120 : Anneaux $\frac{\mathbb{Z}}{m\mathbb{Z}}$. Applications.

I. L'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$

a) Construction

Prop. 1 : Pour $m \in \mathbb{N}$, les $m\mathbb{Z}$ sont les idéaux de $(\mathbb{Z}, +)$.

Def. 2 : Soient $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ on dit a est congru à b modulo m si $b - a \in m\mathbb{Z}$. On note $a = b \ [m]$.

À partir de maintenant on suppose $m \geq 2$.

Thm. 3 : Il existe une unique structure d'anneau commutatif unitaire sur $\frac{\mathbb{Z}}{m\mathbb{Z}}$ t.q. π_m (la surjection) canonique soit un morphisme d'anneau.

Thm. 4 : $\frac{\mathbb{Z}}{m\mathbb{Z}} = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ où $\bar{a} = \{a + qm \mid q \in \mathbb{Z}\}$. Cet ensemble est de cardinal m et est en bijection avec l'ensemble de tous les restes possibles dans la division euclidienne par m.

Rmq. 5 : On identifie $\frac{\mathbb{Z}}{0\mathbb{Z}}$ à $\mathbb{Z}$ et $\frac{\mathbb{Z}}{1\mathbb{Z}}$ à $\{\bar{0}\}$.

b) Structure

Thm. 6 : 1) Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
2) Tout groupe cyclique d'ordre n est isomorphe à $\frac{\mathbb{Z}}{n\mathbb{Z}}$. En particulier, 2 groupes cycliques sont isomorphes ssi ils ont même ordre.

Cor. 7 : Soit $p \in P$, et G un groupe d'ordre p. Alors G est cyclique et $G \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$.

Prop. 8 : $(\frac{\mathbb{Z}}{m\mathbb{Z}}, +)$ est cyclique.

Thm. 9 : Les sous groupes de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont cycliques d'ordres divisant n. Réciproquement, pour tout diviseur d de n, il existe un unique sous groupe de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ d'ordre d, c'est le sous groupe cyclique $(\bar{q}) = \{\bar{0}, \dots, (\theta-1)\bar{q} \mid$ où $q = \frac{n}{d}$. Les générateurs de ce groupe sont les éléments d'ordre d de $\frac{\mathbb{Z}}{m\mathbb{Z}}$.

Thm. 10 : 1) Les idéaux de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont les sous groupe $(\frac{\mathbb{Z}}{m\mathbb{Z}}, +)$.
2) Les idéaux premiers de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont exactement les idéaux maximaux.
3) Les idéaux premiers de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont les $(\bar{p})$ où $p \in P$ et $p \mid n$.

Thm. 11 : Soit $a \in \mathbb{Z}$. Les ASSE :
(i) $\bar{a} \in (\frac{\mathbb{Z}}{m\mathbb{Z}})^\times$
(ii) $\text{pgcd}(a, m) = 1$
(iii) $\bar{a}$ est un générateur de $(\frac{\mathbb{Z}}{m\mathbb{Z}}, +)$.

Prop. 12 : Les diviseurs de 0 de $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont $\frac{\mathbb{Z}}{m\mathbb{Z}} \setminus \left((\frac{\mathbb{Z}}{m\mathbb{Z}})^\times \cup \{0\}\right)$

Prop. 13 : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Soit $k \in \mathbb{Z}$.
$\bar{k}$ est nilpotent ssi $p_1 \cdots p_r$ divise k.

Thm. 14 : (Théorème Chinois) Soient $m_1, \dots, m_r \in \mathbb{N}^* \setminus \{1\}$ et $n = m_1 \cdots m_r$.
$m_1, \dots, m_r$ sont 2 à 2 premier entre eux ssi $\frac{\mathbb{Z}}{m\mathbb{Z}}$ et $\prod_{j=1}^{r} \frac{\mathbb{Z}}{m_j\mathbb{Z}}$.

Dans ce cas, $\Psi : \frac{\mathbb{Z}}{m\mathbb{Z}} \to \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$ est un isomorphisme d'anneaux.

$\bar{x}^m \mapsto (\bar{x}^{m_1}, \dots, \bar{x}^{m_r})$

Et son inverse est :

$\Psi^{-1} : \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{m\mathbb{Z}}$

$(\bar{x}_1^{m_1}, \dots, \bar{x}_r^{m_r}) \mapsto \overline{x_1 u_1 \frac{m}{m_1} + \cdots + x_r u_r \frac{m}{m_r}}^{m}$

où $u_1 \frac{m}{m_1} + \cdots + u_r \frac{m}{m_r} = 1$.

c) Le cas particulier n un nombre premier

Thm. 15 : Les ASSE :
(i) n est premier.
(ii) $\frac{\mathbb{Z}}{m\mathbb{Z}}$ est un corps.
(iii) $\frac{\mathbb{Z}}{m\mathbb{Z}}$ est intègre.

