TABLE DES MATIÈRES

INTRODUCTION

L'objectif de ce cours est de présenter quelques éléments de l'arithmétique. Il s'agit d'un cours officiel destiné aux étudiants de master en mathématiques fondamentale selon le canevas du programme pédagogique. Pour la réalisation de ce polycopié, on a utilisé les références [1, 2, 3, 4, 5, 6, 7, 8].

Ce document contient quatre chapitres.

Dans le chapitre un, on donne quelques rappels et définitions sur la théorie des groupes finis. Les premiers résultats de cette théorie sont indispensables dans la plupart des applications arithmétiques ultérieures.

Le chapitre deux parle de l'arithmétique sur $\mathbb{Z}$ et les congruences. Il est consacré à l'étude de la divisibilté dans $\mathbb{N}$ et $\mathbb{Z}$ qui est le point de départ de l'arithmétique, ainsi les nombres premiers.

Le chapitre trois et quatre, abordent respectivement les nombres et les polynômes de Bernoulli, les nombres et les polynômes d'Euler. On retrouve ces nombres et ces polynômes en arithmétique.

CHAPITRE 1

RAPPELS SUR LA THÉORIE DES GROUPES FINIS

L'objectif de ce chapitre est de rappeler quelques définitions et résultats de base concernant les groupes, les anneaux et les corps. Ces notions sont supposées connues et ne seront pas traitées explicitement en cours.

1.1 Définition d'un groupe

Afin de définir un groupe, il convient de se donner un ensemble G et une loi de composition interne sur G vérifiant certaines conditions.

Définition 1.1.1 *On appelle un groupe un couple* $(G, *)$ *formé d'un ensemble* G *et d'une loi de composition* $(x, y) \rightarrowtail x * y$ *sur* G*, tels que les trois conditions suivantes soient vérifiées :*

1. **Associativité** *: on a* $x * (y * z) = (x * y) * z$ *quels que soient* $x, y, z \in G$*.*

2. **Existance d'un élément neutre** *: il existe un élément $e \in G$ tel que $e * x = x * e = x$ pour tout $x \in G$.*
3. **Existance d'un symétrique pour tout élément de** G *: pour tout $x \in G$, il existe un élément $y \in G$ tel que $x * y = y * x = e$.*

Si de plus, quels que soient $x, y \in G$, on a $x * y = y * x$ (commutativité), on dit que G est un groupe commutatif ou abélien.

Un groupe peut être fini ou infini. S'il est fini, on appelle un ordre du groupe le nombre de ses éléments i.e. son cardinal.

Notations 1.1.2 *Dans la définition ci-dessus, on a utilisé la notation abstraite $*$ pour définir la loi de composition de G. En théorie des groupes, on note en fait la plupart du temps la loi de composition sous-jacente multiplicativement $(x, y) \rightarrowtail xy$ ou bien additivement $(x, y) \rightarrowtail x + y$. En notation multiplicative, on emploie le mot inverse au lieu du mot symétrique et l'inverse d'un élément x se note x^{-1}. Pour tout $x, y \in G$, on a alors la formule $(xy)^{-1} = y^{-1}x^{-1}$. En notation additive, on dit opposé au lieu de symétrique, et l'on note généralement 0 l'élément neutre et $-x$ l'opposé de x. Dans la pratique, la notation additive est utilisée uniquement pour les groupes abéliens. Cela étant, la notation multiplicative est aussi très souvent employée pour les groupes abéliens. Dans toute la suite, on appellera groupe multiplicatif, un groupe dont la loi de composition est notée multiplicativement, et groupe additif, un groupe dont la loi de composition est notée additivement.*

Exemples 1.1.3

1. *L'ensemble réduit à un seul élément e, avec pour la loi de composition $e * e = e$, est un groupe, appelé le groupe trivial.*
2. *L'ensemble $\mathbb{Z}$ des entiers relatifs muni de la loi de composition $(x, y) \rightarrowtail x + y$ est un groupe commutatif, d'élément neutre 0. On l'appelle le groupe additif des entiers relatifs. En remplaçant $\mathbb{Z}$ par $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, on obtient respectivement le groupe additif des nombres rationnels, celui des nombres réels et celui des nombres complexes.*
3. *L'ensemble $\mathbb{Q}^*$ des nombres rationnels non nuls, muni de la loi de composition $(x, y) \rightarrowtail xy$, est un groupe commutatif, d'élément neutre 1. C'est le groupe multiplicatif des nombres rationnels non nuls. On définit de même les groupes multiplicatifs $\mathbb{R}^*$ et $\mathbb{C}^*$.*

4. *Soient X un ensemble et G un groupe multiplicatif. L'ensemble G^X des applications de X à valeurs dans G est un groupe muni de la loi de composition définie par :*

$$(fg)(x) = f(x)g(x) \text{ pour tous } f, g \in G^X \text{ et } x \in X.$$

5. **Produit direct de groupes** *: Soient $G_1, \ldots, G_n$ des groupes multiplicatifs. Posons*

$$G = G_1 \times \ldots \times G_n.$$

La loi de composition sur G définie par l'égalité

$$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n),$$

munit G d'une structure de groupe. L'élément neutre est $(e_1, \ldots, e_n)$ où e_i est l'élément neutre de G_i. L'inverse d'un élément $x = (x_1, \ldots, x_n)$ est donné par la formule

$$x^{-1} = \left(x_1^{-1}, \ldots, x_n^{-1}\right).$$

Le groupe $(G, \cdot)$ est appelé le produit direct des groupes $G_1, \ldots, G_n$, ou bien le groupe produit de $G_1, \ldots, G_n$.

1.1.1 Sous-groupes

Soit G un groupe multiplicatif, d'élément neutre e.

Définition 1.1.4 *Soit H une partie de G. On dit que H est un sous-groupe de G si les conditions suivantes sont réalisées :*

1. *L'élément e appartient à H.*
2. *Pour tous $x, y \in H$, l'élément xy est dans H.*
3. *Pour tout $x \in H$, l'inverse x^{-1} de x est dans H.*

Un sous-groupe de G muni de la loi de composition induite par celle de G est un groupe. Une partie H de G est un sous-groupe de G si et seulement si H n'est pas vide, et si pour tous $x, y \in H$, l'élément $(xy)^{-1}$ est aussi dans H. Si $(H_i)_{i\in I}$ est une famille de sous-groupe de G, l'intersection des H_i est un sous-groupe de G.

Exemples 1.1.5 *1. Les parties G et $\{e\}$ sont des sous-groupes de G. Le sous-groupe $\{e\}$ s'appelle le sous-groupe trivial de G.*

2. *Le sous-ensemble de $\mathbb{R}^*$ formé des nombres réels strictement positifs, ainsi que $\{\pm 1\}$, sont des sous-groupes de $\mathbb{R}^*$.*

3. *Si n est un entier relatif, la partie $nZ = \{nk/k \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{Z}$.*

4. *Soit x un élément de G. Pour tout entier relatif k, on définit x^k comme suite* [1]

$$x^k = \begin{cases} x \cdots x & (k \text{ facteurs}) \text{ si } \quad k \geq 1, \\ e & \text{si } \quad k = 0, \\ (x^{-1})^{-k} & \text{si } \quad k < 0. \end{cases}$$

Quels que soient les entiers relatifs k et k', on vérifie que l 'on a les égalités

$$x^k x^{k'} = x^{k+k'}, \ \ (x^k)^{-1} = x^{-k}, \ \ (x^k)^{k'} = x^{kk'}.$$

Il en résulte que l'ensemble $\left\{x^k/k \in \mathbb{Z}\right\}$ est un sous-groupe abélien de G.

---

1. Soient E un ensemble et $*$ une loi de composition sur E. On définit la composé d'éléments $x_1, \ldots, x_n$ de E par la formule de récurrence :

$$x_1 * x_2 * \cdots * x_n = (x_1 * x_2 * \cdots * x_{n-1}) * x_n.$$

Pour tout $x \in E$ et tout entier $n \geq 1$, on définit la puissance n-ième de x par la formule $x^n = x * x * \cdots * x$ (n facteurs). Supposons $*$ associative. Vérifions alors pour tout entier p tel que $1 \leq p \leq n$, on a l'égalité

$$x_1 * \cdots * x_n = (x_1 * x_2 * \cdots * x_p) * (x_{p+1} * \cdots * x_n).$$

Elle est vraie si $n = 1$. Supposons qu'elle le soit un produit de $n-1$ éléments où $n \geq 2$. Posons $x = x_1 * \cdots x_n$. On a $x = (x_1 * x_2 * \cdots * x_{n-1}) * x_n$. Soit p un entier compris entre 1 et n. L'égalité à prouver étant satisfaite si $p = n$, on peut supposer $p \leq n-1$. D'après l'hypothèse de récurrence, on a donc $x = \Big((x_1 * \cdots * x_p) * (x_{p+1} * \cdots * x_{n-1})\Big) * x_n$. Puisque $*$ est associative, on obtient $x = (x_1 * \cdots * x_p) * \Big((x_{p+1} * \cdots * x_{n-1}) * x_n\Big)$, d'où l'égalité annoncée.

1.1.2 Classe modulo un sous-groupe

Soient G un groupe multiplicatif, d'élément neutre e, et H un sous-groupe de G. On associe à H la relation binaire $\mathcal{R}$ sur G définie pour tous $x, y \in G$

$$x\mathcal{R}y \Leftrightarrow x^{-1}y \in H. \tag{1.1}$$

C'est une relation d'équivalence sur G. La propriété de réflexivité résulte du fait que $e \in H$. Si x, y, z sont dans G, l'égalité $\left(x^{-1}y\right)^{-1} = y^{-1}x$ entraine la propriété de symétrie. En ce qui concerne la transitivité, si l'on a $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x^{-1}y$ et $y^{-1}z$ sont dans H, donc $(x^{-1}y)(y^{-1}z) = x^{-1}z$ l'est aussi, d'où $x\mathcal{R}z$. Pour tout $x \in G$, la classe d'équivalence de x est l'ensemble

$$xH = \{xh / h \in H\}.$$

C'est la classe (à gauche) de x modulo H. L'ensemble des classes des éléments de G modulo H se note G/H. On a ainsi

$$G/H = \{xH / x \in G\}.$$

On déduit de ce qui précède le théorème de Lagrange, qui est à la base de toute la théorie des groupes finis. Si G est fini, il en est de même de H et G/H. Notons dans ce cas $|G|$, $|H|$ et $|G/H|$ leurs cardinaux respectifs.

Théorème 1.1.6 (Lagrange) *Supposons G fini. On a l'égalité $|G| = |H| \times |G/H|$. En particulier, l'ordre de H divise celui de G.*

Démonstration. Pour tout $x \in G$, les ensembles H et xH sont en bijection via l'application qui à h associe xh. Le résultat s'en déduit aussitôt car G est la réunion disjointe de ses classes d'équivalences modulo H. ■

Si l'ensemble G/H est fini (que G soit fini ou non), on dit que $|G/H|$ est l'indice de H dans G.

Exemple 1.1.7 *Supposons G fini d'ordre un nombre premier. Les seuls sous-groupes de G sont G et {e}.*

Remarque 1.1.8 *Supposons que G soit un groupe abélien additif. La relation d'équivalence modulo H définie par (1.1) s'écrit alors sous la forme*

$$x\mathcal{R}y \Leftrightarrow x - y \in H.$$

Pour tout $x \in G$, la classe de x modulo H se note $x + H$. On a

$$x + H = \{x + h / h \in H\} \quad et \quad G/H = \{x + H / x \in G\}.$$

La classe modulo H de l'élément neutre de G est H.

Exemple 1.1.9 (L'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$) *Prenons $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ où $n \in \mathbb{N}$. Quels que soient $x, y \in \mathbb{Z}$ on a l'équivalence*

$$x \text{ et } y \text{ sont en relation modulo } n\mathbb{Z} \Leftrightarrow x - y \in n\mathbb{Z}.$$

Deux entiers relatifs x et y sont donc en relation modulo $n\mathbb{Z}$ si et seulement si n divise $x - y$. Dans ce cas, on dit que x et y sont congrus modulo n et l'on écrit que l'on a la congruence $x \equiv y \mod n$. Pour tout $x \in \mathbb{Z}$, la classe de x modulo $n\mathbb{Z}$ est

$$x + n\mathbb{Z} = \{x + nk / k \in \mathbb{Z}\}.$$

On la note souvent $\overline{x}$ lorsque l'entier n est sous-entendu. On dit aussi que c'est la classe de x modulo n. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est formé des classes d'équivalence modulo n.

Proposition 1.1.10 *Supposons $n \geq 1$. Alors $\mathbb{Z}/n\mathbb{Z}$ est fini de cardinal n et l'on a*

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

Démonstration. Soit $a + n\mathbb{Z}$ un élément de $\mathbb{Z}/n\mathbb{Z}$. Il existe des entiers q et r tels que l'on

ait $a = nq + r$ avec $0 \leq r < n$ (division euclidienne). Puisque $a - r \in n\mathbb{Z}$, on a donc $\overline{a} = \overline{r}$. Par ailleurs, quels que soient a et b distincts compris entre 0 et $n-1$, l'entier n ne divise pas $a - b$, autrement dit, on a $\overline{a} \neq \overline{b}$, d'où le résultat. ■

On dispose de la surjection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ qui à un entier a associe sa classe modulo n. Dans le cas où $n = 0$, et dans ce cas seulement, c'est une bijection.

1.1.3 Groupe quotient d'un groupe abélien

Soit G un groupe abélien additif, d'élément neutre 0. Soit H un sous-groupe de G. On définit sur l'ensemble quotient G/H une loi de composition $\oplus$ comme suit.
Soient u, v des éléments de G/H. Il existe $x, y \in G$ tels que $u = x + H$ et $v = y + H$. On pose alors

$$u \oplus v = (x + y) + H, \tag{1.2}$$

autrement dit, $u \oplus v$ est la classe de $x + y$ modulo H. il faut bien entendu vérifier que cette définition a un sens, i.e. que $u \oplus v$ ne dépend pas des représentants choisis x et y de u et v.
Considérons pour cela des représentants x' et y' respectivement de u et v. Par définition, $x - x'$ et $y - y'$ sont dans H. Puisque G est abélien, il en résulte que

$$(x - x') + (y - y') = x + y - (x' + y') \in H,$$

ce qui signifie que $x + y$ et $x' + y'$ sont en relation modulo H, d'où notre assertion.

Proposition 1.1.11 *L'ensemble G/H muni de la loi $\oplus$ est un groupe abélien. On l'appelle le groupe quotient de G par H.*

Démonstration. Le fait que la loi + sur G soit associative et commutative entraîne qu'il en est de même de $\oplus$. L'élément neutre de $\oplus$ est $0 + H = H$ et pour tout $x \in G$, l'opposé de $x + H$ est $-x + H$, où $-x$ est l'opposé de x dans G, d'où le résultat. ■

Exemple 1.1.12 (Le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$) *Soit n un entier naturel. En prenant pour $(G, +)$ le groupe des entiers relatifs $(\mathbb{Z}, +)$ et pour H le sous-groupe $n\mathbb{Z}$ de $\mathbb{Z}$, on obtient le groupe quotient $(\mathbb{Z}/n\mathbb{Z}, \oplus)$. On notera toujours $+$ la loi $\oplus$ sur $\mathbb{Z}/n\mathbb{Z}$. Le groupe quotient $(\mathbb{Z}/n\mathbb{Z}, +)$ ainsi défini est appelé le groupe additif des entiers relatifs modulo n. Quels que soient $a, b \in \mathbb{Z}$, on a après (1.2),*

$$\overline{a} + \overline{b} = \overline{a + b}.$$

L'élément neutre de $\mathbb{Z}/n\mathbb{Z}$ est $n\mathbb{Z}$. On a par ailleurs

$$k\overline{a} = \overline{ka} \text{ pour tout } k \in \mathbb{Z}.$$

Proposition 1.1.13 *Supposons $n \geq 1$. Le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$ est d'ordre n et ses éléments sont les classes des entiers compris entre 0 et $n - 1$.*

1.1.4 Sous-groupe engendré par un élément -Ordre d'un élément

Soit G un groupe multiplicatif, d'élément neutre e. Pour tout $x \in G$, il existe un plus petit sous-groupe de G qui contient $\{x\}$, à savoir l'intersection des sous-groupes de G qui contiennent $\{x\}$.

Définition 1.1.14 *Soit x un élément de G. On appelle sous-groupe de G engendré par x, l'intersection des sous-groupes de G qui contiennent $\{x\}$. On le notera $< x >$.*

Lemme 1.1.15 *Soit x un élément de G. On a $< x >= \left\{x^k / k \in \mathbb{Z}\right\}$.*

Démonstration. On a vu que $\left\{x^k / k \in \mathbb{Z}\right\}$ est un sous-groupe de G. Il contient $\{x\}$, donc aussi $< x >$. Inversement, soit H un sous-groupe de G tel que x soit dans H. D'après les propriétés de stabilité d'un sous-groupe, l'ensemble $\left\{x^k / k \in \mathbb{Z}\right\}$ est contenu dans H. Par suite, il est contenu dans $< x >$. ■

Exemples 1.1.16 *Soit n un entier naturel.*

1. *Le sous-groupe de $\mathbb{Z}$ engendré par n est $n\mathbb{Z}$.*
2. *Le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ engendré par la classe de 1 est $\mathbb{Z}/n\mathbb{Z}$.*

Définition 1.1.17 *Supposons G fini. Soit x un élément de G. On appelle ordre de x, l'ordre du sous-groupe de G engendré par x.*

Théorème 1.1.18 *Supposons G fini. Soit x un élément de G d'ordre m.*

1. *On a $m \geq 1$ et m divise l'ordre de G.*
2. *On a $x^m = e$ et m est le plus petit entier $k \geq 1$ tel que $x^k = e$.*
3. *Pour tout $n \geq 1$, on a $x^n = e$ si et seulement si m divise n.*
4. *On a $< x >= \left\{e, x, \ldots, x^{m-1}\right\}$.*

Démonstration.

