chapitreXXIII
Groupes cycliques et Algèbre modulaire

Extrait du programme officiel :

Contenus	Capacités & commentaires
Groupes et sous-groupes	
Sous-groupe engendré par une partie.	
Groupes monogènes et cycliques	
Groupe $(\mathbb{Z}/n\mathbb{Z},+)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.	
Groupe monogène, groupe cyclique.	Groupe des racines n-ièmes de l'unité.
Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$. Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$.	
Ordre d'un élément dans un groupe	
Élément d'ordre fini d'un groupe, ordre d'un tel élément.	Si x est d'ordre fini, l'ordre de x est le cardinal du sous-groupe de G engendré par x.
Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour n dans $\mathbb{Z}$, on a $x^n = e \Longleftrightarrow d \mid n$.	
L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.	La démonstration n'est exigible que pour G commutatif.
L'anneau $\mathbb{Z}/n\mathbb{Z}$	
Anneau $\mathbb{Z}/n\mathbb{Z}$.	
Inversibles de $\mathbb{Z}/n\mathbb{Z}$.	L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
Théorème chinois : si m et n sont deux entiers premiers entre eux, isomorphisme naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.	Application aux systèmes de congruences.
Indicatrice d'Euler φ. Calcul de $\varphi(n)$ à l'aide de la décomposition de n en facteurs premiers.	$\leftrightarrows$ I : calcul de $\varphi(n)$ à l'aide d'une méthode de crible.
Théorème d'Euler.	Lien avec le petit théorème de Fermat étudié en première année. $\leftrightarrows$ I : codage RSA.

Plan du cours

XXIII Groupes cycliques et Algèbre modulaire
I Révisions de MPSI : Arithmétique sur $\mathbb{Z}$ 2
1 PGCD . . . 2
2 PPCM . . . 3
3 Nombres premiers . . . 3
4 Congruences . . . 4
II Le groupe $\mathbb{Z}/n\mathbb{Z}$ 5
III Groupes monogènes 6
1 Sous-groupe engendré par une partie . . . 6
2 Groupes monogènes et cycliques . . . 6
3 Ordre d'un élément dans un groupe . . . 7
IV Anneau $\mathbb{Z}/n\mathbb{Z}$ 9
1 Structure . . . 9
2 Théorème Chinois . . . 11
3 Indicatrice d'Euler . . . 13

I Révisions de MPSI : Arithmétique sur $\mathbb{Z}$

1 PGCD

Les démonstrations sont similaires à celles vues pour les polynômes en début d'année, en remplaçant « unitaire » par « positif » et/ou ont été vues en MPSI.

Définition : PGCD

Soient $a, b \in \mathbb{Z}$.
$I = (a) + (b) = a\mathbb{Z} + b\mathbb{Z} = \{au + bv,\ u, v \in \mathbb{Z}\}$ est un idéal non réduit de $(\mathbb{Z}, +, \times)$ qui est un anneau principal.
Son unique générateur positif est appelé **pgcd de** a **et** b, noté $a \wedge b$.
On a donc, par définition, $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$.

Propriété : Relation de Bézout

Si $a, b \in \mathbb{Z}$, on peut trouver $a, b \in \mathbb{Z}$ tels que $au + bv = a \wedge b$.

Propriété : Propriété d'Euclide

Si $a, b, q \in \mathbb{Z}$, $a \wedge b = (a - bq) \wedge b$ (pas nécessairement une division euclidienne).

Propriété : Caractérisation

Soit $(a, b) \in \mathbb{Z}^2$.

$$d = a \wedge b \iff \begin{cases} d \in \mathbb{N} \\ d | a \text{ et } d | b \\ \forall\, c \in \mathbb{Z},\quad (c | a \text{ et } c | b) \implies c | d \end{cases}$$

Il s'agit donc du plus grand diviseur positif au sens de la division.

Définition : Nombre entiers premiers entre eux

$a, b \in \mathbb{K}[X]$ sont dits **premiers entre eux** lorsque $A \wedge B = 1$, c'est-à-dire lorsque les seuls diviseurs communs sont les polynômes constants non nuls.

Théorème : de Bézout

Soit $a, b \in \mathbb{Z}$.

$$a \wedge b = 1 \iff \exists\, u, v \in \mathbb{Z},\quad au + bv = 1$$

Corollaire

Soient $a, b, c \in \mathbb{Z}$.

(i) $a \wedge bc = 1 \iff a \wedge b = a \wedge c = 1$

(ii) Si $d = a \wedge b$, on a $a', b' \in \mathbb{Z}$ tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$.

Théorème : Lemme de Gauß

Soient $a, b, c \in \mathbb{Z}$. Si $a | bc$ et $a \wedge b = 1$, alors $a | c$.

2 PPCM

Définition : PPCM

Le PPCM de deux entiers a, b est l'unique générateur positif $a \vee b$ de l'idéal $a\mathbb{Z} \cap b\mathbb{Z}$ des multiples communs à a et à b.
On a donc $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$.

Propriété

(i) Il s'agit du plus petit multiple positif commun à a et à b au sens de la division.

(ii) On a toujours que $|ab| = (a \wedge b)(a \vee b)$.

3 Nombres premiers

Définition : Nombre premier

Un **nombre premier** est un entier naturel $p \geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.
On notera $\mathscr{P}$ l'ensemble des nombres premiers.

Remarques

R 1 – 1 n'est pas premier.

R 2 – 2 est le seul nombre premier pair.

R 3 – Un nombre premier possède exactement 4 diviseurs : ± 1 et $\pm p$.

R 4 – Pour qu'un nombre entier n soit premier, il faut et il suffit qu'il n'ait pas de diviseur entre 2 et $\sqrt{n}$.

Propriété

L'ensemble des nombres premiers est infini.

