120. Anneaux $\mathbb{Z}/n\mathbb{Z}$ - Applications.

On rappelle que $(\mathbb{Z},+,\cdot)$ est un anneau commutatif euclidien. $n\in\mathbb{N}$.

I. Groupes $(\mathbb{Z}/n\mathbb{Z},+)$

1) Définitions, premières propriétés

Prop. 1 : Les sous-groupes de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$, $n\in\mathbb{N}$.

Déf./Prop. 2 : $(\mathbb{Z}/n\mathbb{Z},+)$ est le groupe quotient de $\mathbb{Z}$ par $n\mathbb{Z}$. L'opération $a \bmod n + b \bmod n = (a+b) \bmod n$ est l'unique loi sur $\mathbb{Z}/n\mathbb{Z}$ faisant de la projection canonique $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$, $k \longmapsto \bar{k} = k \bmod n$ un morphisme de groupes.

Prop. 3 : Si $n=0$, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}$ est un groupe monogène infini. Si $n\geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique de cardinal n. Plus précisément, $\mathbb{Z}/n\mathbb{Z} = \{\bar{0},\bar{1},\dots,\overline{n-1}\} = \langle \bar{1} \rangle$.

Th. 4 : 1) Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
2) Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

Ex. 5 : Pour $n\in\mathbb{N}^*$, on pose $\mu_n = \{z\in\mathbb{C} \,/\, z^n = 1\}$. Alors $(\mu_n,\times) \simeq (\mathbb{Z}/n\mathbb{Z},+)$.

2) Ordre dans $(\mathbb{Z}/n\mathbb{Z},+)$. Générateurs $n\in\mathbb{N}^*$

Notation 6 : Si G est un groupe et $x\in G$ est d'ordre fini, on notera $o(x)$ son ordre.

[Ber] 151 Th. 7 : 1) $o(\bar{1}) = n$
2) Si $k\in\mathbb{Z}$, alors $o(\bar{k}) = \dfrac{n}{\operatorname{pgcd}(k,n)}$

Ex. 8 : Dans $\mathbb{Z}/10\mathbb{Z}$, $o(\bar{4}) = 5$.

Prop. 9 : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont exactement les $\langle \overline{\tfrac{n}{d}} \rangle$, où $d\in\mathbb{N}$ et $d\mid n$. On a alors $\langle \overline{\tfrac{n}{d}} \rangle \simeq \mathbb{Z}/d\mathbb{Z}$

Th. 10 : Soit $k\in\mathbb{Z}$. Sont équivalentes : [Per] 24
1) $\bar{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$
2) $k\wedge n = 1$

Ex. 11 : Les générateurs de $\mathbb{Z}/4\mathbb{Z}$ sont $\bar{1}$ et $\bar{3}$.

Déf. 12 : Pour $n\geq 1$, on définit $\varphi(n) = |\{1\leq k\leq n \,/\, k\wedge n = 1\}|$. 24
Par convention, $\varphi(1)=1$. φ est appelée l'indicatrice d'Euler.

Prop. 13 : Soit p premier et $\alpha\in\mathbb{N}^*$, alors $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

Coro. 14 : Si la décomposition de n en facteurs premiers est $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)$ 25

Prop. 15 : 1) $\mathbb{Z}/n\mathbb{Z}$ admet $\varphi(n)$ générateurs
2) si $d\mid n$, $\mathbb{Z}/n\mathbb{Z}$ admet $\varphi(d)$ éléments d'ordre d.

Coro 16 : $\forall n\geq 1$, $n = \sum_{d\mid n} \varphi(d)$

Ex. 17 : Soit $\mu_n^* = \{\xi\in\mu_n \,/\, \forall 1\leq k\leq n-1,\ \xi^k \neq 1\}$ l'ensemble des racines primitives n-ièmes de l'unité. Alors $|\mu_n^*| = \varphi(n)$. 80

II. Anneaux $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ $n\geq 2$

1) Cas général

Prop. 18 : Les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$, $n\in\mathbb{Z}$.
Si $n\in\mathbb{N}$, l'opération $a \bmod n \cdot b \bmod n = (ab) \bmod n$ est l'unique loi sur $\mathbb{Z}/n\mathbb{Z}$ faisant de la projection canonique un morphisme d'anneaux.