1. La première assertion résulte du Théorème 1.1.6 de Lagrange.
2. Considérons l'ensemble A défini par l'égalité

$$A = \left\{k \in \mathbb{N}/1 \leq k \leq m \text{ et } x^k = e\right\}.$$

Il s'agit de démontrer que l'on a

$$A = \{m\}. \tag{1.3}$$

D'abord, A est non vide. En effet, si A était vide, les éléments $x, \ldots, x^m, x^{m+1}$, seraient distincts deux à deux et l'ordre de $< x >$ serait strictement plus grand que m (Lemme 1.1.15).
Soit u un élément de A. Tout revient à prouver que l'on a $u = m$. Posons

$$B = \left\{e, x, \ldots, x^{u-1}\right\}.$$

Vérifions que $< x >$ est contenu dans B. Soit k un entier relatif. Il existe q et r

dans $\mathbb{Z}$ tels que l'on ait

$$k = uq + r \text{ avec } 0 \leq r < u.$$

Vu que l'on a $x^u = e$, on obtient ainsi

$$x^k = (x^u)^q x^r = x^r \in B,$$

d'où l'assertion. Le cardinal de B étant au plus u, on a donc $m \leq u$. Puisque u appartient à A, on a aussi $u \leq m$, d'où $u = m$, puis l'égalité (1.3).

3. Soit n un entier ≥ 1 tel que $x^n = e$. Il existe des entiers q et r tels que $n = mq + r$ avec $0 \leq q < m$. On obtient $x^r = e$, d'où $r = 0$ (second assertion), donc m divise n. L'implication réciproque est immédiate.
4. En ce qui concerne la dernière assertion, on déduit de ce qui précède que le cardinal de l'ensemble $\left\{e, x, \ldots, x^{m-1}\right\}$ est m. Il est contenu dans $< x >$, qui est aussi d'ordre m, d'où le résultat.

■

Comme conséquence du Théorème 1.1.18, on obtient :

Théorème 1.1.19 *Supposons G fini d'ordre n. Pour tout $x \in G$, on a $x^n = e$.*

1.1.5 Morphismes de groupes

Sauf précision contraire, les groupes considérés dans ce paragraphe sont implicitement supposés multiplicatifs.

Définition 1.1.20 *Soient G et G' des groupes. On appelle morphisme de groupes de G dans G', toute application $f : G \to G'$ telle que l'on ait*

$$f(xy) = f(x)f(y).$$

Exemples 1.1.21 *1. Soient $\mathbb{R}_+^*$ le sous-groupe de $\mathbb{R}^*$ formé des nombres réels strictement positifs et* $\log : \mathbb{R}_+^* \to \mathbb{R}^*$ *la fonction logarithme népérien. La formule*

$$log(xy) = log(x) + log(y),$$

définit un morphisme de $(\mathbb{R}_+^*, \times)$ à valeur dans $(\mathbb{R}, +)$.

2. *Soit G un groupe. Pour tout $\alpha \in G$, l'application $f_\alpha : \mathbb{Z} \to G$ définie par $f(n) = \alpha^n$ est morphisme de groupes. En fait, pour tout morphisme f de $\mathbb{Z}$ dans G, il existe $\alpha \in G$ tel que $f = f_\alpha$, comme on le constate en posant $f(1) = \alpha$.*

3. *Pour tout $n \geq 1$, la surjection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme. Plus généralement, pour tout groupe abélien additif G et tout sous-groupe H de G, l'application $s : G \to G/H$ défnie par $s(x) = x + H$ est un morphisme de groupes. Cela résulte de la définition de la loi de groupe sur G/H.*

Lemme 1.1.22 *Soit $f : G \to G'$ un morphisme de groupes. Soient e et e' les éléments neutres de G et G' respectivement.*

1. *On a $f(e) = e'$.*

2. *Pour tout $x \in G$, on a $f(x^{-1}) = f(x)^{-1}$.*

Démonstration. Pour tout $x \in G$, on a $f(x) = f(xe) = f(x)f(e)$. Par suite, on a $f(x)^{-1}f(x) = f(x)^{-1}f(x)f(e)$, d'où $e' = f(e)$. On obtient alors

$$e' = f(xx^{-1}) = f(x)f(x^{-1}) \quad \text{et} \quad e' = f(x^{-1}x) = f(x^{-1})f(x).$$

■

Lemme 1.1.23 *Soient $f : M \to N$ et $g : N \to P$ des morphismes de groupes. L'application composée $g \circ f : M \to P$ est encore un morphisme de groupes. Si le morphisme $f : M \to N$ est une bijection de M sur N, alors son application réciproque est un morphisme.*

Démonstration. Soient x et y des éléments de M. On a les égalités

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)),$$

d'où la première assertion. En ce qui concerne la seconde, considérons des éléments u et v de N. Il s'agit de montrer que l'on a

$$f^{-1}(uv) = f^{-1}(u)f^{-1}(v). \tag{1.4}$$

Puisque f est une bijection de M sur N, c'est en particulier une injection. Il suffit donc de montrer que les images par f des deux membres de (1.4) sont égales, autrement dit que l'on a $uv = f(f^{-1}(u)f^{-1}(v))$, ce qui résulte du fait que f soit un morphisme. ■

Définition 1.1.24 *Soient G et G' des groupes. On appelle isomorphisme de G sur G', tout morphisme bijectif de G sur G'. On dit que G et G' sont isomorphes s'il existe un isomorphisme de G sur G'.*

Exemple 1.1.25 *La fonction logarithme est un isomorphisme de $\mathbb{R}_*^+$ sur $\mathbb{R}$, le morphisme réciproque étant la fonction exponentielle.*

1.1.6 Noyau et image d'un morphisme de groupes

Lemme 1.1.26 *Soit $f : G \to G'$ un morphisme de groupes.*

1. *Pour tout sous-groupe H de G, l'image $f(H)$ de H par f est un sous-groupe de G'.*
2. *Pour tout sous-groupe H' de G', l'image réciproque $f^{-1}(H')$ de H' par f est un sous-groupe de G.*

Démonstration. La première assertion est laissée en exercice. Démontrons la seconde. Notons e et e' les élément neutres de G et G' respectivement. Soit H' un sous groupe de G'. On a $f(e) = e' \in H'$ donc e appartient à $f^{-1}(H')$. Par ailleur, si x et y sont dans

$f^{-1}(H')$, alors $f(x)$ et $f(y)$ sont dans H' et $f(xy) = f(x)f(y)$ appartient aussi à H', d'où $xy \in f^{-1}(H')$. De même, on a $f(x^{-1}) = f(x)^{-1} \in H'$, donc $x^{-1} \in f^{-1}(H')$. ■

Définition 1.1.27 *Soit $f : G \to G'$ un morphisme de groupes. On appelle image de f le sous-groupe $f(G)$ de G'. On appelle noyau de f le sous-groupe $f^{-1}(\{e'\})$ de G, où e' est l'élément neutre de G', on le note souvent $Ker(f)$. On a donc*

$$Ker(f) = \{x \in G / f(x) = e'\}.$$

Lemme 1.1.28 *Soit $f : G \to G'$ un morphisme de groupes. Pour que f soit injectif il faut et il suffit que $Ker(f)$ soit réduit à l'élément neutre de G.*

Démonstration. Supposons f injectif. Soit x un élément de $Ker(f)$. On a les égalités $f(x) = e' = f(e)$, d'où $x = e$. Supposons $Ker(f) = \{e\}$. Soient x et y deux éléments de G tels que $f(x) = f(y)$. On a $f(x)f(y)^{-1} = e'$, d'où $xy^{-1} = e$ puis $x = y$. ■

Théorème 1.1.29 (Factorisation des morphismes de groupes) *Soient G un groupe abélien additif et f un morphisme de G dans un groupe G'. Le groupe quotient $G/Ker(f)$ est isomorphe à $f(G)$, via l'application qui à $x + Ker(f)$ associe $f(x)$.*

Démonstration. Soient x et y des éléments de G tels que $x - y$ appartienne à $Ker(f)$. On a $f(x - y) = e'$, autrement dit, on a $f(x) = f(y)$. On obtient ainsi une application

$$h : G/Ker(f) \to f(G)$$

définie pour $x \in G$ par l'égalité

$$h(x + Ker(f)) = f(x).$$

C'est un morphisme. En effet, quels que soient $x, y \in G$, on a

$$h((x+y)+Ker(f)) = f(x+y) = f(x)f(y) = h(x+Ker(f))h(x+Ker(f)).$$

Par ailleurs, si $f(x) = e'$, x appartient à $Ker(f)$, d'où $x + Ker(f) = Ker(f)$, donc h est injectif. Par définition, h est une surjection de $G/Ker(f)$ sur $f(G)$, d'où le résultat. ■

Exemple 1.1.30 *Soit U le groupe des nombres complexes de module 1. L'application $\mathbb{R} \to U$ qui à $t \in \mathbb{R}$ associe e^{it} (où $i^2 = -1$) est un morphisme de groupes surjectif de noyau $2\pi\mathbb{Z}$. En particulier, les groupes $\mathbb{R}/2\pi\mathbb{Z}$ et U sont isomorphes.*

1.2 Définition d'un anneau

Définition 1.2.1 *On appelle anneau un triplet formé d'un ensemble A et de deux lois de composition sur A, une addition $(x, y) \to x + y$ et une multiplication $(x, y) \to xy$, tels que les conditions suivantes soient vérifiées :*

1. *Le couple $(A, +)$ est un groupe commutatif.*
2. *La multiplication est associative et possède un élément neutre.*
3. *La multiplication est distributive par rapport à l'addition, ce qui signifie que l'on a*

$$x(y+z) = xy + xz \text{ et } (x+y)z = xz + yz \quad \text{quels que soient } x, y, z \in A.$$

Si de plus la multiplication est commutative, autrement dit, si l'on a $xy = yx$ quels que soient $x, y \in A$, on dit que A est un anneau commutatif.

On notera 0 l'élément neutre de $(A, +)$ et 1, ou 1_A, l'élément neutre de A pour la multiplication. Rappelons que pour tout $x \in A$, il existe un élément de A, noté $-x$, tel que l'on ait $x + (-x) = 0$ ($-x$ est l'opposé de x).

Lemme 1.2.2 *Quels que soient $x, y, z \in A$, on a*

$$x(y-z) = xy - xz \quad et \quad (y-z)x = yx - zx.$$

Démonstration. D'après la condition 3 de Définition 1.2.1, on a $x(y-z)+xz = x(y-z+z) = xy$ et $(y-z)x + zx = (y-z+z)x = yx$, d'où le lemme. ■

On en déduit par exemple les formules $x0 = 0x = 0$, $x(-y) = -xy$ et $(-y)x = -yx$. En particulier, $(-1)x = -x$. Par convention, on a

$$x^0 = 1_A \text{ pour tout } x \in A.$$

Un anneau réduit à un élément, i.e. pour lequel on a $1 = 0$, est dit nul.

Exemples 1.2.3

1. *En munissant $\mathbb{Z}$ des deux lois de composition usuelles (addition et multiplication) on obtient l'anneau des entiers relatifs, qui est commutatif. Les ensembles $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de l'addition de la multiplication usuelles sont aussi des anneaux commutatifs.*

2. ***L'anneau A[X].*** *Soit A un anneau commutatif. Un polynôme à une indéterminée à coefficients dans A est par définition une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments de A qui est nulle à partir d'un certain rang. Les a_n sont appelés les coefficients du polynôme. Sur cet ensemble de polynômes, on définit deux lois de composition, une addition et une multiplication. Si $P = (p_0, p_1, \ldots)$ et $Q = (q_0, q_1, \ldots)$ sont des polynômes à coefficientts dans A, on pose*

$$P + Q = (p_0 + q_0, p_1 + q_1, \ldots) \text{ et } PQ = (s_0, s_1, \ldots) \text{ avec } s_n = \sum_{i+j=n} p_i q_j.$$

On vérifie que que l'on obtient ainsi un anneau commutatif. Pour tout $a \in A$, on note a le polynôme $(a, 0, \ldots, 0, \ldots)$. Posons $X = (0, 1, 0, \ldots, 0, \ldots$. Pour tout entier $n \geq 1$, et tout $a \in A$, on vérifie alors que l'on a $aX^n = (0, \ldots, 0, a, 0, \ldots)$, où le $n+1$-ième terme de la suite est a et où tous les autres sont nuls. Tout polynôme $P = (p_0, p_1, \ldots, p_n, 0, \ldots)$,

dont les cefficients d'indices strictement plus grands que n sont nuls, s'écrit alors

$$P = p_0 + p_1X + \cdots + p_nX^n,$$

qui est la notation polynomiale de P et que l'on utilise exclusivement. On note $A[X]$ *l'anneau ainsi obtenu. Bien entendu, on peut désigner le polyôme* $(0, 1, 0, \ldots)$ *par d'autres lettres que X, pourvu que la lettre choisie n'ait pas été utilisée par ailleurs.*

3. ***Produit direct d'anneaux.*** *Soient* $A_1, \ldots, A_n$ *des anneaux. Il existe sur le produit cartésien*

$$A_1 \times \cdots \times A_n$$

une structure d'anneau, l'addition et la multiplication étant données par les formules

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n), \tag{1.5}$$

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1y_1, \ldots, x_ny_n). \tag{1.6}$$

Si tous les anneaux A_i *sont commutatifs, il en est de même de A. On dit que A est le produit direct des* A_i*, ou encore l'anneau produit des* A_i*. Notons que l'élément neutre multiplicatif de A est* $(1_{A_1}, \ldots, 1_{A_n})$.

1.2.1 Sous-anneaux - Idéaux

Soient A un anneau et B une partie de A.

Définition 1.2.4 *On dit que B est un sous-anneau de A si les conditions suivantes sont vérifiées :*

1. *B est un sous-groupe additif de A.*
2. *Quels que soient x et y dans B, le produit xy est dans B.*
3. *L'élément neutre multiplicatif* 1_A *appartient à B.*

On vérifie que si B est un sous-anneau de A, alors B muni des deux lois de composition

induites par celles de A est un anneau.

Exemples 1.2.5 *1. $\mathbb{Z}$ est un sous-anneau de $\mathbb{R}$, lui-même étant un sous-anneau de $\mathbb{C}$.*

2. Soit i une racine carrée de -1 dans $\mathbb{C}$. L'ensemble $\mathbb{Z}[i]$ des éléments de la forme $a + ib$ avec $a, b \in \mathbb{Z}$ est sous-anneaux de $\mathbb{C}$. On l'appelle l'anneau des entiers de Gauss.

Définition 1.2.6 *Supposons A commutatif. On dit que B est un idéal de A si les deux conditions suivantes sont vérifiées :*

1. *B est un sous-groupe additif de A.*
2. *Quels que soient $x \in B$ et $y \in A$, le produit xy est dans B.*

Exemples 1.2.7 *1. **Idéaux de $\mathbb{Z}$.** Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, où n parcourt $\mathbb{N}$. En effet, ce sont les sous-groupes de $\mathbb{Z}$, et ils vérifient la condition 2 de Définition 1.2.6.*

*2. **Idéaux principaux.** Supposons A commutatif. Soit a un élément de A. L'ensemble des éléments de la forme ax, où x parcourant A, est un idéal de A. On appelle l'idéal principal engendré par a. On le note aA ou (a). Tous les idéaux de $\mathbb{Z}$ sont principaux.*

3. L'ensemble $\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$.

1.2.2 Anneau quotient

Considérons un anneau commutatif A et I un idéal de A. Puisque $(A, +)$ est un groupe abélien et que I est un sous-groupe de A, on peut associer à I la relation d'équivalence $\mathcal{R}$ sur A définie pour tous $x, y \in A$ par la condition

$$x\mathcal{R}y \to x - y \in I.$$

L'ensemble quotient A/I, muni de la loi de composition définie pour tous $x, y \in A$ par

$$(x + I) + (y + I) = (x + y) + I, \tag{1.7}$$

est un groupe abélien, d'élément neutre I i.e. la classe de 0. On va définir une seconde loi de composition sur A/I, appelée multiplication, de sorte que A/I soit, avec l'addition précedente, muni d'une structure d'anneau commutatif. Soient $x+I$ et $y+I$ des éléments de A/I. On définit la multiplication par la formule

$$(x + I)(y + I) = xy + I. \tag{1.8}$$

Pour que cette définition ait sens, il convient de vérifier qu'elle ne dépend pas des représentants x et y de $x + I$ et de $y + I$. Soient x' et y' dans A tels que $x + I = x' + I$ et $y + I = y' + I$. Il existe r et t dans I tels que $x = x' + r$ et $y = y' + t$. On a

$$xy = x'y' + (x't + ry' + rt).$$

Puisque r et t sont dans I, il en est de même de $x't + ry' + rt$, par suite, $xy - x'y'$ appartient a I, d'où notre assertion.

Théorème 1.2.8 *L'ensemble A/I muni de l'addition et la multiplication définies par les formules (1.7) et (1.8) est un anneau commutatif. On l'appelle l'anneau quotient de A par I.*

Démonstration. On sait déjà que $(A/I, +)$ est un groupe abélien. La multiplication dans A étant associative et commutative, il en est de même dans A/I comme on le constate directement. Par ailleurs, $1+I$ est l'élément neutre multiplicatif de A/I (car 1 est l'élément neutre multiplicatif de A). Il reste à vérifier que la multiplication est distributive par rapport à l'addition. Soient x, y, z des éléments de A. On a les égalités

$$(x + I)((y + I) + (z + I)) = (x + I)((y + z) + I) = x(y + z) + I = xy + xz + I = (xy + I) + (xz + I),$$

par suite, on a

$$(x + I((y + I) + (z + I)) = (x + I)(y + I) + (x + I)(z + I).$$

La deuxième égalité de la définition de la distributivité se vérifie de la même façon. ■

Exemples 1.2.9 .

