8 Leçon 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

I. Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ [BER] [ROM]

Relation de congruence, structure de groupe, cyclicité, sous-groupes, groupes d'ordre p^2, théorème de structure des groupes abéliens finis

II. L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

1. Construction et premières propriétés [BER]

Structure d'anneau, cas lorsque n est premier, DEV 1 : Théorème chinois, diviseurs de zéros et éléments nilpotents

2. Le groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$ [ROM]

$(\mathbb{Z}/n\mathbb{Z})^\times$, éléments inversibles, fonction indicatrice d'Euler, DEV 1 : formule générale de l'indicatrice d'Euler, théorème d'Euler, théorème de Fermat, conditions $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique

III. Applications

1. Systèmes de congruences [ROM]

Equations diophantiennes + conditions de résolution, théorème chinois explicite + exemple de système

2. Corps finis [PER]

Sous corps premier, caractéristique, morphisme de Froebenius, construction de $\mathbb{F}_q$

3. Irréductibilité de polynômes [PER]

Critère d'Eisenstein, réduction modulo p, polynômes cyclotomiques, DEV 2 : Irréductibilité de $\Phi_n(X)$ + polynôme minimal d'une racine primitive n-ième de l'unité

Présentation :

- Lorsque l'on fait de l'arithmétique dans $\mathbb{Z}$, on s'intéresse rapidement au reste dans la division euclidienne. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ formalisent cette notion et vont obtenir des propriétés remarquables, héritées de celle de $\mathbb{Z}$.
- Comme tout groupe cyclique est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, il suffit d'étudier ce groupe là pour en déduire des propriétés sur tous les groupes cycliques.
- Le théorème chinois était utilisé par exemple par les généraux chinois pour compter leurs troupes. Ils demandaient à leurs soldats de se ranger par groupe de n_1 personnes et notaient le reste r_1, puis par groupe de n_2 personnes avec $n_1 \wedge n_2 = 1$ et notaient le reste r_2.
- Lorsque p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps. Cela va être utile en théorie des corps car permet de construire tous les corps finis à partir d'un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.
- La réduction modulo p est un outil extrèmement efficace, notamment dans les preuves de théorèmes pour montrer l'irréductibilté de polynômes.

Développements :

- Théorème chinois + application à l'indicatrice d'Euler

  - Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p249-283
- Irréductibilité des polynômes cyclotomiques + degré d'une extension cyclotomique

- Théorie de Galois, Gozard, p69
- Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p384
- Cours d'algèbre, Perrin, p80

Références :

- [BER] Algèbre : le grand combat, Berhuy
- [ROM] Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi
- [PER] Cours d'algèbre, Perrin

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

I Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ [BER] [ROM]

Déf 1 : Soit $n \in \mathbb{N}$ et $a, b \in \mathbb{Z}$. On dit que a est congru à b modulo n si $a-b$ est un multiple de n, c'id il existe $k \in \mathbb{Z}$ tel que $a = b + kn$. On note $a \equiv b\ [n]$.

Lemme 2 : La relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient. Si $a \in \mathbb{Z}$, on note $\overline{a}$ sa classe d'équivalence.

Prop 3 : On définit sur $\mathbb{Z}/n\mathbb{Z}$ la loi $+$ telle que $\overline{a} + \overline{b} = \overline{a+b}$, qui lui confère une structure de groupe abélien.

Remarque 4 : $\forall a \in \mathbb{Z} : \overline{a} = \overline{0} \iff n \mid a$.

Lemme 5 : Pour tout $n \geq 1$, le groupe $\mathbb{Z}/n\mathbb{Z}$ possède n éléments qui sont $\overline{0}, \overline{1}, \dots, \overline{n-1}$.

Prop 6 : Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique d'ordre n, engendré par $\overline{1}$.

Théorème 7 : Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemple 8 : Le groupe μ_n des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Corollaire 9 : Tout groupe d'ordre p premier est cyclique et isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Théorème 10 : Pour $n \geq 2$, tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre qui divise n. Réciproquement, pour tout diviseur d de n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d qui est $H = \langle \overline{q} \rangle$ où $q = \frac{n}{d}$.

Prop 11 : Soit G un groupe d'ordre p^2. Alors G est abélien et en particulier :
$G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Théorème 12 (de structure des groupes abéliens finis) ADMIS :
Soit G un groupe abélien fini. Alors il existe des entiers $d_1, \dots, d_s \geq 2$ tel que $d_1 \mid d_2 \mid \dots \mid d_s$ et
$G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}$
La suite $(d_1, \dots, d_s)$ est unique.

