

ARITHMÉTIQUE DANS \mathbf{Z}

1. NOTIONS DE GROUPES

1.1. Groupe abstrait

1.2. Groupes cycliques et monogènes

DÉFINITION 1.2.0.1. —

Si un groupe multiplicatif G est engendré par l'un de ses éléments g alors il est dit :

- *cyclique* si G est fini ;
- *monogène* sinon.

Un tel élément g est un *générateur* de G .

Une première proposition fondamentale :

THÉORÈME 1.2.0.1. —

Tout groupe monogène G est isomorphe à \mathbf{Z} . Tout groupe cyclique est isomorphe à $\mathbf{Z}/n\mathbf{Z}$ pour un certain $n \in \mathbf{Z}$.

DÉMONSTRATION 1.2.0.1. —

Il suffit de donner de bons isomorphismes :

1. Si G est monogène alors l'homomorphisme :

$$\chi : g^n \mapsto n$$

est une bijection de G dans \mathbf{Z} ;

2. si G est cyclique alors l'homomorphisme χ est un isomorphisme de G dans $\mathbf{Z}/n\mathbf{Z}$.

PROPOSITION 1.2.0.1. —

Tout groupe monogène ou cyclique est abélien.

DÉMONSTRATION 1.2.0.2. —

En effet :

$$g^n g^m = g^{n+m} = g^{m+n} = g^m g^n.$$

PROPOSITION 1.2.0.2. —

Si $f : G \rightarrow H$ est homomorphisme surjectif de groupes et si G est un groupe engendré par g alors H est engendré par $f(g)$.

2. NOTIONS EN ARITHMÉTIQUE

2.1. Sous-groupe de \mathbf{Z}

THÉORÈME 2.1.0.2. —

Tout sous-groupe de \mathbf{Z} est de la forme $a\mathbf{Z}$ avec $a \in \mathbf{Z}$.

DÉMONSTRATION 2.1.0.3. —

Soit G un sous-groupe de \mathbf{Z} . Si G est réduit à $\{0\}$ alors $G = 0\mathbf{Z}$.

Sinon, soit $x = |x| \in G$ l'élément minimal de G non nul (qui existe puisque $G \subset \mathbf{Z}$).

$x\mathbf{Z} \subset G$ puisque G est un groupe.

Soit $y \in G$. Par division euclidienne, il existe un unique couple $(a, b) \in \mathbf{Z} \times \{0, 1, \dots, x-1\}$ tel que $y = ax + b$. On a $y - ax \in G$ mais aussi $y - ax = b \in G$.

Or $b < x$ donc $b = 0$ et donc $y \in x\mathbf{Z}$.

On notera $x\mathbf{Z} = \mathbf{x}$.

2.2. pgcd et ppcm

DÉFINITION 2.2.0.2. —

Soient $a, b \in \mathbf{Z}$. On dit de manière équivalente que « a divise b » ou :

$$a \mid b \iff \mathbf{b} \subset \mathbf{a} \iff \exists c \in \mathbf{Z}, a = cb.$$

DÉFINITION 2.2.0.3. —

Soient $a, b \in \mathbf{Z}$.

On a que $\mathbf{a} + \mathbf{b}$ est un sous-groupe de \mathbf{Z} de la forme \mathbf{d} avec $d \in \mathbf{Z}$. On note $\text{pgcd}(a, b) = d$.

$\mathbf{a} \cap \mathbf{b}$ est un sous-groupe de \mathbf{Z} de la forme \mathbf{m} avec $m \in \mathbf{N}$. On note $\text{ppcm}(a, b) = m$.

PROPOSITION 2.2.0.3. —

Soient $a, b \in \mathbf{Z}$. On a les propositions suivantes :

$$1. \text{pgcd}(a, b) = d \iff (\forall x \in \mathbf{Z}, x \mid a \text{ et } x \mid b \iff x \mid d);$$

$$2. \text{ppcm}(a, b) = m \iff (\forall x \in \mathbf{Z}, a \mid x \text{ et } b \mid x \iff m \mid x).$$

DÉMONSTRATION 2.2.0.4. —

Soient $a, b \in \mathbf{Z}$.