1. ***L'anneau quotient*** $\mathbb{Z}/n\mathbb{Z}$**.**
   Soit n un entier naturel non nul. On a vu que $n\mathbb{Z}$ est un idéal de $n\mathbb{Z}$. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est ainsi muni d'une structure d'anneau commutatif, pour laquelle l'addition et la multiplication sont données par (formules (1.7) et (1.8))

   $$\overline{a} + \overline{b} = \overline{a+b} \text{ et } \overline{a}\overline{b} = \overline{ab} \text{ quels que soient } a, b \in \mathbb{Z}$$

   L'élément neutre additif est $\overline{0} = n\mathbb{Z}$. . L'élément neutre multiplicatif est $\overline{1} = 1 + n\mathbb{Z}$, i.e. est l'ensemble des entiers a tels que n divise $a - 1$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ s'appelle l'anneau des entiers modulo n.
2. *Soit $F \in A[X]$ un polynôme à coefficients dans un anneau commutatif A. On peut considérer l'anneau quotient $A[X]/(F)$, où (F) est l'idéal principal de $A[X]$ engendré par F. Nous étudierons ces anneaux notamment si $A = \mathbb{Z}/p\mathbb{Z}$, où p est premier. Notons au passage que l'on peut poser comme définition $C = \mathbb{R}[X]/(X^2 + 1)$.*

1.2.3 Groupe des éléments inversibles - Corps - Anneaux intègres

Définition 1.2.10 *Soient A un anneau et a un élément de A. On dit que a est un élément inversible de A s'il possède un inverse pour la multiplication, autrement dit, s'il existe $b \in A$ tel que l'on ait $ab = ba = 1$. On notera A^* l'ensemble des éléments inversibles de A.*

Si $a \in A$ est inversible, il existe un unique élément $b \in A$ tel que $ab = ba = 1$ et on le note a^{-1}. Si x et y sont dans A^*, le produit xy l'est aussi et son inverse est $y^{-1}x^{-1}$. La multiplication induit ainsi sur A une loi de composition. Plus précisèment :

Proposition 1.2.11 *L'ensemble A^*, muni de la multiplication induite par celle de A, est un groupe. On l'appelle le groupe des éléments inversibles de A, ou le groupe des unités de A.*

Lemme 1.2.12 *Soient A et B des anneaux. Le groupe des éléments inversibles de l'anneau produit $A \times B$ est $A^* \times B^*$. Autrement dit, on a $(A \times B)^* = A^* \times B^*$. En particulier, si A et B sont*

finis, on a $|(A \times B)^*| = |A^*| \times A^*|$.

Démonstration. Soit (a, b) un élément inversible de $A \times B$. Il existe $(c, d) \in A \times B$ tel que $(a, b)(c, d) = (c, d)(a, b) = (1_A, 1_B)$. D'après la formule (1.6), on obtient ainsi les égalités $ac = ca = 1_A$ et $bd = db = 1_B$, ce qui prouve que $a \in A^*$ et que $b \in B^*$. Inversement, si (a, b) est un élément de $A^* \times B^*$, il existe $c \in A$ et $d \in B$ tels que $ac = ca = 1_A$ et $bd = db = 1_B$. Par suite, on a $(a, b)(c, d) = (c, d)(a, b) = (1_A, 1_B)$, d'où $(a, b) \in (A \times B)^*$. ■

Lemme 1.2.13 *Soient A un anneau commutatif et I un idéal de A Alors, I = A si et seulement si il existe un élément inversible dans I.*

Démonstration. Supposons qu'il existe $x \in I \cap A^*$. Dans ce cas, xx^{-1} est dans I, par suite, pour tout $y \in A$, l'élément $y1 = y$ est aussi dans I, d'où $I = A$. ■

Définition 1.2.14 *Un anneau A est un corps si l'on a* $1 \neq 0$*, et si tout élément non nul de A est inversible i.e. si l'on a* $A^* = A - \{0\}$.

Par définition, un corps possède donc au moins deux éléments, à savoir 0 et 1. Si A est un anneau commutatif et est un corps, on dit que A est un corps commutatif. Les anneaux $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ sont des corps commutatifs.

Définition 1.2.15 *Soit K un corps. On appelle sous-corps de K tout sous-anneau L de K qui est un corps. On dit alors que K est un surcorps de L.*

Les seuls idéaux d'un corps commutatif K sont $\{0\}$ et K. Le produit de deux éléments non nuls dans un corps est non nul. Les corps commutatifs sont en particulier des anneaux intègres :

Définition 1.2.16 *Un anneau A est dit intègre s'il est commutatif, non réduit à* 0 *i.e. on a* $1 \neq 0$*, et si le produit de deux éléments non nuls de A est non nul.*

Les anneaux $\mathbb{Z}$ et $\mathbb{Z}[i]$ sont intègres, et plus généralement, tout sous-anneau d'un corps commutatif est un anneau intègre.

Proposition 1.2.17 *Soit A un anneau intègre fini. Alors A est un corps.*

Démonstration. Soit a un élément non nul de A. Il s'agit de montrer que a est inversible. On considère pour cela l'application de A à valeurs dans A qui à x associe ax. Elle est injective, car pour tout $x, y \in A$, si l'on a $ax = ay$, alors, $a(x - y) = 0$ et puisque A est intègre, cela entraîne $x = y$. L'anneau A étant fini, cette application est donc aussi une surjection, en particulier, 1 possède un antécédent, autrement dit, il existe $b \in A$ tel que $ab = 1$ (et $ba = 1$ car A est commutatif), d'où le résultat. ■

Exemples 1.2.18

1. *Soit n un entier ≥ 1. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.*
2. *Si A et B sont des anneaux non nuls, l'anneau produit $A \times B$ n'est jamais intègre, comme le montre l'égalité $(1, 0)(0, 1) = (0, 0)$.*

Définition 1.2.19 *Un anneau est dit principal s'il est intègre et si tous ses idéaux sont principaux.*

Définition 1.2.20 *Un anneau A est dit euclidien si les conditions suivantes sont satisfaites :*

1. *Il est intègre.*
2. *Il existe une application $\sigma : A - \{0\} \to \mathbb{N}$ telle que pour tous a et b dans A avec $b \neq 0$, il existe q et r dans A tels que l'on ait*

$$a = bq + r \ \ avec \ \ r = 0 \ \ ou \ \ \sigma(r) < \sigma(b).$$

On dit que σ est un stathme euclidien.

Exemples 1.2.21 *Les anneaux $\mathbb{Z}$ et $K[X]$, où K est un corps commutatif, sont des anneaux euclidiens. Il en est de même de $\mathbb{Z}[i]$.*

Lemme 1.2.22 *Tout anneau euclidien est principal.*

Démonstration. Soient A un anneau euclidien et I un idéal non nul de A. Il existe a non nul dans I tel que $\sigma(a)$ soit minimum. Vérifions que $I = (a)$. Soit x un élément de I. Il existe q et r dans A tels que $x = aq + r$ avec $r = 0$ ou $\sigma(r) < \sigma(a)$. Puisque r est dans I, le caractère minimal de a entraîne $r = 0$, donc x est dans (a), d'où le résultat (l'inclusion inverse est immédiate). ■

1.2.4 Morphismes d'anneaux

Définition 1.2.23 *Soient A et B des anneaux. On appelle morphisme d'anneaux de A dans B, toute application f de A dans B vérifiant les conditions suivantes :*

1. *On a les égalités*

$$f(x + y) = f(x) + f(y) \text{ et } f(xy) = f(x)f(y) \text{ quels que soient } x, y \in A.$$

2. *On a $f(1_A) = 1_B$.*

Par exemple, si A est un anneau commutatif et I un idéal de A, la surjection canonique $A \to A/I$, qui à x associe $x + I$, est un morphisme d'anneaux.

Lemme 1.2.24 *Soient $f : A \to B$ un morphisme d'anneaux et A', B' des sous-anneaux de A et B respectivement.*

1. *L'image $f(A')$ est un sous-anneau de B.*
2. *L'image réciproque $f^{-1}(B')$ est un sous-anneau de A.*

Démonstration.

1. On sait déjà que $f(A')$ est un sous-groupe additif de B. Par ailleurs, on a $f(1_A) = 1_B$ et $1_A \in A'$ d'où $1_B \in f(A')$. Si x et y sont dans $f(A')$, il existe u et v dans A' tels que $x = f(u)$ et $y = f(v)$, donc $xy = f(u)f(v) = f(uv)$ appartient à $f(A')$.
2. On a vu que $f^{-1}(B')$ est un sous-groupe de A. L'égalité $f(1_A) = 1_B \in B'$, entraîne que $1_A \in f^{-1}(B')$. Si x et y sont dans $f^{-1}(B')$, alors $f(x)$ et $f(y)$ sont dans B', et $f(xy) = f(x)f(y) \in B'$ d'où $xy \in f^{-1}(B')$.

■

De façon analogue aux morphismes de groupes, on démontre que l'application composée de deux morphismes d'anneaux est un morphisme d'anneaux, et que si un morphisme d'anneaux est une bijection, son application réciproque est aussi un morphisme d'anneaux.

Définition 1.2.25 *Soient A et B des anneaux. On appelle isomorphisme de A sur B tout morphisme d'anneaux bijectif de A sur B. S'il existe un isomorphisme entre A et B, on dit que A et B sont isomorphes.*

Lemme 1.2.26 *Soient A et B des anneaux commutatifs, $f : A \to B$ un morphisme d'anneaux et I un idéal de B. Alors, $f^{-1}(I)$ est un idéal de A.*

Démonstration. Considérons des éléments $x \in A$ et $y \in f^{-1}(I)$. L'élément $f(x)f(y)$ est dans I i.e. $f(xy) \in I$, donc $xy \in f^{-1}(I)$. L'assertion en résulte puisque $f^{-1}(I)$ est un sous-groupe additif de A. ■

Remarque 1.2.27 *L'image d'un idéal par un morphisme n'est pas en général un idéal, comme le montre l'injection $\mathbb{Z} \to \mathbb{Q}$. Cela étant, A et B étant des anneaux commutatifs, si $f : A \to B$ est un morphisme surjectif de A sur B, et I un idéal de A, alors $f(I)$ est un idéal de B.*

Définition 1.2.28 *Soit $f : A \to B$ un morphisme d'anneaux. On appelle noyau de f, et on note $Ker(f)$, l'ensemble des éléments $x \in A$ tels que $f(x) = 0$. Le sous-anneau $f(A)$ de B s'appelle l'image de f.*

Théorème 1.2.29 (Factorisation des morphismes d'anneaux) *Soient A un anneau commutatif, B un anneau et $f : A \to B$ un morphisme d'anneaux. Alors, $Ker(f)$ est un idéal de A, et l'anneau quotient $A/Ker(f)$ est isomorphe à $f(A)$, via l'application qui à $x + Ker(f)$ associe $f(x)$.*

Démonstration. Le fait que $Ker(f)$ soit un idéal de A résulte directement des définitions. Notons $h : A/Ker(f) \to f(A)$ l'application définie par

$$h(x + Ker(f)) = f(x).$$

Compte tenu du Théorème 1.1.29, on sait que h est bien définie et que c'est un isomorphisme de groupes. Par ailleurs, si $x + \ker(f)$ et $y + \ker(f)$ sont dans $A/\ker(f)$, on a

$$h((x + Ker(f))(y + Ker(f))) = h((x + Ker(f))) = f(xy) = f(x)f(y),$$

qui n'est autre que $h((x + Ker(f))(y + Ker(f)))$. Puisque l'on a

$$h(1_A + Ker(f)) = f(1_A) = 1_B,$$

h est donc un morphisme d'anneaux, d'où le résultat. ■

En illustration de ce qui précède, établissons l'énoncé suivant qui caractérise, à isomorphisme près, les anneaux quotients de

Proposition 1.2.30 *Soit A un anneau. Les conditions suivantes sont équivalentes :*

1. *L'anneau A ne possède pas de sous-anneaux autres que lui-même.*
2. *Il existe $n \in \mathbb{N}$ tel que A soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Pour tout $n \in \mathbb{N}$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ n'a pas de sous-anneaux autres que lui-même. En effet, si B est un sous-anneau de $\mathbb{Z}/n\mathbb{Z}$, alors $\overline{1}$ est dans B, donc le sous-groupe engendré par $\overline{1}$, i.e. $\mathbb{Z}/n\mathbb{Z}$, est contenu dans B, d'où $B = \mathbb{Z}/n\mathbb{Z}$. En particulier, tout anneau isomorphe à $\mathbb{Z}/n\mathbb{Z}$, pour un certain entier n, possède cette propriété. Inversement, supposons la première condition réalisée. Considérons l'application $f : \mathbb{Z} \to A$ définie par $f(n) = n1_A$. C'est un morphisme d'anneaux. Son image est un sous-anneau de A. D'après l'hypothèse faite, on a donc $f(Z) = A$. Par ailleurs, il existe $n \in \mathbb{N}$ tel que l'on ait $\ker(f) = n\mathbb{Z}$. Par suite, A est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ (Th. 1.2.29). ■

CHAPITRE 2

ARITHMÉTIQUE SUR $\mathbb{Z}$ ET CONGRUENCES

2.1 Un peut d'historique

Phythagore (572 à 501) avant notre ère : Attribution une valeur mystique à certaines nombres et les classent selon leurs propriétés arithmétiques ou géométriques.

Définition 2.1.1 (Nombre parfait) *Tout nombre égale à la somme des ses diviseurs propres.*

Exemple 2.1.2 $6 = 1 + 2 + 3$; $28 = 1 + 2 + 4 + 7 + 14$.

Définition 2.1.3 (Nombres amincaux) *Si chacun est la somme des diviseurs propres de l'autres.*

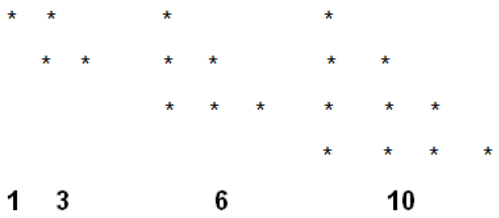
Exemple 2.1.4 220 *et* 284 *sont des nombres amicaux car :*

- *Les diviseurs propre de* 220 *sont :*1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110.

- *Les diviseurs propre de* 284 *sont :*1, 2, 4, 71, 142.

- *Avec* $220 = 1+2+4+71+142$, *et* $284 = 1+2+4+5+10+11+20+22+44+55+110$.

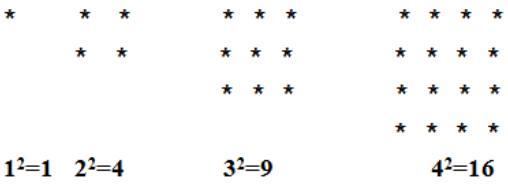
Définition 2.1.5 (Nombres triangulaires)



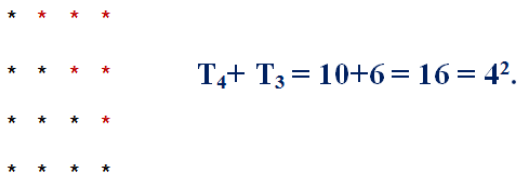
L'utilisation de ces représentations pour obtenir diverses relations. Par exemple, la figure suivante illustre le fait que le n-ième nombre triangulaire $T_n = 1+2+\cdots+n$ *vaut* $T_n = \frac{n(n+1)}{2}$.

$$T_4 = \frac{4\times 5}{2} = 10.$$

Définition 2.1.6 (Nombres carrés)



La somme de deux nombres triangulaires successifs est un carré



La somme des n premiers nombres impairs est un carré $1 + 3 + 5 + 7 + 9 = 25 = 5^2$.

2.2 L'arithmétique sur $\mathbb{N}$ et nombres premiers

Soit $\mathbb{N}$ l'ensemble des entiers positifs ou nuls. Si $n \in \mathbb{N}$ nous dénoterons par $n\mathbb{N}$ l'ensemble des multiples entiers de n : $n\mathbb{N} = \{na/a \in \mathbb{N}\}$.

Définition 2.2.1 *Nous dirons qu'un entier $n \in \mathbb{N}$ divise un entier $m \in \mathbb{N}$, et nous écrivons $n \mid m$, si $m \in n\mathbb{N}$.*

Remarque 2.2.2 *Si $0 \mid n$ alors $n = 0$.*

Démonstration. $0 \mid n \Rightarrow n \in 0\mathbb{N} \Rightarrow n = 0a$ avec $a \in \mathbb{N} \Rightarrow n = 0$. ■

Proposition 2.2.3 **(i)** *On a : $n \mid nm$, $n \mid 0$, $1 \mid n$ et $n \mid n$.*

(ii) *Si $m \mid n$ et $n \mid r$ alors $m \mid r$.*

(iii) *Si $n \mid a$ et $n \mid b$ alors $a \mid (a + b)$.*

(iv) *Si $a \mid a$ et $n \mid a + r$ alors $n \mid r$.*

Démonstration.

(i) 1. $n \mid nm \Rightarrow nn \in n\mathbb{N} \Rightarrow nm = na$ avec $a = m$.

2. $n \mid 0 \Rightarrow 0 \in n\mathbb{N} \Rightarrow 0 = na$ avec $a = 0$.

3. $1 \mid n \Rightarrow n \in 1\mathbb{N} \Rightarrow n = 1a$ avec $a = n$.

4. $n \mid n \Rightarrow n \in n\mathbb{N} \Rightarrow n = na$ avec $a = 1$.

(ii) $m \mid n$ implique $n = ma_1$ et $n \mid r$ implique $r = na_2 \Rightarrow r = ma_1a_2 \Rightarrow m \mid r$.

(iii) $n \mid a$ implique $a = na_1$ et $n \mid b$ implique $b = na_2 \Rightarrow a + b = n(a_1 + a_2) \Rightarrow n \mid (a + b)$.

(iv) $n \mid a$ implique $a = na_1$ et $n \mid a + r$ implique $a + r = na_2 \Rightarrow r = n(a_1 - a_2) \Rightarrow n \mid r$.

■

Définition 2.2.4 *Nous dirons qu'un entier $n > 1$ est composé s'il admet une factorisation $n = ab$ avec $a, b > 1$, sinon, nous dirons qu'il est premier.*

Proposition 2.2.5 *Tout entier composé n possède un diviseur $1 \leq d \leq \sqrt{n}$.*

Démonstration. Supposons n composé, alors $n = ab$ avec $a, b > 1$ et $a, b > n$. Supposons que tous les diviseurs sont superieurs à $\sqrt{n}$. a et b sont des diviseurs alors : $a > \sqrt{n}, b > \sqrt{n} \Rightarrow ab > n$ (Contradiction). ■

Remarque 2.2.6 *Si un entier $n > 1$ n'est pas divisible par aucun nombre premier $\leq \sqrt{n}$ alors il est premier.*

Exemple 2.2.7 101 *est premier car il n'est pas divisible ni par* 2, *ni par* 3, *ni par* 5 *et ni par* 7.

Théorème 2.2.8 (Théorème fondamental de l'arithmétique) *Tout nombre $n > 1$ se factorise en produit de nombres premiers. ≪Cette factorisation est unique à l'ordre des facteurs prés≫.*

Démonstration. Supposons que n n'est pas premier.
Divisons n par son plus petit diviseur d_1. d_1 est forcement premier.
Si le quotient $\frac{n}{d_1}$ n'est pas premier, divisons le par son plus petit diviseur d_2. d_2 est forcement premier.
Si le quotient $\frac{n}{d_1 d_2}$ n'est pas premier, divisons le par son plus petit diviseur d_3. d_3 est forcement premier...