Déf. 19 : Soit $\bar{k}\in\mathbb{Z}/n\mathbb{Z}$. $\bar{k}$ est dit inversible s'il existe $\bar{k'}\in\mathbb{Z}/n\mathbb{Z}$ tel que $\bar{k}\cdot\bar{k'} = \bar{1}$. On note $\mathbb{Z}/n\mathbb{Z}^\times$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z}^\times,\cdot)$ est un groupe. [Per] 24

[Pa] 24 Th. (20) : Soit $k \in \mathbb{Z}$. Alors, $\bar{k} \in \mathbb{Z}/n\mathbb{Z}^\times$ SSI $k \wedge n = 1$

Coro. (21) : $|\mathbb{Z}/n\mathbb{Z}^\times| = \varphi(n)$

Th. (22) : $\begin{array}{ccc}(\mathrm{Aut}((\mathbb{Z}/n\mathbb{Z},+)),\circ) & \to & (\mathbb{Z}/n\mathbb{Z}^\times,\cdot) \\ f & \mapsto & f(\bar{1})\end{array}$ est un isomorphisme de groupes

24 Coro (23) : $|\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$

2) Cas $n = p$ premier

Th. (24) : Soit $n \in \mathbb{N}$. Alors $\mathbb{Z}/n\mathbb{Z}$ est intègre SSI $n = 0$ ou n est premier.

Coro. (25) : Si p est premier, alors $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ est un corps. On a alors $|\mathbb{Z}/p\mathbb{Z}^\times| = p - 1$.

179 Th. (26) : (petit théorème de Fermat)
Soit p premier et $a \in \mathbb{Z}$. Alors, $a^p \equiv a\ [p]$. De plus, si $a \wedge p = 1$, alors $a^{p-1} \equiv 1\ [p]$.

Th. (27) : Soit p premier. Alors, $\mathbb{F}_p^*$ est cyclique. On a donc $(\mathbb{F}_p^*, \cdot) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}, +)$.

3) Théorème des restes chinois

Th. (28) : (théorème des restes chinois)
Soient $a, b \in \mathbb{N}^*$. Alors $\begin{array}{cccc}\Psi : & \mathbb{Z}/ab\mathbb{Z} & \to & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & x \bmod ab & \mapsto & (x \bmod a, x \bmod b)\end{array}$
est un morphisme d'anneaux bien défini. De plus, Ψ est un isomorphisme SSI $a \wedge b = 1$

Rq (29) : Le Th. (28) s'étend à une famille $a_1 \dots a_n$ d'entiers
[Pa] deux à deux premiers entre eux.

25 Coro (30) : Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$, alors $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \left(\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)$

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

Appli (31) : (système de congruences) [Ba]
L'ensemble solution de $\begin{cases} x \equiv -1\ [3] \\ x \equiv 2\ [4] \\ x \equiv -1\ [7] \end{cases}$ est $\{34 + 84k,\ k \in \mathbb{Z}\}$ 469

III. Applications

1) Théorème de structure des groupes abéliens finis (g.a.f.) [Ba]

Cadre (32) : $(G, \cdot)$ est un groupe abélien , noté multiplicativement 346

Déf. (33) : Un caractère linéaire sur G est un morphisme de groupes $\chi : G \to (\mathbb{C}^*, \cdot)$. On note $\hat{G}$ le groupe des caractères linéaires sur G.

