui, à tout élément $(x_1, x_2) \in A$, associe sa première composante x_1, est un morphisme d'anneaux unitaire (appelé première projection).

(iii) L'application $p_2 : A \to A_2$ qui, à tout élément $(x_1, x_2) \in A$, associe sa seconde composante x_2, est un morphisme d'anneaux unitaire (appelé seconde projection).

Preuve. Simple vérification, laisséee au lecteur. □

Remarque 5.6.1. *Attention : l'anneau $A_1 \times A_2$ n'est pas intègre (même si A_1 et A_2 le sont). En effet, les éléments $(1_{A_1}, 0_{A_2})$ et $(0_{A_1}, 1_{A_2})$ sont non-nuls, alors que leur produit l'est.*

Proposition 5.6.2 (théorème chinois)**.** *Soient deux entiers $n \geq 2$ et $m \geq 2$. L'anneau produit $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ est isomorphe à l'anneau $\mathbb{Z}/nm\mathbb{Z}$ ssi n et m sont premiers entre eux.*

Preuve. D'après le théorème chinois, on sait que, pour n et m premiers entre eux, l'application $\bar{x} \to (\tilde{x}, \hat{x})$, où $\bar{x} = x + nm\mathbb{Z}$, $\tilde{x} = x + n\mathbb{Z}$ et $\hat{x} = x + m\mathbb{Z}$, réalise un isomorphisme de groupes de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Il est clair, par définition même des multiplications dans ces différents anneaux, que c'est aussi un isomorphisme d'anneaux unitaire. La réciproque est évidente. □

5.7 Notion d'idéal

Définition 5.7.1. *Soit A un anneau commutatif unitaire. On appelle* idéal *de A toute partie non-vide I de A qui vérifie les deux conditions suivantes :*

(1) I est un sous-groupe du groupe additif A,

(2) pour tous $x \in I$ et $a \in A$, on a $xa \in I$.

Exemples 5.7.1.

(a) $\{0\}$ et A sont des idéaux de A.

(b) Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un idéal de l'anneau $\mathbb{Z}$.

(c) Dans l'anneau $\mathcal{R}(\mathbb{R}, \mathbb{R})$, l'ensemble des fonctions qui s'annulent en 0 est un idéal.

Lemme 5.7.1. *Soit A un anneau commutatif unitaire.*

(a) si I est un idéal de A qui contient 1*, alors* $I = 1$.

(b) si I est un idéal de A qui contient un élément de $U(A)$, alors $I = A$.

Preuve. Supposons $1 \in I$. Tout $a \in A$ s'écrit $a = 1 \cdot a$ donc, comme $1 \in I$, il résulte de la définition (2) que $a \in I$. On a alors $A \subset I$, donc $A = I$, ce qui prouve (a). Supposons maintenant que I contienne un élément x inversible dans A. On a $1 = xx^{-1}$ avec $x \in I$ et $x^{-1} \in A$, donc $1 \in I$, et on applique (a) pour conclure que $I = A$. □

Proposition 5.7.1. *Soient A et B des anneaux commutatifs unitaires. Soit $f : A \to B$ un morphisme d'anneaux unitaires. On a*
(i) Pour tout idéal J de B, l'image réciproque $f^{-1}(J)$ est un idéal de A.
(ii) En particulier, $\operatorname{Ker} f = \{x \in A; f(x) = 0_B\}$ *est un idéal de A.*
(iii) Pour tout idéal I de A, l'image directe $f(I)$ est un idéal de l'anneau $f(A) = \operatorname{Im} f$.

Preuve. Sous les hypothèses de (i), on sait déjà que $f^{-1}(J)$ est un sous-groupe additif de A. Soit $x \in f^{-1}(J)$ et $a \in A$. On a $f(xa) = f(x)f(a)$ avec $f(a) \in B$ et $f(x) \in J$, donc $f(xa) \in J$ puisque J est un idéal de B, c'est-à-dire $xa \in f^{-1}(J)$, ce qui prouve que $f^{-1}(J)$ est un idéal de A. On obtient (ii) en appliquant (i) à $J = \{0_B\}$.

Pour (iii), considérons un idéal I de A. On sait que $f(I)$ est un sous-groupe additif de B. Soit $y \in f(I)$, de sorte qu'il existe un $x \in I$ tel que $y = f(x)$. Pour tout élément $b \in B$ qui appartient à $\operatorname{Im} f$, il existe $a \in A$ tel que $b = f(a)$; on a alors $yb = f(x)f(a) = f(xa)$ avec $ax \in I$ puisque $x \in I$ et que I est un idéal, et donc $yb \in f(I)$. ceci prouve que $f(I)$ est un idéal de $\operatorname{Im} f$. □

Proposition 5.7.2. *Soit A un anneau commutatif unitaire. L'intersection de deux idéaux de A est un idéal de A. Plus généralement, l'intersection d'une famille quelconque d'idéaux de A est un idéal de A.*

