CHAPITRE 1

Relations binaires

Relations binaires

Soit E et F deux ensembles. Se donner une relation binaire de E vers F c'est se donner une partie du produit $E \times F$, qu'on appelle son graphe.

Lorsque $E = F$ on parle d'une relation binaire sur E.

Exemples :

1. Le graphe de la relation de divisibilité sur $\mathbb{N}$, est ainsi le sous-ensemble de $\mathbb{N} \times \mathbb{N}$ défini par $\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid \exists k \in \mathbb{N}, y = k \cdot x\}$.
2. La relation d'égalité sur $\mathbb{N}$ est l'ensemble $\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x = y\}$.

Notation : Si $\mathcal{R}$ est une relation binaire de E vers f, plutôt que d'écrire $(x, y) \in \mathcal{R}$ pour dire que x et y sont reliés par $\mathcal{R}$ on utilise la notation $x \mathcal{R} y$.

Relations d'ordre

Définition 1.1. *Une relation d'ordre sur l'ensemble E est une relation binaire cR qui est*

Réflexive : $\forall x \in E, \quad x \mathcal{R} x.$
Antisymétrique : $\forall x, y \in E, \quad x \mathcal{R} y \text{ et } y \mathcal{R} x \implies x = y.$
Transitive : $\forall x, y, z \in E, \quad x \mathcal{R} y \text{ et } y \mathcal{R} z \implies x \mathcal{R} z.$

Cette relation est un ordre total si pour tous x, y de on a $x \mathcal{R} y$ ou bien $y \mathcal{R} x$.

Exemples :

— La relation d'ordre usuelle $\leq$ sur $\mathbb{N}$ un ordre total, car pour tout couple (x, y) l'une au moins des assertions $x \leq y$, $y \leq x$ est satisfaite.
— La relation $<$ n'est pas une relation d'ordre car elle n'est pas réflexive.
— La relation de divisibilité est une relation d'ordre sur $\mathbb{N}$, mais ce n'est pas un ordre total car, si x et y sont deux entiers, en général, aucun des deux ne divise l'autre. réflexive.

Relations d'équivalence

Définition 1.2. *Une relation d'équivalence E est une relation binaire $\mathcal{R}$ qui est*

Réflexive : $\forall x \in E, \quad x \mathcal{R} x.$
Symétrique : $\forall x, y \in E, \quad x \mathcal{R} y \implies y \mathcal{R} x.$
Transitive : $\forall x, y, z \in E, \quad x \mathcal{R} y \text{ et } y \mathcal{R} z \implies x \mathcal{R} z.$

Exemples :
— La relation d'égalite est une relation d'équivalence.
— Soit n un entier naturel non nul, la relation de congruence modulo n est une relation d'équivalence. (Si $n = 0$ la congruence modulo n est la relation d'égalité.)
— La relation de parallélisme sur l'ensemble des droites est une relation d'équivalence, à condition de considérer qu'une droite est parallèle à elle-même.

Définition 1.3. *Si $\mathcal{R}$ est une relation d'équivalence sur E et a un élément de E la classe d'équivalence de x est l'ensemble $\{x \in E \mid a \mathcal{R} x\}$.*

Théorème 1.1. *Si $\mathcal{R}$ est une équivalence sur E les classes d'équivalence selon $\mathcal{R}$ forment une partition de E, c'est à dire qu'elles sont deux à deux disjointes et de réunion E.*

Démonstration : Les classes d'équivalence recouvrent E car, par réflexivité, tout x de E appartient à sa classe.

Notons $\overline{x}$ la classe de x. Il reste à démontrer que si $\overline{x}$ et $\overline{y}$ ont une intersection non vide elles sont identiques. Or dire que $z \in \overline{x}$ et $z \in \overline{y}$ c'est dire que $x \mathcal{R} z$ et $y \mathcal{R} z$. Par symétrie, de $y \mathcal{R} z$ on déduit $z \mathcal{R} y$, qui avec $x \mathcal{R} z$ donne par transitivité $x \mathcal{R} y$. Donc $y \in \overline{x}$, et, par symétrie $x \in \overline{y}$. ■

Définition 1.4. *Soit $\mathcal{R}$ une relation d'équivalence sur E, et $*$ une loi de composition binaire sur E. On dit cette loi est compatible avec $\mathcal{R}$ si, pour tous x, x', y, y' de E*

$$x \equiv x' \pmod{\mathcal{R}} \text{ et } y \equiv y' \pmod{\mathcal{R}} \implies x' * y' \equiv x * y \pmod{\mathcal{R}}.$$

Théorème 1.2. *Si $*$ est une opération binaire sur E, compatible ave l'équivalence $\mathcal{R}$. Notons $E/\mathcal{R}$ l'ensemble des classes d'équivalence. On peut définit une loi de composition sur $E/\mathcal{R}$ en posant $\overline{x} * \overline{x'} = \overline{x * y}$.*

Démonstration : Il faut s'assurer que ceci définit bien $\overline{x} * \overline{x'}$ de manière unique, c'est à dire que si l'on remplace x par un x' définissant la même classe, et y par y' définissant la même classe, $\overline{x' * y'} = \overline{x * y}$, ce qui n'est pas autre chose que l'hypothèse de compatibilité de $*$ avec $\mathcal{R}$. ■

CHAPITRE 2

Algorithme d'Euclide

Définition 2.1 (La relation de divisibilité)**.** *Soit a, d deux entiers relatifs. On dit que d est un diviseur de a et on le notera $d \mid a$ si a est un multiple de d.*

Remarques :

— Tous les entiers divisent 0. 0 ne divise que 0.

— d divise a si et seulement si il divise $|a|$. Si d divise a, $|d| \leq |a|$.

Définition 2.2. *Un nombre premier est un entier positif p qui a exactement 2 diviseurs, 1 et p.*

Soit a et b deux entiers non tous les deux nuls. Le plus grand commun diviseur de a et b, noté $\text{pgcd}(a, b)$ est le plus grand entier qui divise a et b.

Proposition 2.1. *On ne change pas le* pgcd *de deux entiers en ajoutant ou retranchant à l'un un multiple de l'autre.*

Démonstration : Soit $b' = b + au$. Si d divise a et b il divise aussi b et au et donc leur somme b'. De même, si d divise a et b', il divise aussi b' et au et donc $b' - au = b$. Les diviseurs de a et b sont donc les mêmes que ceux de a et b'. ∎

Corollaire 2.1. *Soient a et b deux entiers, $0 \leq a < b$.*

1. *Si $a \neq 0$, $\text{pgcd}(a, b) = \text{pgcd}(r, a)$ où r est le reste de la division de b par a.*
2. *Si $a = 0$, $\text{pgcd}(a, b) = b$.*

Démonstration : Si $a \neq 0$, et si q est le quotient de la division, $r = b - aq$ s'obtient en retranchant de b un multiple de a.

Si $a = 0$, il est divisible par tous les entiers, les diviseurs communs de 0 et b sont donc les diviseurs de b et le plus grand d'entre eux est b. ∎

```python
def pgcd(a, b):
    """ 0 <= a < b Renvoie le pgcd de a et b  """
    while a > 0:
        r , b = a, b % a
    return b
```

Théorème 2.1 (Théorème de Bezout). *Si d est le plus grand diviseur commun de x et y, il existe u et v entiers tels que $ux + vy = d$.*

Démonstration : On peut supposer, sans perte de généralité, que $0 \leq x < y$. On raisonne par récurrence sur la valeur de x. Si $x = 0$, l'énoncé du théorème est vrai car $\text{pgcd}(x, y) = y = ux + vy$ avec $u = 0$ et $v = 1$.

Supposons le vrai pour toutes les valeurs de x plus petites que $a \geq 1$, prouvons qu'il l'est encore pour $x = a$. Soit donc b un entier $\geq a$, q et r le quotient et le reste de la division de b par a, et enfin $d = \text{pgcd}(a, b)$.

Puisque d est aussi le pgcd de r et a, et puisque r est plus petit que a, par hypothèse de récurrence il existe u' et v' tels que $d = u'r + v'a$.

En remplaçant r par $b - qa$ dans cette égalité on obtient $d = u'(b - qa) + v'a = (v' - u'q)a + u'bx$ et le théorème est encore vrai pour a et b en choisissant $u = v' - u'q$ et $v = u'$. ∎

Cette récurrence conduit immédiatemment à la fonction Python gcdex(a,b) qui renvoie, d, u, v avec $d = \text{pgcd}(a, b)$, et $d = au + bv$.

```python
def gcdex(a,b):
    if a == 0:
        return(b, 0 , 1)
    d, u, v = gcdex(b % a, a)
    return(d, v - u *(b // a), u)
```

Théorème 2.2 (Lemme de Gauss). *Si a est premier avec b et divise bc, alors il divise c.*

Démonstration : Puisque a est premier avec b il existe u et v tels que $ua + vb = 1$ et donc $c = uac + vbc$, somme de deux multiples de a, est un multiple de a. ∎

Coût de l'algorithme d'Euclide

Théorème 2.3. *Soit $0 < a < b$. Le nombre de divisions effectuées en calculant* $\text{pgcd}(a,b)$ *par l'algorithme d'Euclide, est majoré par* $2\log_2(a)+1$.

Démonstration : Notons $r_{-1} = b$, $r_0 = a$. Les quotients et restes q_i, r_i des t divisions effectuées pour obtenur $\text{pgcd}(a,b)$ sont définis par

$$\begin{array}{lllllll} r_{-1} & = & q_1 & \times & r_0 & + & r_1, \qquad r_1 < r_0 \\ r_0 & = & q_2 & \times & r_1 & + & r_2, \qquad r_2 < r_1 \end{array}$$

$$\begin{array}{lllllll} r_{t-3} & = & q_{t-1} & \times & r_{t-2} & + & r_{t-1}, \qquad r_{t-1} < r_{t-2} \\ r_{t-2} & = & q_t & \times & r_{t-1} & + & r_t, \qquad r_t = 0. \end{array}$$

et $r_{t-1} = \text{pgcd}(a,b) \geq 1$.

Commençons par remarquer que $\mathbf{r_2 < r_0/2}$. C'est trivial si $r_1 \leq r_0/2$ car $r_2 < r_1$. Sinon, on a $r_1 > r_0/2$ et le quotient q_2 est 1. D'où $r_2 = r_0 - r_1 < r_0 - r_0/2 = r_0/2$.

Mais on démontre exactement de la même façon que $r_{j+2} < r_j$, pour tout $j \geq 0$, puis, par une récurrence immédiate, que $r_{2j} < a/2^j$ pour tout $j \geq 1$.

Si $t = 1$, la majoration $1 \leq 2\log_2(a)+1$ est triviale.