Rq (34) : Si $G = \mathbb{Z}/n\mathbb{Z}$, alors $\hat{G} \simeq G$. 347

Lemme (35) : (prolongement des caractères)
Soit $H \leq G$ et $\begin{array}{cccc}\rho_H : & \hat{G} & \to & \hat{H} \\ & \chi & \mapsto & \chi_{|H}\end{array}$. ρ_H est un morphisme de groupes.
Si $[G:H]$ est fini, alors ρ_H est surjective. DVP 1

Th. (36) : (théorème de structure des g.a.f.) 358
Soit G un g.a.f., $|G| \geq 2$. Alors il existe $d_1 \dots d_s \geq 2$ tels que $d_1 | d_2 | \dots | d_s$ et $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$. De plus, $d_1 \dots d_s$ sont uniques et ne dépendent que de la classe d'isomorphisme de G.

Ex. (37) : 1) Si $|G| = 60$, alors $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ ou $G \simeq \mathbb{Z}/60\mathbb{Z}$
2) Si p premier et $|G| = p^2$, alors G est abélien et $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p^2\mathbb{Z}$.

Coro. (38) : Si G est un g.a.f., alors $G \simeq \hat{G}$

2) Éléments sur les corps finis. Carrés [Pe]

a°/

Déf./Prop. (39) : Soit K un corps commutatif et $\begin{array}{cccc}f : & \mathbb{Z} & \to & K \\ & n & \mapsto & n.1_K\end{array}$. Alors f est un morphisme d'anneaux et $\mathrm{Ker} f = \{0\}$ ou $\mathrm{Ker} f = \mathbb{Z}/p\mathbb{Z}$, p premier. 0, ou p est appelée caractéristique de K, notée $\mathrm{car}(K)$. 72

72 Déf. 40 : Si $car(K) = 0$, on dit que $\mathbb{Q}$ est le sous-corps premier de K.
Si $car(K) = p$, on dit que $\mathbb{F}_p$ est le sous-corps premier de K.

Prop./Déf. 41 : Si K est fini, alors il existe p premier et $\alpha \in \mathbb{N}^*$ tel que $|K| = p^\alpha = q$.

Prop. 42 : Si $car(K) = p > 0$, alors $F : \begin{array}{l} K \to K \\ x \mapsto x^p \end{array}$ est un morphisme de corps
73 appelé morphisme de Frobenius. Si K est fini, c'est un automorphisme.
Si $K = \mathbb{F}_p$, c'est l'identité.

Th. 43 : Soit $q = p^\alpha$. Alors, il existe un unique corps de cardinal q, à isomorphisme près. On le note $\mathbb{F}_q$.

Th. 44 : $(\mathbb{F}_q^*, \cdot)$ est cyclique. On a donc $(\mathbb{F}_q^*, \cdot) \simeq (\mathbb{Z}/(q-1)\mathbb{Z}, +)$
74

3) Polynômes cyclotomiques

[Pa]
Déf. 45 : Soit $n \in \mathbb{N}^*$. Le n-ième polynôme cyclotomique est
80 $\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi) \in \mathbb{C}[X]$.

Prop. 46 : $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d \mid n} \Phi_d$

Ex. 47 : $\Phi_1 = X - 1$; $\Phi_2 = X + 1$; $\Phi_3 = X^2 + X + 1$; $\Phi_p = X^{p-1} + \dots + X + 1$ p premier
81
Th. 48 : $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$

82 Th. 49 : $\forall n \in \mathbb{N}^*$, Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$

Appli. 50 : (théorème de Dirichlet faible)
DVP2 [FGN3] 31 Soit $n \in \mathbb{N}^*$. Alors, il existe une infinité de nombres premiers congrus à 1 modulo n.

~~4) Chiffrement RSA~~

Faire b°/ carrés dans les corps finis
[Pa] [NH2G2] aller jusqu'au symbole de Legendre et à la loi de réciprocité quadratique

<u>Références</u>

- [Be] Berhuy, Algèbre : le grand combat (2e éd.)
- [Pe] Perrin, Cours d'algèbre
- [FGN1] Francinou..., Oraux X-ENS Algèbre 1
- [NH2G2] Caldero, Nouvelles... Tome 1