Preuve. On montre le premier point. Soient I_1 et I_2 deux idéaux de A. On sait déjà que $I = I_1 \cap I_2$ est un sous-groupe additif de A. Soient $x \in I$ et $a \in A$. On a $xa \in I_i$ pour $i \in \{1, 2\}$ puisque I_i est un idéal, et donc $xa \in I$. Ce qui prouve que I est un idéal de A. □

Proposition et définition 5.7.1. *Soit A un anneau commutatif unitaire. Pour tout $x \in A$;*
(i) l'ensemble $xA = \{xy; y \in A\}$ est un idéal de A, appelé l'idéal principal engendré par x ;
(ii) xA est le plus petit idéal de A contenant x ;
(iii) on a : $(xA = A) \iff (x \in U(A))$.

Preuve. Il est clair que xA n'est pas vide. Soient $y \in xA$ et $z \in xA$ quelconques : ; il existe $a, b \in A$ tels que $y = xa$ et $z = xb$, donc $y - z = x(a - b) \in xA$, ce qui prouve que xA est un sous-groupe additif. Soient $y \in xA$ et $c \in A$ quelconques ; il existe $a \in A$ tel que $y = xa$, donc $yc = x(ac) \in xA$. On conclut que xA est un idéal de A.

Soit I un idéal de A contenant x. Comme $x \in I$, on a $xA \subset I$, d'où (ii).

Si $xA = A$, alors il existe $a \in A$ tel que $xa = 1 \in A$, ce qui prouve que $x \in U(A)$. L'implication réciproque découle du Lemme 5.7.1. □

Corollaire 5.7.1. *Soit A un anneau commutatif unitaire.*

$$(A \text{ est un corps}) \Longleftrightarrow (\text{les seuls idéaux de } A \text{ sont } \{0\} \text{ et } A).$$

Preuve. Supposons que A est un corps. Soit I un idéal de A. Si $I \neq \{0\}$, alors il existe un élément non-nul de, donc inversible dans A. La Proposition ci-dessus implique que $I = A$. Supposons que A n'admet que les deux idéaux triviaux. Soit x un élément non-nul de A. Alors xA est un idéal distinct de $\{0\}$. Donc $xA = A$, d'où x est inversible d'après (iii) de la proposition ci-dessus. Ceci prouve que A est un corps. □

Proposition et définition 5.7.2. *Soit A un anneau commutatif unitaire.*

(i) Si I et J sont des idéeaux de A, alors l'ensemble $I + J = \{x + y; x \in I, y \in J\}$ est un idéal de A, appelé l'idéal somme de I et J, et c'est le plus peitit idéal contenant I et J ;

(ii) En particulier, si x et y sont des éléments de A, l'ensemble $xA + yA$ est le plus petit idéal de A contenant x et y.

Preuve. Soient I et J deux idéaux de A. Il est clair que $I + J$ est un sous-groupe additif de A. Soient $z \in I + J$ et $a \in A$ quelconques ; il existe $x \in I$ et $y \in J$ tels que $z = x + y$, d'où $za = xa + ya \in I + J$ car $xa \in I$ et $ya \in J$. Ce qui prouve que $I + J$ est un idéal de A. Il est clair que I et J sont des parties de $I + J$. Pour montrer que c'est le plus petit, supposons que K est un idéal de A contenant $I + J$. En particulier, K est stable par addition, et donc, quels que soient $x \in I \subset K$ et $y \in J \subset K$, on a $x + y \in K$. Donc $I + J \subset K$. Ce qui prouve le premier point. Le point (ii) s'en déduit avec $I = xA$ et $J = yA$. □

Remarque 5.7.1. *L'union de deux idéaux n'est en général pas un idéal. Par exemple $A = \mathbb{Z}$, $I = 2\mathbb{Z}$ et $J = 3\mathbb{Z}$.*

5.8 Caratéristique d'un anneau

Pour tout idéal I de l'anneau $\mathbb{Z}$, il existe un unique $k \in \mathbb{N}$ tel que $I = k\mathbb{Z}$. Soit A un anneau commutatif unitaire. Pour tout $x \in A$, on note $2x = x + x$, $3x = x + x + x$ et de même $nx = \underbrace{x + \cdots + x}_{n}$ pour tout entier $n \geq 2$. On pose naturellement $1x = x$ et $0x = 0$, ce qui définit la notation nx pour $n \in \mathbb{N}$. Si l'on considère maintenant un entier $m \leq 0$, on convient que $mx = n(-x) = -(nx)$ où $n = -m \in \mathbb{N}$. On a ainsi défini la notation nx pour tout $x \in A$ et tout $n \in \mathbb{Z}$. On note que $nx = (n1_A)x$ pour tout $x \in A$ et $n \in \mathbb{Z}$.