Si $t = 2$, r_1 n'est pas nul, d'où $a \geq 2$, et la majoration triviale $t \leq 2\log_2(a)+1$.

Si $t = 2k+1 \geq 3$, $r_{t-1} = r_{2k}$, et donc $a/2^k > 1$, car $1 \leq r_{2k} < a/2^k$. On en déduit $k < \log_2(a)$, et $t = 2k+1 < 2\log_2(a)+1$.

Si $t = 2k$, avec $k \geq 2$, $r_{2k-2} > r_{2k-1} = r_{t-1} \geq 1$ donc $r_{2k-2} = r_{2(k-1)} \geq 2$ et $2 < a/2^{(k-1)}$ c'est à dire $2^k < a$ soit $k < \log_2(a)$ qui donne $t = 2k < 2\log_2(a)$.

Ainsi, dans tous les cas $t \leq 2(\log_2(a)+1)$ ■

Si toutes les opérations arithmétiques se faisaient en temps constant, le coût de l'algorithme d'Euclide serait $O(\log_2 a)$.

Mais si l'on manipule des grands nombres, ce qu'on se propose de faire, le coût des opérations arithmétiques élémentaires, c'est à dire la durée de leur exécution, dépend de la taille des opérandes. La multiplication et la division en particulier, coûtent cher. Le coût de la multiplication ou de la division, de deux entiers de même taille n [1], sur un ordinateur de bureau sans utilisation de logiciels sophistiqués est $O(n^2)$, c'est à dire qu'il est proportionnel à n^2, la constante de proportionnalité dépendant évidemment de la machine qui les exécute.

Si les entiers manipulés par calcul de $\text{pgcd}(a,b)$, restaient jusqu'au bout de même taille que la valeur initiale de b, le côut de cet algorithme serait $(\log_2 a)(\log_2 b)^2$. Mais, dans le cas de l'algorithme d'Euclide, les opérations se font sur des entiers de plus en plus petits, et on peut démontrer que le le coût du cacul de $\text{pgcd}(a,b)$ est $O\left((\log a)(\log b)\right)$.

1. La taille d'un entier x c'est le nombre de chiffres de son écriture en base 2, $\lceil \log_2(n) \rceil$

CHAPITRE 3

Groupes

3.1 Generalités

Définition 3.1. *Un groupe G est la donnée d'un ensemble G muni d'une loi de composition binaire $* : G \times G \mapsto G$ satisfaisant les propriétés suivantes :*

- *elle est associative : $x * (y * z) = (x * y) * z$ pour tous x, y, z.*
- *elle admet un élément neutre e tel que $e * x = x * e = x$ pour tout x.*
- *Tout élément est inversible : pour tout x, il existe un y tel que $x * y = y * x = e$.*

Si $x * y = y * x$ pour tous x, y, on dit que G est un groupe commutatif.

Notations :

- Notation mutiplicative : on abrège $x * y$ en xy. Pour $n \geq 0$, on définit x^n par $x^0 = 1$ et $x^{n+1} = x * x^n$, et x^{-n} est l'inverse de x^n.
- Notation additive : Lorsque la loi de composition est commutative, on peut utiliser la notation additive : le symbole opératoire est $+$, l'élément neutre est noté 0, on n'utilise pas d'abréviation pour représenter $x+y$. L'inverse de x est appelé son opposé, et noté $-x$. Enfin $x + x + \cdots + x$, où x apparait n fois, est noté $n.x$.
- *Le groupe (G, e)* est un raccourci pour *le groupe (G), d'élément neutre e.*

Définition 3.2. *Un sous-groupe de G est un sous-ensemble H de G tel que :*

- *L'élément neutre de G appartient à H.*
- *H est stable par composition : $\forall x, y \in H, x * y \in H$.*

— *H est stable par inversion :* $\forall x \in H, x^{-1} \in H$.

On vérifie simplement que l'intersection $H = \bigcap_{i \in I} H_i$ d'une famille quelconque de sous-groupes de G est encore un sous-groupe de G.

Définition 3.3. *Groupe engendré par une partie de G. Soit X un sous-ensemble du groupe G. Il existe des sous-groupes de G qui contiennent X, G tout entier par exemple. Puisque l'intersection de tous ces sous-groupes est encore un sous-groupe de G, c'est le plus petit d'entre eux. On l'appelle le sous-groupe de G engendré par X.*

Lorsque le sous-groupe engendré par le singleton $\{x\}$ coïncide avec G on dit que G est un groupe monogène et que x est un générateur de G.

Proposition 3.1. *Soit x un élément d'un groupe G. Alors, ou bien :*

— *Les x^n, pour $n \geq 0$ sont tous distincts, et dans ce cas le sous-groupe de G engendré par $\{x\}$ est l'ensemble $\{x^n \mid n \in \mathbb{Z}\}$. On dit que l'élément x est d'ordre infini.*

— *Il existe un plus petit entier $k \geq 1$ tel que $x^k = e$. Le sous-groupe de G engendré par x est alors l'ensemble de cardinal k, $\{x^i \mid 0 \leq i < k\}$. On dit que x est d'ordre fini et que le sous-groupe engendré par $\{x\}$ est un groupe cyclique d'ordre k.*

3.2 Le groupe additif $\mathbb{Z}$

Exemple : Tout entier non nul du groupe additif $\mathbb{Z}$ des entiers relatifs est d'ordre infini. Ce groupe admet deux générateurs 1 et -1.

Théorème 3.1 (Sous-groupes de $\mathbb{Z}$.)**.** *Tout sous-groupe H de $\mathbb{Z}$ est formé de l'ensemble des multiples d'un entier naturel d, c'est à dire de la forme :*

$$H = d\mathbb{Z} = \{d \cdot x \mid x \in \mathbb{Z}\}.$$

Démonstration : L'ensemble $d\mathbb{Z}$ est évidemment un sous-groupe car la somme de deux multiples de d et l'opposé d'un multiple de d sont encore des multiples de d.

Réciproquement soit H un sous de $\mathbb{Z}$. S'il est réduit à $\{0\}$ il est égal à $0\,\mathbb{Z}$. Sinon il contient un élément non nul x et même un élément strictement positf car x et $-x$ appartiennent tous deux à H. L'ensemble des éléments strictement positifs de H n'est pas vide, soit d son plus petit élément. Prouvons que tout élément x de H est multiple de d. Soient q et r le quotient et le reste de la division euclidienne de x par d :

$$x = q \cdot d + r, \quad 0 \leq r < d.$$

Le reste $r = q \cdot d$ est un entier naturel plus petit que d qui appartient à H. Et, puisque d est le plus petit entier strictement positif de H, $r = 0$. ∎

3.3 Le théorème de Lagrange

Définition 3.4 (Congruence à gauche)**.** *Soit H un sous-groupe du groupe G. On appelle congruence à gauche modulo H la relation binaire $\mathcal{R}$, définie sur G par*

$$x \mathcal{R} y \iff x^{-1}y \in H.$$

Cette relation est une relation d'équivalence, et la classe d'équivalence de x est l'ensemble $xH = \{xh \mid h \in H\}$, de même cardinal que H.

Démonstration :

1. Il faut prouver que $\mathcal{R}$ est réflexive, symétrique et transitive. Elle est réflexive parce que, pour tout x de G, $x^{-1}x$ est l'élément neutre de G qui appartient à H, elle est symétrique parce que si $x^{-1}y$ est un élément de H il en est de même de son inverse $y^{-1}x$. Et elle est transitive par ce que si $x^{-1}y$ et $y^{-1}z$ appartiennent à H il en est de même du produit $(x^{-1}y)(y^{-1}z) = x^{-1}z$.
2. y est équivalent à x s'il existe un h de H tel que $x^{-1}y = h$, soit $y = xh$. Enfin puisque $h \mapsto xh$ est une bijection de H sur xH on a $|xH| = |H|$.

Théorème 3.2. (Théorème de Lagrange) *Si G est une* groupe fini*, le cardinal de tout sous-groupe H de G est un diviseur du cardinal de G.*

Démonstration : Puisque la congruence à gauche modulo H est une relation d'équivalence sur G le cardinal de G est la somme des cardinaux des classes, tous égaux au cardinal de H donc un multiple de celui-ci.

Corollaire 3.1. *Dans un groupe fini de cardinal n et d'élément neutre e, noté multiplicativement tout élément x satisfait $x^n = e$.*

Démonstration : Soit x un élément de G. Puisque G est fini x est d'ordre fini k, et $x^k = e$. Mais k est le cardinal du sous-groupe de G engendré par x, c'est donc un diviseur de $n = \text{card}(G)$, et il existe q tel que $n = qk$, puis $x^n = (x^k)^q = e^q = e$.

3.4 Homomorphismes de groupes

Soient deux groupes G et G' dont les opérations sont notées par le même symbole $*$.

Définition 3.5. *Une application f de G dans G' est un homomorphisme si*

$$\forall x, y \in G : f(x * y) = f(x) * f(y).$$

Si $G = G'$ on dit que f est un endomorphisme de G.

Proposition 3.2. *Si $f : G \longrightarrow G'$ est un homomorphisme de (G, e) dans (G', e'), on a*

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

Démonstration :

1. Pour tout x de G, $f(x) = f(x)f(e)$ car $x = xe$. En multipliant les deux termes de cette égalité à gauche par l'inverse de $f(x)$ on obtient $e' = f(e)$.
2. L'égalité $xx^{-1} = e$ donne $f(x)f(x^{-1}) = f(e) = e'$.

Définition 3.6. *Soit f un homomorhisme de (G, e) dans (G', e'). Le noyau de f est le sous-ensemble de G, noté* $\ker(f)$ *défini par*

$$\ker(f) = \left\{x \in G \mid f(x) = e'\right\}.$$

Proposition 3.3. *Le noyau d'un homomorphisme de (G, e) dans (G', e') est un sous-groupe de G et f est une application injective si et seulement si* $\ker(f) = \{e\}$.

Démonstration : Le noyau de f n'est pas vide car $f(e) = e'$. Il est stable par composition, car si x et y appartiennent à $\ker(f)$, on a $f(xy) = f(x)f(y) = e'e' = e'$ et donc xy appartient à $\ker(f)$. Enfin il est stable par inversion car si $x \in \ker(f)$, $f(x^{-1}) = (f(x))^{-1} = e'^{-1} = e'$.

Si $\ker(f)$ n'est pas réduit à e, soit x un élément de $\ker(f)$ distinct de e. On a alors $f(x) = e' = f(e)$, e' a deux antécédents distincts, et f n'est pas injective.