Continuant ainsi, on obtient une suite décroissante d'entiers $n > \frac{n}{d_1} > \frac{n}{d_1 d_2} > \ldots$.
Cette suite ne peut se prolonger indéfiniment. Après un certain nombre k de diviseurs, le diviseurs $q = \frac{n}{d_1 d_2 \cdots d_k}$ sera premier, on obtient alors $n = d_1 d_2 \cdots d_k \times q$. ■

Lemme 2.2.9 (Lemme de Gauss) *Si un nombre premier divise le produit de deux nombres entiers alors il divise l'un des facteurs.*

Le lemme de Gauss peut se reformuler de la façons suivante.

Lemme 2.2.10 *Si un eniter q divise le produit nm de deux entiers sans diviser m et n, alors q n'est pas premier.*

Remarque 2.2.11 *Soit a, b deux entiers non nuls.*

- *$pgcd(a, b)$:= le plus grand diviseur commun de a et b.*
- *$pgcd(a, b)$:= le plus petit multiple commun de a et b.*
- *Si $pgcd(a, b) = 1$: a et b sont relativement premier c'est à dire sans diviseur commun, on note ça généralement $a \perp b$.*

Théorème 2.2.12 (Division euclidienne) *Soit $b \in \mathbb{N}^*$. Alors $\forall a \in \mathbb{N}, \exists q, r \in \mathbb{N} : a = bq + r$, $0 \leq r < b$. Les entiers q et r sont déterminés uniquement par a et b.*

Démonstration. Soit q le plus grand entier $\leq \frac{a}{b}$.
Par définition on a : $q \leq \frac{a}{b}$ et $\frac{a}{b} < q + 1$
$\Rightarrow qb \leq a$ et $a < (q+1)b = qb + b \Rightarrow a - qb \geq 0$ et $a - qb < b \Rightarrow 0 \leq a - qb < b$,
posons $r = a - qb$. Alors on a $0 \leq r < b$. Cela montre l'existance des couples (q, r).
L'unicité est évidente car la condition $0 \leq a - qb < b$ équivaut à la condition $qb \leq a < (q+1)b$, qui équivaut aux conditions $q \leq \frac{a}{b}$ et $\frac{a}{b} < q + 1$.
Supposons $\exists q_1, r_1 \in \mathbb{N} : a = bq_1 + r_1$ avec $0 \leq r_1 < b$, donc $0 \leq r_1 = a - bq_1 < b \Leftrightarrow bq_1 \leq a$ et $a < (q_1 + 1)b \Leftrightarrow q_1 \leq \frac{a}{b}$ et $\frac{a}{b} < q_1 + 1$ donc q_1 est le plus grand d'où $q_1 = q$. ■

Lemme 2.2.13 *Si $a = qb + r$, $0 \leq r < b$ alors $pgcd(a, b) = pgcd(b, r)$.*

Démonstration. Si un entier d divise a et b alors il divise $r = a - qb$. Inversement si d divise b et r alors il divise $a = qb + r$. Cela montre que tout diviseur commun de a et b est un diviseur commun de b et r. En particulier le plus grand diviseur commun de a et b est égal au plus grand diviseur commun de b et r. ■

Algorithme d'Euclid $a, b \geq 1$.

$a = bq_1 + r_1, 0 < r_1 < b,$

$b = r_1q_2 + r_2, 0 < r_2 < r_1,$

$r_1 = r_2q_3 + r_3, 0 < r_3 < r_2,$

$\vdots$

$r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1},$

$r_{n-1} = r_nq_{n+1} + 0,$

alors $pgcd(a, b) = pgcd(b, r_1) = pgcd(r_1, r_2) = \cdots = pgcd(r_{n-1}, r_n) = r_n$.

Exemple 2.2.14 $pgcd(3456, 465) = 3$, *car*

$3456 = \underline{465} \times 7 + \underline{201},$

$456 = \underline{201} \times 2 + \underline{63},$

$201 = \underline{63} \times 3 + \underline{12},$

$63 = \underline{12} \times 5 + \underline{3},$

$12 = \underline{3} \times 4 + 0.$

Théorème 2.2.15 (Bézut) *Pour tout entier $a, b \geq 1$, il existe $u, v \in \mathbb{Z}$ tel que : $pgcd(a, b) = u \times a + v \times b$.*

Démonstration. Supposons que $a \geq b$. Nous raisonnons par induction sur b.

Le résultat est évident pour $b = 1$, et plus particulièrement si $b \mid a$ alors $pgcd(a, b) = b = 0 \times a + 1 \times b$.

Sinon, on a $a = qb + r$ avec $0 < r < b$ alors $pgcd(a, b) = pgcd(b, r)$ (par Lemme 2.2.13), comme $r < b$ on peut supposer (l'hypothèse d'induction) que l'on a $pgcd(b, r) = x \times b +$

$y \times r$, pour $x, y \in \mathbb{Z}$. Alors

$$\begin{aligned} pgcd(a,b) &= x \times b + y \times (a - bq) = y \times a + (x - qy) \times b \\ &= u \times a + v \times b \ \text{(par le changement } u = y \text{ et } v = x - qy). \end{aligned}$$

■

Proposition 2.2.16 *$a \perp b \Leftrightarrow \exists u, v \in \mathbb{Z} : 1 = ua + vb$.*

Démonstration.

1. $\Rightarrow$? Soit $a \perp b$, alors $pgcd(a,b) = 1$. D'après le théorème de Bezout $\exists u, v \in \mathbb{Z} : 1 = u \times a + v \times b$.
2. $\Leftarrow$? Soit d un diviseur commun de a et b alors d est diviseur de $u \times a + v \times b = 1$, ainsi $d = 1$.

■

Proposition 2.2.17 *$a \perp b$ et $a \perp c$ alors $a \perp ab$.*

Retour au Lemme de Gauss (Démonstration)

Il suffit de montrer que si un nombre P ne divise pas a et b alors il ne divise pas leur produit ab.
En effet si P ne divise pas a alors $P \perp a$ de même pour b (c'est à dire $P \perp b$) alors $P \perp ab$ (par Proposition 2.2.17).

2.2.1 Retour au théorème fondamental de l'arithmétique

L'existance de la factorisation a déjà été démontré.
L'unicité : Nous allons raisonner par induction sur n. Le résultat est clair si n est premier. On peut donc supposer que n est composé : $n = p_1 \times p_2 \times \cdots \times p_k = q_1 \times q_2 \times \cdots \times q_r$

avec $p_1 \leq p_2 \leq \cdots \leq p_k$ et $q_1 \leq q_2 \leq \cdots \leq q_r$.

Nous allons montrer que $k = r$ et que $p_i = q_i$, $1 \leq i \leq k$.

Le facteur p_k divise n alors il doit diviser l'un des facteurs q_i (par le lemme de Gauss).

Donc $p_k \leq q_r$.

Le même raisonnement pour $q_r \leq p_k$ alors $q_r = p_k$. Par suite $\frac{n}{p_k} = p_1 p_2 \cdots p_{k-1} = q_1 q_2 \cdots q_{r-1}$.

Comme $\frac{n}{p_k} > n$, l'hypothèse d'induction entraîne que $k - 2 = r - 1$ et que $p_i = q_i$ pour tout $1 \leq i \leq k - 1$.

Remarque 2.2.18 *Il est commode de regrouper les facteurs égaux d'une factorisation en facteurs premiers, cela donne une factorisation dont les facteurs sont des puissances de nombres premiers distinctes.*

1. $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

2. *Si* $m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ *alors*
   - $mn = p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_k^{a_k+b_k}$,
   - $pgcd(m,n) = p_1^{a_1 \wedge b_1} p_2^{a_2 \wedge b_2} \cdots p_k^{a_k \wedge b_k}$,
   - $ppcm(m,n) = p_1^{a_1 \vee b_1} p_2^{a_2 \vee b_2} \cdots p_k^{a_k \vee b_k}$,

   avec $a \wedge b = min(a,b)$ *et* $a \vee b = max(a,b)$.

Proposition 2.2.19 *Pour tout entier* $m, n \geq 1$, *on a*

$$pgcd(m,n) \times ppcm(m,n) = m \times n.$$

En particulier, si $m \perp n$ *alors* $ppcm(m,n) = m \times n$.

Théorème 2.2.20 (Euclide) *Il existe une infinité de nombres premiers.*

Démonstration. Supposons par absurde qu'il existe une liste finie de nombres premiers distincts $p_1 < \ldots < p_s$. Posons

$$\begin{aligned} N &= p_1 \times \cdots \times p_s + 1 \\ &= \prod_{i=1}^{s} p_i + 1, \text{ comme } N \text{ et } N+1 \text{ sont premiers entre eux.} \end{aligned}$$

Alors $p_i \nmid N$ pour tout $i = 1, \ldots, s$. Or , d'après le théorème fondamental d'arithmétique, il existe au moins un nombre premier p tel que $p|N$, et $p \neq p_i$ pour tout $i = 1, \ldots, s$. ■

2.3 Nombres Mersenne et de Fermat

Définition 2.3.1 (Nombres de Fermat : 1601-1665) $F_n = 2^{2^n} + 1$.

Exemples 2.3.2 $F_0 = 2^1 + 1 = 3$, $F_1 = 2^2 + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$, $F_4 = 2^{16} + 1 = 65537$.

Conjecture 2.3.3 (Fermat) *Les nombres de Fermat F_n sont premiers ?*

Fausse (Euler) Puisque F_5 est composé ($F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$). Il a démontré aussi que F_n est composé pour $1 \leq n \leq 50$.

Définition 2.3.4 (Nombres de Mersenne) $M_n = M_n(2) = 2^n - 1$.

Exemples 2.3.5 $M_2 = 2^2 - 1 = 3$, $M_3 = 2^3 - 1 = 7$, $M_4 = 2^4 - 1 = 15$, $M_5 = 2^5 - 1 = 31$, $M_6 = 2^6 - 1 = 127$.

Définition 2.3.6 (Nombres Répunit) *Ces nombres sont le cas particulier de $M_n(a) = 1 + a + \cdots + a^{n-1} = \frac{a^n-1}{a-1}$ où $a = 10$, c'est à dire :*

$$M_n(10) = 1 + 10 + \cdots + 10^{n-1} = \frac{10^n - 1}{9}.$$

$M_n(10)$ s'appelle répunit car son développement en décimal est formé du chiffre 1 *répété n fois.*

Exemples 2.3.7 $M_2(10) = 11$, $M_3(10) = 111$, $M_4(10) = 1111$, $M_5(10) = 11111$.

2.4 Retour à l'algorithme d'Euclid

$a = bq_1 + r_1, 0 < r_1 < b,$

$b = r_1q_2 + r_2, 0 < r_2 < r_1,$

$r_1 = r_2q_3 + r_3, 0 < r_3 < r_2,$

$\vdots$

$r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1},$

$r_{n-1} = r_nq_{n+1} + 0.$

Posons $p_i = q_{n+1-i}$ la suite $p_1, p_2, \ldots, p_n$ est obtenue en renversant la suite $(B_0, B_1, \ldots, B_n)$ par :

$$B_0 = B_1 = 1 \text{ et } B_k = p_kB_{k-1} + B_{k-2} \quad \text{pour} \quad 2 \leq k \leq n.$$

Proposition 2.4.1 *On a $pgcd(a, b) = (-1)^n(B_nb - B_{n-1}a)$.*

Démonstration. On a : $a = bq_1 + r_1$ sa forme matricielle :

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r_1 \end{pmatrix}.$$

De façons analogue pour le reste alors

$$\begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$$

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} q_3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_2 \\ r_3 \end{pmatrix}$$

$\vdots$

$$\begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}.$$

Par suite

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} \tag{2.1}$$

Posons $J = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ remarquons

$$J\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} = -\begin{pmatrix} -q & 1 \\ 1 & 0 \end{pmatrix}J = -\begin{pmatrix} 0 & 1 \\ 1 & q \end{pmatrix}^{-1} J.$$

Par suite en multipliant la relation (2.1) par J on obtient

$$J\begin{pmatrix} a \\ b \end{pmatrix} = J\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$$

$$\begin{pmatrix} -a \\ b \end{pmatrix} = -\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}^{-1} J\begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$$

$$\begin{pmatrix} -a \\ b \end{pmatrix} = (-)^2\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}^{-1}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}^{-1} J\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$$

$$\vdots$$

$$\begin{pmatrix} -a \\ b \end{pmatrix} = (-)^n\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}^{-1}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}^{-1}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix}^{-1} J\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix},$$

donc

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} -a \\ b \end{pmatrix} = (-)^n\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}^{-1}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix}^{-1} J\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}$$

$$\vdots$$

$$\begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} -a \\ b \end{pmatrix} = (-)^n\begin{pmatrix} -r_{n-1} \\ r_n \end{pmatrix}.$$

Comme $p_i = q_{n+1-i}$, on aura

$$(-)^n\begin{pmatrix} -r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & p_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & p_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & p_n \end{pmatrix}\begin{pmatrix} -a \\ b \end{pmatrix}.$$

On remarque que $(1, p_1) = (B_0, B_1)$, on a aussi

$$(B_{k-1}, B_k)\begin{pmatrix} 0 & 1 \\ 1 & p_{k+1} \end{pmatrix} = (B_k, B_{k-1} + p_{k+1}B_k) = (B_k, B_{k+1}) \quad \text{pour } 1 \le k \le n.$$

On a

$$(0,1)\begin{pmatrix} 0 & 1 \\ 1 & p_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & p_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & p_n \end{pmatrix} = (B_{n-1}, B_n). \tag{2.2}$$

Alors

$$(-)^n(0,1)\begin{pmatrix} -r_{n-1} \\ r_n \end{pmatrix} = (0,1)\begin{pmatrix} 0 & 1 \\ 1 & p_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & p_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & p_n \end{pmatrix}\begin{pmatrix} -a \\ b \end{pmatrix}.$$

De la relation (2.2) on obtient

$$\begin{aligned} (-)^n r_n &= (B_{n-1}, B_n)\begin{pmatrix} -a \\ b \end{pmatrix} \\ &= -B_{n-1}a + B_n b, \end{aligned}$$

donc $r_n = (-1)^n \{B_n b - B_{n-1}a\}$, et comme le $pgcd(a,b) = r_n$ on obtient que $pgcd(a,b) = (-1)^n \{B_n b - B_{n-1}a\}$. ■

2.5 Congruences

Pour tout entier $n \in \mathbb{Z}$. Posons $n\mathbb{Z} = \{na / a \in \mathbb{Z}\}$.

Définition 2.5.1 *Soit $n \geq 0$ (enteir positif). On dit que deux entiers $a, b \in \mathbb{Z}$ sont congrus modulo n si leur différence $a - b$ est divisible par n autrement dit $a - b \in n\mathbb{Z}$. Nous écrivons $a \equiv b[n]$, $a \equiv b$* modulo *n, $a \equiv b$* mod *n pour indiquer que a est congru à b modulo n.*

Proposition 2.5.2 (Division euclidienne dans $\mathbb{Z}$) *Soit n un enteir positif. Alors pour tout entier $a \in \mathbb{Z}$, il existe des entiers $q, r \in \mathbb{Z}$ avec $0 \leq r < n$ tel que $a = nq + r$, les entiers q et r sont déterminés uniquement par a et n.*

Proposition 2.5.3 *Soit n un entier positif, tout entier $a \in \mathbb{Z}$ est congru modulo n à un et un seul entier $r \in \{0, 1, \ldots, n-1\}$.*

Démonstration. Posons $a = qn + r$, $0 \leq r < n$, alors

$a \equiv r[n]$, $r \in \{0, 1, \ldots, n-1\}$.
L'unicité de r provient de l'unicité du reste de la division euclidienne. ■

Remarque 2.5.4 *$a \equiv r[n]$ et $b \equiv r[n] \Leftrightarrow a \equiv b[n]$.*

Proposition 2.5.5 *Si $b \perp n$, $\exists$ un enteir $k > 0$; $b^k \equiv 1[n]$.*

Démonstration. Soit r_k le reste de la division euclidienne de b^k par n. $r_1, \ldots, r_n$ ne peuvent être tous différents car $0 \leq r_i < n$.
On a donc $r_{i+k} = r_i$ pour deux exposants $0 \leq i < i + k \leq n$. Dans ce cas : $b^{i+k} \equiv b^i[n]$.
Alors n divise $b^{i+k} - b^i = b^i(b^k - 1) \Rightarrow n$ divise $b^k - 1 \Rightarrow b^k - 1 = qn \Rightarrow b^k \equiv 1[n]$. ■

Définition 2.5.6 *Soit $a \in \mathbb{Z}$ un entier relativement premier à $n > 0$. On dit que le plus petit entier $e > 0$, tel que : $a^e \equiv 1[n]$ est l'ordre de a modulo n, nous notrons $ord(a, n)$.*

Proposition 2.5.7 *Si $e = ord(a, n)$ alors $\forall K > 0 : a^K \equiv 1[n] \Leftrightarrow e \mid n$.*

Démonstration.

1. $\Leftarrow$**?)** Supposons $e \mid n$ c'est à dire $K = qe$ alors
   $a^k = a^{Ke} = (a^e)^q \equiv 1^q[n] \equiv 1[n]$.
2. $\Rightarrow$**?)** Supposons $q^k \equiv 1[n]$, et $K = qe + r$ pour $0 \leq K < e$ alors
   $1 \equiv a^K[n] \Rightarrow 1 \equiv a^{qe+r}[n] \Rightarrow 1 \equiv (a^e)^q a^r[n] \Rightarrow 1 \equiv a^r[n]$ pour $0 \leq K < e$.
   On ne peut avoir $r > 0$, car cela contredit la minimalité de e donc $r = 0$ et ça donne $r = 0$, alors $K = qe$ ainsi $e \mid K$.

■

Proposition 2.5.8 *Soit n un eniter positif. Si $x \equiv$ dénote la relation de congruence modulo n alors on a :*

1. ***Réflexivité :*** *$x \equiv x$.*
2. ***Transitivité :*** *Si $x \equiv y$ et $y \equiv z$ alors $x \equiv z$.*

3. ***Symétrie :*** $x \equiv y$ *alors* $y \equiv x$.
4. *Si* $x \equiv y$ *et* $u \equiv v$ *alors* $x + u \equiv y + v$ *et* $xu \equiv yv$.