Propriété

Si $p \in \mathscr{P}$ et $n \in \mathbb{Z}$, alors $p | n$ ou (exclusif) $p \wedge n = 1$.

Propriété

Soient $p \in \mathscr{P}$ et $a_1, \dots, a_n \in \mathbb{Z}$.

$$p | (a_1 \times \cdots \times a_n) \text{ si et seulement si } p \text{ divise l'un des } a_k.$$

Théorème : fondamental de l'arithmétique – Décomposition primaire

Soit $n \in \mathbb{Z}^*$. On peut trouver $k \in \mathbb{N}$, $p_1, \dots, p_k$ premiers deux à deux distincts, $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ tels que

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

appelée décomposition primaire de n.
De plus, cette écriture est unique à l'ordre des facteurs près.
$p_1, \dots, p_k$ sont les diviseurs premiers de n.

Définition

Soit $p \in \mathscr{P}$ et $n \in \mathbb{Z}^*$. On appelle **valuation p-adique** de n l'entier

$$v_p(n) = \max \left\{ i \in \mathbb{N} \mid p^i \text{ divise } n \right\}.$$

Remarque

La décomposition primaire se réécrit $n = \pm \prod_{p\in\mathscr{P},\ p|n} p^{v_p(n)} = \pm \prod_{p\in\mathscr{P}} p^{v_p(n)}$.

Propriété

Soient $n, m \in \mathbb{Z}^*,\ p \in \mathscr{P}$.

(i) $v_p(n) \neq 0 \Longleftrightarrow p|n$

(ii) $v_p(n\times m) = v_p(n) + v_p(m)$

(iii) $n|m \Longleftrightarrow \forall\, p \in \mathscr{P},\quad v_p(n) \leqslant v_p(m)$

(iv) $v_p(n \wedge m) = \min(v_p(n), v_p(m))$
$v_p(n \vee m) = \max(v_p(n), v_p(m))$

Remarque

Si $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ et $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ avec des exposants éventuellement nuls, alors

$$a \wedge b = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

$$a \vee b = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

Exercices

Ex 1 – Montrer que $\sqrt{n} \in \mathbb{Q}$ si et seulement si n est un carré parfait.

Si $\sqrt{n} = \frac{a}{b}$, alors $a^2 = n \times b^2$, $\forall\, p \in \mathscr{P},\ \ 2v_p(a) = v_p(n) + 2v_p(b)$ donc $\forall\, p \in \mathscr{P},\ \ v_p(n) \in 2\mathbb{N}$, donc n est un carré parfait.

Ou encore : si $\sqrt{n} = \frac{a}{b}$ sous forme irréductible, alors $a^2 = n \times b^2$ donc $b^2 | a^2$. Or $a \wedge b = 1$ donc $b^2 = a^2 \wedge b^2 = 1$ donc $n = a^2$.

Ex 2 – Exprimer le nombre de diviseurs positifs de n à l'aide de ses valuations p-adiques.

$$\prod_{p\in\mathscr{P}, p|n} (v_p(n)+1).$$

4 Congruences

Définition : Congruence

Soit $n \in \mathbb{N}^*$. On dit que $a, b \in \mathbb{Z}$ sont **congrus modulo** n et on note $a \equiv b\ [n]$ lorsque $n|(a-b)$ ie lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

Propriété

C'est une relation d'équivalence sur $\mathbb{Z}$.

Propriété

$\forall\, a \in \mathbb{Z},\ \ \exists!\, r \in [\![0, n-1]\!]\ |\ a \equiv r\ [n]$. r est le reste de la division euclidienne de k par n.
Ainsi, la relation d'équivalence $\cdot \equiv \cdot\ [n]$ possède exactement n classes d'équivalences.

Propriété : Compatibilité de + et ×

Soient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $c \equiv d\ [n]$. Alors $a + c \equiv b + d\ [n]$ et $a \times c \equiv b \times d\ [n]$.
Plus généralement, si $m \in \mathbb{N}$, $a^m \equiv b^m\ [n]$.

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

Soit $n \in \mathbb{N}$ tel que $n \geqslant 1$ fixé.

Définition : $\mathbb{Z}/n\mathbb{Z}$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble (quotient) des n classes d'équivalences de $\cdot \equiv \cdot\ [n]$, notées $\overline{0}, \overline{1}, \dots, \overline{n-1}$. Ainsi

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

Remarque

$\overline{k}$ est l'ensemble des entiers congrus à k modulo n, donc l'ensemble des $k + n\ell$ pour $\ell \in \mathbb{Z}$.
On peut toujours se ramener à un entier r entre 0 et $n-1$ en prenant le reste de la division euclidienne de k par n : $k \equiv r\ [n]$ donc $\overline{k} = \overline{r} = \overline{r + pn}$ pour tout $p \in \mathbb{Z}$.

Définition : Surjection canonique

L'application surjective $\left|\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ k & \longmapsto & \overline{k} \end{array}\right.$ est appelée **surjection canonique**.

Lemme

Soient $a, b, c, d \in \mathbb{Z}$ tels que $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$. Alors $\overline{a+b} = \overline{c+d}$

Démonstration

En effet $a \equiv c\ [n]$ et $b \equiv d\ [n]$ implique $a + b \equiv c + d\ [n]$. □

Ce lemme rend licite la définition suivante, car la somme de deux entiers modulo n ne dépend pas du choix de leurs représentants.

Définition

Si $a, b \in \mathbb{Z}$, on pose $\overline{a} + \overline{b} = \overline{a+b}$, ce qui définit une loi de composition interne $+$ sur $\mathbb{Z}/n\mathbb{Z}$.

Propriété

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif isomorphe à $(\mathbb{U}_n, \times)$.