Réciproquements si $\ker(f) = \{e\}$ et si $f(x') = f(x)$. En multipliant à droite les deux termes de cette égalité par $(f(x))^{-1}$ on obtient $e' = f(x')(f(x))^{-1} = f(x')f(x^{-1}) = f(x'x^{-1})$, donc $x'x^{-1} \in \ker(f)$, puis $x'x^{-1} = e$ et enfin $x' = x$.

3.5 Le groupe $\mathbb{Z}/n\mathbb{Z}$

Définition 3.7 (Congruence modulo n.)**.** *Soit $n > 1$, entier fixé. Deux entiers a et b sont congrus modulo n, et on l'écrit $a \equiv b \pmod{n}$, si et seulement si $b - a$ est multiple de n.*

La classe de a modulo n est l'ensemble des entiers a' congrus à a modulo n. C'est l'ensemble $\{a + n\mathbb{Z}\}$ des entiers obtenus en ajoutant à a un multiple de n. On le note $\overline{a}$. Chacun des élements de $\overline{a}$ est appelé un représentant de cette classe. Deux sont disjointes ou confondues. La classe d'équivalence de a coïncide avec la classe du reste de la division euclidienne de a par n.

Chaque classe d'équivalence est donc l'un des éléments de l'ensemble $\left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}$ que l'on note $\mathbb{Z}/n\mathbb{Z}$.

On définit alors une addition sur cet ensemble par $\overline{a} + \overline{b} = \overline{a+b}$. Cette définition est correcte parce que si $\overline{a} = \overline{a'}$ et $\overline{b} = \overline{b'}$, $a' - a$ et $b' - b$ sont des multiples de n, il en est de même de $(a' + b') - (a + b) = (a' - a) + (b' - b)$, donc $\overline{a' + b'} = \overline{a + b}$. Ainsi, la classe de $a + b$ ne dépend que de $\overline{a}$ et $\overline{b}$; elle ne dépend pas pas des représentants a et b choisis dans chacune des classes $\overline{a}$ et $\overline{b}$.

Définition 3.8. *Le groupe* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$ *est l'ensemble des classes d'équivalence modulo* n*, muni de l'addition* $+$ *définie par*

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

C'est un groupe commutatif de cardinal n*, engendré par* $\overline{1}$*.*

Notation : La notation $\overline{x}$ est suffisante lorsqu'il n'y a pas d'ambiguïté sur n. Si l'on manipule à la fois des classes de congruences modulo a et des classes modulo b, x mod a est la classe de x modulo a et x mod b, la classe de x modulo b.

3.6 Groupe quotient G/H

Définition 3.9. *Un sous-groupe distingué ou sous-groupe normal de* G *si, pour tout* x *de* G *et tout* h *de* H*,* xhx^{-1} *appartient aussi à* H *.*

Soit G un groupe quelconque, noté multiplicativent et H un sous-groupe de G. Soit G/H l'ensemble des classes d'équivalence de la congruence $\mathcal{R}$ de la définition 3.4 :

$$x\mathcal{R}y \iff x^{-1}y \in H.$$

Notons $\overline{x}$ la classe de de x, $\overline{x} = xH = \{xh \mid h \in H\}$. Nous voudrions définir une loi de composition $*$ sur G/H comme nous l'avons fait pour l'addition de $\mathbb{Z}/n\mathbb{Z}$, c'est à dire en posant

$$\overline{a} * \overline{b} = \overline{ab}. \tag{3.1}$$

Puisque $\overline{a} = aH$ et $\overline{b} = bH$, pour que cette définition soit correcte il faut que, pour tous h, k dans H, le produit $(ah)(bk)$ soit équivalent au produit ab c'est à dire que $(ab)^{-1}(ah)(bk) = b^{-1}hbk$ soit un élément de H. Mais puisque $k \in H$, ce produit est un élément de H si et seulement si $b^{-1}hb$ est un élément de H.

Ainsi la définition 3.1 est correcte si et seulement si G est un sous-groupe distingué de H et nous pouvons énoncer le théorème :

Théorème 3.3. *Soit* H *un sous-groupe distingué de* G*. Notons* G/H *l'ensemble des classes d'équivalence* $\overline{x} = xH$ *de la congruence définie par*

$$x \equiv y \pmod{H} \iff x^{-1}y \in H.$$

G/H *muni de la loi de composition définie par* $\overline{a} * \overline{b} = \overline{a * b}$*, est un groupe qu'on appelle le groupe quotient de* G *par* H*.*

Remarque : Nous aurions pu définir le groupe quotient G/H en considérant la congruence à droite modulo H définie par $x\mathcal{R}'y \iff xy^{-1} \in H$ et pour laquelle la classe d'équivalence de a est $Ha = \{ha \mid h \in H\}$. Aurions-nous ainsi obtenu une autre groupe ? Heureusement, non, car dire que H est un sous-groupe distingué de G, c'est dire que pour tout a de G, $aH = Ha$. Ainsi les deux choix définissent les mêmes classes, donc le même ensemble G/H et la même loi de composition.

3.7 Exposant d'un groupe

Définition 3.10 (Exposant d'un groupe)**.** *Vu le théorème de Lagrange, si G est un groupe fini de cardinal $|G|$, ce cardinal est un multiple commun des ordres de éléments de G. On définit l'exposant de G, $\exp(G)$, comme plus petit multiple commun de ces ordres :*

$$\exp(G) = \text{ppcm}\left\{\text{ordre}(x) \mid x \in G\right\}.$$

Exemple : Soit $\mathfrak{S}_3$ le groupe symétrique des permutations de $\{1,2,3\}$. Ce groupe à 6 éléments : l'identité Id est d'ordre 1, les deux cycles, $(1,2,3)$ et $(1,3,2)$ sont d'ordre 3, et enfin les 3 transpositions sont d'ordre 2. L'exposant de ce groupe est donc $\text{ppcm}(1,2,3) = 6$.

Lemme 1. *Soient x et y deux éléments du groupe G tels que $xy = yx$. S'ils sont d'ordres finis a et b premiers entre eux, leur produit $z = xy$ est d'ordre ab.*

Démonstration :

— L'ordre de z est un diviseur de ab car

$$z^{ab} = (xy)^{ab} = x^{ab}y^{ab} = (x^a)^b(y^b)^a = 1 \times 1 = 1$$

— Soit k tel que $(xy)^k = 1$. Puisque x et y commutent cela s'écrit encore $x^k = y^{-k}$, et on en déduit

$$1 = (x^a)^a = x^{ka} = y^{-ka},$$

ce qui prouve que ka est un multiple de l'ordre de y, donc un multiple de b. Mais puisque b est premier avec a et divise ka il divise k. Et donc k est un multiple de b. Par symétrie, on prouve de la même façon que k est un multiple de a. C'est donc un multiple commun de a et b donc un multiple de ab puisque ces deux nombres sont premiers entre eux.

Lemme 2. *Si G est un groupe commutatif et x, y deux éléments de G d'ordres respectifs u et v, il existe un élément de G dont l'ordre est le* ppcm *de u et v.*

Démonstration : Soit $r \in \mathbb{N}^*$ et $p_1, p_2, \ldots, p_r$ les nombres premiers distincts intervenant dans les décompositions en facteurs premiers de u ou de v. On peut écrire :

$$u = \prod_{i=1}^{r} p_i^{\alpha_i} \quad \text{et} \quad v = \prod_{i=1}^{r} p_i^{\beta_i}$$

Par définition du plus petit commun multiple :

$$\text{ppcm}(u,v) = \prod_{i=1}^{r} p_i^{\max(\alpha_i,\beta_i)},$$

où les α_i, β_i sont positifs ou nuls. On définit

$$I = \{i \in \{1, \dots, r \mid \alpha_i \geq \beta_i\}, \quad u' = \prod_{i \in I} p_i^{\alpha_i} \quad \text{et l'entier} \quad k = u/u'$$
$$J = \{i \in \{1, \dots, r \mid \alpha_i < \beta_i\}, \quad v' = \prod_{j \in J} p_j^{\beta_j} \quad \text{et l'entier} \quad m = v/v'.$$

u' divise u, v' divise v, et u', v' sont premiers entre eux. Puisque l'ordre de x est $u = ku'$, celui de $x' = x^k$ est u'. De même, l'ordre de $y' = y^m$ est v', et puisque u' et v' sont premiers entre eux, l'ordre de $x'y'$ est le produit

$$u' \cdot v' = \prod_{i \in I} p_i^{\alpha_i} \prod_{j \in J} p_j^{\beta_j} = \prod_{i=1}^{r} p_i^{\max(\alpha_i, \beta_i)} = \text{ppcm}(u, v).$$

Théorème 3.4. *Si G est un groupe commutatif il contient un élément dont l'ordre est le plus petit commun multiple de tous les ordres..*

Démonstration : Soit $G = \{x_1, x_2, \dots, x_n\}$. On définit $y_1 = x_1$. Par le lemme précédent il existe un y_2 dont l'ordre est le ppcm de $\{\text{ordre}(x_1), \text{ordre}(x_2)\}$, puis y_3 un élément dont l'ordre est le ppcm de $(\text{ordre}\, y_2, \text{ordre}(x_3))$ et ainsi de suite. A chaque étape l'ordre de y_k est le ppcm des ordres de $x_1, x_2, \dots, x_k$.

Ce théorème serait faux sans l'hypothèse de commutativité. Considérons par exemple le groupe symétrique $\mathfrak{S}_3$. Ses éléments sont d'ordre $1, 2, 3$, son exposant est donc le plus petit multiple commun de $1, 2, 3$, c'est à dire 6, mais il n'a pas délément d'ordre 6.

CHAPITRE 4

Permutations

Définition 4.1. *Soit $f : E \longleftrightarrow E$ une application d'un ensemble E dans lui-même. Une partie de E stable par f est une partie A de E qui contient son image, c'est à dire telle que $f(A) \subset A$.*

Définition 4.2. *Une permutation d'un ensemble fini E est une bijection de E sur lui-même. On note $\mathfrak{S}(E)$ l'ensemble des permutations de E. Cet ensemble, muni de l'opération de composition des applications est un groupe, dont l'élément neutre est l'application identité id_E de E dans E.*

Notation : $\mathfrak{S}_n$ désigne l'ensemble des permutations de $\{1, 2, \ldots, n\}$.

