P. Maurer
ENS Rennes

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

Devs :

- Théorème de structure des groupes abéliens finis
- Loi de réciprocité quadratique

Références :

1. Gozard, Théorie de Galois
2. Ulmer, Théorie des groupes
3. Perrin, Cours d'algèbre
4. Gourdon, Algèbre
5. Colmez, Elements d'analyse et d'algèbre
6. Caldero, H2G2
7. FGN, Oraux X-ENS Algèbre 1

1 L'ensemble $\mathbb{Z}/n\mathbb{Z}$, vu comme groupe, anneau et corps

1.1 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$

Définition 1. *Soit $n \in \mathbb{N}$. On note $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$. Si $x, y \in \mathbb{N}$, on note $x \equiv y$ si $x - y \in n\mathbb{Z}$, et on dit que x et y sont congrus modulo n.*

Proposition 2. *Les sous-groupes propres (et les idéaux) de $\mathbb{Z}$ sont les $n\mathbb{Z}$ pour $n \in \mathbb{N}$.*

Définition 3. *Soit $n \in \mathbb{N}$. Le groupe quotient de $(\mathbb{Z}, +)$ par $n\mathbb{Z}$ est noté $\mathbb{Z}/n\mathbb{Z}$. On note généralement $\bar{x}$ la classe d'un entier x dans $\mathbb{Z}/n\mathbb{Z}$. Ainsi, $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$.*

Proposition 4. *Le groupe $\mathbb{Z}/n\mathbb{Z}$ est abélien, et cyclique d'ordre n.*

Proposition 5. *Tout groupe cyclique G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ avec $n = |G|$.*

Exemple 6. Le groupe $\mathbb{U}_n$ des racines $n^{\text{èmes}}$ de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Proposition 7. *Soit $n \geq 2$. Le groupe $\mathbb{Z}/n\mathbb{Z}$ possède, pour chaque diviseur d de n, un unique sous-groupe d'ordre d : ce sous-groupe est $\left\langle \frac{n}{d}\bar{1} \right\rangle$, et il est cyclique.*

En fait, tous les groupes abéliens finis peuvent s'exprimer en fonction de $\mathbb{Z}/n\mathbb{Z}$. Pour présenter ce résultat, on commence par de brefs rappels sur la théorie des représentations et de théorie des groupes.

Définition 8.
Soit G un groupe fini.
On appelle caractère d'une représentation (V, ρ) de G l'application $\chi_V : G \to \mathbb{C}$ définie par $\chi_V(g) := \mathrm{Tr}(\rho(g))$.
Si V est de dimension 1, $\mathrm{GL}(V)$ est isomorphe à $\mathbb{C}^*$, donc la représentation V s'identifie à un morphisme de groupes $\chi : G \to \mathbb{C}^*$. On appelle caractère linéaire de G un tel morphisme, et on note $\hat{G}$ l'ensemble des caractères linéaires de G.

Proposition 9. *Si V est une représentation de dimension 1 de G et χ le caractère linéaire associé, on a $\chi_V = \chi$: le caractère du caractère linéaire est le caractère linéaire lui-même.*
Muni du produit $(\chi_1\, \chi_2)(g) := \chi_1(g)\, \chi_2(g)$, l'ensemble $\hat{G}$ des caractères linéaires de G est un groupe commutatif. On l'appelle le groupe dual de G.

Proposition 10. *Soit G un groupe abélien fini.*

1. *Si $x \in G$ est d'ordre a et si $y \in G$ est d'ordre b, et si $a \wedge b = 1$, alors xy est d'ordre ab.*
2. *Si $a, b \in \mathbb{N}^*$ et si G contient des éléments d'ordre a et b, alors il contient un élément d'ordre $\mathrm{ppcm}(a, b)$.*
3. *Soit N le maximum des ordres des éléments de G. Alors on a $x^N = 1$ pour tout $x \in G$. On dit que N est l'exposant du groupe G.*

Développement 1 :

Lemme 11. *Soit G un groupe abélien fini. Alors G est isomorphe à $\hat{\hat{G}}$.*

Lemme 12. *Soit G un groupe abélien fini. Alors G et $\hat{G}$ ont le même exposant.*

Théorème 13. *(Théorème de structure des groupes abéliens finis, existence)*
Soit G un groupe abélien fini. Alors il existe $r \in \mathbb{N}$ et des entiers $N_1, \dots, N_r$, où N_1 est l'exposant de G et qui vérifient $N_{i+1} | N_i$ pour tout $i \leq r - 1$, et qui sont tels que

$$G \simeq \prod_{i=1}^{r} \mathbb{Z}/N_i\mathbb{Z}.$$

1.2 L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ et le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$

Définition 14. *On définit l'anneau $\mathbb{Z}/n\mathbb{Z}$ comme le quotient de l'anneau $\mathbb{Z}$ par $n\mathbb{Z}$.*