Démonstration

En effet,

- $+$ est une loi de composition interne sur $\mathbb{Z}/n\mathbb{Z}$,
- commutative car si $a, b \in \mathbb{Z}$, $\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{a} + \overline{b}$,
- d'élément neutre $\overline{0}$ car pour tout $a \in \mathbb{Z}$, $\overline{a} + \overline{0} = \overline{a+0} = \overline{a}$,
- associative car si $a, b, c \in \mathbb{Z}$,
$$\left(\overline{a} + \overline{b}\right) + \overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a} + \left(\overline{b} + \overline{c}\right),$$
- si $a \in \mathbb{Z}$, $\overline{a} + \overline{-a} = \overline{0}$ donc $\overline{-a} = -\overline{a}$ est l'opposé de $\overline{a}$.

De plus, on remarque que si $k \equiv \ell\ [n]$, alors $\mathrm{e}^{\frac{2ik\pi}{n}} = \mathrm{e}^{\frac{2i\ell\pi}{n}}$ ne dépend pas du choix du représentant de $\overline{k}$.

Donc $f : \left|\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z}, +) & \longrightarrow & (\mathbb{U}_n, \times) \\ \overline{k} & \longmapsto & \mathrm{e}^{\frac{2ik\pi}{n}} \end{array}\right.$ est

- bien définie,
- un morphisme car pour tout $k, \ell \in \mathbb{Z}$, $f\left(\overline{k} + \overline{\ell}\right) = f\left(\overline{k}\right) f\left(\overline{\ell}\right)$,
- injectif car $\operatorname{Ker} f = \left\{\overline{k},\ \mathrm{e}^{\frac{2ik\pi}{n}} = 1\right\} = \left\{\overline{k},\ n|k\right\} = \left\{\overline{0}\right\}$
- bijectif car de plus $|\mathbb{Z}/n\mathbb{Z}| = n = |\mathbb{U}_n|$. □

Remarque

On a alors facilement, pour $k\in\mathbb{Z}$, $k\cdot\overline{a}=\overline{ka}$.

Exemple

Table d'addition dans $\mathbb{Z}/4\mathbb{Z}$.

III Groupes monogènes

1 Sous-groupe engendré par une partie

Définition : Groupe engendré par une partie

Soit $(G,*)$ un groupe, A partie non vide de G.

On appelle **sous-groupe engendré par** A le plus petit (au sens de l'inclusion) sous-groupe de G contenant A, noté $\langle A\rangle$.

On dit alors que A est une **partie génératrice** de $\langle A\rangle$.

Remarque

À mettre en parallèle avec la définition de Vect en algèbre linéaire.

Propriété

Les éléments de $\langle A\rangle$ sont exactement les produits (pour x) d'éléments de A ou de A^{-1}.

Autrement dit, $x\in\langle A\rangle$ si et seulement s'il existe $k\in\mathbb{N}$, $(a_1,\dots,a_k)\in A^k$ et $(\varepsilon_1,\dots,\varepsilon_k)\in\{-1,1\}^k$ tel que $x=a_1^{\varepsilon_1}*\cdots*a_k^{\varepsilon_k}$.

Démonstration

On note H l'ensemble de tels éléments.

On vérifie que H est un sous-groupe de $(G,*)$ par caractérisation (partie non vide de G stable par $*$ et par inverse).

Puis tout sous-groupe de G contenant A contient nécessairement H par stabilités.

Donc H est bien le plus petit sous-groupe de G contenant A : $H=\langle A\rangle$. □

Remarque

On a aussi que $\langle A\rangle$ est l'intersection de tous les sous-groupes contenant A (car c'est un sous-groupe, contenant A, plus petit que tous les autres.)

Exemples

E 1 – $\mathfrak{S}_n$ est engendré par les cycles.
(Toute permutation se décompose en produit de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.)

E 2 – $\mathfrak{S}_n$ est engendré par les transpositions.
(Les cycles eux-mêmes se décomposent en produit de transpositions. Cette fois, il n'y a plus unicité de la décomposition, mais seulement de la parité du nombre de termes.)

E 3 – Soit $\mathbb{K}$ un corps. $\mathcal{GL}_n(\mathbb{K})$ est engendré par les matrices de transvection $T_{i,j}(\lambda)$ (avec $i\neq j$), de dilatation $D_i(a)$ (avec $a\neq 0$) et de permutation $P_{i,j}$.
(C'est une conséquence du pivot de Gauß) : par opérations élémentaires, on peut transformer une matrice inversible en I_n.)

2 Groupes monogènes et cycliques

Propriété

Soit $a \in G$. Le sous-groupe engendré par a noté $\langle a \rangle$ plutôt que $\langle \{a\} \rangle$ est

$$\langle a \rangle = \left\{ a^k,\ k \in \mathbb{Z} \right\}$$

On dit que a en est un ***générateur****.*

Remarque

En notation additive, on a $\langle a \rangle = \{ka,\ k \in \mathbb{Z}\}$.

Définition : Groupe monogène

Un groupe G est dit **monogène** s'il est engendré par un seul élément, c'est-à-dire s'il existe $a \in G$ tel que $G = \langle a \rangle$.

Un groupe G est dite **cyclique** si et seulement s'il est monogène et fini.

Exemple

$(\mathbb{U}_n, \times)$ est cyclique engendré par $e^{\frac{2i\pi}{n}}$.

Propriété

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique, dont les générateurs sont exactement les $\overline{k}$ avec $k \wedge n = 1$.

Démonstration

On a en effet $\mathbb{Z}/n\mathbb{Z} = \left\{a \cdot \overline{1}, a \in \mathbb{Z}\right\} = \langle \overline{1} \rangle$ fini.