D'après la proposition précédente la relation "$\equiv \mod n$" est une relation d'équivalence sur $\mathbb{Z}$.
On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence, aussi appelées **classes de congruences modulo** n.

Définition 2.5.9 *On définit alors les deux operations suivantes :*

$$\overline{a} + \overline{b} := \overline{a+b} \quad \forall a, b \in \mathbb{Z}/n\mathbb{Z}.$$

$$\overline{a} \times \overline{b} := \overline{a \times b} \quad \forall a, b \in \mathbb{Z}/n\mathbb{Z}.$$

Il facile de vérifier que, muni de ces deux lois, $\mathbb{Z}/n\mathbb{Z}$ est élevé au rang d'anneau commutatif.

Théorème 2.5.10 *Soit* $n \in \mathbb{Z}, n > 1$, *et* $a \in \mathbb{Z}$. *Alors*

(1) *si* $n|a$, *alors* $\overline{a} = \overline{0}$ *dans* $\mathbb{Z}/n\mathbb{Z}$;

(2) $pgcd(n, a) = 1$ *si et seulement si* $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$;

(3) *Si* $1 < pgcd(n, a) < n$, *alors* $\overline{a}$ *est un diviseur de* $\overline{0}$.

Démonstration.

(1) $n|a \Rightarrow n|(a-0) \Rightarrow a \equiv 0 \mod n$.

(2) Si $pgcd(n, a) = 1$, alors par Bezout il existe $r, s \in \mathbb{Z}$ tels que $1 = nr + as$. Ainsi

$$\overline{1} = \overline{nr + as} = \overline{nr} + \overline{as} = \overline{0} + \overline{as} = \overline{as}.$$

D'où $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$.
La réciproque est banale puisque si $\overline{a}$ est une unité, alors il existe $s \in \mathbb{Z}$ tel que $\overline{1} = \overline{as}$ et donc il existe $r \in \mathbb{Z}$ tel que $1 = as + rn$, i.e $pgcd(n, a) = 1$.

(3) Remarquons d'abord que si $1 < pgcd(n,a) < n$, alors a est nécéssairement non nul. Soit donc $d = pgcd(a,n)$. Alors il existe $r, s \in \mathbb{Z}$ tels que $ar + ns = d$. En outre, il existe $e, f \in \mathbb{Z}/\{0\}$ tels que $n = ed$ et $a = fd$. Par conséquent,

$$\overline{ae} = \overline{fde} = \overline{f}\,\overline{n} = \overline{f}\,\overline{0} = \overline{0}.$$

Ainsi $\overline{a}$ est un diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$.

■

2.6 Théorème de Chinois

Pour tout entier $n \geq 1$, rappelons que $\mathbb{Z}/n\mathbb{Z}$ désigne l'anneau des entiers modulo n.

Théorème 2.6.1 (Théorème de Chinois) *Soient m et n des entiers naturels non nuls premiers entre eux. L'application*

$$f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

définie pour tout $a \in \mathbb{Z}$ par l'égalité

$$f(a) = (a + m\mathbb{Z}, a + n\mathbb{Z}).$$

est un morphisme d'anneaux surjectif, de noyau $mn\mathbb{Z}$. En particulier, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes, via l'application qui à tout élément $a + mn\mathbb{Z}$ de $\mathbb{Z}/mn\mathbb{Z}$ associe le couple $(a + m\mathbb{Z}, a + n\mathbb{Z})$.

Remarque 2.6.2 *Le contenu essentiel de cet énoncé réside dans le fait que f soit une application surjective de $\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Autrement dit, étant donnés des entiers relatifs a et b, il existe $c \in \mathbb{Z}$ tel que l'on ait*

$$c \equiv a \mod m \ \ et \ \ c \equiv b \mod n. \tag{2.3}$$

Démonstration. Il résulte directement de la définition de la structure d'anneau produit sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (Exemples 1.2.3) que f est un morphisme d'anneaux. Vérifions que l'on a

$$Ker(f) = mn\mathbb{Z}.$$

Si a est un élément de $Ker(f)$, on a $(a + m\mathbb{Z}, a + n\mathbb{Z}) = (m\mathbb{Z}, n\mathbb{Z})$ autrement dit, on a $a \equiv 0 \mod m$ et $a \equiv 0 \mod n$. Puisque m et n sont premiers entre eux, on en déduit que mn divise a, i.e. que $a \in mn\mathbb{Z}$. Inversement, si a est dans $mn\mathbb{Z}$, alors a est divisible par m et n, donc a est dans $Ker(f)$, d'où l'assertion.
Prouvons que f est surjectif. Considérons pour cela un élément $(a + m\mathbb{Z}, a + n\mathbb{Z})$ de $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Puisque m et n sont premiers entre eux, il existe des entiers u et v tels que l'on ait

$$mu + nv = 1. \tag{2.4}$$

Posons alors

$$c = b(mu) + a(nv). \tag{2.5}$$

On vérifie que l'on a les congruences $c \equiv a \mod m$ et $c \equiv b \mod n$, autrement dit que $f(c) = (a + m\mathbb{Z}, a + n\mathbb{Z})$, d'où l'assertion, et le résultat (Théorème 1.2.29). ■

Remarque 2.6.3 *La démonstration précédente est effective, au sens où si a et b sont deux entiers relatifs donnés, elle permet d'expliciter un entier c vérifiant les congruences (2.3). En effet, il suffit pour cela de déterminer des entiers u et v vérifiant l'égalité (2.4), ce que l'on peut faire en utilisant par exemple l'algorithme d'Euclide. On peut alors prendre comme entier c celui défini par l'égalité (2.5). Il est unique modulo $mn\mathbb{Z}$.*

Exemple 2.6.4 *Soit n un entier naturel impair. Notons r le nombre de ses diviseurs premiers. Soit S l'ensemble des solutions dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ de l'équation*

$$x^2 = 1.$$

En notant |S| le cardinal de S, vérifions que l'on a

$$|S| = 2^r. \tag{2.6}$$

Soit $n = p_1^{n1} \cdots p_r^{nr}$ *la décomposition de n en produit de nombres premiers. Soit*

$$f : \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/p_i^{n_i}\mathbb{Z},$$

le morphisme d'anneaux défini par $f(x + n\mathbb{Z}) = (x + p_1^{n_1}\mathbb{Z}, \ldots, x + p_r^{n_r}\mathbb{Z})$*. D'après le théorème chinois, c'est un isomorphisme. Posons*

$$T = \left\{(\varepsilon_1 + p_1^{n_1}\mathbb{Z}, \ldots, \varepsilon_r + p_r^{n_r}\mathbb{Z})/\varepsilon_i = \pm 1 \text{ pour } i = 1, \ldots, r\right\}.$$

Vérifions que l'on a

$$S = f^{-1}(T). \tag{2.7}$$

Soit $x + n\mathbb{Z}$ *un élément de S. Pour tout* $i = 1, \ldots, r$*, on a* $x^2 \equiv 1 \mod p_i^{n_i}$*. Le pgcd de* $x - 1$ *et* $x + 1$ *est* 1 *ou* 2*. Puisque n est impair,* $p_i^{n_i}$ *divise donc* $x - 1$ *ou bien* $x + 1$*. Par suite,* $f(x + n\mathbb{Z})$ *est dans T , et S est contenu dans* $f^{-1}(T)$*. Inversement, si* $x + n\mathbb{Z}$ *est dans* $f^{-1}(T)$*, on a* $x^2 \equiv 1 \mod p_i^{n_i}$ *pour tout i. Cela implique* $x^2 \equiv 1 \mod n$*, autrement dit,* $x + n\mathbb{Z}$ *est dans S, d'où (2.7). Puisque T est de cardinal* 2^r *(les* p_i *sont impairs), il en est de même de S. Cela établit l'égalité (2.6).*

Afin d'expliciter S, on est donc amené à résoudre les systèmes de r congruences

$$x \equiv \varepsilon_1 \mod p_1^{n_1}, \ldots, x \equiv \varepsilon_r \mod p_1^{n_r}.$$

pour les 2^r *systèmes de signes* $(e_1, \ldots, e_r)$*. Il suffit en fait d'en résoudre* 2^{r-1} *par un choix convenable de systèmes de signes, en prenant ensuite les solutions opposées à celles déjà obtenues. Par exemple, si* $n = 735$*, l'ensemble S est formé des classes modulo n des entiers* ± 1*,* ± 146*,* ± 244 *et* ± 344*.*

Il convient de remarquer que la résolution de l'équation $x^2 = 1$ *dans* $\mathbb{Z}/n\mathbb{Z}$ *nécessite, a priori, la connaissance de la factorisation de n en produit de nombres premiers. Si l'on savait résoudre*

cette équation sans utiliser cette factorisation, il serait alors facile de trouver la factorisation de n. En effet, si a est un entier tel que $a^2 \equiv 1 \mod n$ *et* $a \not\equiv \pm 1 \mod n$*, le calcul du pgcd de* $a+1$ *(ou* $a-1$*) avec n fournit un diviseur non trivial de n. Le problème de la factorisation des entiers serait ainsi résolu.*

2.6.1 Reformulation du théorème de chinois (Enoncé traditionnel)

Soit $n_1, \ldots, n_r \in \mathbb{N}, n_i > 1 \ \forall i = \overline{1,r}$, avec $pgcd(n_i, n_j) = 1$ si $i \neq j$. Soit $a_1, \ldots, a_r \in \mathbb{Z}$. Alors, il existe un unique $a \in \mathbb{Z}$ tel que

$$a \equiv \begin{cases} a_1 \mod n_1, \\ \ldots \\ a_r \mod n_r. \end{cases}$$

Exemple 2.6.5 *Prenons* $n_1 = 7, n_2 = 11, n_3 = 13$ *ainsi que* $a_1 = a_2 = a_3 = -1$*. On cherche* $a \in \mathbb{Z}$ *tel que*

$$a \equiv \begin{cases} -1 \mod 7, \\ -1 \mod 11 \\ -1 \mod 13. \end{cases}$$

On trouve

$$1000 \equiv \begin{cases} -1 \mod 7, \\ -1 \mod 11 \\ -1 \mod 13. \end{cases}$$

Ainsi $a \equiv 1000 \mod 7 \times 11 \times 13 = 1001$.

2.7 La fonction indicatrice d'Euler

Il s'agit de la fonction $\varphi : \mathbb{N}^* \to \mathbb{N}$ définie comme suit.

Définition 2.7.1 (Fonction indicatrice d'Euler) *Pour tout* $n \geq 1$*, l'entier* $\varphi(n)$ *est le nombre*

des entiers compris entre 1 *et n, et premiers avec n. Autrement dit,* $\varphi(n)$ *est le nombre des entiers k pour lesquels on a*

$$1 \leq k \leq n \text{ et } pgcd(k, n) = 1.$$

Par exemple, on a $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, et pour tout nombre premier p, on a $\varphi(p) = p - 1$. Plus généralement :

Lemme 2.7.2 *Pour tout nombre premier p et tout entier* $r \geq 1$*, on a*

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

Démonstration. Il y a p^{r-1} entiers multiples de p entre 1 et p^r, d'où l'assertion. ■

Explicitons $\varphi(n)$ pour tout $n \geq 1$. On va voir en particulier que $\frac{\varphi(n)}{n}$ ne dépend que de l'ensemble des diviseurs premiers de n. Considérons pour cela le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ formé des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Rappelons d'abord l'énoncé suivant :

Lemme 2.7.3 *Soit n un entier* ≥ 1*. Soient a un entier et* $\overline{a}$ *sa classe modulo* $n\mathbb{Z}$*. Alors* $\overline{a}$ *est inversible dans l'anneau* $\mathbb{Z}/n\mathbb{Z}$ *si et seulement si a et n sont premiers entre eux. Autrement dit, on a*

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{a} / 1 \leq a \leq n \text{ et } pgcd(a, b) = 1\}.$$

Démonstration. Supposons $\overline{a}$ inversible. Il existe $b \in \mathbb{Z}$ tel que l'on ait $ab \equiv 1 \mod n$, autrement dit, il existe $c \in \mathbb{Z}$ tel que $ab + nc = 1$, ce qui prouve que a et n sont premiers entre eux. Inversement, il existe des entiers u et v tels que l'on ait $au + nv = 1$. Ainsi $\overline{a}$ est inversible, d'inverse la classe de u modulo n. ■

Corollaire 2.7.4 *L'ordre de* $(\mathbb{Z}/n\mathbb{Z})^*$ *est* $\varphi(n)$*.*

Corollaire 2.7.5 *L'anneau* $\mathbb{Z}/n\mathbb{Z}$ *est un corps si et seulement si n est premier.*

Démonstration. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si tous ses éléments non nuls sont inversibles. Par suite, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si $\varphi(n) = n - 1$, ce qui implique l'assertion. ■

Corollaire 2.7.6 *Soient m et n des entiers naturels non nuls premiers entre eux. On a*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Démonstration. Les entiers m et n étant premiers entre eux, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ sont isomorphes (Théorème 2.6.1). Les groupes des éléments inversibles de ces anneaux ont donc le même ordre. Le corollaire 2.7.4 et le lemme 1.2.12 entraînent alors le résultat. ■

Théorème 2.7.7 *Soit n un entier ≥ 1. On a l'égalité*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \tag{2.8}$$

où p parcourt l'ensemble des diviseurs premiers de n.

Démonstration. On peut suppoer $n \geq 2$. Soit $\{p_1, \ldots, p_r\}$ l'ensemble des diviseurs premiers de n. Soit

$$n = \prod_{i=1}^{r} p_i^{n_i},$$

la décomposition en facteurs premiers de n. D'après le corollaire 2.7.6, on a

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

Par ailleurs, on a (Lemme 2.7.2)

$$\varphi\left(p_i^{n_i}\right) = p_i^{n_i}\left(1 - \frac{1}{p_i}\right),$$

d'où l'égalité (2.8). ■

Indiquons quelques propriétés de la fonction φ.

Corollaire 2.7.8 *Pour tout $n \geq 3$, l'entier $\varphi(n)$ est pair.*

Démonstration. Compte tenu de l'égalité (2.8), si n possède un diviseur premier impair p, alors $p-1$ est pair, et il en est donc de même de $\varphi(n)$. Si n est une puissance de 2, disons $n = 2^r$ avec $r \geq 2$, alors $\varphi(n) = 2^r - 1$. ■

Corollaire 2.7.9 *Soient m et n des entiers naturels non nuls tels que m divise n. Alors $\varphi(m)$ divise $\varphi(n)$.*

Démonstration. Soit P_m (resp. P_n) l'ensemble des diviseurs premiers de m (resp. de n). On a les égalités (Théorème 2.7.7)

$$\frac{\varphi(n)}{\varphi(m)} = \frac{n}{m} \prod_{p \in P_n - P_m} \left(1 - \frac{1}{p}\right). \tag{2.9}$$

Pour tout nombre premier $p \in P_n - P_m$, p divise n sans diviser m, donc p divise n résulte que le second membre de l'égalité (2.9) est un entier. ■

L'implication réciproque de ce corollaire est fausse, comme le montre les égalités $\varphi(3) = \varphi(4) = 2$. Remarquons que l'énoncé précédent peut aussi se déduire du résultat suivant, qui est une conséquence du théorème chinois :

Lemme 2.7.10 *Soient m et n des entiers naturels non nuls tels que m divise n. L'application $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^*$ définie par $f(a + n\mathbb{Z}) = a + m\mathbb{Z}$, est un morphisme de groupes surjectif de $(\mathbb{Z}/n\mathbb{Z})^*$ sur $(\mathbb{Z}/m\mathbb{Z})^*$.*

Démonstration. On remarque d'abord que f est bien définie. Le fait que f soit un morphisme de groupes résulte directement de la définition. On écrit ensuite n sous la forme $n = m'r$, où m et m' ont les mêmes facteurs premiers et où r est premier à m'. L'entier m divise m' et r est premier à m. Soit $d + m\mathbb{Z}$ un élément de $(\mathbb{Z}/m\mathbb{Z})^*$. D'après le théorème chinois, il existe un entier a tel que

$$a \equiv d \mod m \quad \text{et} \quad a \equiv 1 \mod r.$$

Vérifions que a est premier à n. Supposons qu'il existe un nombre premier p qui divise a et n. Alors, p ne divise pas r, donc p divise m'. Par suite, p divise m et d, ce qui contredit

le fait que d et m sont premiers entre eux. On a ainsi $f(a+n\mathbb{Z}) = d+m\mathbb{Z}$, d'où l'assertion. ■

Lemme 2.7.11 *Pour tout $n \geq 1$, on a l'égalité*

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

où d parcourt l'ensemble des diviseurs de n.

Démonstration. Considérons l'ensemble $F = \left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n} = 1\right\}$. Pour tout diviseur d de n, posons $F_d = \left\{\frac{a}{d} / 1 \leq a \leq d \text{ et } pgcd(a,d) = 1\right\}$. L'ensemble F est la réunion disjointe des F_d, d'où le résultat vu que le cardinal de F est n et que celui de F_d est $\varphi(d)$. ■

2.8 Le théorème d'Euler

Euler a démontré cet énoncé en 1760 :

Théorème 2.8.1 *Soit n un entier naturel non nul. Pour tout entier a premier avec n, on a*

$$a^{\varphi(n)} \equiv 1 \mod n. \tag{2.10}$$

Pour le vérifier, on peut utiliser directement Théorème 1.1.19, ou bien le cas particulier ≪abélien≫ de ce théorème dont la démonstration se simplifie alors notablement.

Proposition 2.8.2 *Soit G un groupe abélien fini d'ordre n, d'élément neutre e. Pour tout $x \in G$, on a $x^n = e$.*

Démonstration. Soit x un élément de G. L'application qui à $g \in G$ associé gx est une bijection de G. On en déduit l'égalité

$$\prod_{g\in G} gx = \prod_{g\in G} g.$$

Il convient ici de noter que les produits ne dépendent pas de l'ordre choisi des éléments car G est abélien. On obtient

$$x^n \prod_{g \in G} g = \prod_{g \in G} g.$$

ce qui conduit à l'égalité $x^n = e$. ■

On obtient alors la congruence (2.10), en prenant $G = (\mathbb{Z}/n\mathbb{Z})^*$, qui est d'ordre $\varphi(n)$.