Cor. 16 : $(\frac{\mathbb{Z}}{p\mathbb{Z}})^\times = \frac{\mathbb{Z}}{p\mathbb{Z}} \setminus \{0\}$ où $p \in P$.

II. Etude de $(\frac{\mathbb{Z}}{m\mathbb{Z}})^\times$

a) L'indicatrice d'Euler et $(\frac{\mathbb{Z}}{m\mathbb{Z}})^\times$

Def. 17 : On appelle indicatrice d'Euler et on note $\varphi(n)$ le nombre d'entiers inférieurs à n qui sont premiers à n.

Cor. 18 : $\varphi(n) = \left|(\frac{\mathbb{Z}}{m\mathbb{Z}})^\times\right|$.

Prop. 19 : Si $p \in P$, $\varphi(p) = p - 1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ $(\alpha \in \mathbb{N}^*)$.

Prop. 20 : $\text{Aut}(\frac{\mathbb{Z}}{m\mathbb{Z}}) \simeq (\frac{\mathbb{Z}}{m\mathbb{Z}})^\times$.

Thm. 21 : Soit $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en facteur premier. On a :

- $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \simeq \prod_{i=1}^{r}\left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)^\times$

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

[ROM] p.281-282 **Thm. 22** : (Euler) Pour tout $a\in\mathbb{N}$ premier à n on a $a^{\varphi(n)} = 1\ [n]$.

Cor. 23 : (Fermat) Pour $p\in\mathcal{P}$, $a\in\mathbb{N}$ tq a et p sont premiers entre eux on a : $a^p = a\ [p]$.

[FGE] p.30 **Thm. 24** : [ADMIS] Un groupe d'ordre n est cyclique ssi $\text{pgcd}(n,\varphi(n)) = 1$.

[PER] p.24 **Prop. 25** : $n\in\mathbb{N}^*$, $n = \sum_{d|n}\varphi(d)$.

[PER] p.25 **Prop. 26** : $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ est cyclique, isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$ $(p\in\mathcal{P})$.

b) Cyclicité de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$?

Le théorème 21 nous donne une décomposition en produit de $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$

Lemme 27 : Soient $a, b\in G$ (G un groupe) d'ordres p et q. Si a et b commutent et p, q premiers entre eux alors ab est d'ordre pq.

Lemme 28 : Pour $k\in\mathbb{N}^*$, $p\in\mathcal{P}$ on a $(1+p)^{p^k} = 1+\lambda p^{k+1}$ avec $\lambda\in\mathbb{N}^*$ premier à p.

[PER] p.25-27 DEV1 **Thm. 29** : 1) Si $p\in\mathcal{P}$ tq $p\geq 3$, soit $\alpha\geq 2$ on a :

$$\left(\mathbb{Z}/p^\alpha\mathbb{Z}\right)^\times \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z} \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}.$$

2) Si $\alpha\geq 3$, alors $\left(\mathbb{Z}/2^\alpha\mathbb{Z}\right)^\times$ n'est pas cyclique.

Thm. 30 : $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ est cyclique ssi $n = 1, 2, 4, p^\alpha, 2p^\alpha$ avec $p\in\mathcal{P}$ tq $p\geq 3$ et $\alpha\geq 1$.

III – Applications

a) Équations diophantienne et systèmes de congruence

On cherche à résoudre l'équation diophantienne dans $\mathbb{Z}$:

(E) : $ax = b\ [n]$, $a\in\mathbb{N}^*$, $b\in\mathbb{Z}$.

Prop. 31 : L'ensemble des sol. de $ax = 1\ [n]$ où $\text{pgcd}(a,n) = 1$ est $S = \{x_0 + kn \mid k\in\mathbb{Z}\}$ où x_0 est une solution particulière obtenue avec l'algo. d'Euclide. [ROM] p.282

Cor. 32 : Si a et n premiers entre eux une solution de (E) est $S' = \{bx_0 + kn \mid k\in\mathbb{Z}\}$ (x_0 de la prop. 31).

Thm. 33 : (E) a des solutions entières ssi $\delta := \text{pgcd}(a,n)$ divise b. Dans ce cas, en notant $a = \delta a'$ et $n = \delta n'$ (a', n' premiers entre eux) l'ensemble des solutions de (E) est $\{b'x_0' + kn' \mid k\in\mathbb{Z}\}$ où x_0' sol. particulière de $a'x = 1\ [n']$.