Si $k \wedge n = 1$, alors on a une relation de Bézout $ku + nv = 1$ avec $u, v \in \mathbb{Z}$. Alors pour tout $a \in \mathbb{Z}$, $a = auk + nva \equiv auk\ [n]$ donc $\overline{a} = au\overline{k}$ donc $\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle$.

Si, réciproquement, $\mathbb{Z}/n\mathbb{Z} = \langle \overline{k} \rangle$, alors on a $a \in \mathbb{Z}$ tel que $\overline{1} = a\overline{k} = \overline{ak}$ donc on a $\ell \in \mathbb{Z}$ tel que $1 = ak + n\ell$ donc $n \wedge k = 1$ par théorème de Bézout. $\square$

Remarque

De même, les générateurs de $\mathbb{U}_n$ sont les $e^{\frac{2ik\pi}{n}}$ avec $k \wedge n = 1$, appelées **racines primitives n^e de l'unité**.

Exemple : À observer sur un dessin

Générateurs de $\mathbb{Z}/6\mathbb{Z}$ et détails de la génération pour $n = 5$ par exemple.

3 Ordre d'un élément dans un groupe

$(G, *)$ est un groupe d'élément neutre e.

Définition : Ordre d'un élément

On dit que $a \in G$ est **d'ordre fini** s'il existe $k \in \mathbb{N}^*$ tel que $a^k = e$.
Dans ce cas, on appelle **ordre de** a le plus petit $k \in \mathbb{N}^*$ tel que $a^k = e$.

Remarque

$f : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ k & \longmapsto & a^k \end{array} \right.$ est un morphisme de groupe donc son noyau est de la forme $m\mathbb{Z}$ où $m \in \mathbb{N}$.

Soit $m = 0$ et a n'est pas d'ordre fini (sa seule puissance égale à e est a^0.)

Soit $m>0$ et m est le plus petit élément >0 du noyau de f : il s'agit de l'ordre de a.

Exemple : À observer sur un dessin

Dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{5}$ est d'ordre 6 et $\overline{2}$ est d'ordre 3.

Propriété

Soit a un élément de G d'ordre fini m.

- *Si $k\in\mathbb{Z}$, $a^k=e$ si et seulement si $k\in m\mathbb{Z}$ ie m divise k.*
- *$\langle a\rangle=\left\{a^k, k\in[\![0,m-1]\!]\right\}$ et $|\langle a\rangle|=m$.*

Démonstration

- Avec $f:\left|\begin{array}{ccc}\mathbb{Z} & \longrightarrow & G\\ k & \longmapsto & a^k\end{array}\right.$, $\operatorname{Ker} f=m\mathbb{Z}$ d'où le résultat.
- On a déjà $\left\{a^k, k\in[\![0,m-1]\!]\right\}\subset\langle a\rangle$.
  Puis, si $k\in\mathbb{Z}$, par division euclidienne, on a $q,r\in\mathbb{Z}$ tel que $k=mq+r$ avec $0\leqslant r\leqslant m-1$ et alors $a^k=(a^m)^q*a^r=a^r$ d'où l'autre inclusion.
  Puis, les termes sont deux à deux distincts car si $a^k=a^\ell$ avec $0\leqslant k\leqslant \ell\leqslant m-1$, alors $a^{\ell-k}=e$ donc par minimalité de m, $k=\ell$.
  D'où le cardinal égal à m.

$\square$

Propriété

Tout groupe monogène infini est isomorphe à $(\mathbb{Z},+)$.
Tout groupe monogène fini (donc cyclique) de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z},+)$

Démonstration

Si G est engendré par a et infini, $f:\left|\begin{array}{ccc}(\mathbb{Z},+) & \longrightarrow & (G,*)\\ k & \longmapsto & a^k\end{array}\right.$ alors f est un morphisme de groupes surjectif car $G=\langle a\rangle$, et injectif car si $k\in\operatorname{Ker} f$, $a^k=1$ donc a d'ordre fini, donc G est fini.

Si G est engendré par a et de cardinal n, alors a est d'ordre n, donc $a^n=e$, $f:\left|\begin{array}{ccc}(\mathbb{Z}/n\mathbb{Z},+) & \longrightarrow & (G,*)\\ \overline{k} & \longmapsto & a^k\end{array}\right.$ est bien définie (quel que soit le représentant k de $\overline{k}$, la valeur de a^k est la même car $a^n=e$), est un morphisme de groupe et est surjectif, donc est un isomorphisme car $n=|\mathbb{Z}/n\mathbb{Z}|=|G|$. $\square$

Théorème : de Lagrange (HP)

Soit $(G,*)$ un groupe fini, H un sous-groupe de G. Alors $|H|$ divise $|G|$.

Démonstration

On montre que la relation définie par $x\mathscr{R}y\Longleftrightarrow x^{-1}*y\in H$ est une relation d'équivalence sur G (facile).

Puis on montre que toutes les classes d'équivalence ont même cardinal : celui de H. En effet, il s'agit des $xH=\{x*h, h\in H\}$ et l'application (translation) $f:h\mapsto x*h$ est une bijection de H sur xH (de réciproque $h\mapsto x^{-1}*h$.)

Comme les classes d'équivalences forment une partition de G, $|G|=n|H|$ où n est le nombre de classes, d'où le résultat. $\square$

Propriété

Soit $(G,*)$ un groupe fini de neutre e.

(i) Tout élément de G est d'ordre fini.

(ii) L'ordre de tout élément de G divise le cardinal de G.

(iii) Pour tout $a \in G$, $a^{|G|} = e$.

Démonstration

(i) $\langle a \rangle$ est un sous-groupe de G, donc d'ordre fini. Donc on a $i < j$ tel que $a^i = a^j$ et $a^{j-i} = e$ avec $j - i \in \mathbb{N}^*$.