Définition 4.3. *Le support d'une permutation σ de E est le sous-ensemble de E noté $\mathrm{supp}(\sigma)$, défini par $\mathrm{supp}(\sigma) = \{x \in E \mid \sigma(x) \neq x\}$. C'est une partie de E stable par σ.*

Démonstration : Soit $x \in \mathrm{supp}(\sigma)$, et $y = \sigma(x)$. Si y n'appartenait pas à $\mathrm{supp}(\sigma)$ on aurait $\sigma(y) = y$ et y aurait 2 antécédents x et y. ∎

Exemple : Voici par exemple un élément de $\mathfrak{S}_{10}$, une permutation de $\{1, 2, \ldots, 10\}$, définie par le tableau de se valeurs :

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 1 & 4 & 8 & 3 & 7 & 5 & 9 & 2 \end{pmatrix}.$$

Elle a deux points fixes, 4 et 7 et 9. Son support est donc $\mathrm{supp}(\sigma_1) = \{1, 2, 3, 5, 6, 8, 10\}$.

Proposition 4.1. *Si σ_1 et σ_2 sont deux permutations de support disjoints elles commutent, c'est à dire que $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.*

Démonstration : Si x n'appartient pas à $\mathrm{supp}(\sigma_1) \cup \mathrm{supp}(\sigma_2)$, on a évidemment $\sigma_2 \circ \sigma_1(x) = x$.

Si $x \in \mathrm{supp}(\sigma_1)$, par la définition 4.3 il en est de même de $\sigma_1(x)$, qui n'appartient donc pas à $\mathrm{supp}(\sigma_2)$. On a donc $\sigma_2(\sigma_1(x)) = \sigma_1(x)$. Dans l'autre sens, puisque $x \in \mathrm{supp}(\sigma_1)$ il n'appartient pas $\mathrm{supp}(\sigma_2)$ et donc $\sigma_2(x) = x$, puis $\sigma_1 \circ \sigma_2(x) = \sigma_1(x)$.

Si $x \in \mathrm{supp}(\sigma_2)$ on procède de la même façon, en inversant les rôles de σ_1 et σ_2. ■

Définition 4.4. *Soit $k \geq 2$, $x_1, x_2, \cdots, x_k$ une suite finie d'éléments distincts de E et σ l'application de support $\{x_1, x_2, \cdots, x_k\}$, qui envoie x_i sur x_{i+1} pour $i < k$ et x_k sur x_1. Cette application est notée $(x_1, x_2, \ldots, x_k)$ et on dit que c'est un cycle d'ordre k.*

- *Une transposition est un cycle d'ordre 2, $(x_1, x_2) = (x_2, x_1)$ qui envoie x_1 sur x_2 et x_2 sur x_1.*
- *Une permutation circulaire de E est un cycle de support E tout entier.*

Proposition 4.2. *Le cycle $\sigma = (x_1, x_2, \ldots, x_k)$ est un élément d'ordre k du groupe $\mathfrak{S}(E)$, c'est à dire que k est le plus petit entier > 0 tel que $\sigma^k = \mathrm{id}_E$.*

Définition 4.5. *Orbite d'un élément de E. Soit σ une permutation de E et x un élément de E. L'orbite de x sous l'action de σ est la plus petite partie de E, $\mathrm{orb}(x)$, contenant x et stable par σ.*

Cette définition est correcte : il existe des partie stables de E contenant x, E tout entier par exemple. L'intersection de toutes ces parties est encore une partie stable de E contenant x, et c'est la plus petite d'entre-elles.

Proposition 4.3. *Soit σ une permutation de E et x un élément de E. Soit $F = \mathrm{orb}(x)$ l'orbite de x. La restriction de σ à F est une permutation circulaire de F.*

Démonstration : Soit la suite $(x_n)_{n\geq 0}$ définie par $x_0 = x$ et $x_n = \sigma(x_{n-1})$ pour $n \geq 1$, c'est à dire la suite $(\sigma^n(x))_{n\geq 0}$. Puisqu'elle prend ses valeurs dans l'ensemble fini E, celles-ci ne sont pas toutes distinctes. Soit k le plus petit entier tel qu'il existe $i < k$ avec $x_i = x_k$. Alors $i = 0$ sinon cette égalité s'écrirait $\sigma(x_{i-1}) = \sigma(x_{k-1})$, et, puisque σ est injective on en déduirait $x_{i-1} = x_{k-1}$ contredisant la minimalité de k. On a donc $x_0 = x_k = \sigma(x_{k-1})$, et l'ensemble $F = \{x_0, \ldots, x_{k-1}\}$ est stable par σ. Par définition de la stabilité, une partie stable qui contient $x = x_0$ contient tous les éléments de F. Enfin, par définition de la suite (x_n) et de l'entier k, $\sigma|_F$ est le cycle $(x, x_1, \ldots, x_{k-1})$. ■

Théorème 4.1. *Quelle que soit la permutation $\sigma \in \mathfrak{S}(E)$ distincte de id_E il existe un unique ensemble de cycles $c_1, c_2, \ldots c_r$ de supports deux à deux disjoints tels que $\sigma = c_1 \circ c_2 \cdots \circ c_r$.*

Démonstration : Par récurrence sur le cardinal de $\mathrm{supp}(\sigma)$. Si ce cardinal est 0 c'est que $\sigma = \mathrm{id}_E$. Sinon, soit x un élément du support de σ.

1. Soit k le cardinal de l'orbite de x, et c_1 le cycle $(x, \sigma(x), \ldots, \sigma^{k-1}(x))$. Alors c_1 et σ coïncident sur $\mathrm{orb}(x)$.
2. Considérons la permutation $\sigma_1 = c_1^{-1} \circ \sigma$. Si y appartient à $\mathrm{orb}(x)$ on a $\sigma_1(y) = \sigma(y)$ par définition de c_1 et donc $\sigma_1(y) = c_1^{-1}(\sigma(y)) = c_1^{-1}(c_1(y)) = y$.
3. Si y n'appartient pas à l'orbite de x, $\sigma(y)$ n'y appartient pas non plus, et puisque cette orbite est le support de c_1 de c_1, $\sigma_1(y) = \sigma(y)$.

Le support de σ_1 est donc $\mathrm{supp}\,\sigma - \mathrm{orb}(x) \subsetneq \mathrm{supp}(\sigma)$. Par hypothèse de récurrence σ_1 est un produit de cycles deux à deux disjoints $\sigma_1 = c_2 \circ c_3 \cdots \circ c_q$ soit $c_1^{-1} \circ \sigma = c_2 \circ c_3 \cdots \circ c_q$ et donc $\sigma = c_1 \circ c_2 \cdots \circ c_q$. ■

Exemple 1. *Considérons la permutation σ donnée par son tableau de valeurs*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 2 & 4 & 7 & 9 & 8 & 5 & 6 & 1 \end{pmatrix}.$$

Les égalités $\sigma(1) = 3, , \sigma(3) = 2, \sigma(2) = 10$ et $\sigma(10) = 2$ donnent l'orbite $\mathrm{orb}(1) = \{1, 2, 2, 10\}$ et le cycle $c_1 = (1, 2, 2, 10)$. L'égalité $\sigma(4) = 4$ donne $\mathrm{orb}(4) = 4$. Les égalités $\sigma(5) = 7, \sigma(7) = 8, \sigma(8) = 5$ donnent $\mathrm{orb}(5) = \{5, 7, 8\}$ et le cycle $c_2 = (5, 7, 8)$. Enfin $\sigma(9) = 6$ et $\sigma(9) = 6$ donne $\mathrm{orb}(6) = \{6, 9\}$ et le cycle $c_3 = (6, 9)$ avec la factorisation

$$\sigma = (1, 3, 2, 10) \circ (5, 7, 8) \circ (6, 9).$$

Théorème 4.2. *Toute permutation est un produit de transpositions.*

Démonstration : Puisque toute permutation est un produit de cycles il suffit de démontrer que tout cycle est un produit de transpositions. Ce qui est vrai car

$$(x_1, x_2, \ldots, x_k) = (x_1, x_2) \circ (x_2, x_3) \circ \cdots \circ (x_{k-1}, x_k).$$

■

Signature d'une permutation de $\mathfrak{S}_n$

Une paire est un ensemble de cardinal 2. Notons $\mathcal{P}_n$ l'ensemble des paires d'éléments de l'ensemble $\{1, 2, \ldots, n\}$.

Soit σ un élément de $\mathfrak{S}_n$, c'est à dire une permutation de l'ensemble $\{1, 2, \ldots, n\}$. On dit que la paire $\{i, j\}$ est une inversion de σ si $\sigma(j) - \sigma(i)$ et $j - i$ sont de signes opposés.

Définition 4.6. *La signature d'une permutation $\sigma \in \mathfrak{S}_n$ est $(-1)^N$ où N est le nombre des inversions de σ, qu'on note $\varepsilon(\sigma)$.*

Proposition 4.4. *La signature de σ est égale au produit :*

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}. \tag{4.1}$$

Démonstration : Puisque, pour $x \neq 0$, le signe de x est $\operatorname{sgn}(x) = x/|x|$, la signature de σ est :

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

En définissant $\Phi(\{i,j\}) = \{\sigma(i),\sigma(j)\}$, qui est une bijection dont l'inverse est $\{x,y\} \mapsto \{\sigma^{-1}(x),\sigma^{-1}(y)\}$, et en notant $f(\{i,j\}) = |j-i|$, le dernier dénominateur s'écrit encore :

$$D = \prod_{1\leq i<j\leq n} |\sigma(j)-\sigma(i)| = \prod_{\{i,j\}\in\mathcal{P}_n} f(\Phi(\{i,j\})) = \prod_{\{i,j\}\in\mathcal{P}_n} f(\{i,j\})$$

car, puisque Φ est bijective, $\{\Phi(\{i,j\}) \mid \{i,j\} \in \mathcal{P}_n\}$ est égal à $\mathcal{P}$. D'où $D = \prod_{1\leq i<j\leq n}(j-i)$. ∎

Théorème 4.3. *L'ensemble $\mathfrak{S}_n$, muni de l'opération de composition des applications $\circ$ est un groupe, ainsi que l'ensemble $\{-1,1\}$ muni de l'opération de multiplication des entiers, et la signature $\sigma \mapsto \varepsilon(\sigma)$ est un morphisme du premier dans le second :*

$$\forall \sigma_1,\sigma_2 \in \mathfrak{S}_n, \quad \varepsilon(\sigma_2\circ\sigma_1) = \varepsilon(\sigma_1)\times\varepsilon(\sigma_2).$$

Démonstration : On a :

$$\begin{aligned}
\varepsilon(\sigma_2\circ\sigma_1) &= \prod_{1\leq i<j\leq n} \frac{\sigma_2(\sigma_1)(j)-\sigma_2(\sigma_1(i))}{j-i} \\
&= \prod_{1\leq i<j\leq n} \frac{\sigma_2(\sigma_1)(j)-\sigma_2(\sigma_1(i))}{\sigma_1(j)-\sigma_1(i)} \times \prod_{1\leq i<j\leq n} \frac{\sigma_1(j)-\sigma_1(i)}{j-i} \\
&= \left(\prod_{1\leq i<j\leq n} \frac{\sigma_2(\sigma_1)(j)-\sigma_2(\sigma_1(i))}{\sigma_1(j)-\sigma_1(i)}\right) \times \varepsilon(\sigma_1)
\end{aligned}$$

par (4.1) appliquée à σ_1.