II L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

1) Construction et premières propriétés [BER] [ROM]

Prop 13 : Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$, avec $n \in \mathbb{N}$.

Prop 14 : On munit $\mathbb{Z}/n\mathbb{Z}$ d'une structure d'anneau en posant la multiplication $\overline{a} \times \overline{b} = \overline{ab}$. Alors la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux.

Remarque 15 : Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont ses sous-groupes additifs.

Prop 16 : Il y a équivalence entre :
- n est un nombre premier
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est intègre
- $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps

Théorème 17 (chinois) : Soit $n_1, \dots, n_r \geq 1$ des entiers deux à deux premiers entre eux. Alors le morphisme des projections $\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ est surjectif de noyau $(n_1 \times \dots \times n_r)$. En particulier, on a un isomorphisme d'anneaux : $\mathbb{Z}/n_1 \dots n_r\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$ DEV 1) a)

Corollaire 18 : Soit $n \geq 2$ et $n = p_1^{m_1} \times \dots \times p_r^{m_r}$ sa

décomposition en facteurs premiers. Alors :

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

Prop 19 : Soit $n \geq 2$ et $a \in \mathbb{Z}$. Alors :

- $\bar{a}$ est un diviseur de zéro ssi $n \wedge a$ et n et a ne sont pas premiers entre eux.
- $\bar{a}$ est nilpotent ssi tout diviseur premier p de n est aussi un diviseur premier de a.

2) Le groupe des inversibles $(\mathbb{Z}/n\mathbb{Z})^\times$ [ROM]

Rom 282

Déf 20 : Pour $n \geq 2$, on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Exemple 21 : pour $n = 0$, $\mathbb{Z}^\times = \{-1 ; 1\}$ et pour $n = 1$, $\frac{\mathbb{Z}}{\mathbb{Z}} = \{\bar{0}\}$ n'est pas un anneau.

Théorème 22 : Soit $a \in \mathbb{Z}$. On a équivalence entre :

1) $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$
2) a est premier avec n
3) $\bar{a}$ est un générateur du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$.

Déf 23 : La fonction indicatrice d'Euler est $\ell : \mathbb{N}^* \to \mathbb{N}$, qui à tout $n \geq 1$ associe $\ell(n)$ le nombre d'entiers de $[\![1 ; n]\!]$ premiers avec n.

Exemple 24 : Si p est premier, $\ell(p) = p - 1$.

Prop 25 : pour $n \geq 2$: $|(\mathbb{Z}/n\mathbb{Z})^\times| = \ell(n)$

Rom 288

Prop 26 :
- Soit $n, m \geq 2$ premiers entre eux. Alors $\ell(nm) = \ell(n) \cdot \ell(m)$
- Soit p premier et $\alpha \geq 1$. Alors $\ell(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$

Corollaire 27 : Soit $n \geq 2$ et $n = p_1^{\alpha_1} \times \dots \times p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Alors :

$$\ell(n) = \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

DEV 1) b)

Théorème 28 (d'Euler) : Pour tout $a \in \mathbb{Z}$ premier avec n, on a $a^{\ell(n)} \equiv 1 \ [n]$.

Rom 283

Théorème 29 (de Fermat) : Soit p premier. Pour tout $a \in \mathbb{Z}$ premier avec p, on a $a^{p-1} \equiv 1 \ [p]$.

Prop 30 : pour tout entier $n \geq 2$, on a $n = \sum_{d \mid n} \ell(d)$

Rom 292

Théorème 31 : Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique et isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.

Rom 293

Théorème 32 (ADMIS) : Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi $n = 2, 4, p^\alpha$ ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$.

III Applications

1) Systèmes de congruences [ROM]

Rom 289

Déf 33 : On souhaite résoudre l'équation diophantienne dans $\mathbb{Z}$: $ax \equiv b \ [n]$ où $n \geq 2$, $a \in \mathbb{N}^*$ et $b \in \mathbb{Z}$ (*)

Prop 34 : Si $b = 1$, cette équation a des solutions ssi a est premier avec n. Dans le cas, l'ensemble des solutions est $S = \{x_0 + kn \ ; \ k \in \mathbb{Z}\}$ où x_0 solution particulière.

Corollaire 35 : Si $a \wedge n = 1$ et $b \in \mathbb{Z}$, l'ensemble des solutions est $S = \{x_0 + kn \ ; \ k \in \mathbb{Z}\}$ où x_0 solution particulière

Théorème 36 : Soit $\delta = \text{pgcd}(a, n)$ et $a = \delta a'$, $n = \delta n'$ avec $a' \wedge n' = 1$. L'équation (*) admet des solutions ssi δ divise b. Alors l'ensemble des solutions est $S = \{b' x_0' + kn' \ ; \ k \in \mathbb{Z}\}$ où x_0' solution particulière de $a'x \equiv 1 \ [n']$.