(ii) L'ordre de a est la cardinal du sous-groupe $\langle a \rangle$ de G, donc d'après le théorème de Lagrange (HP), il divise celui de G.
Seule la démonstration dans le cas commutatif est au programme.
En effet, dans ce cas, on considère le produit $\left(\prod_{x\in G} x\right) \in G$ et on effectue le changement de variable (bijectif) $x \mapsto a * x$.
Par commutativité, on obtient $\prod_{x\in G} x = \prod_{x\in G} (a*x) = a^{|G|} \prod_{x\in G} x$. Comme $\prod_{x\in G} x$ est régulier (car inversible), on en déduit que $a^{|G|} = e$.

(iii) Conséquence du (ii). □

IV Anneau $\mathbb{Z}/n\mathbb{Z}$

1 Structure

Lemme

Soient $a, b, c, d \in \mathbb{Z}$ tels que $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$. Alors $\overline{ab} = \overline{cd}$

Démonstration

Comme pour la somme : $a \equiv c\ [n]$ et $b \equiv d\ [n]$ implique $ab \equiv cd\ [n]$. □

Ce lemme rend licite la définition suivante, car le produit de deux entiers modulo n ne dépend pas du choix de leurs représentants.

Définition

Si $a, b \in \mathbb{Z}$, on pose $\overline{a} \times \overline{b} = \overline{ab}$, ce qui définit une loi de composition interne $\times$ sur $\mathbb{Z}/n\mathbb{Z}$.

Propriété

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Démonstration

On a déjà que $(\mathbb{Z}/n\mathbb{Z}, +)$ a une structure de groupe abélien.
Reste à voir que $\times$ est associative, distributive sur $+$, commutative et admet un neutre $\overline{1}$ de façon similaire à ce qui a été vu pour $+$. □

Propriété

Le groupe des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des $\overline{k}$ pour $k \in \mathbb{Z}$ tel que $k \wedge n = 1$.

Démonstration

$\overline{k}$ est inversible si et seulement s'il existe $\ell \in \mathbb{Z}$ tel que $\overline{k\ell} = \overline{k\ell} = \overline{1}$ si et seulement si $k\ell \equiv 1\ [n]$ si et seulement s'il existe $u \in \mathbb{Z}$ tel que $1 = k\ell + un$, ce qui permet de conclure par théorème de Bézout. □

Méthode : Calcul de l'inverse d'un élément inversible

Si $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ (donc si $k \wedge n = 1$), on trouve l'inverse de $\overline{k}$ soit « de tête », soit en utilisant l'algorithme d'Euclide étendu pour trouver une relation de Bézout entre k et n.

Exemples

E 1 – Inversibles et leurs inverses dans $\mathbb{Z}/12\mathbb{Z}$.

E 2 – Inverse de $\overline{23}$ dans $\mathbb{Z}/120\mathbb{Z}$.

Corollaire

$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

Démonstration

On élimine le cas $n = 1$ car $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$. On a alors que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si pour tout $k \in [\![1, n-1]\!]$, $\overline{k}$ est inversible si et seulement si pour tout $k \in [\![1, n-1]\!]$, k est premier avec n si et seulement si les seuls diviseurs positifs de n sont 1 et n si et seulement si $n \geqslant 2$ premier. □

2 Théorème Chinois

Théorème : chinois

Soient $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$.

1re formulation *Si $a, b \in \mathbb{Z}$, alors $\begin{cases} k \equiv a\ [n] \\ k \equiv b\ [m] \end{cases} \iff k \equiv c\ [nm]$ où c est une solution particulière, qui existe bien.*

2e formulation *Pour tout $k \in \mathbb{Z}$, note $(k \bmod n)$, $(k \bmod m)$ et $(k \bmod nm)$ les classes de k dans $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$ et $\mathbb{Z}/nm\mathbb{Z}$ respectivement. On a alors*

(i) Si $k, \ell \in \mathbb{Z}$, et si $(k \bmod nm) = (\ell \bmod nm)$, alors $(k \bmod n) = (\ell \bmod n)$ et $(k \bmod m) = (\ell \bmod m)$.

(ii) L'application

$$f : \begin{array}{|ccc} \mathbb{Z}/nm\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ (k \bmod nm) & \longmapsto & (k \bmod n, k \bmod m) \end{array}$$

est un isomorphisme d'anneaux.

Méthode : Résolution de système de congruences

Trouver une solution particulière au système de congruence se fait soit en testant les valeurs, soit en trouvant des entiers de Bézout : on a $u, v \in \mathbb{Z}$ tels que $n \cdot u + m \cdot v = 1$. Alors $c = nub + mva$ est une solution particulière car $nu \equiv 1\ [m]$ et $mv \equiv 1\ [n]$.

On peut aussi résoudre directement le système en remarquant qu'il est équivalent à $k = a + n \cdot u = b + m \cdot v$ avec $u, v \in \mathbb{Z}$ et en résolvant l'équation diophantienne $n \cdot u - m \cdot v = b - a$ par la méthode habituelle.

Démonstration

1re formulation La méthode ci-dessus donne l'existence d'une solution particulière c.

Puis
$$\begin{cases} k \equiv a \ [n] \\ k \equiv b \ [m] \end{cases} \iff \begin{cases} k \equiv c \ [n] \\ k \equiv c \ [m] \end{cases} \iff k-c \text{ est divisible par } n \text{ et } m$$
$$\underset{n\wedge m=1}{\iff} nm \mid (k-c) \iff k \equiv c \ [nm].$$

2e formulation

(i) $k \equiv \ell \ [n]\, m$ donc $nm \mid (k-\ell)$ donc $n \mid (k-\ell)$ et $n \mid (k-\ell)$ donc $k \equiv \ell \ [n]$ et $k \equiv \ell \ [m]$.