1. Soit $x \in \mathbf{Z}$. $x \mid a$ et $x \mid b \iff \mathbf{a} \subset \mathbf{x}$ et $\mathbf{b} \subset \mathbf{x} \iff \mathbf{a} + \mathbf{b} \subset \mathbf{x} \iff x \mid \text{pgcd}(a, b)$.
2. Soit $x \in \mathbf{Z}$. $a \mid x$ et $b \mid x \iff \mathbf{x} \subset \mathbf{a}$ et $\mathbf{x} \subset \mathbf{b} \iff \mathbf{x} \subset \mathbf{a} \cap \mathbf{b} \iff \text{ppcm}(a, b) \mid x$.

THÉORÈME 2.2.0.3 (Identité de BEZOUT). —

Si $a, b \in \mathbf{Z}$ alors il existe $u, v \in \mathbf{Z}$ tels que $au + bv = \text{pgcd}(a, b)$.

En particulier, si a et b sont premiers entre eux alors $au + bv = 1$.

3. NOTIONS MODULAIRES

3.1. Passage au quotient

DÉFINITION 3.1.0.4. —

Soit $a \in \mathbf{Z}$, \mathbf{Z}/\mathbf{a} est le sous-ensemble de \mathbf{Z} obtenu par le quotient de \mathbf{Z} par \mathbf{a} .

Si $x \in \mathbf{Z}$ alors \bar{x} est la classe d'équivalence de x dans \mathbf{Z}/\mathbf{a} .

Si $\bar{x} = \bar{y} \in \mathbf{Z}/\mathbf{a}$ alors pour x, y des représentants de leurs classes respectives :

$$x = y + ua$$

avec $u \in \mathbf{Z}$. Il arrive de le noter :

$$x \equiv y \pmod{a}.$$

PROPOSITION 3.1.0.4. —

Soit $a \in \mathbf{N}$, $\mathbf{Z}/\mathbf{a} = \{\bar{0}, \bar{1}, \dots, \overline{a-1}\}$.

On étend naturellement les opérations sur \mathbf{Z} à \mathbf{Z}/\mathbf{a} en identifiant les opérations de \mathbf{Z} à \mathbf{Z}/\mathbf{a} . On pourra alors confondre x et son représentant \bar{x} dans \mathbf{Z}/\mathbf{a} .

PROPOSITION 3.1.0.5. —

Soient $x, y \in \mathbf{Z}$:

1. $\overline{x + y} = \bar{x} + \bar{y}$;
2. $\overline{xy} = \bar{x} \cdot \bar{y}$.

DÉMONSTRATION 3.1.0.5. —

Soient $x, y \in \mathbf{Z}$.

1. si $x = ua + b$ et $y = va + c$ tels que dans les divisions euclidiennes respectives alors

$$\overline{x+y} = \overline{(u+v)a + b+c} = \overline{b+c} = \overline{b} + \overline{c} = \overline{x} + \overline{y};$$

2. de même :

$$\overline{xy} = \overline{(ua+b)(va+c)} = \overline{a(uva+uc+bv)+bc} = \overline{bc} = \overline{b} \cdot \overline{c} = \overline{x} \cdot \overline{y}.$$

3.2. Inverse modulaire

DÉFINITION 3.2.0.5. —

L'inverse par la multiplication modulo $n \in \mathbf{Z}$ d'un entier $a \in \mathbf{Z}$ est un entier $u \in \mathbf{Z}$ satisfaisant à

$$a^{-1} \equiv u \pmod{n}.$$

C'est-à-dire de manière équivalente :

$$au \equiv 1 \pmod{n}.$$

PROPOSITION 3.2.0.6. —

$a \in \mathbf{Z}$ est inversible dans \mathbf{Z}/n si, et seulement si, n est premier avec a .