Prop. 34 : Soient m, n premiers entre eux, $a, b\in\mathbb{Z}$. L'ensemble des solutions de $\begin{cases} x = a\ [m] \\ x = b\ [n]\end{cases}$ est $\{avn + bum + kmn \mid k\in\mathbb{Z}\}$ avec $u, v\in\mathbb{Z}$ tq $um + vn = 1$. [CVA] p.201-204

Thm. 35 : On considère le système :

(S) : $\begin{cases} x = a\ [m] \\ x = b\ [n]\end{cases}$. Notons $\delta = \text{pgcd}(m,n)$ et $\mu = \text{ppcm}(m,n)$.

Si $a = b$ dans $\mathbb{Z}/\delta\mathbb{Z}$ alors l'ensemble des sol. de (S) est $\{x_0 + k\mu \mid k\in\mathbb{Z}\}$ où $\begin{cases} x_0 = \frac{1}{\delta}(avn + bum) \\ um + vn = \delta\end{cases}$. DEV2

Appli. 36 : $\begin{cases} x = 3\ [21] \\ x = 10\ [35]\end{cases}$ l'ensemble des solutions est $\{45 + 105k \mid k\in\mathbb{Z}\}$.

b) Codage RSA

Principe : Bob transmet un message codé m à Alice. Celui qui code doit connaître la clef publique et celui qui décode doit connaître la clef privé.

Préparatifs : Bob choisit 2 nombres premier p, q (distincts), on note $n = pq$, $\varphi(n) = (p-1)(q-1)$ on choisit e premier à $\varphi(n)$ on cherche d tq $de = 1\ [\varphi(n)]$ (en utilisant Bézout). (n, e) est la clef publique, (n, d) est la clef privé. [CVA] p.209

Codage : Bob calcul le message codé $M = m^e\ [n]$ puis envoie à Alice.

Décodage : Alice reçoit M, calcule $M^d\ [n]$ (ie $m^{ed}\ [n]$), Alice récupère m (car $m^{ed} = m\ [n]$).

c) Caractéristique d'un anneau et d'un corps

A anneau, K corps.

Def. 36 : $\theta_A : \mathbb{Z} \to A$, $m \mapsto m 1_A$ est un morphisme de groupe.
Son noyau est un sous groupe de $\mathbb{Z}$, i.e un $c\mathbb{Z}$ ($c \geq 0$)
c est appelé caractéristique de A, noté $car(A)$.

[BERS p.394 - 395]

Prop. 37 : $car(A) > 0$ ssi $m.1_A = 0_A$ a une solution non nulle.
De plus, $\forall m \in \mathbb{Z}$, si $m 1_A = 0_A$ alors $car(A) | m$.

Rmq. 38 : Si B est sous anneau de A alors $car(A) = car(B)$.

Prop. 39 : A contient un sous anneau isomorphe à $\frac{\mathbb{Z}}{car(A)\mathbb{Z}}$.

Rmq. 40 : Si $car(A) | m$ alors $m.a = 0_A$ pour tout $a \in A$.

Prop. 41 : $\frac{\mathbb{Z}}{car(K)\mathbb{Z}} \simeq Im(\theta_K) \subset K$ intègre, donc $car(K)\mathbb{Z}$ est un idéal premier. $car(K) = 0$ ou un nombre premier.

[PERS p.72]

Prop. 42 : Si $car(K) = 0$ alors le sous corps premier de K est $\mathbb{Q}$.
Si $car(K) = p$, le sous corps premier de K est $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

Cor. 43 : Le cardinal d'un corps fini est une puissance d'un nombre premier.

d) Carrés dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$, $p \in P$

Def. 44 : On note $\mathbb{F}_p^2 = \{x \in \frac{\mathbb{Z}}{p\mathbb{Z}} \mid \exists y \in \frac{\mathbb{Z}}{p\mathbb{Z}}, x^2 = y\}$ et $\mathbb{F}_p^{\times 2} = \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^\times \cap \mathbb{F}_p^2$.

[PERS p.74 - 75]

Prop. 45 : $\mathbb{F}_2^2 = \mathbb{F}_2$, si $p \geq 3$ $|\mathbb{F}_p^2| = \frac{p+1}{2}$ et $|\mathbb{F}_p^{\times 2}| = \frac{p-1}{2}$.

Thm. 46 : $p \geq 3$. $x \in \mathbb{F}_p^2$ ssi $x^{\frac{p-1}{2}} = 1$.

Cor. 47 : $p \geq 3$. -1 est un carré dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ ssi $p = 1 [4]$.