Corollaire 2.8.3 (Petit théorème de Fermat) *Soit p un nombre premier. Pour tout entier a non divisible par p, on a*

$$a^{p-1} \equiv 1 \mod p.$$

En particulier, pour tout entier a, on a $a^p \equiv a \mod p$.

Démonstration. Cela résulte de l'´égalité $\varphi(p) = p - 1$. ■

Exemples 2.8.4

1. *Vérifions que l'écriture décimale de 3^{1000}, qui possède quatre cent soixante dix huit chifres, se termine par 01. Il s'agit de déterminer l'entier a compris entre 0 et 99 tel que $3^{1000} \equiv a \mod 100$. On a $\varphi(100) = 40$. D'après le théorème d'Euler, on obtient $3^{40} \equiv 1 \mod 100$. Puisque $1000 = 40 \times 5$, on a donc $3^{1000} \equiv 1 \mod 100$, d'où $a = 1$.*

2. *Vérifions que l'´ériture décimale de 2^{1000}, qui possède trois cent deux chifres, se termine par 76. Le raisonnement précédent ne s'applique pas directement (car 2 n'est pas premier avec 100). On a $2^{1000} \equiv 0 \mod 4$. L'idée est alors de déterminer la congruence de 2^{1000} modulo 25 et d'utiliser le théorème chinois. On a $2^{20} \equiv 1 \mod 25$ (théorème d'Euler), d'où $2^{1000} \equiv 1 \mod 25$. Il en résulte que $2^{1000} \equiv -24 \mod 100$ (cf. le théorème chinois), d'où l'assertion.*

Les applications du théorème d'Euler sont innombrables, par exemple en cryptographie. Donnons ici une illustration de ce théorème, en prouvant un résultat concernant la non primalité des entiers de la forme $2^{2^n} + k$ où k est un entier.

Proposition 2.8.5 (Schinzel) *Soit k un entier relatif distinct de 1. Il existe une infinité d'entiers n tels que $2^{2^n} + k$ ne soit pas un nombre premier.*

Démonstration. On peut supposer k impair. Soit a un entier naturel. Il suffit de prouver l'existence d'un entier n tel que $2^{2^n} + k$ ne soit pas premier et que $2^{2^n} + k > a$. Puisque k est distinct de 1, il existe $s \in \mathbb{N}$ et un entier impair h tels que

$$k - 1 = 2^s h.$$

Soit t un entier naturel tel que l'on ait

$$p = 2^{2^t} + k > a \text{ et } t > s.$$

On peut supposer que p est un nombre premier. Il existe un entier impair h_1 tel que

$$p - 1 = 2^s h_1.$$

D'après le théorème d'Euler, on a

$$2^{\varphi(h_1)} \equiv 1 \mod h_1,$$

d'où l'on déduit la congruence

$$2^{s+\varphi(h_1)} \equiv 2^s \mod (p-1).$$

Puisque l'on a $t > s$, on obtient

$$2^{t+\varphi(h_1)} \equiv 2^t \mod (p-1).$$

L'entier p étant premier impair, on a $2^{p-1} \equiv 1 \mod p$. Il en résulte que

$$2^{t+\varphi(h_1)} + k \equiv 0 \mod p.$$

L'entier $2^{2^t+\varphi(h_1)} + k$, qui est strictement plus grand que p, n'est donc pas premier. Il est plus grand que a, d'où le résultat. ■

2.9 Exercices

Exercise 1 *Le produit de trois entiers consécutifs peut-il être un carré ?*

Exercise 2 *Montrer que* $pgcd(m+n, n) = pgcd(m, n)$.

Exercise 3 *Montrer que si n est composé alors* $M_n(a) = 1 + a + \cdots + a^{n-1}$ *est aussi composé* $(a \neq 1)$.

Exercise 4 (Euclid) *Montrer que si le nombre* $q = 2^p - 1$ *est premier, alors le nombre* $2^{p-1} \times q$ *est parfait* $p \geq 1$.

Exercise 5

1. *Montrer que pour faire la liste des diviseurs* $d \geq 1$ *d'un entier n il suffit de savoir faire la liste de ses diviseurs* $d \leq \sqrt{n}$.
2. *En déduire la liste des diviseurs de* 72 *et* 124, *puis déterminer le* $pgcd(72, 124)$.

Exercise 6 *Montrer que si* $m/pgcd(m, n)$ *et* $n/pgcd(m, n)$ *alors n et m sont premiers entre eux.*

Exercise 7 *Montrer l'existence d'une infinité de nombres premiers.*

Exercise 8 *Montrer que* M_n *(nombre de Mersenne) soit premier, il est nécéssaire (mais pas suffisant) que n soit premier.*

Exercise 9 (Nombres de Fermat) *Soit* $F_n = 2^{2^n} + 1$ *pour* $n \geq 0$.

1. *Calculer* F_0, F_1, F_2, F_3 *et* F_4.
2. *Vérifier que* $F_5 = 641 \times 6700417$.

3. *Que devener vous de la conjecture de Fermat.*

Exercise 10 (Goldbach) *Montrer que les nombres de Fermat sont relativement premier deux à deux.*

Exercise 11 *Soit a un entier naturel impair.*

1. *Démontrer que* $a^2 \equiv 1\,[8]$.
2. *Démontrer que* $a^4 \equiv 1\,[16]$.
3. *Démontrer que si* $a \equiv 1\,[2^n]$ *alors* $a^2 \equiv 1\left[2^{n+1}\right]$.

Exercise 12 *Démontrer que chacune des relations suivantes est vraie pour tout $n \in N$.*

1. 5 *divise* $2^{2n+1} + 3^{2n+1}$.
2. 6 *divise* $n^3 - n$.
3. 6 *divise* $5n^3 + n$.
4. 7 *divise* $2^{n+2} + 3^{2n+1}$.

Exercise 13 *Monter que si n est impair alors n divise* $2^{n!} - 1$.

Exercise 14 *Considérons la suite des nombres* $(F_n)_{n\geq 0}$ *tel que* $\{F_n\}_{n\geq 0} = \{0, 1, 1, 2, 3, 5, 8, 13, \ldots\}$

1. *Donner la formule de récurrence pour la suite* $(F_n)_{n\geq 0}$.
2. *Montrer que :*

   a) $F_n = \frac{1}{\sqrt{5}}\left(\varphi^n - \widetilde{\varphi}^n\right)$ *(formule de Binet) avec* $\varphi = \frac{1+\sqrt{5}}{2}$ *et* $\widetilde{\varphi} = \frac{-1}{\varphi}$.

   b) $F_n \sim \frac{\varphi^n}{\sqrt{5}}$ *au voisinage de l'infinie.*

   c) $\forall k \geq 1 :\ F_{2k} = 2F_{k-1}F_k + F_k^2$.

   d) $\forall k \geq 0 :\ F_{2k+1} = F_{k+1}^2 + F_k^2$.

Exercise 15 *Résoudre les équations*

$$19x \equiv 2 \mod 140 \text{ et } 57x \equiv 87 \mod 105.$$

Exercise 16 *Résoudre le systhème de congruences*

$$\begin{cases} 2x \equiv 3 \mod 15 \\ 4x \equiv 3 \mod 7 \\ 3x \equiv 5 \mod 8. \end{cases}$$

Exercise 17 *Soit $n \geq 2$ un entier et $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ sa décomposition on produit de facteurs premiers, où $p_1 < p_2 < \dots < p_k$.*

1. *Montrer que $k \leq \frac{\log n}{\log 2}$.*
2. *Pour $1 \leq i \leq k$, montrer que $p_i \geq i + 1$.*
3. *En déduire que*
$$\varphi(n) \geq \frac{\log 2}{2} \frac{n}{\log n}.$$

Exercise 18 *Un nombre entier m est appelé un **nombre de Carmichael** s'il vérifie les deux propriétés suivantes :*

(i) *m n'est pas premier ;*

(ii) *pour tout entier a premier avec m, on a*

$$a^{m-1} \equiv 1 \mod m.$$

Démontrer que $m = 561$ est un nombre de Carmichael (c'est en fait le plus petit nombre de Carmichael).

Indication : *On poura utiliser le théorème chinois.*

CHAPITRE 3

NOMBRES ET POLYNÔMES DE BERNOULLI

Les nombres de Bernoulli sont parmi les objets les plus fascinants des mathématiques. On les retrouve en arithmétique, en théorie des nombres, en analyse et même en topologie.

3.1 Un peu d'histoire

On raconte que **Gauss écolier** découvrit la formule

$$S(n) = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Un seul exemple suffit pour l'expliquer. Pour $n = 12$, on a

$$\begin{aligned} 2S(12) = S(12) + S(12) &= 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 + 12 \\ &+ 12 + 11 + 10 + 9 + 8 + 7 + 6 + 5 + 4 + 3 + 2 + 1 \\ &= 13 + 13 + 13 + 13 + 13 + +13 + 13 + 13 + 13 + 13 + 13 + 13 \\ &= 12 \times 13. \end{aligned}$$

La formule de Gauss était bien connue par les Pythagoriciens qui savaient calculer aussi la somme des nombres impairs successifs

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

Dans l'antiquité la somme des carrés successifs était aussi connue

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Au 11^{im} siècle, le mathématicien musulman, **Al-Karagi**, découvrit l'identité remarquable

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2 = \frac{n^2(n+1)^2}{4}.$$

Au 17^{im} siècle, **Pascal**, **Fermat** et **Wallis** ont obtenu la valeur de l'intégrale

$$\int_0^1 x^k dx = \frac{1}{k+1},$$

pour un exposant entier k, en calculant la somme

$$S_k(n) = 1^k + 2^k + \cdots + n^k.$$

Par exemple, pour montrer que l'on a

$$\int_0^1 x^4 dx = \frac{1}{5},$$

il suffit de savoir que

$$1^4 + 2^4 + \cdots + n^4 = \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}.$$

Formule facile à vérifier sa justesse par récurrence mais il est difficile de la trouver.

Johann Faulhaber (1580-1635) fut le premier à montrer que $S_k(n)$ est un polynôme de degré $k+1$ dans la variable n dans son livre *Academia Algebrae*, publié en 1631, il donne les coefficients de ce polynôme pour toutes les valeurs de $k \leq 23$. Ces formules furent popularisées plus tard par **Jacques Bernoulli** (1654-1705) qui en obtint le crédit.

Méthode de Pascal pour calculer le polyôme $S_k(n)$ à partir des polyômes $S_r(n)$ pour $r < n$. Observons que le terme de rang n d'une suite arbitraire $a_0, a_1, a_2, a_3, \ldots a_n$ est égal au premier a_0 augmenté des accroisements intermédiaires :

$$a_n = a_0 + (a_1 - a_0) + (a_2 - a_1) + \cdots + (a_n - a_{n-1}).$$

On dit que c'est une somme de télescopique. Par exemple, la différence entre deux carrés successifs est le nombre impair $2n - 1 = n^2 - (n-1)^2$. Par suite,

$$\begin{aligned}\sum_{k=1}^{n}(2k-1) &= \sum_{k=1}^{n}(k^2 - (k-1)^2) \\ &= 1^2 + (2^2 - 1^2) + (3^2 - 2^2) + \cdots + (n^2 - (n-1)^2) \\ &= n^2.\end{aligned}$$

Alors $n^2 = \sum_{k=1}^{n}(2k-1) = 1 + 3 + 5 + \cdots + (2n-1)$.

Pour la somme des carrés, calculons la différence entre deux cubes successifs :

$n^3 - (n-1)^3 = 3n^2 - 3n + 1$. Donc

$$\begin{aligned} n^3 &= \sum_{k=1}^{n} (3k^2 - 3k + 1) \\ &= 3\sum_{k=1}^{n} k^2 - 3\sum_{k=1}^{n} k + 3\sum_{k=1}^{n} 1 \\ &= 3(1^2 + 2^2 + \cdots + n^2) - 3\frac{n(n+1)}{2} + n. \end{aligned}$$

Alors

$$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 &= \frac{n^3}{3} + \frac{n(n+1)}{2} - \frac{n}{3} \\ &= \frac{2n^3 + 3n(n+1) - 2n}{6} \\ &= \frac{n(n+1)(2n+1)}{6}. \end{aligned}$$

Plus généralement Pascal observe que la différence $n^{p+1} - (n-1)^{p+1}$ est un polynôme de degré inférieur à p. En effet, par la *formule du binôme* on a

$$n^{p+1} - (n-1)^{p+1} = \binom{p+1}{1} n^p - \binom{p+1}{2} n^{p-1} + \binom{p+1}{3} n^{p-2} - \cdots$$

Par somme télescopique on obtient

$$n^{p+1} = \binom{p+1}{1} \sum_{i=1}^{n} i^p - \binom{p+1}{2} n^{p-1} \sum_{i=1}^{n} i^{p-1} + \binom{p+1}{3} n^{p-2} \sum_{i=1}^{n} i^{p-2} - \cdots$$

On en tire que

$$(p+1)S_p(n) = n^{p+1} + \binom{p+1}{2} S_{p-1}(n) - \binom{p+1}{3} S_{p-2}(n) + \cdots$$

Par exemple, si $p = 5$ la méthode de Pascal donne

$$6S_5(n) = n^6 + 15S_4(n) - 20S_3(n) + 15S_2(n) - 6S_1(n) + S_0(n).$$

Supposons que l'on connaisse déjà les formules

$$\begin{aligned}
1S_0(n) &= n \\
2S_1(n) &= n^2 + n \\
3S_2(n) &= n^3 + \frac{3}{2}n^2 + \frac{1}{2}n \\
4S_3(n) &= n^4 + 2n^3 + n^2 \\
5S_4(n) &= n^5 + \frac{5}{2}n^4 + \frac{5}{3}n^3 - \frac{1}{6}n.
\end{aligned}$$

La régularité des coefficients n'est pas évidente. Le premier à découvrir une loi générale est **Faulhaber**.

3.1.1 Formule de Faulhaber

Il existerait une suite de nombres "magiques"

$$f_0 = 1, f_1 = \frac{1}{2}, f_2 = \frac{1}{6}, f_3 = 0, f_4 = \frac{-1}{30}, f_5 = 0, f_6 = \frac{1}{42}, f_7 = 0, \cdots$$

pour lesquels on a

$$pS_{p-1}(n) = f_0\binom{p}{0}n^p + f_1\binom{p}{1}n^{p-1} + f_2\binom{p}{2}n^{p-2} + \cdots + f_{p-1}\binom{p}{p-1}n.$$

Nous dirons que c'est la formule de Faulhaber et que les nombres $f_0, f_1, f_2, \ldots$ sont les nombres de Faulhaber. Il se trouve que l'on peut calculer les nombres de Faulhaber sans connaitre les polynômes $S_p(n)$. Pour cela il suffit de poser $n = 1$ dans la formule de Faulhaber. En effet on a $S_{p-1}(1) = 1$ pour $p \geq 1$. On obtient par suite une relation

$$p = f_0\binom{p}{0} + f_1\binom{p}{1} + f_0\binom{p}{2} + \cdots + f_{p-1}\binom{p}{p-1}.$$

Nous dirons que c'est la relation fondamentale. C'est une série d'équations que l'on peut résoudre successivement :

$$\begin{aligned}
1 &= f_0 \text{ donc } f_0 = 1,\\
2 &= f_0 + 2f_1 \text{ donc } f_1 = \frac{1}{2},\\
3 &= f_0 + 3f_1 + 3f_2 \text{ donc } f_2 = \frac{1}{6},\\
4 &= f_0 + 4f_1 + 6f_2 + 6f_3 \text{ donc } f_3 = 0,\\
5 &= f_0 + 5f_1 + 10f_2 + 10f_3 + 5f_4 \text{ donc } f_4 = \frac{-1}{30},\\
6 &= f_0 + 6f_1 + 15f_2 + 20f_3 + 15f_4 + 6f_5 \text{ donc } f_5 = 0,\\
7 &= f_0 + 7f_1 + 21f_2 + 35f_3 + 35f_4 + 21f_5 + 7f_6 \text{ donc } f_6 = \frac{1}{42},\\
&etc \quad \cdots
\end{aligned}$$

On constate que $f_{2n+1} = 0$ sauf si $n = 0$. Pour démontrer cette observation et bien d'autres il est important de mieux comprendre la relation fondamentale. Dans cette relation, le membre de droite contient tout les termes de la forme $f_k\binom{p}{k}$ sauf le terme $f_p\binom{p}{p}$. Si on ajoute ce terme aux membres, la relation fondamentale prend une forme légèrement différente :

$$p + f_p =_0 \binom{p}{0} + f_1\binom{p}{1} + f_0\binom{p}{2} + \cdots + f_{p-1}\binom{p}{p-1} + f_p\binom{p}{p}.$$

3.1.2 Série génératrice exponentielle des nombres de Faulhaber

Quiconque est familier avec le produit de deux séries de Taylor éprouve ici une certaine émotion. En effet, si

$$\left(a_0 + a_1\frac{x}{1!} + a_2\frac{x^2}{2!} + \cdots\right)\left(b_0 + b_1\frac{x}{1!} + b_2\frac{x^2}{2!} + \cdots\right) = c_0 + c_1\frac{x}{1!} + c_2\frac{x^2}{2!} + \cdots$$

alors

$$c_n = \sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}.$$

Introduisons la série

$$F(x) = f_0 + f_1\frac{x}{1!} + f_2\frac{x^2}{2!} + f_3\frac{x^3}{3!} + \cdots$$

On dit que $F(x)$ est la série génératrice exponentielle des nombres de Faulhaber. L'idée des séries génératrices est due à Euler. On dit que $F(x)$ est exponentielle à cause de la présence des factorielles. On peut exprimer la relation fondamentale entre les nombres de Faulhaber comme une égalité entre séries :

$$(0 + f_0) + (1 + f_1)\frac{x}{1!} + (2 + f_2)\frac{x^2}{2!} + \cdots = \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots\right)\left(f_0 + f_1\frac{x}{1!} + f_2\frac{x^2}{2!} + \cdots\right).$$

On peut donner à cette relation une forme plus compacte en utilisant les séries :

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots \quad \text{et} \quad xe^x = 0 + 1\frac{x}{1!} + 2\frac{x^2}{2!} + \cdots$$

La relation devient $xe^x + F(x) = e^x F(x)$. Il en résulte que $xe^x = (e^x - 1)F(x)$ et par suite que

$$F(x) = \frac{xe^x}{e^x - 1}.$$

3.2 Nombres de Bernoulli

Définition 3.2.1 *Euler introduit toutefois une autre série génératrice :*

$$B(x) = \frac{x}{e^x - 1} = B_0 + B_1\frac{x}{1!} + B_2\frac{x^2}{2!} + \cdots$$

On dit que les coefficients B_n de cette série sont les nombres de ***Bernoulli****.*

Les séries $B(x)$ et $F(x)$ ne différent que légèrement :

$$F(x) = \frac{xe^x}{e^x - 1} = \frac{x}{e^x - 1} + x = B(x) + x.$$

Par suite

$$f_n = \begin{cases} B_n \ \text{ si } n \neq 0, \\ B_1 - 1 \ \text{ si } n = 1 \end{cases}$$

Mais il y a une autre relation entre $B(x)$ et $F(x)$:

$$B(-x) = \frac{-x}{e^{-x} - 1} = \frac{-xe^x}{1 - e^x} = \frac{xe^x}{e^x - 1} = F(x).$$

En comparant les coefficients de $B(-x)$ et de $F(x)$, on trouve que

$$(-1)^n B_n = f_n \ \text{ pour } \ \ n \geq 0.$$

Comment peut-on concilier cette relation avec la précédente ? Pour cela il faut que $-f_1 = f_1 - 1$ et que $(-1)^n f_n = f_n$ pour $n \neq 1$. La première condition signifie que l'on a $f_1 = \frac{1}{2}$. La deuxième signifie que l'on a $f_n = 0$ pour n impair > 1. Nous avons montré sans le vouloir que les nombres de Faulhaber de rang impair > 1 sont nuls !.