(ii) f est bien définie d'après (i).
Puis, pour $k, \ell \in \mathbb{Z}$, par définition des additions sur $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$,

$$\begin{aligned} f\Big((k \bmod nm) + (\ell \bmod nm)\Big) &= f\Big((k+\ell) \bmod nm\Big) \\ &= \Big((k+\ell) \bmod n, (k+\ell) \bmod m\Big) \\ &= (k \bmod n, k \bmod m) + (\ell \bmod n, \ell \bmod m) \\ &= f\Big(k \bmod nm\Big) + f\Big(\ell \bmod nm\Big) \end{aligned}$$

On montre exactement de la même manière que

$$f\Big((k \bmod nm) \times (\ell \bmod nm)\Big) = f\Big(k \bmod nm\Big) \times f\Big(\ell \bmod nm\Big)$$

On a enfin que $f(1 \bmod nm) = (1 \bmod n, 1 \bmod m) = 1_{\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}}$.
Donc f est un morphisme d'anneaux.
La bijectivité correspond à la 1re méthode. Mais elle peut se retrouver plus facilement : comme le cardinal est le même au départ et à l'arrivée, on se contente de montrer l'injectivité (qui équivaut alors à la bijectivité) : si $f(k \bmod nm) = 0_{\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}}$, alors $\begin{cases} k \equiv 0 \ [n] \\ k \equiv 0 \ [m] \end{cases}$ donc $k \equiv 0 \ [nm]$ soit en utilisant la première formulation, soit en remarquant que $n \mid k$, $m \mid k$ et $n \wedge m = 1$ donc $nm \mid k$.
Finalement, $\operatorname{Ker} f = \{0_{\mathbb{Z}/n\mathbb{Z}}\}$ et f est un isomorphisme.

□

Exercice : CCINP 94

1. **Énoncer le théorème de Bézout dans $\mathbb{Z}$.**
2. **Soit a et b deux entiers naturels premiers entre eux.**
   Soit $c \in \mathbb{N}$.
   Prouver que : $(a|c$ et $b|c) \iff ab|c$.
3. **On considère le système (S) : $\begin{cases} x \equiv 6 \ [17] \\ x \equiv 4 \ [15] \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.**
   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
   (b) *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

---

1. Théorème de Bézout :
   Soit $(a, b) \in \mathbb{Z}^2$.
   $a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2 \,/\, au + bv = 1$.
2. Soit $(a, b) \in \mathbb{N}^2$. On suppose que $a \wedge b = 1$.
   Soit $c \in \mathbb{N}$.

   Prouvons que $ab|c \implies a|c$ et $b|c$.
   Si $ab|c$ alors $\exists k \in \mathbb{Z} \,/\, c = kab$.
   Alors, $c = (kb)a$ donc $a|c$ et $c = (ka)b$ donc $b|c$.
   Prouvons que $(a|c$ et $b|c) \implies ab|c$.

   $a \wedge b = 1$ donc $\exists (u, v) \in \mathbb{Z}^2 \,/\, au + bv = 1$. (1)
   De plus $a|c$ donc $\exists k_1 \in \mathbb{Z} \,/\, c = k_1 a$. (2)
   De même, $b|c$ donc $\exists k_2 \in \mathbb{Z} \,/\, c = k_2 b$. (3)
   On multiplie (1) par c et on obtient $cau + cbv = c$.
   Alors, d'après (2) et (3), $(k_2 b)au + (k_1 a)bv = c$, donc $(k_2 u + k_1 v)(ab) = c$ et donc $ab|c$.
   On a donc prouvé que $(a|c$ et $b|c) \iff ab|c$.

3. (a) **Première méthode** (méthode générale) :
Soit $x \in \mathbb{Z}$.

$$x \text{ solution de}(S) \iff \exists (k,k') \in \mathbb{Z}^2 \text{ tel que } \begin{cases} x = 6+17k \\ x = 4+15k' \end{cases}$$
$$\iff \exists (k,k') \in \mathbb{Z}^2 \text{ tel que } \begin{cases} x = 6+17k \\ 6+17k = 4+15k' \end{cases}$$

Or $6+17k = 4+15k' \iff 15k'-17k = 2$.
Pour déterminer une solution particulière x_0 de (S), il suffit donc de trouver une solution particulière (k_0, k'_0) de l'équation $15k'-17k=2$.
Pour cela, cherchons d'abord, une solution de l'équation $15u+17v=1$.
17 et 15 sont premiers entre eux.
Déterminons alors un couple (u_0, v_0) d'entiers relatifs tel que $15u_0+17v_0=1$.
On a : $17 = 15\times 1+2$ puis $15 = 7\times 2+1$.
Alors $1 = 15-7\times 2 = 15-7\times(17-15\times 1) = 15-17\times 7+15\times 7 = 15\times 8-17\times 7$
Donc $8\times 15+(-7)\times 17 = 1$
Ainsi, $16\times 15+(-14)\times 17 = 2$.

On peut prendre alors $k'_0 = 16$ et $k_0 = 14$.

Ainsi, $x_0 = 6+17\times k_0 = 6+17\times 14 = 244$ est une solution particulière de (S).

Deuxième méthode :
En observant le système (S), on peut remarquer que $x_0 = -11$ est une solution particulière.
Cette méthode est évidemment plus rapide mais ne fonctionne pas toujours.

(b) x_0 solution particulière de (S) donc $\begin{cases} x_0 & = & 6 & [17] \\ x_0 & = & 4 & [15] \end{cases}$.