Définissons maintenant $g(\{k,l\}) = \dfrac{\sigma_2(k)-\sigma_2(l)}{k-l}$, de sorte que, encore par (4.1), $\varepsilon(\sigma_2) = \prod_{\{i,j\}\in\mathcal{P}_n} g(\{i,j\})$. On peut écrire ensuite

$$\prod_{1\leq i<j\leq n} \frac{\sigma_2(\sigma_1)(j)-\sigma_2(\sigma_1(i))}{\sigma_1(j)-\sigma_1(i)} = \prod_{\{i,j\}\in\mathcal{P}_n} g(\{\sigma_1(j),\sigma_1(i)\}) = \prod_{\{i,j\}\in\mathcal{P}_n} g(\Phi(\{i,j\}))$$

où Φ est l'application $\{i,j\} \mapsto \{\sigma_1(j),\sigma_1(i)\}$, qui est trivialement bijective, d'après le paragraphe précédent, et donc

$$\prod_{1\leq i<j\leq n} \frac{\sigma_2(\sigma_1)(j)-\sigma_2(\sigma_1(i))}{\sigma_1(j)-\sigma_1(i)} = \prod_{\{i,j\}\in\mathcal{P}_n} g(\Phi(\{i,j\})) = \prod_{\{i,j\}\in\mathcal{P}_n} g(\{i,j\})) = \varepsilon(\sigma_2).$$

∎

Définition 4.7. *Le sous-ensemble de $\mathfrak{S}_n$ formé des permutations de signature 1 est un sous groupe qu'on appelle le groupe alterné d'indice n, noté A_n.*

Théorème 4.4. *La signature d'une transposition est -1.*

Démonstration : Considérons les inversions de la transposition $(4,8)$ de $\mathfrak{S}_{10}$. Il faut compter les couples $(k<l)$ qui sont une inversion. Si k et l n'appartiennent pas à $\{4,8\}$ on a $(\sigma(k),\sigma(l))=(k,l)$ donc pas d'inversion. Il suffit donc de considérer les couples de la forme $(4,l),(4,8),(k,4)$.

1	2	3	4	5	6	7	8	9	10

— Les couples $(4,5),(4,6),(4,7)$ d'images $(8,5),(8,6),(8,7)$ apportent 3 inversions.
— $(4,8)$, d'image $(8,4)$ apporte une inversion.
— Les couples $(5,8),(6,8),(7,8)$ d'images $(5,4),(6,4),(7,4)$ apportent 3 inversions.

Dans le cas général, on montre de la même façon on voit que, , le nombre d'inversions de la transposition (i,j) est le nombre impair $1+2(j-i)$. ■

Corollaire 4.1. *La signature du cycle $(x_1,x_2,\dots,x_p)$ est $(-1)^{p-1}$.*

Démonstration : Vu l'égalité $(x_1,x_2,\dots,x_p)=(x_1,x_2)\circ\cdots\circ(x_{p-1},x_p)$ ce cycle est un produit de $p-1$ transpositions. ■

Proposition 4.5. *Soit σ une permutation égale au produit $c_1\circ c_2\circ\cdots\circ c_k$ de cycles de supports disjoints d'ordres respectifs $a_1,a_2,\dots,a_k$. Alors :*

— *Sa signature est : $\varepsilon(\sigma)=\prod_{i=1}^{k}(-1)^{a_i-1}$.*
— *Son ordre, le plus petit entier $k>0$ tel que $\sigma^k=\mathrm{Id}$, est le plus petit multiple commun des a_i, $1\le i\le k$.*

Démonstration : Le premier point résulte immédiatement du corollaire 4.1.

Quand au deuxième point il résulte de ce que, puisque $c_1,\cdots c_k$ sont de supports disjoints, ils commutent deux à deux, ce qui permet déécrire :

$$\sigma^m=c_1^m\circ c_2^m\circ\cdots\circ c_k^m.$$

De plus les supports des c_i^m sont tous disjoint (car $\mathrm{supp}(c_i^m)\subset\mathrm{supp}(c_i)$). Leur produit est donc égal à l'identité si et seulement si chacun d'eux est l'identite, c'est à dire si m est un multiple de a_i pour tout i. ■

Exemple 2. *Considérons la permutation σ de l'Exemple 1. Puisque elle est le composé $\sigma=(1,3,2,10)\circ(5,7,8)\circ(6,9)$, sa signature est le produit des 3 signatures $\varepsilon(\sigma)=(-1)^3\times(-1)^2\times(-1)=1$.*

Et son ordre est le ppcm de $4,3,2$ c'est à dire 12.

Exercice 4.1. *Calculer la décomposition en produit de cycles disjoints, la signature et l'ordre de la permutation σ de $\mathfrak{S}_{10}$ donnée par le tableau de ses valeurs*

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\2&10&1&4&7&9&8&5&3&9\end{pmatrix}.$$

CHAPITRE 5

Anneaux et corps

Définition 5.1. *Un anneau est un ensemble A muni de deux opérations une addition $+$ et une multiplication $\times$ satisfaisant les propriétés suivantes :*

1. *A muni de l'addition est un groupe commutatif d'élément neutre 0.*
2. *La multiplication est associative, possède un élément neutre 1, différent de 0, et elle est distributive par rapport à l'addition, c'est-à-dire que,*

$$\forall x, y, z \in A, \quad x \times (y + z) = (x \times y) + (x \times z).$$

La multiplication n'est pas nécessairement commutative. Si elle l'est on dit que A est un anneau commutatif.

Exemple : L'ensemble $\mathbb{Z}$ des entiers relatifs est un anneau commutatif.

Notation : On abrège en général le produit $a \times b$ en ab.

Définition 5.2 (Groupe multiplicatif des éléments inversibles)**.** *On dit que l'élément a de l'anneau A est inversible s'il admet un inverse pour la multiplication c'est à dire s'il existe $b \in A$ tel que $a \times b = b \times a = 1_A$. Cet inverse est noté a^{-1}.*

L'ensemble des éléments inversibles de A, muni de la seule multiplication est un groupe qu'on note $A^\times$.

Démonstration : Cet ensemble n'est pas vide car il contient 1_A et il est stable par multiplication. En effet si a et b sont inversibles d'inverses a' et b', $b'a'$ est l'inverse de ab car

$$(b'a')(ab) = b'(a'(ab)) = b'((a'a)b) = b'(1_A b) = b'b = 1_A.$$

et, de même $(ab)(b'a') = 1_A$. ■

Remarque : Dans le cas d'un anneau non commutatif, il est important de noter que l'inverse d'un produit est le produit des inverses de ses facteurs mais en les permutant.

Exercice 5.1. *Démontrer que si A est un anneau, $x \times 0 = 0 \times x = 0$ pour tout x, et en déduire que 0 n'est pas inversible.*

Solution : Soit $x_0 = x \times 0$. Par distributivité $x_0 + x_0 = x \times 0 + x \times 0 = x \times (0+0) = x \times 0 = x_0$. En ajoutant l'opposé de x_0 aux deux membres de cette égalité on obtient $(-x_0 + x_0) + x_0 = -x0 + x_0$ c'est à dire $0 + x_0 = 0$ et donc $x_0 = 0$. On montre de la même façon que $0 \times x = 0$.

Si x était un inverse de 0 on aurait donc $0 = x \times 0 = 1$ ce qui est exclu par la définition d'un anneau, 5.1. ■

Définition 5.3. *Un morphisme de l'anneau A dans l'anneau B est une application f de A dans B qui envoie l'élément unitaire de A sur l'élément unitaire de B, $f(1_A) = f(1_B)$, et telle que, pour tous x, y de A :*

$$f(x+y) = f(x) + f(y) \quad \text{et} \quad f(x \times y) = f(x) \times f(y).$$

Un isomorphisme d'anneaux est un morphisme qui est une bijection.

Proposition 5.1. *Si $f : A \longrightarrow B$ est un morphisme d'anneau, l'image d'un élément inversible x de A est un élement inversible de B, et $f(x)^{-1} = f(x^{-1})$.*

Démonstration : Soit $x \in A^\times$, et y son inverse. Puisque f est un morphisme, on a $1_B = f(1_A) = f(xy) = f(x)f(y)$. Ce qui montre que $f(x)$ et que son inverse est $f(y) = f(x^{-1})$. ■

Corollaire 5.1. *Si f est un isomorphisme de l'anneau A sur l'anneau B, $B^\times = f(A^\times)$.*

Définition 5.4 (corps)**.** *Un corps est un anneau satisfaisant de plus la propriété suivante : Tout élément différent de 0 est inversible pour la multiplication.*

Dire que A est c'est donc dire que $A^\times = A - \{0\}$.

Définition 5.5. *Un élément non nul $a \in A$ est appelé un diviseur de 0 s'il existe $b \in A$, $b \neq 0$ tel que $ab = 0$.*

Définition 5.6. *On dit qu'un anneau A est intègre s'il ne contient pas de diviseur de 0, c'est à dire si le produit de deux éléments non nuls n'est jamais nul.*

Proposition 5.2. *Pour qu'un anneau soit un corps il est nécessaire mais non suffisant qu'il soit intègre.*

Démonstration : Si A n'est pas intègre, il existe a et b non nuls tels que $a \times b = 0$. Si a admettait un inverse a' on en déduirait que $0 = a' \times 0 = a' \times (a \times b) = (a' \times a) \times b = 1 \times b = b$. Ce qui contredit l'hypothèse $b \neq 0$.

Mais l'intégrité de l'anneau A ne suffit pas à faire de celui-ci un corps. $\mathbb{Z}$ par exemple est intègre mais tout $x \neq \pm 1$ n'est pas inversible. ■

Théorème 5.1. *Si K est un corps fini commutatif, l'ensemble de ses éléments non nuls muni de la multiplication est un groupe cyclique.*

Démonstration : Soit n le cardinal du groupe multiplicatif $K^\star$. Par le théorème de Lagrange tout élément de $K^\star$ satisfait $x^n = 1$, et, par définion, de l'exposant e, on a $e \leq n$. Mais,puisque les n éléments de $K^\star$ sont racines du polynôme $X^e - 1$, on a $e \geq n$. Et, par le théorème 3.4 il existe un élément d'ordre n. ■

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

Rappelons que le groupe additf $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des classes

$$\left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}.$$

muni de l'addition définie par $\overline{a} + \overline{b} = \overline{a+b}$.