Remarque 3.2.2 *On peut associer plusieurs séries génératrices à une suite des nombres $a_0, a_1, a_2, \ldots$ Par exemple, les deux séries*

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots \quad et \quad g(x) = a_0 + a_1 \frac{x}{1!} + a_2 \frac{x^2}{2!} + \cdots$$

Pour les distinguer nous dirons que $f(x)$ est la série génératrice ordinaire et que $g(x)$ est la série génératrice exponentielle. Nous dirons aussi que $a_n = g^{(n)}(0)$ est un coefficient de Taylor de $g(x)$.

Depuis Euler, les nombres de Bernoulli sont définis comme les coefficients de Taylor de la série génératrice exponentielle

$$B(x) = \frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}.$$

La relation $(e^x - 1)B(x) = x$ entraîne que l'on a

$$\sum_{k=0}^{n} B_k \binom{n}{k} = \begin{cases} 1 & \text{si } n = 1, \\ 0 & \text{si } n > 1. \end{cases}$$

Par suite,

$$\begin{aligned} B_0 &= 1 \\ 2B_1 + B_0 &= 0 \text{ donc } B_1 = \frac{-1}{2} \\ 3B_2 + 3B_1 + B_0 &= 0 \text{ donc } B_2 = \frac{1}{6} \\ 4B_3 + 6B_2 + 4B_1 + B_0 &= 0 \text{ donc } B_3 = 0 \\ 5B_4 + 10B_3 + 10B_2 + 5B_1 + B_0 &= 0 \text{ donc } B_4 = \frac{-1}{30} \end{aligned}$$

Les premières valeurs de B_n sont les suivantes :

B_0	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8	B_9
1	$\frac{-1}{2}$	$\frac{1}{6}$	0	$\frac{-1}{30}$	0	$\frac{1}{42}$	0	$\frac{-1}{30}$	0

Remarquer que $|B_{2n}| < 1$ pour $n \leq 6$.

Proposition 3.2.3 *On a*

$$B(x) + \frac{x}{2} = \frac{x}{2} \coth\left(\frac{x}{2}\right).$$

De plus, $B_{2n+1} = 0$ *pour tout* $n > 0$.

Démonstration. Observons d'abord que

$$\coth\left(\frac{x}{2}\right) = \frac{e^{\frac{x}{2}} + e^{-\frac{x}{2}}}{e^{\frac{x}{2}} - e^{-\frac{x}{2}}} = \frac{e^x + 1}{e^x - 1}.$$

Si on substitue $a = e^x$ dans l'identité

$$\frac{a+1}{a-1} = \frac{2}{a-1} + 1,$$

on obtient que

$$\frac{e^x+1}{e^x-1} = \frac{2}{e^x-1} + 1.$$

Par suite,

$$\frac{x}{2}\coth\left(\frac{x}{2}\right) = \frac{x}{2}\frac{e^x+1}{e^x-1} = \frac{x}{e^x-1} + \frac{x}{2} = B(x) + \frac{x}{2}.$$

La fonction $B(x) + \frac{x}{2}$ est paire puisque $\coth(x)$ est une fonction impaire. Cela montre que $B_{2n+1} = 0$ pour $n > 0$. CQFD ■

3.3 Polynômes de Bernoulli

Définition 3.3.1 *On définit les polynômes de Bernoulli $B_n(t)$ par la série génératrice*

$$B(x)e^{xt} = \sum_{n=0}^{\infty} B_n(t)\frac{x^n}{n!}.$$

Cette définition implique que

$$B_n(t) = \sum_{i=0}^{n} \binom{n}{i} B_i t^{n-i}.$$

On trouve

$$\begin{aligned}
B_0(x) &= 1 \\
B_1(x) &= x - \frac{1}{2} \\
B_2(x) &= x^2 - x + \frac{1}{6} \\
B_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x \\
B_4(x) &= x^4 - 2x^3 + x^2 - \frac{1}{30} \\
B_5(x) &= x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x \\
B_5(x) &= x^6 - 3x^5 + \frac{5}{2}x^4 - \frac{1}{2}x^2 + \frac{1}{42}.
\end{aligned}$$

Remarquer que $B_n(0) = B_n$.

Les polynômes de Bernoulli satisfont plusieurs identités remarquables. En voici quelques unes.

Proposition 3.3.2 *Pour tout entier $n \geq 1$, on a*

$$B_n'(t) = nB_{n-1}(t).$$

Démonstration. En effet, on a

$$\sum_{n=0}^{\infty} B_n'(t)\frac{x^n}{n!} = \frac{d}{dt}B(x)e^{tx} = xB(x)e^{tx} = x\sum_{n=0}^{\infty} B_n(t)\frac{x^n}{n!} = \sum_{n=0}^{\infty} nB_{n-1}(t)\frac{x^n}{n!}.$$

CQFD ■

Proposition 3.3.3 *Pour tout entier $n \geq 0$, on a*

$$B_n(s+t) = \sum_{i=0}^{n} \binom{n}{i} B_i(s)t^{n-i}.$$

Démonstration. En effet, on a $B(x)e^{(s+t)x} = (B(x)e^{sx})e^{tx}$. CQFD ■

Proposition 3.3.4 *On a $B_n(t+1) - B_n(t) = nt^{n-1}$ pour tout $n \geq 0$.*

Démonstration. En effet, on a

$$\frac{xe^{(t+1)x}}{e^x - 1} - \frac{xe^{tx}}{e^x - 1} = \frac{xe^{tx}(e^x - 1)}{e^x - 1} = xe^{tx} = \sum_{n=0}^{\infty} nt^{n-1}\frac{x^n}{n!}.$$

CQFD ■

Proposition 3.3.5 *On a $B_n(1-t) = (-1)^n B_n(t)$ pour tout $n \geq 0$.*

Démonstration. En effet,

$$\frac{xe^{(1-t)x}}{e^x-1} = \frac{xe^xe^{-tx}}{e^x-1} = \frac{xe^{-tx}}{1-e^{-x}} = \frac{(-x)e^{t(-x)}}{e^{-x}-1} = \sum_{n=0}^{\infty} B_n(t)\frac{(-x)^n}{n!}.$$

CQFD ■

En particulier, on obtient que $B_n(1) = (-1)^n B_n(0)$ pour tout $n = 0$. Comme $B_n(0) = B_n$ est nul si n est impair > 1, cela montre que

$$B_n(1) = B_n(0) \text{ pour } n \neq 1.$$

De plus, on obtient que $B_n(\frac{1}{2}) = (-1)^n B_n(\frac{1}{2})$. Cela montre que $B_n(\frac{1}{2}) = 0$ si n est impair.

Proposition 3.3.6 *Pour tout entier $p > 0$ et tout entier $n \geq 1$ on a*

$$\sum_{k=0}^{n-1} k^p = \frac{1}{p+1}[B_{p+1}(n) - B_{p+1}(0)] = \int_0^n B_p(x)dx.$$

Démonstration. En effet, on a $B_{p+1}(k+1) - B_{p+1}(k) = (p+1)k^p$ d'après la Proposition 3.3.4. Cela implique par somme télescopique que

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

La seconde formule provient de l'identité $B'_{p+1}(x) = (p+1)B_p(x)$ de la Proposition 3.3.2. CQFD ■

Nous pouvons maintenant démontrer la formule de Faulhaber. En effet,

$$\begin{aligned} p\sum_{k=0}^{n} k^{p-1} = pn^{p-1} + B_p(n) - B_p(0) &= pn^{p-1} + n^p - \frac{p}{2}n^{p-1} + \sum_{i=2}^{p-1} B_i\binom{p}{i}n^{p-i} \\ &= n^p + \frac{p}{2}n^{p-1} + \sum_{i=2}^{p-1} B_i\binom{p}{i}n^{p-i}. \end{aligned}$$

Une autre identité remarquable satisfaite par les polynômes de Bernoulli est la formule

de multiplication :

Proposition 3.3.7 *Pour tout entiers $q \geq 1$ et $n \geq 0$, on a*

$$qB(qx) = q^n \sum_{k=0}^{n-1} B_n\left(x + \frac{k}{q}\right).$$

Démonstration. Posons

$$P_n(t) = \sum_{k=0}^{n-1} q^n B_n\left(x + \frac{k}{q}\right).$$

Pour k fixé, on a

$$\sum_{k=0}^{n-1} q^n B_n\left(x + \frac{k}{q}\right)\frac{x^n}{n!} = \sum_{k=0}^{n-1} B_n\left(x + \frac{k}{q}\right)\frac{(qx)^n}{n!} = \frac{qxe^{t+\frac{k}{q}}}{e^{qx}-1} = \frac{qxe^{tqx}}{e^{qx}-1}e^{kx}$$

Par suite,

$$\begin{aligned}\sum_{n=0}^{\infty} P_n(t)\frac{x^n}{n!} &= \frac{qxe^{tqx}}{e^{qx}-1}\sum_{k=0}^{q-1} e^{kx} = \frac{qxe^{tqx}}{e^{qx}-1}\frac{e^{qx}-1}{e^x-1} \\ &= q\frac{xe^{tqx}}{e^x-1} = \sum_{n=0}^{\infty} qB_n(qt)\frac{x^n}{n!}.\end{aligned}$$

CQFD ■

Proposition 3.3.8 *On a*

$$x\coth(x) = \sum_{n=0}^{\infty} 2^{2n}B_{2n}\frac{x^{2n}}{(2n)!} \quad et \quad x\cot(x) = 1 - \sum_{n=0}^{\infty} 2^{2n}|B_{2n}|\frac{x^{2n}}{(2n)!}.$$

Démonstration. Le premier développement provient de l'identité $x\coth(x) = x + B(2x)$. Le second s'obtient en remplacant x par ix dans le premier et en utilisant le fait que l'on a $(-1)^n B_{2n} = -|B_{2n}|$ pour $n > 0$. CQFD. ■

En déduire aussi la propostion suivante.

Proposition 3.3.9 *On a*

$$x \tanh\left(\frac{x}{2}\right) = \sum_{n=0}^{\infty} 2(2^{2n}-1)B_{2n}\frac{x^{2n}}{(2n)!}.$$

3.4 Exercices

Exercise 19 *Montrer que* $x + B(x) = e^x B(x) = B(-x)$.

Exercise 20 *Montrer que*

$$\frac{e^{tx}-1}{e^x-1} = \sum_{n=0}^{\infty} \frac{B_{n+1}(t) - B_{n+1}(0)}{n+1}\frac{x^n}{n!}.$$

En déduire que

$$\frac{B_{n+1}(m+1) - B_{n+1}(0)}{n+1} = 0^n + 1^n + 2^n + \cdots + m^n.$$

Suggestion : utiliser l'identité

$$\frac{e^{(m+1)x}-1}{e^x-1} = 1 + e^x + e^{2x} + \cdots + e^{mx}.$$

Exercise 21 *Montrer que pour tout entier* $n \geq 0$, *on a*

$$2^n B_n\left(\frac{1}{2}\right) = (2-2^n)B_n \;\; et \;\; 4^{2n}B_{2n}\left(\frac{1}{4}\right) = (2-2^{2n})B_{2n}.$$

Suggestion : utiliser la formule de multiplication et l'identité $B_{2n}(1-x) = B_{2n}(x)$.

Exercise 22 *Montrer que pour tout entier* $n \geq 0$, *on a*

$$2.3^{2n}B_{2n}\left(\frac{1}{3}\right) = (3-3^{2n})B_{2n} \;\; et \;\; 2.6^{2n}B_{2n}\left(\frac{1}{6}\right) = (2-2^{2n})(3-3^{2n})B_{2n}.$$

CHAPITRE 4

NOMBRES ET POLYNÔMES D'EULER

4.1 Nombres d'Euler et nombres de Genocchi

Définition 4.1.1 *Les nombres d'**Euler** sont définies comme les coefficients de taylor de la sécante hyperbolique*

$$sech(x) = \frac{2e^x}{e^{2x}+1} = \sum_{n=0}^{\infty} E_n \frac{x^n}{n!}.$$

Remarque 4.1.2 *On a $E_{2n+1} = O$, $n \geq 0$.*

Démonstration. La sécante hyperbolique est une fonction paire c'est à dire $sech(-x) = sech(x)$, donc

$$\frac{2e^x}{e^{2x}+1} = \frac{2e^{-x}}{e^{-2x}+1} \Leftrightarrow \sum_{n=0}^{\infty} E_n \frac{x^n}{n!} = \sum_{n=0}^{\infty} E_n (-1)^n \frac{x^n}{n!},$$

ainsi $E_n = E_n(-1)^n$, donc

$$\begin{cases} E_{2k} = E_{2k} & \text{si} \quad n = 2k \\ E_{2k+1} = -E_{2k+1} & \text{si} \quad n = 2k+1, \end{cases}$$

d'où $E_{2k+1} = 0$. CQFD ■

Définition 4.1.3 *Les nombres de* ***Genocchi*** *sont définies par la série génératrice :*

$$\begin{aligned} G(x) &= \frac{2x}{e^x+1} = \sum_{n=0}^{\infty} G_n \frac{x^n}{n!}. \\ &= x - \frac{x^2}{2!} + \frac{x^4}{4!} - 3\frac{x^6}{6!} + 17\frac{x^8}{8!} - 155\frac{x^{10}}{10!} + \cdots \end{aligned}$$

où $G_1 = 1$, $G_{2n+1} = 0$, $n \geq 0$.

Proposition 4.1.4 $G(x) = x - x\tanh\left(\frac{x}{2}\right)$.

Démonstration. $G(x) = \frac{2x}{e^x+1} = x - x\frac{e^x-1}{e^x+1} = x - x\tanh\left(\frac{x}{2}\right)$. ■

Proposition 4.1.5 $G_{2n} = -2(2^{2n}-1)B_{2n}$ *pour* $n > 0$.

Démonstration. D'après la proposition précédente on a : $G(x) = x - x\tanh\left(\frac{x}{2}\right)$, alors

$$x\tanh\left(\frac{x}{2}\right) = \sum_{k=0}^{\infty} -G_{2n}\frac{x^{2n}}{2n!}.$$

Mais par Proposition 3.3.9, on a

$$x\tanh\left(\frac{x}{2}\right) = \sum_{n=0}^{\infty} 2(2^{2n}-1)B_{2n}\frac{x^{2n}}{(2n)!}.$$

Par suite,

$$G_{2n} = -2(2^{2n}-1)B_{2n}.$$

■

On en déduit que $(-1)^n G_{2n} > 0$.

Théorème 4.1.6 (Genocchi) *Les nombres G_{2n} sont des entiers impairs.*

Démonstration. On a $|G_{2n}| = 2(2^{2n} - 1)|B_{2n}|$. Il suffit donc de montrer que le dénominateur de B_{2n} divise $2(2^{2n} - 1)$. Par le théorème de von Staudt-Clausen [1] il suffit de montrer que si $p-1$ divise $2n$ et p est premier, alors p divise $2(2^{2n}-1)$. C'est clair si $p = 2$. Supposons p impair. Dans ce cas, p divise $2^{p-1} - 1$ par le théorème de Fermat. Mais si a divise b alors $2^a - 1$ divise $2^b - 1$. Donc $2^{p-1} - 1$ divise $2^{2n} - 1$ puisque $p - 1$ divise $2n$. Cela entraîne que p divise $2(2^{2n} - 1)$. De plus, G_{2n} est impair puisque le dénominateur de B_{2n} est pair. ■

4.2 Polynômes d'Euler et polynômes de Genocchi

L'introduction suivante avait uniquement pour but de réfléchir sur le cheminement que pourrait avoir suivit Euler dans sa découverte. Par la suite nous allons travailler exclusivement avec les polynômes d'Euler car ils sont standards.

1. Le théorème de von Staudt-Clausen est un résultat sur la partie fractionnaire des nombres de Bernoulli non entiers.
Précisément, si $n = 2k$ est un entier pair non nul et si l'on ajoute $\frac{1}{p}$ à B_n pour tous les nombres premiers p tel que $p - 1$ divise n, on obtient un nombre entier :

$$B_{2k} + \sum_{(p-1|2k)} \frac{1}{p}.$$

Par conséquent, les nombres de Bernoulli non nuls de rang pair B_{2k} ($k \geq 1$) s'écrivent :

$$B_{2k} = A_{2k} - \sum_{(p-1|2k)} \frac{1}{p}.$$

où A_{2k} est un nombre entier.
Ce fait permet immédiatement de caractériser les dénominateurs des nombres de Bernoulli B_n non entiers comme le produit de tous les nombres premiers p tel que $p - 1$ divise n ; par conséquent, les dénominateurs sont sans carré et, si n est pair, divisibles par 6.
Le résultat fut nommé ainsi en l'honneur de Karl Von Staudt et Thomas Clausen, qui l'ont découvert indépendamment en 1840.