Rmq 48 : Ce résultat permet de démontrer le théorème des deux carrés.

e) Irréductibilité de certains polynômes

Thm. 49 : (Eisenstein) Soit $P = a_m X^m + \dots + a_0 \in \mathbb{Z}[X]$. Si il existe $p \in P$ tq :

[PERS p.76 - 77]

- $p \nmid a_m$
- $p | a_i$ $\forall i \in \{0, \dots, m-1\}$
- $p^2 \nmid a_0$

Alors P est irréductible dans $\mathbb{Q}[X]$. Si $pgcd(a_0, \dots, a_m) = 1$ alors P est irréductible dans $\mathbb{Z}[X]$.

Thm. 50 : Soit $p \in P$ et $P \in \mathbb{Z}[X]$. En notant $\bar{P}$ la réduction de P dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ tq $\deg(\bar{P}) \neq 0$. Si $\bar{P}$ irréductible dans $\frac{\mathbb{Z}}{p\mathbb{Z}}$ alors P irréductible dans $\mathbb{Q}[X]$.

Def. 51 : On note $\mu_m = \{\zeta \in \mathbb{C} \mid \zeta^m = 1\}$ et μ_m^* ses générateurs. ($m \in \mathbb{N}^*$)

[PERS p.80 - 81]

Def. 52 : Pour $m \in \mathbb{N}^*$ on définit le m-ème polynôme cyclotomique
$\Phi_m = \prod_{\zeta \in \mu_m^*} X - \zeta$

Prop. 53 : Φ_m est unitaire de degré $\varphi(m)$.

Prop. 54 : $\Phi_m \in \mathbb{Z}[X]$.

Thm. 55 : Φ_m est irréductible dans $\mathbb{Z}[X]$.

Rmq. 56 : La réduction modulo p est cruciale dans la démonstration de 55.

Rmq. 57 : La connaissance de polynômes irréductibles permet de construire des corps finis, en effet :

[PERS p.925]

Thm. 58 : Soit $P \in \mathbb{F}_p[X]$ irréductible de degré n, alors $\mathbb{F}_{p^n} \simeq \frac{\mathbb{F}_p[X]}{(P)}$

Rmq. 59 : Il est possible de dénombrer le nombre de polynômes irréductible unitaire dans $\mathbb{F}_p[X]$.

f) Structure des groupes abéliens

G un groupe abélien.

Thm. 60 [ADMIS] (structure des groupes abéliens finis) Si G est fini alors il existe $d_1, \dots, d_s$ des entiers supérieurs à 2 tq $d_1 | \dots | d_s$ et

[PERS p.358]

$$G \simeq \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{d_s\mathbb{Z}}$$

$(d_1, \dots, d_s)$ est unique et ne dépend que de la classe d'isomorphisme de G.

Def. 61 : $d_1, \dots, d_s$ sont appelés invariants de similitudes de G.

Cor. 62 : Deux groupes abéliens sont isomorphes ssi ils ont même invariants de similitudes.

Références:

[CROM]: Rombaldi, Mathématiques pour l'agrégation algèbre et géométrie

[FRAN]: Francinou, Algèbre 1 - Oraux X-ENS

[PERR]: Perrin, Cours d'Algèbre.

[CVAL]: Caldero, Carnet de voyage en Algèbrie

[BERH]: Berhuy, Algèbre le grand combat

[FGN]: Francinou, Algèbre 1. Exercices de mathématiques pour l'agrégation.

Commentaires:

- Pour le thm. 29 il y a un "sens" dans CROM p.16. Le résultat est dur à montrer (produit semi direct, Burnside, p-Sylow ...). C'est M. Mansuy qui m'a incité à mettre ce résultat.

- Les thm. 6 et cor. 7 auraient peut être leurs place dans III-j) pour en faire une partie sur l'utilisation de $\mathbb{Z}/n\mathbb{Z}$ en théorie des groupes (où on pourrait alors ajouter thm. 29).

- On peut, peut-être, diminuer la partie sur les polynômes cyclotomique en supposant la notion connue.

- Je pense que l'irréductibilité des polynômes cyclotomiques peut être fait en dev. (à bien justifier).

- La notion de symbole de Legendre et loi de reciprocité quadratique peuvent être mit dans III-d). Je pense que la loi de reciprocité quadratique peut-être fait en dev..

- On peut parler de nombres de Carmichael.

- Pour le codage RSA (III-b)) Science Etonnante a fait une vidéo dessus qui permet de bien comprendre l'idée, elle s'appelle "L'Algorithme qui sécurise Internet (entre autres...)".