On vérifie qu'on définit bien une loi de composition en posant $\overline{a} \times \overline{b} = \overline{a \times b}$, que cette opération est associative, distributive par rapport à l'addition et admet un élément neutre $1 = \overline{1}$, ce qui établit la proposition :

Proposition 5.3. *Pour tout entier $n \geq 2$, $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication définie par $\overline{a} \times \overline{b} = \overline{a \times b}$, est un anneau commutatif de cardinal n.*

Remarque : Pour $n = 1$, toutes les propriétés d'un anneau sont satisfaites sauf une, $0 \neq 1$, car dans ce cas $\mathbb{Z}/n\mathbb{Z}$ est réduit au singleton $\{0\}$ qui est élément neutre de l'addition et de la multiplication.

Le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 5.4. *L'élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si a est premier avec n. Autrement dit :*

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \mid a \in \mathbb{Z}, \operatorname{pgcd}(a, n) = 1\}.$$

Démonstration : C'est une conséquence immédiate du théorème de Bezout. En effet, $\overline{a}$ est inversible si et seulement si il existe u tel que $\overline{a} \times \overline{u} = \overline{1}$, autrement dit s'il existe u et v tels que $au - 1 = nv$, soit $au - nv = 1$. ■

Définition 5.7. *L'indicatrice d'Euler est la fonction $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ qui renvoie $\varphi(n) = \operatorname{card}(\mathbb{Z}/n\mathbb{Z})^\times$, le nombre des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Puisque 0 n'est jamais inversible on a toujours $\varphi(n) \leq n - 1$.*

Théorème 5.2. *Soit a premier avec n et φ l'indicatrice d'Euler. Alors $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Démonstration : C'est le théorème de Lagrange appliqué au groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ dont le cardinal est $\varphi(n)$. ■

Théorème 5.3. *L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps, noté $\mathbb{F}_p$, si et seulement si p est premier.*

Démonstration : Si n n'est pas premier, il existe $2 \leq a \leq b < n$ avec $ab = n$. On a donc $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$ et $\overline{a} \times \overline{b} = \overline{n} = 0$. L'anneau $\mathbb{Z}/n\mathbb{Z}$ n'est donc pas intègre.

Si p est premier, tous les entiers $1 \leq a \leq p-1$ sont inversibles car premiers avec p, tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont donc inversibles. ■

5.2 Le groupe multiplicatif $\mathbb{F}_p^\times$

Pour p premier on note $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$ l'ensemble des éléments non nuls de $\mathbb{F}_p$. Cet ensemble muni de la multiplication est un groupe. Puisqu'il est de cardinal $p-1$, tout élément a de ce groupe satisfait $a^{p-1} = 1$. On a donc le théorème suivant.

Théorème 5.4 (Petit théorème de Fermat)**.** *Pour tout premier p et tout a non multiple de p on a*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{5.1}$$

Théorème 5.5 (Théorème de Wilson)**.** *Pour que p soit premier, il faut et il suffit que*

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

Démonstration : Si p n'est pas premier $p = ab$, $2 \leq a \leq b \leq p-1$. Il en résulte que $(p-1)!$ est un multiple de $ab = p$ donc congru à 0 modulo p.

Si p est premier les seuls éléments de $\mathbb{Z}/p\mathbb{Z}$ égaux à leur inverse sont $\overline{1}$ et $\overline{-1} = \overline{p-1}$. En effet l'équation $x^2 = \overline{1}$ s'écrit encore $(x-\overline{1})(x+\overline{1}) = 0$ qui implique $x = \overline{1}$ ou $x = \overline{-1}$. Réordonnons alors les termes du produit $1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$ en plaçant en première position 1 et $p-1$ et plaçant chacun des autres entiers à côté de son inverse modulo p, on obtient la congruence :

$$(p-1)! \equiv 1 \cdot (-1) \cdot (x_1 \cdot x_1^{-1}) \cdot \ldots (x_k \cdot x_k^{-1}) \equiv -1 \pmod{p}.$$

■

Le théorème suivant est un cas particulier du théorème 5.1.

Théorème 5.6 ($\mathbb{F}_p^\times$ est cyclique)**.** *Pour tout p premier le groupe multiplicatif $\mathbb{F}_p^\times$ des éléments non nuls de $\mathbb{F}_p$ est un groupe cyclique.*

Exemple : 3 est un générateur de $F_7^\times$ car, modulo 7,

$$1 \equiv 3^0,\ 2 \equiv 3^2,\ 3 \equiv 3^1,\ 4 \equiv 3^4,\ 5 \equiv 3^5,\ 6 \equiv 3^3.$$

5.3 Produit cartésien d'anneaux

Définition 5.8. *Soit A_1 et A_2 deux anneaux. L'ensemble $A = A_1 \times A_2$ muni des opérations $+$ et $\times$ définies par*

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

est un anneau qu'on appelle le produit des anneaux A_1 et A_2. L'élément neutre de l'addition est $0_A = (0_{A_1}, 0_{A_2})$ et l'élément neutre de la multiplication est $1_A = (1_{A_1}, 1_{A_2})$.

Proposition 5.5. *L'élément $(x_1, x_2) \in A_1 \times A_2$ est inversible si et seulement si x_1 est un élément inversible de A_1 et x_2 un élément inversible de A_2. Autrement dit*

$$(A_1 \times A_2)^\times = A_1^\times \times A_2^\times.$$

Démonstration : Soit $(x_1, x_2) \in A$. Il est inversible si et seulement si il existe (y_1, y_2) tels que $(x_1, x_2) \times (y_1, y_2) = (x_1 y_1, x_2 y_2) = 1_A = (1_{A_1}, 1_{A_2})$, c'est à dire si et seulement si il existe (y_1, y_2) tels que $x_1 y_1 = 1$ et $x_2 y_2 = 1$, donc si et seulement si $x_1 \in A_1^\times$ et $x_2 \in A_2^\times$ ∎

CHAPITRE 6

Théorème des restes chinois

Lemme 3. *Si le système de congruences*

$$\begin{cases} x & \equiv & a & \pmod{p} \\ x & \equiv & b & \pmod{q} \end{cases}$$

a des solutions, soit x_0 l'une d'entre elles. Il est alors équivalent à l'unique congruence $x \equiv x_0 \pmod{\text{ppcm}(p,q)}$.

Si p et q sont premiers entre eux, il a des solutions pour tout choix de a et b, et il est donc équivalent à une unique congruence modulo pq.

Démonstration : Si x_0 est une solution, x en est une autre si et seulement si $x \equiv a \equiv x_0 \pmod{p}$, et $x \equiv b \equiv x_0 \pmod{q}$, ce qui équivaut à $x - x_0 \equiv 0 \pmod{p}$ et $x - x_0 \equiv 0 \pmod{q}$; c'est dire que $x - x_0$ est un multiple commun de p et q, ou encore que $x - x_0$ est un multiple du $\text{ppcm}(p,q)$.

Supposons p et q premiers entre eux. Alors x est solution de la première congruence si et seulement si $x = a + kp$, avec $k \in \mathbb{Z}$. Pour qu'il soit solution de la deuxième congruence il faut et il suffit que $a + kp \equiv b \pmod{q}$, soit $pk \equiv b - a \pmod{q}$. Puisque p, q sont premiers entre eux, il existe u et v tels

$$up + vq = 1$$

ce qui implique $bup + bvq = b$ et donc $bup \equiv b \pmod{q}$. On obtient donc une solution $x = a + kp$ en choissant $k = bu$. On peut expliciter cette solution en calculant u par l'algorithme d'Euclide étendu appliqué au couple (p,q) qui renvoie le couple (u,v). ■

De ce lemme on déduit immédiatement par récurrence le théorème suivant.

Théorème 6.1 (Le théorème des restes chinois). *Si $q_1, q_2, \ldots, q_r$ sont deux à deux premiers entre eux, le système de congruences*

$$\begin{cases} x & \equiv & a_1 & \pmod{q_1} \\ x & \equiv & a_2 & \pmod{q_2} \\ & \vdots & & \\ x & \equiv & a_r & \pmod{q_r} \end{cases} \tag{6.1}$$

est équivalent à une unique congruence

$$x \equiv a \pmod{q_1 q_2 \ldots q_r}$$

Démonstration : Si r est plus grand que 1 on résoud d'abord le système réduit aux deux premières congruences. Celles-ci sont alors remplacées par une unique congruence modulo $q_1 q_2$. On continue ainsi tant qu'il reste plus d'une congruence. ∎

Autre démonstration du théorème des restes chinois

En utilisant la notion de produit d'anneau, on peut donner une démonstration très rapide du théorème des restes chinois.

Proposition 6.1. *Si a et b sont premiers entre eux l'application*

$$\begin{array}{rccc} f: & (\mathbb{Z}/ab\mathbb{Z}) & \longrightarrow & (\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}) \\ & x \bmod ab & \longmapsto & (x \bmod a, x \bmod b) \end{array}$$

est bien définie, et c'est un isomorphisme d'anneau.

Démonstration : D'abord, cette définition est sans ambiguïté, car si x et x' sont deux représentants de la classe $x \bmod ab$, leur différence $x' - x$ est un multiple de ab donc un multiple de a et un multiple de b ce qui implique $x \bmod a = x' \bmod a$ et $x \bmod b = x' \bmod b$.

On vérifie très simplement que f est un morphisme d'anneau. De plus, si $f(x \bmod ab) = 0$, $x \bmod a$ et $x \bmod b$ sont nuls, donc x est un multiple de a et un multiple de b, c'est à dire un multiple de ab car ces deux nombres sont premiers entre eux, et donc $x \bmod ab = 0$. Le noyau de f est donc nul et f est une injection.

Mais puisque les deux anneaux $(\mathbb{Z}/ab\mathbb{Z})$ et $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$ sont de même cardinal fini ab, f est une bijection. Elle est donc surjective, et quels que soient les entiers x et y, il existe z tel que $f(z \bmod ab) = (z \bmod a, z \bmod b) = (x \bmod a, y \bmod b)$, c'est à dire tel que $z \equiv x \bmod a$ et $z \equiv y \bmod b$. ∎

6.1 Application à l'indicatrice d'Euler

Théorème 6.2. *L'indicarice d'Euler est une fonction arithmétique multiplica tive, c'est à dire que, pour tout couple (a, b) d'entiers premiers entre eux $\varphi(ab) = \varphi(a)\varphi(b)$.*

Démonstration : Considérons à nouveau l'isomophisme f défini ci dessus. Puisque c'est un isomorphisme, l'image de $(\mathbb{Z}/ab\mathbb{Z})^\times$ est l'ensemble des éléments inversibles de l'anneau produit $(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z})$, c'est à dire $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$, et donc $\varphi(ab) = \varphi(a)\varphi(b)$. ■

Corollaire 6.1. *La fonction d'Euler possède les propriétés suivantes :*

1. *Si p est premier $\varphi(p) = p - 1$.*
2. *Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ alors $\varphi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{\alpha_i - 1} = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$*

Démonstration :

1. Si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps de cardinal p et ses $p-1$ éléments non nuls sont inversibles.
2. Puisque φ est multiplicative et les $p_i^{\alpha_i}$ deux à deux premiers entre eux on a $\varphi(n) = \prod_{i=1}^{k} \varphi(p^{\alpha_i})$. Or $\varphi(p^\alpha)$ est le nombre des inversibles de l'anneau$\mathbb{Z}/p^\alpha\mathbb{Z}$.