Si p est un entier ≥ 0, on définit la somme alternée des puissances p-ième des entiers successifs en posant

$$A_p(n) = n^p - (n-1)^p + (n-2)^p - \cdots + (-1)^n 0^p$$

pour tout entier $n \geq 0$. Il est naturel de chercher un polynôme qui donne les valeurs de cette somme. Par exemple, on vérifie facilement que l'on a

$$A_2(n) = \frac{n^2 + n}{2}.$$

pour tout entier $n \geq 0$. De façon générale, si $a_0, a_1, a_2, \ldots$ est une suite de nombres, considérons la suite des sommes alternés

$$\begin{aligned}
\sigma_0 &= a_0 \\
\sigma_1 &= a_1 - a_0 \\
\sigma_2 &= a_2 - a_1 + a_0 \\
\sigma_3 &= a_3 - a_2 + a_1 - a_0 \\
&\ldots
\end{aligned}$$

On trouve que $a_n = \sigma_n + \sigma_{n-1}$ pour tout $n > 0$. Inversement, si on a $a_n = b_n + b_{n-1}$ pour une suite de nombres $b_0, b_1, b_2, \ldots$ et si $b_0 = a_0$, alors on a $\sigma_n = b_n$ pour tout $n \geq 0$. Pour résoudre notre problème, il suffirait donc de trouver un polynôme $H_p(x)$ satisfaisant aux deux conditions :(i) $x^p = H_p(x) + H_p(x-1)$ et (ii) $H_p(0) = 0$. Remarquer que la première condition entraîne que $H_p(x)$ est de degré p. Un tel polynôme n'existe pas si $p = 1$! (bien qu'il existe si $p = 2$). En effet, si $H_1(x) = ax + b$, alors la condition $x = H_1(x) + H_1(x-1)$ implique que $a = \frac{1}{2}$ et $b = \frac{1}{4}$. La deuxième condition $H_1(0) = 0$ est alors impossible à

satisfaire. En fait, on trouve que

$$\begin{aligned} A_1(1) &= 1 \\ A_1(2) &= 2-1=1 \\ A_1(3) &= 3-2+1=2 \\ A_1(4) &= 4-3+2-1=2 \\ A_1(5) &= 5-4+3-2+1=3 \\ A_1(6) &= 6-5+4-3+2-1=3 \\ &\dots \end{aligned}$$

On voit que

$$A_1(n) = \begin{cases} \frac{n}{2}+\frac{1}{2} & \text{si } n \text{ est impair,} \\ \frac{n}{2} & \text{si } n \text{ est pair .} \end{cases}$$

On peut réunir cette description dans une seule formule :

$$A_1(n) = \frac{n}{2} + \frac{1-(-1)^n}{4}.$$

Il parait raisonnable de chercher un polynôme $H_p(x)$ et une constante C_p telles que l'on ait

$$A_p(n) = H_p(n) + (-1)^n C_p$$

pour tout entier $n \geq 0$. Dans ce cas, la condition $H_p(x) + H_p(x-1) = x^p$ est toujours satisfaite car

$$\begin{aligned} H_p(n) + H_p(n-1) &= H_p(n) + (-1)^n C_p + H_p(n-1) + (-1)^{n-1} C_p \\ &= A_p(n) + A_p(n-1) = n^p. \end{aligned}$$

Remarquer que $A_p(0) = 0$ si $p > 0$; dans ce cas, $C_p = -H_p(0)$. De plus, $A_0(0) = 1$ et $A_0(1) = 0$; par suite, $H_0 = C_0 = \frac{1}{2}$. Nous allons supposer à priori que les polynômes

$H_p(t)$ pour $p \geq 0$ admettent une série génératrice

$$\sum_{p=0}^{\infty} H_p(t)\frac{x^p}{p!}$$

de la forme $H(x)e^{xt}$ pour une série

$$H(x) = \sum_{n\geq 0} H_n \frac{x^n}{n!}.$$

Cette hypothèse est motivée par l'exemple des polynôme de Bernoulli. Elle permet de racourcir le raisonnement si elle s'avère juste. Il n'y a pas de raison de l'écarter tant qu'elle n'engendre pas de contradiction. Elle implique que l'on a $H_p = H_p(0)$ et que

$$H_p(x) = \sum_{k=0}^{p} \binom{p}{k} H_k x^{p-k}.$$

En terme de séries génératrices, la condition $H_p(t) + H_p(t-1) = t^p$ devient

$$H(x)e^{xt} + H(x)e^{x(t-1)} = e^{xt}.$$

Mais on a $H(x)e^{xt} + H(x)e^{x(t-1)} = e^{xt}H(x)(1+e^{-x})$. Par suite, $H(x)(1+e^{-x}) = 1$. Nous avons montré que

$$H(x) = \frac{1}{1+e^{-x}} = \frac{e^x}{e^x+1}.$$

Définition 4.2.1 *Les polynômes d'Euler $E_n(t)$ sont définis par la série génératrice*

$$\frac{2e^{xt}}{e^x+1} = \sum_{n=0}^{\infty} E_n(t)\frac{x^n}{n!}.$$

Remarque 4.2.2 *On a $E_n(t+1) = 2H_n(t)$. La différence entre les polynômes $H_n(t)$ et les polynômes d'Euler est mineure. Les polynômes d'Euler sont unitaires.*

Proposition 4.2.3 *On a $E_n(t) = \sum_{k=0}^{n} \binom{n}{k} E_k(0)t^{n-k}$.*

Démonstration. Pour $k = 0$, on a : $\frac{2}{e^x+1} = \sum_{n=0}^{\infty} E_n(0)\frac{x^n}{n!}$

alors

$$\begin{aligned}\frac{2}{e^x+1}e^{xt} &= \left(\sum_{n=0}^{\infty} E_n(0)\frac{x^n}{n!}\right)\left(\sum_{n=0}^{\infty}\frac{x^n t^n}{n!}\right)\\ &= \sum_{n=0}^{\infty} b_n(t)\frac{x^n}{n!}\end{aligned}$$

tel que : $b_n(t) = \sum_{k=0}^{n}\binom{n}{k}E_k(0)t^{n-k}$. CQFD ■

Remarque 4.2.4 $E_{2n}(0) = 0$, $n \geq 0$.

Démonstration. Soit $g(x) = 1 - \frac{2}{e^x+1} = \frac{e^x-1}{e^x+1} = \tanh(\frac{x}{2})$. On remarque que $g(x) = -g(-x)$, c'est à dire $g(x)$ impair.

$$\begin{aligned}1 - \sum_{n=0}^{+\infty} E_n(0)\frac{x^n}{n!} &= -1 + \sum_{n=0}^{+\infty}(-1)^n E_n(0)\frac{x^n}{n!}\\ 2 &= \sum_{n=0}^{+\infty}(1+(-1)^n)E_n(0)\frac{x^n}{n!}.\end{aligned}$$

Par identification, on obtient.

— si $n = 0$ on a : $(1 + (-1)^0)E_0(0) = 2$, ce qui donne $E_0(0) = 1$,

— si $n = 2k$: $2E_{2k}(0) = 0$, ce qui donne $E_{2k}(0) = 0$.

■

On trouve que

$$\begin{aligned}
E_0(x) &= 1 \\
E_1(x) &= x - \frac{1}{2} \\
E_2(x) &= x^2 - x \\
E_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{4} \\
E_4(x) &= x^4 - 2x_3 + x \\
E_5(x) &= x^5 - \frac{5}{2}x^4 + \frac{5}{2}x^2 + \frac{1}{2} \\
E_6(x) &= x^6 - 3x^5 + 5x^3 - 3x \\
E_7(x) &= x^7 - \frac{7}{2}x^6 + \frac{35}{4}x^4 - \frac{21}{2}x^2 + \frac{17}{8} \\
&\dots
\end{aligned}$$

Nous verrons que les coefficients de $E_n(x)$ sont des entiers divisés par une puissance de 2. Nous verrons que ces coefficients sont entiers si n est pair.

Proposition 4.2.5 **(i)** $E_n(t+1) + E_n(t) = 2t^n$.

(ii) $E_n(1-t) = (-1)^1 E_n(t)$.

Démonstration.

(i) On a

$$\frac{2e^{x(t+1)}}{e^x+1} + \frac{2e^{xt}}{e^x+1} = \frac{2e^{xt}e^x + 2e^{xt}}{e^x+1} = 2e^{xt},$$

alors

$$\sum_{n=0}^{+\infty} \left(E_n(t+1) + E_n(t)\right) \frac{x^n}{n!} = \sum_{n=0}^{+\infty} 2t^n \frac{x^n}{n!} \Rightarrow E_n(t+1) + E_n(t) = 2t^n.$$

(ii) On aussi

$$\frac{2e^{-xt}}{e^{-x}+1} = \frac{2e^{x(1-t)}}{e^x+1} \Rightarrow \sum_{n=0}^{+\infty} E_n(t)\frac{(-x)^n}{n!} = \sum_{n=0}^{+\infty} E_n(1-t)\frac{(x)^n}{n!} \Rightarrow E_n(1-t) = (-1)^1 E_n(t).$$

■

Proposition 4.2.6 *Pour tout entier $p > 0$ et tout entier $n \geq 1$ on a*

$$n^p - (n-1)^p + \cdots + (-1)^n 0^p = \frac{E_p(n+1) + (-1)^p E_p(0)}{2}.$$

Démonstration. Par l'identité $E_p(x+1) + E_p(x) = 2x^p$, on obtient

$$\begin{aligned} & 2 \quad [n^p - (n-1)^p + \cdots + (-1)^n 0^p] \\ = & \quad \Big[E_p(n+1) + E_p(n)\Big] - \Big[E_p(n) + E_p(n-1)\Big] + \cdots + (-1)^n \Big[E_p(1) + E_p(0)\Big] \\ = & \quad E_p(n+1) + (-1)^n E_p(0). \end{aligned}$$

CQFD ■

Proposition 4.2.7 *Pour $n \geq 1$, $E_{n-1}(x) = \frac{2}{n}\left\{B_n(x) - 2^n B_n(\frac{x}{2})\right\}$.*

Démonstration. On sait bien que $\frac{1}{a+1} = \frac{1}{a-1} - \frac{2}{a^2-1}$.
On pose $a = e^x$ alors $\frac{1}{e^x+1} = \frac{1}{e^x-1} - \frac{2}{e^{2x}-1}$, ainsi

$$\frac{2xe^{xt}}{e^x+1} = \frac{2xe^{xt}}{e^x-1} - 2\frac{2xe^{xt}}{e^{2x}-1} = 2\frac{xe^{xt}}{e^x-1} - 2\frac{2xe^{2x\frac{t}{2}}}{e^{2x}-1}.$$

Il s'ensuite que

$$\begin{aligned} x\sum_{n=0}^{+\infty} E_n(t)\frac{(x)^n}{n!} &= 2\sum_{n=0}^{+\infty} B_n(t)\frac{(x)^n}{n!} - 2\sum_{n=0}^{+\infty} B_n\left(\frac{t}{2}\right)\frac{(2x)^n}{n!} \\ \Rightarrow \sum_{n=0}^{+\infty} E_n(t)\frac{(x)^{n+1}}{n!} &= 2\sum_{n=0}^{+\infty}\left[B_n(t) - 2^n B_n\left(\frac{t}{2}\right)\right]\frac{(x)^n}{n!} \\ \Rightarrow \sum_{n=0}^{+\infty} nE_{n-1}(t)\frac{(x)^n}{n!} &= 2\sum_{n=1}^{+\infty}\left[B_n(t) - 2^n B_n\left(\frac{t}{2}\right)\right]\frac{(x)^n}{n!} \end{aligned}$$

Donc $nE_{n-1}(t) = 2\left[B_n(t) - 2^n B_n\left(\frac{t}{2}\right)\right] \Rightarrow E_{n-1}(x) = \frac{2}{n}\left[B_n(x) - 2^n B_n\left(\frac{x}{2}\right)\right]$ pour $n \geq 1$. ■

Proposition 4.2.8

1. $E_n = 2^n E_n\left(\frac{1}{2}\right)$.
2. $E_n(t) = \frac{1}{2}\sum_{k=0}^{n}\binom{n}{k}E_k(2t-1)^{n-k}$.

Démonstration.

1. On a

$$\begin{aligned} Sech(x) &= \frac{2e^x}{e^{2x}+1} = \frac{2e^{\frac{1}{2}\times 2x}}{e^{2x}+1} \\ &= \sum_{n=0}^{+\infty} E_n\left(\frac{1}{2}\right)\frac{(2x)^n}{n!} \quad \text{par le changement } x = 2x \text{ et } t = \frac{1}{2} \\ &= \sum_{n=0}^{+\infty} 2^n E_n\left(\frac{1}{2}\right)\frac{(x)^n}{n!}, \end{aligned}$$

   d'autre coté $Sech(x) = \sum_{n=0}^{+\infty} E_n(t)\frac{(x)^n}{n!}$.
   Donc $E_n = 2^n E_n\left(\frac{1}{2}\right)$.

2. On sait que $\frac{2e^{xt}}{e^x+1} = \sum_{n=0}^{+\infty} E_n(t)\frac{(x)^n}{n!}$, alors

$$\begin{aligned} \frac{2e^{2xt}}{e^x+1} &= \frac{2e^{2xt}e^{-x}e^x}{e^x+1} = \frac{2e^{2x}}{e^{2x}+1}e^{(2t-1)x} \\ \Rightarrow \sum_{n=0}^{+\infty} E_n(t)\frac{(2x)^n}{n!} &= \left(\sum_{n=0}^{+\infty} E_n(t)\frac{(x)^n}{n!}\right)\left(\sum_{n=0}^{+\infty}(2t-1)^n\frac{(x)^n}{n!}\right) \\ \Rightarrow 2^n E_n &= \sum_{k=0}^{n}\binom{n}{k}E_k(2t-1)^{n-k} \\ \Rightarrow E_n &= \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}E_k(2t-1)^{n-k}. \end{aligned}$$

■

Définition 4.2.9 (Polynôme de Genocchi) *On définit les polynômes de Genocchi par la fonction génératrice :*

$$G(x)e^{xt} = \frac{2xe^{xt}}{e^x+1} = \sum_{n=0}^{+\infty} G_n(t)\frac{(x)^n}{n!},$$

avec $G_n = G_n(0)$, $G_n(t) = \sum_{k=0}^{n}\binom{n}{k}G_k t^{n-k}$.

On trouve

$$\begin{aligned} G_1(x) &= 1 \\ G_2(x) &= 2x - 1 \\ G_3(x) &= 3x^2 - 3x \\ G_4(x) &= 4x^3 - 6x^2 + 1 \\ G_5(x) &= 5x^4 - 10x^3 + 5x \\ G_6(x) &= 6x^5 - 15x^4 + 15x^2 - 3 \\ &\dots \end{aligned}$$

Les coefficients de $G_n(x)$ sont entiers puisque les nombres de Genocchi sont entiers. Remarquer que $G_n(x)$ est un polynôme de degré $n-1$.

Proposition 4.2.10 *On a :* $G_n(t) = nE_{n-1}(t)$.

Démonstration. En effet,

$$G(x)e^{xt} = x\frac{2e^{xt}}{e^x+1} = x\sum_{n=0}^{\infty} E_n(t)\frac{(x)^n}{n!} = \sum_{n=1}^{\infty} nE_{n-1}(t)\frac{(x)^n}{n!}.$$

Par suite, $G_n(t) = nE_{n-1}(t)$. ■

Corollaire 4.2.11 *Si* 2^k *est la plus grande puissance de* 2 *divisant* $n+1$*, alors les coefficients du polynôme* $2^kE_n(x)$ *sont entiers.*

Démonstration. Les coefficients du polynôme $(n+1)E_n(x) = G_{n+1}(x)$ sont entiers. Le résultat cherché est alors conséquence du fait que ces coefficients sont des entiers divisés par une puissance de 2. CQFD ■

Corollaire 4.2.12 *Les coefficients des polynômes* $E_{2n}(x)$ *sont entiers.*

Exercices

Exercise 23 *Démontrer les identités :*

$$E_n(s+t) = \sum_{k=0}^{n} \binom{n}{k} E_k(s) t^{n-k} \quad et \quad G_n(s+t) = \sum_{k=0}^{n} \binom{n}{k} G_k(s) t^{n-k}.$$

Exercise 24 *Montrer que*

$$G_n(t) = 2^n \left[B_n\left(\frac{x+1}{2}\right) - B_n\left(\frac{x}{2}\right) \right].$$

Exercise 25 *Montrer que la suite de polynômes $E_0(x), E_1(x), E_2(x), \ldots$ est la seule satisfaisant aux conditions suivantes :*

1. $E_0(x) = 1$,
2. $E_n'(x) = nE_{n-1}(x)$ *pour tout* $n > 0$,
3. $E_{2n-1}(\frac{1}{2}) = E_{2n}(0) = 0$ *pour tout* $n > 0$.

Exercise 26 *Montrer que la suite de polynômes $G_1(x), G_2(x), G_3(x), \ldots$ est la seule satisfaisant aux conditions suivantes :*

1. $G_1(x) = 1$,
2. $G_n'(x) = nG_{n-1}(x)$ *pour tout* $n > 0$,
3. $G_{2n}(\frac{1}{2}) = E_{2n+1}(0) = 0$ *pour tout* $n > 0$.

BIBLIOGRAPHIE

[1] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 4th ed.,1960, https ://faculty.ksu.edu.sa/rizwanbutt/Documents/.

[2] M. Hindry, *Cours d'arithmétique*, Université Denis Diderot Paris 7, (2005), https ://webusers.imj-prg.fr/ marc.hindry/.

[3] A. Joyal, *Les nombres de Bernoulli*, pour le camp mathématique UQAM(2003), http ://www.campmath.uqam.ca.

[4] A. Joyal, *Arithmétique*, pour le camp mathématique UQAM(2003), http ://www.campmath.uqam.ca.

[5] A. Kraus, *Cours d'arithmétique*, Université de Pierre et Marie Curie, (2013), https ://webusers.imj-prg.fr/ benjamin.girard/.

[6] S. Louboutin, *Résumé de cours Arithmétique*, Bureau 112, I.M.L, (2005), http ://lumimath.univ-mrs.fr/coursL2/.

[7] J. -P. Serre, *Cours d'arithmétique*, Presses Universitaires de France, 1970, http ://plouffe.fr/simon/math/.

[8] N. Touafek, *Eléments sur l'arithmétique*, Cours Master 1, Université de Jijel.