DÉMONSTRATION 3.2.0.6. —

Soient $a, u, n, m \in \mathbf{Z}$.

$$au \equiv 1 \pmod{n} \iff au = 1 + mn \iff au - mn = 1$$

ce qui revient à dire que $\text{pgcd}(a, n) = 1$.

THÉORÈME 3.2.0.4. —

\mathbf{Z}/p est un corps si, et seulement si, p est premier.

DÉMONSTRATION 3.2.0.7. —

\mathbf{Z}/p est un anneau. Or $x \in \mathbf{Z}/p$ est inversible si x est premier avec p et donc tout x est inversible si p est premier.

3.3. Petit théorème de Fermat

THÉORÈME 3.3.0.5 (Petit théorème de FERMAT). —

Soient p un nombre premier et $a \in \mathbf{Z}$. Alors :

$$a^p \equiv a \pmod{p}.$$

DÉMONSTRATION 3.3.0.8. —

On procède par récurrence sur a :

1. Pour $a = 1$ c'est vérifié.
2. Pour tout $k \in \mathbf{Z}$ on a :

$$(k+1)^p \equiv k^p + 1 \pmod{p}.$$

En effet les coefficients binomiaux à l'exceptions des premier et dernier termes disparaissent en raison d'un facteur proportionnel à p .

3. Si la proposition est vérifiée pour $a = k$ alors pour $a = k+1$ elle est également vérifiés en raison du résultat précédent :

$$(k+1)^p \equiv k^p + 1 \equiv k+1 \pmod{p}.$$

Première généralisation. — On peut aller plus loin en généralisant ce résultat :

THÉORÈME 3.3.0.6 (Théorème d'EULER). —

Soit $n > 0$ et a entier premier avec n alors :

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

Avec bien entendu φ l'indicatrice d'EULER.

Pour démontrer ce résultat on aura besoin du théorème de LAGRANGE :

THÉORÈME 3.3.0.7 (Théorème de LAGRANGE). —

Pour tout groupe G et tout sous-groupe H de G , l'ordre (i.e. le cardinal) de H divise l'ordre de G :

$$\#H \mid \#G.$$

DÉMONSTRATION 3.3.0.9 (Théorème d'EULER). —

Le groupe $(\mathbf{Z}/n)^*$ des entiers inversibles de l'anneau \mathbf{Z}/n est constitué des classes d'entiers inversibles modulo n , i.e. premiers avec n . Il y en a exactement $\varphi(n)$ donc ce groupe est d'ordre $\varphi(n)$.

Puisque a est premier avec n , \bar{a} est dans le groupe $(\mathbf{Z}/n)^*$. \bar{a} a donc un ordre dans ce groupe, disons m et cet ordre divise $\varphi(n)$ tel que $mk = \varphi(n)$. On a donc :

$$a^{\varphi(n)} \equiv a^{mk} \equiv (a^m)^k \equiv 1^k \equiv 1 \pmod{n}.$$

DÉMONSTRATION 3.3.0.10 (Théorème de LAGRANGE). —

Le cardinal de l'ensemble G/H est appelé *indice* de H dans G et est noté $[G : H]$.

De plus, ces classes forment une partition de G et chacune d'entre elles a le même cardinal que H . On a alors :

$$\sharp G = \sharp H \times [G : H].$$

Seconde généralisation. — Une seconde généralisation de ce résultat est possible. Elle est donnée par :

THÉORÈME 3.3.0.8. —

Si p est un nombre premier et m et n tels que

$$m \equiv n \pmod{p-1},$$

alors pour tout $a \in \mathbf{Z}$ on a :

$$a^m \equiv a^n \pmod{p}.$$

DÉMONSTRATION 3.3.0.11. —

En effet, soit a est divisible par p et les deux membres sont égaux à 0, soit a ne l'est pas et en supposant $n > m$:

$$a^{n-m} = \left(a^{p-1}\right)^{(n-m)/(p-1)} = 1^{(n-m)/(p-1)} = 1.$$