Proposition 15. *Soit $n \in \mathbb{N}$ avec $n \geq 2$, et $a \in \mathbb{N}$. Alors $\bar{a}$ est un élément inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a est premier avec n.*

Proposition 16. *Soit $n \in \mathbb{N}$, avec $n \geq 2$. Les conditions suivantes sont équivalentes :*

- *n est un nombre premier,*
- *$\mathbb{Z}/n\mathbb{Z}$ est intègre,*
- *$\mathbb{Z}/n\mathbb{Z}$ est un corps.*

Pour p un nombre premier, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$. $\mathbb{F}_p$ est donc un corps fini, de cardinal p.

Corollaire 17. *Dans $\mathbb{Z}/n\mathbb{Z}$, les diviseurs de zéro sont les éléments non nuls et non inversibles.*

Proposition 18. *Les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $p\mathbb{Z}/n\mathbb{Z}$ avec $p|n$ premier.*

Définition 19. *(Indicatrice d'Euler)*
Pour $n \geq 1$, on définit la fonction indicatrice d'Euler par

$$\varphi : \begin{cases} \mathbb{N}^* & \to & \mathbb{N}^* \\ n & \mapsto & \mathrm{Card}(\{x \in [\![1,n]\!] \,:\, x \wedge n = 1\}) \end{cases}.$$

Proposition 20. *On a $\varphi(1) = 1$. Si $n \geq 2$, $\varphi(n)$ est le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, et $\varphi(n)$ est l'ordre du groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 21. *Soit p un nombre premier, et $n \in \mathbb{N}^*$. On a $\varphi(p^n) = p^n - p^{n-1}$.*

Théorème 22. *(Euler). Soit $n \geq 2$ un entier, et a un entier relatif premier avec n.*
Alors $a^{\varphi(n)} \equiv 1[n]$.

Théorème 23. *(Wilson). Un entier $n \geq 2$ est premier si et seulement si $(p-1)! \equiv -1[p]$.*

Théorème 24. *(des restes chinois). Soient $n, m \in \mathbb{N}$ avec $n, m \geq 2$ et $n \wedge m = 1$. Alors les anneaux $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$ sont isomorphes.*

Corollaire 25. *Soit $n, m \in \mathbb{N}$ avec $n, m \geq 2$ et $n \wedge m = 1$. Alors $\varphi(nm) = \varphi(n)\,\varphi(m)$.*

Corollaire 26. *Soit $n \geq 2$ un entier, décomposé en facteurs premiers sous la forme $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Alors $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$.*

Proposition 27. *(formule de Gauss). Pour $n \in \mathbb{N}^*$, $n = \sum_{d|n} \varphi(d)$.*

2 Arithmétique dans $\mathbb{Z}/n\mathbb{Z}$

2.1 Nombres premiers

Proposition 28. *(Chiffrement RSA).*

Soit p, q deux nombres premiers distincts et $n = pq$. Soit $c, d \in \mathbb{N}$ tels que $cd \equiv 1[\varphi(n)]$. Alors pour tout $t \in \mathbb{Z}$, on a $t^{cd} \equiv t[n]$.

Remarque 29. L'application $g : \bar{t} \mapsto \bar{t}^c$ s'appelle fonction de chiffrement, et $f : \bar{t} \mapsto \bar{t}^d$ fonction de déchiffrement. La proposition affirme que $f \circ g(\bar{t}) = \bar{t}$, ce qui permet de chiffrer puis de déchiffrer un message. Le couple (n, c) s'appelle la clef publique, l'entier d la clef secrète.

Définition 30. *On dit qu'un nombre $n \geq 2$ est de Carmichael s'il n'est pas premier et si pour tout $a \in \mathbb{Z}$, $a^k \equiv a[n]$.*

Proposition 31. *Il existe une infinité de nombres de Carmichael, et le plus petit d'entre eux est 561. En particulier, la réciproque du théorème de Fermat n'est pas vérifiée.*

Théorème 32. *(Sophie Germain).*
Soit p un nombre premier impair tel que $2p+1$ soit premier. Alors l'équation $x^p + y^p + z^p = 0$ n'admet aucune solution entière telle que $xyz \not\equiv 0[p]$.

2.2 Carrés et somme de carrés

On se donne p un nombre premier et $n \geq 1$.

Rappel 33. *Si $q = p^n$ est une puissance de p, il existe un unique corps $\mathbb{F}_q$ à q éléments.*

Réciproquement, le cardinal d'un corps fini est toujours une puissance d'un nombre premier p.