Soit A un anneau commutatif unitaire. On vérifie aisément que, pour tout $n \in \mathbb{Z}$, on a :

$$(n1_A = 0_A) \Longleftrightarrow (nx = 0_A \text{ pour tout } x \in A).$$

Proposition et définition 5.8.1. *Soit A un anneau commutatif unitaire. Il existe un unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to A$. Il est défini par $f(n) = n1_A$ pour tout $n \in \mathbb{Z}$. On l'appelle le morphisme canonique de $\mathbb{Z}$ dans A.*

Définition 5.8.1. *Soit A un anneau commutatif unitaire. On appelle* caractéristique *de A, notée* $\operatorname{car} A$*, l'unique entier $k \in \mathbb{N}$ tel que* $\operatorname{Ker} f = k\mathbb{Z}$*, où f est le morphisme canonique de $\mathbb{Z}$ dans A.*

Exemples 5.8.1.

(a) L'anneau $\mathbb{Z}$ est de caractéristique nulle, ainsi que les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(b) Pour tout $n \geq 2$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caratéristique n. En particulier, pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caratéristique p.

(c) Soit A un anneau commutatif unitaire. Pour tout sous-anneau unitaire B de A, on a :

$$\operatorname{car} A = \operatorname{car} B.$$

5.9 Multiples, diviseurs et idéaux principeaux

Définition 5.9.1. *Soit A un ACU (anneau commutatif unitaire). Soient x et y deux éléments de A. On dit que x est un* diviseur *de y dans A, ou encore que x divise y dans A, ou encore que y est un multiple de x dans A, lorsqu'il existe $a \in A$ tel que $y = xa$. On note alors : $x|y$.*

Proposition 5.9.1. *Soit A un ACU. Pour tout $x, y \in A$, on a :*

$$(x|y) \Leftrightarrow (y \in xA) \Leftrightarrow (yA \subset xA).$$

Preuve. Si $x|y$ alors il existe $a \in A$ tel que $y = xa$. Donc $y \in xA$. De plus, tout élément de yA est da la forme yb avec $b \in A$, donc de la forme $x(ab)$, et donc appartient à xA, ce qui montre que $yA \subset xA$. La réciproque est claire. □

En particulier, pour tous entiers $n, m \in \mathbb{Z}$ on note que $n|m$ ssi $m\mathbb{Z} \subset n\mathbb{Z}$. On rappelle les divisions euclidiennes dans les anneaux $\mathbb{Z}$ et $K[X]$.

Proposition 5.9.2. *Quels que soient des entiers a et b, avec $b \neq 0$, il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ uniques tels que $a = bq + r$ et $0 \leq r < |b|$.*

Par exemple,

$$12 = 5 \cdot 2 + 2, \quad 12 = -5 \cdot (-2) + 2.$$

Proposition 5.9.3. *Soit K un corps commutatif. Quels que soient des polynômes F et G dans $K[X]$, avec $G \neq 0$, il existe $Q \in K[X]$ et $R \in K[X]$ uniques tels que $F = GQ + R$ et $0 \leq \deg R < \deg G$.*

Par exemple, dans $\mathbb{R}[X]$,

$$X + 1 = (2X + 1) \cdot \frac{1}{2} + \frac{1}{2},$$
$$X^3 + 1 = (X + 2) \cdot (X^2 - 2X - 4) + 9.$$

Définition 5.9.2. *On appelle* anneau euclidien *un ACU qui est intègre, et pour lequel il existe une application $\delta : A^* \to \mathbb{N}$ vérifiant les deux conditions suivantes :*

1. *pour tous $a, b \in A^*$, $(a|b) \Rightarrow (\delta(a) \leq \delta(b))$;*
2. *pour tout $a \in A$ et $b \in A^*$, il existe $q, r \in A$ tels que :*

$$(a = bq + r) \quad et \quad (r = 0 \ \ ou \ \ \delta(r) < \delta(b)).$$

Une application δ vérifiant ces deux conditions s'appelle un stathme euclidien*. Dans la condition 2, on dit que q est un quotient et r un reste dans la* division euclidienne *de a par b.*

Exemple 5.9.1. *L'anneau $Z[i] = \{a + ib; a, b \in \mathbb{Z}\}$ est euclidien, pour le stathme défini par*

$$\delta(z) = z\bar{z} \quad pour\ tout\ z \in \mathbb{Z}[i] \setminus \{0\}.$$

La preuve est laissée en exercice.

Remarque 5.9.1. *La définition d'un stathme n'impose pas de conditions d'unicité de (q, r) dans la seconde condition. L'unicité de (q, r) dans la division euclidienne de $\mathbb{Z}$ tient au fait qu'on y a remplacé la condidtion ($r = 0$ ou $[r| < |b|$) par la condition plus forte $0 \leq r < |b|$.*

Par exemple, pour $a = 19$ et $b = 3$, on a

$$19 = 6 \cdot 3 + 1 = 7 \cdot 3 + (-2)$$

avec $r = 1$ et $r' = -2$ qui vérifient tous les deux

$$\delta(r) = 1 < \delta(3) = 3 \quad et \quad \delta(r') = |-2| = 2 < \delta(3) = 3.$$