Remarque 37 : Le théorème chinois peut être utilisé pour résoudre un système de congruences.

Rom 285

Théorème 38 (Chinois) : Soit $n_1, \dots, n_k$ des entiers premiers entre eux deux à deux et $n = n_1 \dots n_k$. On note π_k la surjection canonique π_{n_k}. Alors l'application

$f : \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$ est un isomorphisme d'anneaux

$\pi_n(k) \mapsto (\pi_i(k))_i$ d'inverse :

$f^{-1} : \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ où les n_i sont tel que

$(\pi_i(a_i)) \mapsto \pi_n\left(\sum_{i=1}^{r} a_i m_i \frac{n}{n_i}\right)$ $\sum_{i=1}^{r} m_i \frac{n}{n_i} = 1$

Exemple 39 : Le système

$\begin{cases} k \equiv 2\ [4] \\ k \equiv 3\ [5] \\ k \equiv 1\ [9] \end{cases}$ admet pour solutions l'ensemble $S = \{ 838 + 180q \ ; \ q \in \mathbb{Z} \}$

2) Corps fini [PER]

Soit K un corps commutatif

Déf 40 : On appelle sous-corps premier de K le plus petit sous corps de K.

Déf 41 : Soit le morphisme $\ell : \mathbb{Z} \to K$ tel que $\ell(n) = n \cdot 1_K$ Alors le générateur de $\ker(\ell)$ est appelé caractéristique de K. Pour un corps K, $\text{car}(K) = 0$ ou p un nombre premier.

Prop 42 : • Si $\text{car}(K) = 0$, $\mathbb{Q}$ est le sous-corps premier de K

• Si $\text{car}(K) = p > 0$, $\mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$ est le sous-corps premier de K

Prop 43 : Si K est fini, $\text{car}(K) = p > 0$ et $|K| = p^m$ où $m = [K : \mathbb{F}_p]$

Exemple 44 : Il n'y a pas de corps de cardinal 6.

Prop 45 : Si $\text{car}(K) = p > 0$, l'application $F : K \to K$, $F(x) = x^p$ est un morphisme de corps. Si K est fini, c'est un automorphisme. Si $K = \mathbb{F}_p$, c'est l'identité.

Théorème 46 : Soit p premier et $n \in \mathbb{N}^*$. Soit $q = p^n$. Alors il existe un corps K à q éléments, c'est le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$. En particulier, K est unique à isomorphisme près. On le note $\mathbb{F}_q$.

Exemple 47 : on peut construire le corps $\mathbb{F}_4$ de deux manières :

• C'est le corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$

• On a l'isomorphisme $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$

3) Irréductibilité de polynômes [PER]

Théorème 48 (critère d'Eisenstein) : Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ avec $n \geq 1$. Soit p premier tel que : $p \nmid a_n$, $p \mid a_k \ \forall k \in [\![0, n-1]\!]$ $p^2 \nmid a_0$. Alors P est irréductible dans $\mathbb{Q}[X]$.

Appli 49 : Il existe des polynômes irréductibles de tous degrés dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.

Théorème 50 (réduction modulo p) : Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ avec $n \geq 1$. Soit p premier tel que $p \nmid a_n$. Alors si $\bar{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, P est irréductible dans $\mathbb{Q}[X]$.

Appli 51 : $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$.

Déf 52 : On note $\mathbb{U}_n^*$ le groupe des racines n-èmes primitives de l'unité, càd des racines n-èmes de l'unité d'ordre n. Son cardinal est $\varphi(n)$.

Déf 53 : On appelle n-ième polynôme cyclotomique le polynôme : $\Phi_n(X) = \prod_{\xi \in \mathbb{U}_n^*} (X - \xi)$

Prop 54 : Φ_n est unitaire, de degré $\varphi(n)$ et dans $\mathbb{Z}[X]$

Théorème 55 : Le polynôme cyclotomique $\Phi_n(X)$ est irréductible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$. DEV 2

Corollaire 56 : Si ξ est une racine primitive n-ème de l'unité dans un corps de caractéristique nulle, son polynôme minimal sur $\mathbb{Q}$ est Φ_n, et donc on a $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$.

Appli 57 (théorème de Dirichlet faible) : Soit $n \in \mathbb{N}$ et $n \geq 2$. Alors il existe une infinité de nombres premiers p vérifiant $p \equiv 1\ [n]$.