   Ce nombre est le cardinal de l'intervalle $[\![0, p^\alpha - 1]\!]$ moins le nombre des multiples de p appartenant à cet intervalle, c'est à dire $p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

■

CHAPITRE 7

Symbole de Jacobi

7.1 Le symbole de Legendre

Définition 7.1. *Soit n un entier naturel non nul. On dit que l'entier relatif a est un résidu quadratique modulo n s'il existe un entier x tel que*

$$x^2 \equiv a \pmod{n},$$

c'est à dire si l'élément $\overline{a} = \overline{x}^2$ de $\mathbb{Z}/n\mathbb{Z}$ est un carré.

Proposition 7.1. *Il y a exactement $(p-1)/2$ carrés non nuls dans $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration : Tout élément de $\mathbb{Z}/p\mathbb{Z}$ est la classe d'un $x \in [\![-(p-1)/2, (p-1)/2]\!]$. Puisque le carré de $-x$ est le même que celui de x, chaque carré non nul s'écrit $\overline{x}^2$ avec $x \in [\![1, (p-1)/2]\!]$, et cette écriture est unique car la congruence $x^2 \equiv x'^2 \pmod{p}$ s'écrit

$$(x'-x)(x'+x) \equiv 0 \pmod{p}$$

et implique $x = x'$ ou $x' + x = kp \geq p$, ce qui est incompatible avec $x, x' \leq (p-1)/2$. ■

Définition 7.2. *Le symbole de Legendre de a modulo p, noté $\left(\frac{a}{p}\right)$ est défini pour tout entier a et tout nombre premier p impair, par*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \text{ est un multiple de } p \\ +1 \text{ si } a \text{ non multiple de } p \text{ est un carré modulo } p \\ -1 \text{ si } a \text{ non multiple de } p \text{ n'est pas un carré modulo } p \end{cases}$$

Théorème 7.1. *Le critère d'Euler. Si p est un nombre premier impair n*

$$\forall a \in \mathbb{Z}, \quad \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \tag{7.1}$$

Démonstration : Si a est multiple de p, $\left(\frac{a}{p}\right) = 0$, et $a \equiv 0 \pmod{p}$. Suppsons donc a non multiple de p.

Si $a \equiv x^2 \pmod{p}$ est un résidu quadratique, $a^{(p-1)/2}$ est congru à x^{p-1}, donc à 1 grâce au petit théorème de Fermat.

Si a n'est pas un carré modulo p, pour tout x non mutiple de p, l'équation $xy \equiv a \pmod{p}$ possède une unique solution y modulo p, $y = x^{-1}a$, où x^{-1} est un inverse de x modulo p. Et cette solution y n'est pas congrue à x modulo p car a n'est pas un carré modulo p. En regroupant ainsi les $p-1$ termes du produit $(p-1)!$ en $(p-1)/2$ paires $\{x, y\}$, solutions de $xy \equiv a \pmod{p}$, On obtient

$$(p-1)! \equiv (x_1 \cdot y_1) \cdot (x_2 \cdot y_2) \cdots (x_{(p-1)/2}, y_{(p-1)/2}) \equiv a^{(p-1)/2}.$$

et la conclusion car, grâce au théorème de Wilson, $(p-1)! \equiv -1 \pmod{p}$. ■

Proposition 7.2. *Le symbole de legendre est multiplicatif en a, c'est à dire que, pour tous a, b*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Démonstration : Cela résulte immédiatement du critère d'Euler, qui donne

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

■

Proposition 7.3 (Lemme de Zolotarev.)**.** *Soit Soit p un nombre premier impair et a non multiple de p. Puisque $\overline{a}$ est inversible, la multiplication par $\overline{a}$, $\mu_{\overline{a}} : x \longrightarrow \overline{a}x$, est une permutaion de $(\mathbb{Z}/p\mathbb{Z})^\times$, et le symbole de Legendre $\left(\frac{a}{p}\right)$ est la signature de cette permutation :*

$$\left(\frac{a}{p}\right) = \varepsilon(\mu_{\overline{a}}).$$

Démonstration : On définit les applications ψ et $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{-1, 1\}$, par $\psi(\overline{a}) = \left(\frac{a}{p}\right)$ et $\phi(\overline{a}) = \varepsilon(\mu_{\overline{a}})$. La première, ψ_a est multiplicative par multiplicativité en a de $\left(\frac{a}{p}\right)$. La seconde, ϕ est, elle aussi, multiplicative, car la signature de $\mu_{\overline{ab}} = \mu_{\overline{a}} \circ \mu_{\overline{b}}$ est

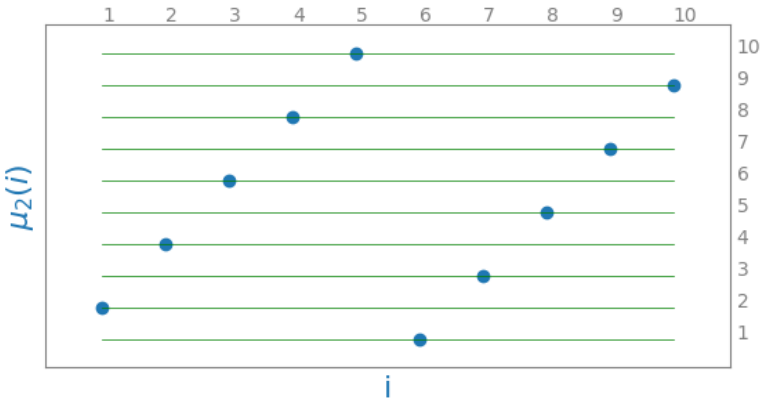

FIGURE 7.1 – Graphe de la multiplication par 2 dans $(\mathbb{Z}/11\mathbb{Z})^\times$

le produit des signatures de $\mu_{\overline{a}}$ et $\mu_{\overline{b}}$. Soit g un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$. Alors $\psi(g) = \left(\frac{g}{p}\right) = -1$ car g n'est pas un carré.

Puisque $g^{p-1} = 1$, μ_g est le cycle $(1, g, \ldots, g^{p-2})$. C'est donc un cycle d'ordre pair $p-1$, sa signature est donc -1. Enfin, les deux applications ϕ et ψ sont multiplicatives et coïncident sur le générateur g elles sont donc identiques. ■

Du critère d'Euler, $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/4} \pmod p$ on déduit immédiatement, la proposition :

Proposition 7.4. *Le symbole de Legendre de -1 ne dépend que de la classe de p modulo 4,*

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, & p = 4k+1 \\ -1, & p = 4k+3 \end{cases}$$

Le symbole de Legendre de 2, ne dépend, lui, que de la classe de p modulo 8.

Proposition 7.5. *Les symbole de Legendre $\left(\frac{2}{p}\right)$ est donné par*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1, & \text{si p} \equiv 1 \quad \text{ou} \quad \text{p} \equiv 7 \pmod 8 \\ -1, & \text{si p} \equiv 3 \quad \text{et} \quad \text{p} \equiv 5 \pmod 8 \end{cases} \tag{7.2}$$

Démonstration :

Par le lemme de Zolotarev $\left(\frac{2}{p}\right)$ est la signature de la substitution $x \mapsto 2x$ de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Considérons par exemple, $p = 11$. La figure 7.1 montre le graphe de μ_2. L'ensemble des inversions de μ_2 est $\{(i,j) \mid i < j,\ \mu_2(i) > \mu_2(j)\}$. Partitionnons cet ensemble de couples

selon la valeur de i, déterminons le nombre $inv(i)$ des inversion des couples (i,j) de premier terme i.

Pour $i=1, \mu_2(i)=2$; il faut compter les $j>1$ tels que $\mu_2(j)<2$. Il n'y en qu'un c'est $i=6$, avec $\mu_2(6)=1$. $inv(1)=1$.

Pour $i=2, \mu_2(i)=4$; il faut compter les $j>1$ tels que $\mu_2(j)<4$. Il y en a 2, 6, et 7 avec $\mu_2(7)=3$; et donc $inv(2)=3$.

Et ainsi de suite, $inv(4)=4$, $inv(5)=5$. Et, à partir de $i=6=(p+1)/2$ il n'y a pas de nouvelle inversion car μ_2 st croissante sur l'intervalle $[6-10]$.

Dans le cas général le nombre des inversions de μ_2 est $1+2+\cdots+(p-1)=(p^2-1)/8$ qui est pair si et seulement si $p\equiv\pm1 \pmod 8$. ■

Donnons enfin, sans démonstration, la loi de réciprocité quadratique, publiée par Gauss en 1801.

Théorème 7.2 (Loi de réciprocité quadratique)**.** *Si p et q sont deux nombres premiers impairs les symboles de Legendre $\left(\frac{p}{a}\right)$ et $\left(\frac{q}{p}\right)$ sont liés par*

$$\left(\frac{p}{q}\right)=(-1)^{(p-1)/2}(-1)^{(q-1)/2}\left(\frac{q}{p}\right).$$

Le coefficient $(-1)^{(p-1)/2}(-1)^{(q-1)/2}$ est 1 sauf dans le cas où p et q sont tous deux congrus à 3 modulo 4.

7.2 Le symbole de Jacobi

Le symbole de Jacobi prolonge la défintion du symbole de Legendre en l'étendant à tout couple d'entiers naturels (a,n), avec n impair. Lorsque n est premier, il coïncide avec le symbole de Legendre ; on peut donc le représenter par la même notation que celui-ci sans créer d'ambiguïté.

Définition 7.3. *Soit a un entier arbitraire et n, impair, $n=\prod_{i=1}^{k} p_i$ où les p_i sont premiers. Le symbole de Jacobi $\left(\frac{a}{b}\right)$ est le produit des symboles de Legendre $\left(\frac{a}{p_i}\right)$*

$$\left(\frac{a}{n}\right)=\prod_{i=1}^{k}\left(\frac{a}{p_i}\right).$$

Les propriétés du symbole de Legendre s'étendent au symbole de Jacobi.