On en déduit que x solution de (S) si et seulement si $\begin{cases} x-x_0 & = & 0 & [17] \\ x-x_0 & = & 0 & [15] \end{cases}$

c'est-à-dire x solution de $(S) \iff (17|x-x_0 \text{ et } 15|x-x_0)$.
Or $17\wedge 15 = 1$ donc d'après 2., x solution de (S) $\iff (17\times 15)|x-x_0$.
Donc l'ensemble des solutions de (S) est $\{x_0+17\times 15k,\ k\in\mathbb{Z}\} = \{244+255k,\ k\in\mathbb{Z}\}$.

3 Indicatrice d'Euler

Définition : Indicatrice d'Euler

L'**indicatrice d'Euler** est l'application définie sur $\mathbb{N}^*$ par $\varphi(n) = \left|\left\{k\in [\![1,n]\!],\ n\wedge k = 1\right\}\right|$.

Remarques

R 1 – $\varphi(1) = 1$.

R 2 – Si $n \geqslant 2$, $\varphi(n)$ est la cardinal du groupe $U_{\mathbb{Z}/n\mathbb{Z}}$ des inversibles de $\mathbb{Z}/n\mathbb{Z}$ (donc le nombre d'éléments inversibles).

R 3 – Il s'agit aussi du nombre de générateurs du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Propriété

Si p est premier, alors $\varphi(p) = p-1$. Et si, plus généralement, $k\in\mathbb{N}^*$, $\varphi\left(p^k\right) = p^{k-1}(p-1)$.

Démonstration

En effet, tous les entiers entre 1 et $p-1$ sont non divisibles par p donc premier avec lui.
Puis les entiers premiers avec p^k sont les entiers n'admettant pas p comme diviseur premier.
Combien y a-t-il de multiple de p entre 1 et p^k ?

Autant que de $\ell \in \mathbb{N}$ tel que $1 \leqslant \ell p \leqslant p^k$, c'est-à-dire, ℓ étant entier, $1 \leqslant \ell p \leqslant p^{k-1}$ soit exactement p^{k-1}.
D'où, finalement, $\varphi(p) = p^k - p^{k-1}$. □

Propriété

Soient $n, m \in \mathbb{N}^*$ tels que $n \wedge m = 1$.

(i) Si $k \in \mathbb{Z}$, et si $(k \bmod nm) \in U_{\mathbb{Z}/nm\mathbb{Z}}$ alors $(k \bmod n) \in U_{\mathbb{Z}/n\mathbb{Z}}$ et $(k \bmod m) \in U_{\mathbb{Z}/m\mathbb{Z}}$.

(ii) L'application

$$g : \left| \begin{array}{ccc} U_{\mathbb{Z}/nm\mathbb{Z}} & \longrightarrow & U_{\mathbb{Z}/n\mathbb{Z}} \times U_{\mathbb{Z}/m\mathbb{Z}} \\ (k \bmod nm) & \longmapsto & (k \bmod n, k \bmod m) \end{array} \right.$$

est un isomorphisme de groupes (multiplicatifs).

Démonstration

(i) Si $(k \bmod nm) \in U_{\mathbb{Z}/nm\mathbb{Z}}$ alors $k \wedge (nm) = 1$ donc $k \wedge n = k \wedge m = 1$ (pas de diviseur commun non trivial) donc $(k \bmod n) \in U_{\mathbb{Z}/n\mathbb{Z}}$ et $(k \bmod m) \in U_{\mathbb{Z}/m\mathbb{Z}}$.

(ii) Par (i), (et le (i) du théorème chinois), g est bien définie et comme f (du théorème chinois) était un morphisme d'anneaux, g est bien un morphisme de groupes multiplicatifs.
Comme restriction de f, g est injectif, reste à montrer la surjectivité : soit $a, b \in \mathbb{Z}$ tel que $(a \bmod n, b \bmod m) \in U_{\mathbb{Z}/n\mathbb{Z}} \times U_{\mathbb{Z}/m\mathbb{Z}}$.
Par surjectivité de f, on a $c \in \mathbb{Z}$ tel que $(a \bmod n, b \bmod m) = f(c \bmod nm)$. Reste à voir si $(c \bmod nm) \in U_{\mathbb{Z}/nm\mathbb{Z}}$.
Or $(a \bmod n) = (c \bmod n) \in U_{\mathbb{Z}/n\mathbb{Z}}$ et $(b \bmod m) = (c \bmod m) \in U_{\mathbb{Z}/m\mathbb{Z}}$ donc $c \wedge n = c \wedge m = 1$ et comme $n \wedge m = 1$, $c \wedge (mn) = 1$ d'où $(c \bmod nm) \in U_{\mathbb{Z}/nm\mathbb{Z}}$ puis $(a \bmod n, b \bmod m) = g(c \bmod nm)$: g est surjective.

□

Corollaire

φ est multiplicative, c'est-à-dire que si $n \wedge m = 1$, alors $\varphi(nm) = \varphi(n)\varphi(m)$.

Démonstration

En effet, avec l'isomorphisme de la question précédente,

$$\left|U_{\mathbb{Z}/nm\mathbb{Z}}\right| = \left|U_{\mathbb{Z}/n\mathbb{Z}} \times U_{\mathbb{Z}/m\mathbb{Z}}\right| = \left|U_{\mathbb{Z}/n\mathbb{Z}}\right| \times \left|U_{\mathbb{Z}/m\mathbb{Z}}\right|.$$

□

Corollaire

Plus généralement, si $n_1, \ldots, n_r$ sont deux à deux premiers entre eux,

$$\varphi(n_1 \cdots n_r) = \varphi(n_1) \cdots \varphi(n_r).$$

Démonstration

Récurrence. □

Corollaire

Si $p_1, \ldots, p_r$ sont les diviseurs premiers distincts de n,

$$\varphi(n) = n \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right).$$

Exercice : La même formule, avec des probabilités

Soit $\Omega = [\![1, n]\!]$ où n est un entier non premier supérieur ou égal à 2, muni de la probabilité uniforme. Si $d|n$, on note $A_d = \{kd \mid k \in \Omega \text{ et } kd \in \Omega\}$.