Proposition 7.6. *Propriétés du symbole de Jacobi*

1. $\left(\frac{a}{n}\right)=0$ *si et seulement si a n'est pas premier avec n.*
2. *Périodicité :* $\left(\frac{a}{n}\right)$ *ne dépend que de la classe a modulo n.*

3. *Multiplicativité :* $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ *et* $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.
4. *Règle* $a = 2$ *:* $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} +1, & \text{si n} \equiv 1 \quad \text{ou} \quad \text{n} \equiv 7 \pmod 8 \\ -1, & \text{si n} \equiv 3 \quad \text{et} \quad \text{n} \equiv 5 \pmod 8 \end{cases}$
5. *Réciprocité quadratique : Si* a *et* b *sont impairs*

$$\left(\frac{a}{b}\right) = (-1)^{(a-1)/2}(-1)^{(b-1)/2}\left(\frac{b}{a}\right).$$

La loi de réciprocité quadratique appliquée au calcul de $\left(\frac{a}{b}\right)$, avec la périodicité donne pour tous a et b impairs, $0 < a < b$ la formule $\left(\frac{a}{b}\right) = (-1)^{(a-1)/2}(-1)^{(b-1)/2}\left(\frac{r}{a}\right)$, où r est le reste de la division de b par a.

On en déduit immédiatemment l'algorithme suivant qui n'utilise la multiplicativité que lorsque a est pair. Quand il est impair on utilise la proposition ce-dessus. Ce qui nous conduit à l'algorithme suivant très proche de l'algorithme d'Euclide.

```
1  def jacobi(a,b):
2      """ Calcul de jacobi (a,b) pour 0 <= a < b avec b impair """
3      res = 1
4      while a > 0:
5          while a % 2 == 0:
6              if (b % 8) != 1 and  (b % 8) != 7:
7                res = -res
8              a //= 2
9          if a % 4 == 3 and  b % 4 == 3:
10             res = -res
11         r = b % a
12         a , b = r , a
13     if b == 1: # pgcd(a,b) = 1
14         return res
15     else: # pgcd(a,b) > 1
16         return 0
```

CHAPITRE 8

Test de Solovay-Strassen

Théorème 8.1 (Solovay-Strassen)**.** *L'entier impair $n \in \mathbb{N}$, est premier si et seulement si il satisfait le crirère d'Euler, c'est à dire si pour tout a premier avec n :*

$$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}. \tag{8.1}$$

Démonstration : Cette condition est nécessaire, c'est le Theorème 7.1.

Par contraposition, démontrons que si n n'est pas premier il existe un entier a premier avec n tel que $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$. Distinguons deux cas :

1. Si n est sans facteur carré, c'est un produit de nombres premiers deux à deux distincts, soit p l'un d'entre eux, et $q = n/p$. Choisissons d'abord u non carré modulo p. Puisque $\text{pgcd}(p, q) = 1$, par le théorème des restes chinois, il existe a tel que :

$$a \equiv u \pmod{p} \quad \text{et} \quad a \equiv 1 \pmod{q} \tag{8.2}$$

Vu la multiplicativité en b du symbole de jacobi $\left(\frac{a}{b}\right)$

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \times \left(\frac{a}{q}\right) = \left(\frac{u}{p}\right) \times \left(\frac{1}{q}\right) = -1.$$

Puisque n est multiple de a, la congruence $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$ impliquerait $a^{\frac{n-1}{2}} \equiv -1 \pmod{q}$. Ce qui est exclu car $a \equiv 1 \pmod{q}$.

2. Sinon on peut écritre $n = p^\alpha q$, avec $\alpha \geq 2$ et $\text{pgcd}(p,q) = 1$. Choisissons $a = 1 + p^{\alpha-1}q$. Par multiplicativité du symbole de jacobi on a :

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p^\alpha q}\right) = \left(\frac{a}{p}\right)^\alpha \left(\frac{a}{q}\right) = 1$$

car a est congru à 1 modulo p et q. Si $a^{(n-1)/2}$ était congru à 1 modulo n, qui est un multiple de p^α il serait aussi congru à 1 modulo p^α.

Développons $a^{(n-1)/2} = (1 + p^\alpha q)^{(n-1)/2}$ par la formule du binôme. Tous les termes, à partir du troisième sont nuls modulo p^α, car $2(\alpha - 1) \geq \alpha$, et donc

$$a^{\frac{n-1}{2}} \equiv 1 + \frac{n-1}{2} p^{\alpha-1} q \pmod{p^\alpha}.$$

La plus grande puissance de p qui divise $a^{\frac{n-1}{2}} - 1$ est donc $p^{\alpha-1}$. Ce nombre $a^{\frac{n-1}{2}}$ n'est donc pas congru à 1 modulo p^α.

Soit n un entier impair. Un entier a satisfaisantt $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$ nous incite à conjecturer que n est premier. D'où la définition suivante.

Définition 8.1. *Soit n un entier impair non premier. On dit que a est un faux témoin de primalité de n si* $\text{pgcd}(a,n) = 1$ *et*

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$$

c'est à dire si dans $\mathbb{Z}/n\mathbb{Z}$ on a l'égalité $\overline{\left(\frac{a}{n}\right)} = \overline{a}^{\frac{n-1}{2}}$.

Proposition 8.1. *Soit n impair non premier. Le nombre de ses faux témoins dans l'intervalle $\{1, 2, \ldots, n-1\}$ est plus petit que $n/2$. Autrement dit, si on choisit a au hasard, avec quiprobabilité dans $\mathbb{Z}/n\mathbb{Z} - \{0\}$, la probabilité pour que a soit un faux témoin de primalité de n est plus petite que $1/2$.*

Démonstration : La congruence $\left(\frac{a}{n}\right) \equiv \overline{a}^{\frac{n-1}{2}}$ équivaut à $\overline{\left(\frac{a}{n}\right)}\overline{a}^{\frac{n-1}{2}} \equiv \overline{1}$ parce que $\left(\frac{a}{n}\right) \equiv \pm 1$ est son propre inverse. L'application $\psi : \overline{a} \mapsto \overline{\left(\frac{a}{n}\right)}\overline{a}^{\frac{n-1}{2}}$ est multiplicative car c'est le produit de deux fonctions multiplicatives. C'est donc un endomorphisme du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, et a est un faux témoin si et seulement si $\overline{a}$ appartient à $\ker(\psi)$. Le théorème de Solovay-Strassen dit qu'il existe des entiers qui ne sont pas des faux témoins ; $\ker(\psi)$ est donc un sous-groupe strict de $(\mathbb{Z}/n\mathbb{Z})^\times$. Son cardinal est ainsi un diviseur de $\text{card}\,(\mathbb{Z}/n\mathbb{Z})^\times$, donc majoré par $\text{card}\,(\mathbb{Z}/n\mathbb{Z})^\times/2 \leq (n-1)/2$.

Ce qui nous conduit à l'algorithme suivant, pour tester la primalité de n.

Test de Solovay Strassen

1. On choisit un entier k et on répète au plus k fois :
2. On tire au hasard a entre 1 et $n-1$. Si $\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$ on a prouvé que n n'est pas premier, et on s'arrête là.
3. Si aucun des k tirages n'a permis de conclure, on n'a rien prouvé, mais, si n est premier, la probabilité de cet évènement était inférieure à 2^{-k}.

Pour implémenter le test de Solovay-Strassen il faut calculer rapidement les $a^k \pmod{n}$, les exponentielles modulo n. Commençons par ce point.

L'exponentiation rapide

Soit k et x deux entiers non nuls. On peut calculer $k \times x$ de la manière suivante : on écrit k et x sur une première ligne. Puis, sur la ligne suivante, on remplace k par sa moitié et x par $x+x$. Et ainst de suite jusqu'à obtenir $k = 1$. Pour calculer $19 \times 23 = \underbrace{23 + 23 + \cdots + 23}_{19}$ on écrit donc :

k	x
19	23
9	46
4	92
2	184
1	368

On obtient le produit cherché en additionnant les nombres de la colonne des x qui figurent à droite d'une valeur impaire de k. Pour cet exemple ce sont 23, à droite de 19, 46, à droite de 9 et 368 à droite 1. Ce qui donne

$$19 \times 23 = 23 + 46 + 368 = 437.$$

Explication : l'écriture de k en base 2. Rajoutons une colonne à gauche dans laquelle on écrit 0 ou 1 selon que la valeur de k est paire ou impaire.

	c	k	x
1	1	19	23
2	1	9	46
4	0	4	92
8	0	2	184
16	1	1	368

Les nombres de la colonne c sont, en partant du chiffre des unités, les chiffres de l'écriture en base 2 de 19. D'où

$$19 = 1 + 2 + 16 \text{ et } 19 \times 23 = 1 \times 23 + 2 \times 23 + 16 \times 23 = 437.$$

Le même algorithme permet de calculer rapidement l'expression :

$$x * x * x * \cdots * x$$

dans laquelle x figure k fois et $*$ est une opération binaire associative quelconque. Remplaçant l'addition de $\mathbb{Z}$: $(x, y) \longrightarrow x+y$, par la multiplication modulo n : $(x, y) \longrightarrow (x*y) \,\%\, n$, la fonction python expMod ci-dessous calcule x^k modulo n.

```python
def expMod(x,k,n):
    """ Calcul de x^k modulo n """
    res = 1
    while k > 0:
        if k % 2 == 1:
            res = (res * x) % n
        k = k // 2
        x = (x * x) % n
    return res
```

Nous disposon maintenant de tous les éléments pour définir la fonction Python ci-dessous qui implémente le test de Solovay-Strassen.

```python
def solovayStrassen(n,k):
    for i in range(k):
        a = random.randint(1,n-1)
        d = gcd(a, n)
        if d > 1:
            return False
        j = jacobi(a,n)
        r = expMod(a,(n-1)//2,n)
        if (r - j) % n  != 0:
            return False
    print("Non prouvé mais n est certainement premier")
    return True
```

Application : Calcul de grands nombres pseudo-premiers

```python
def next_pseudo_prime(x, k=100):
    """ Renvoie le plus petit pseudo-premier >= x """
    if x % 2 == 0:
        x += 1
    while not solovayStrassen(x,k):
        x += 2
    return x
```

```
%%time
x = 10**499
next_pseudo_prime(x)
```

```
CPU times: user 2.93 s, sys: 4.77 ms, total: 2.93 s
Wall time: 2.93 s
```

```
10000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000153
```

FIGURE 8.1 – Le plus petit nombre premier de 500 chiffres décimaux