1. **Quelle est la probabilité de A_d ?**
2. **Soit P l'ensemble des diviseurs premiers de n.**
   (a) **Démontrer que $(A_p)_{p\in P}$ est une famille d'événements indépendants.**
   (b) **En déduire que $\varphi(n) = n \prod_{p\in P}\left(1-\frac{1}{p}\right)$.**

---

1. $\mathbb{P}(A_d) = \frac{|A_d|}{|\Omega|} = \frac{\frac{n}{d}}{n} = \frac{1}{d}$.
2. (a) Si $p_1, \dots, p_\ell$ sont des diviseurs premiers deux à deux distincts de n, comme ils sont premiers, $\bigcap_{j=1}^{\ell} A_{p_j} = A_{p_1\cdots p_\ell}$.
   $$\mathbb{P}\left(\bigcap_{j=1}^{\ell} A_{p_j}\right) = \mathbb{P}(A_{p_1\cdots p_\ell}) = \frac{1}{p_1\cdots p_\ell} = \prod_{j=1}^{\ell}\mathbb{P}(A_{p_j}).$$
   (b) Les $\overline{A}_p$ sont aussi indépendant, $A = \bigcap_{p\in P}\overline{A}_p$, $\mathbb{P}(A) = \frac{\varphi(n)}{n} = \prod_{p\in P}\left(1-\frac{1}{p}\right)$.

Théorème : d'Euler

Si $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ tel que $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1 \ [n]$.

Corollaire : Petit théorème de Fermat

Si p est premier et $a \in \mathbb{Z}^*$ non divisible par p, alors $a^{p-1} \equiv 1 \ [p]$.
Dans tous les cas (que a soit divisible ou non par p), $a^p \equiv a \ [p]$.

Théorème : de Fermat-Wiles, ou grand théorème de Fermat

Si $n \in \mathbb{N}$ tel que $n \geqslant 3$, alors l'équation $x^n + y^n = z^n$ n'admet aucune solution dans $\mathbb{N}_*^3$.

Démonstration : Non exigible[1]

□

Exercice : Une identité remarquable (et classique)

1. **Soient $n \in \mathbb{N}^*$ et $k \in \mathbb{N}$ un diviseur de n. Parmi tous les nombres rationnels de la forme $\frac{q}{n}$ où $1 \leqslant q \leqslant n$, combien y en a-t-il qui s'écrivent sous forme irréductible avec k au dénominateur ?**
2. **Montrer que, si $n \in \mathbb{N}^*$, $n = \sum_{k|n}\varphi(k)$.**

---

1. Notons F_k l'ensemble des nombres rationnels de la forme $\frac{q}{m}$ où $1 \leqslant q \leqslant m$ qui s'écrivent sous forme irréductible avec k au dénominateur et $E_k = \{\ell \in [\![0, k-1]\!] \mid \ell \wedge k = 1\}$ si $k \neq 1$ (remarquons qu'alors $0 \notin E_k$), $E_1 = \{1\}$.

   L'application $f : \begin{array}{ccc} E_k & \longrightarrow & F_k \\ \ell & \longmapsto & \frac{\ell}{k} \end{array}$ est *bijective* [b]. En effet,
   - si $k = 1$, f est l'identité de $F_1 = E_1 = \{1\}$;
   - sinon,
     - ⋆ elle est *bien définie* car si $\ell \in E_k$, $\frac{\ell}{k}$ est un nombre rationnel de la forme $\frac{q}{m}$ car $k|m$ avec $1 \leqslant q \leqslant m$ car $\frac{\ell}{k} \in]0, 1]$, qui s'écrit sous forme irréductible avec k au dénominateur car $\ell \wedge k = 1$ et donc $f(\ell) \in F_k$;
     - ⋆ elle est *injective* car si $\ell, \ell' \in E_k$ tels que $f(\ell) = f(\ell')$, alors $\frac{\ell}{k} = \frac{\ell'}{k}$ donc $\ell = \ell'$;

1. J ai découvert une démonstration véritablement merveilleuse que ce cadre est trop étroit pour contenir...

- ⋆ elle est *surjective* car si $r \in F_k$, $r \in \mathbb{Q} \cap]0,1]$ et r s'écrit forme irréductible avec k au dénominateur, donc on a $l \in [\![1,k]\!]$ avec $k \wedge \ell = 1$ tel que $r = \frac{\ell}{k}$. Comme $k \neq 1$, $\ell \neq k$ donc $\ell \in [\![1,k-1]\!]$, $\ell \in E_k$ et donc $r = f(\ell)$.

Ainsi, le nombre de rationnels de la forme $\frac{q}{m}$ où $1 \leqslant q \leqslant m$ qui s'écrivent sous forme irréductible avec k au dénominateur est le nombre d'entiers l tels que $0 \leqslant l \leqslant k-1$ et $k \wedge l = 1$ si $k \neq 1$, 1 sinon : il y en a donc $\varphi(k)$.

2. Si on note $F = \left\{\frac{q}{m}\ ;\ 1 \leqslant q \leqslant m\right\}$, alors $F = \bigsqcup_{k|m} F_k$ car tout rationnel de F s'écrit de manière unique sous forme irréductible avec un diviseur de m au dénominateur.

   Donc $|F| = \sum_{k|m} |F_k|$, et comme $|F| = \left|[\![1,m]\!]\right| = m$, $\boxed{m = \sum_{k|m} \varphi(k)}$ d'après la question précédente.

---

b. On peut aller un peu plus vite oralement en invoquant simplement l'existence et l'unicité de la forme irréductible des fractions.