Notation 34. *On pose $\mathbb{F}_q^2 := \{y \in \mathbb{F}_q \,:\, \exists x \in \mathbb{F}_q,\ y = x^2\}$, et $\mathbb{F}_q^{*2} := \mathbb{F}_q^* \cap \mathbb{F}_q^2$.*

Proposition 35. *Si $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$. Si $p > 2$, on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.*

Proposition 36. *On suppose $p > 2$ et on se donne $a \in \mathbb{F}_q^*$. Alors*

$$a^{\frac{q-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_q^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_q^* \end{cases}.$$

Définition 37. *On définit le symbole de Legendre pour $p > 2$ et $a \in \mathbb{F}_p$ par*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^*, \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^*, \\ 0 & \text{si } a = 0. \end{cases}$$

Proposition 38. *Soit p un nombre premier impair et a un élément de $\mathbb{F}_p^*$. On a*

$$|\{x \in \mathbb{F}_p \,:\, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

Développement 2 :

Théorème 39. *(Loi de réciprocité quadratique)*
Soit p et q deux nombres premiers impairs distincts. Alors on a

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Exemple 40. Calcul du symbol de Legendre :
$\left(\frac{23}{59}\right)=(-1)^{11.29}\left(\frac{59}{23}\right)=-\left(\frac{13}{23}\right)=\cdots=\left(\frac{2}{3}\right)=-1.$

Lemme 41. *Pour tout nombre premier p impair, 8 divise p^2-1.*

Proposition 42. *Pour tout nombre premier p impair, on a $\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$.*

3 Application aux polynômes irréductibles

3.1 Irréductibilité sur $\mathbb{Z}$ et sur $\mathbb{Q}$

Définition 43. *Pour $P\in\mathbb{Z}[X]$ non nul, on appelle contenu de P, noté $c(P)$ le plus grand diviseur commun de ses coefficients, à un signe près.*
Un polynôme est dit primitif si $c(P)=1$.

Lemme 44. *(Gauss)*
On a $c(PQ)=c(P)\,c(Q)$ modulo $\{-1,1\}$.

Théorème 45. *(Critère d'Eisenstein)*
Les polynômes de $\mathbb{Z}[X]$ irréductibles sont :

i. Les nombres premiers $p\in\mathbb{Z}$,

ii. Les polynômes de degré plus grand que 1 primitifs et irréductibles dans $\mathbb{Q}[X]$.

Soit $P=\sum_{i=1}^{n}a_iX^i\in\mathbb{Z}[X]$, et p un élément irréductible de $\mathbb{Z}$ tel que $p\nmid a_n$, $p^2\nmid a_0$ et $p|a_i$ pour tout $i\in[\![0,n-1]\!]$. Alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple 46. Le polynôme $\Phi_{p,\mathbb{Q}}(X)=\sum_{i=1}^{p-1}X^i$ est irréductible sur $\mathbb{Q}$ pour p premier.

Théorème 47. *(Réduction). Soit $P=\sum_{i=1}^{n}a_iX^i\in\mathbb{Z}[X]$ et $\overline{P}$ son image dans $\mathbb{F}_p[X]$, si $a_n\not\equiv 0[p]$. Si $\overline{P}$ est irréductible sur $\mathbb{F}_p[X]$, alors P est irréductible dans $\mathbb{Z}[X]$.*

Exemple 48. Si p est premier, X^p+X+1 est irréductible sur $\mathbb{F}_p[X]$ donc sur $\mathbb{Z}[X]$.

3.2 Polynômes cyclotomiques

Définition 49. *Soit $m\in\mathbb{N}^*$. On considère l'ensemble $\mathbb{U}_m=\{z\in\mathbb{C}:\ z^m=1\}$ des racines $m^{\text{èmes}}$ de l'unité. $\mathbb{U}_m$ est un groupe cyclique, isomorphe à $\mathbb{Z}/m\mathbb{Z}$ via $e^{\frac{2i\pi k}{n}}\mapsto\overline{k}$.*

On appelle racine primitive $m^{\text{ème}}$ de l'unité tout générateur de $\mathbb{U}_m$, c'est-à-dire tout élément $\zeta\in\mathbb{U}_m$ tel que $\zeta^d\neq 1$ pour tout diviseur d strict de m. On note $\mu_m^*(\mathbb{C})$ l'ensemble des racines primitives $m^{\text{èmes}}$ de l'unité.

Proposition 50. *$\mu_m^*(\mathbb{C})$ a pour cardinal $\varphi(m)$.*

Exemple 51. On a $\mu_1^*(\mathbb{C})=\{1\}$, $\mu_2^*(\mathbb{C})=\{-1\}$, $\mu_3^*(\mathbb{C})=\{j,\bar{j}\}$ et $\mu_4^*(\mathbb{C})=\{i,-i\}$.

Définition 52. *Soit $m\in\mathbb{N}^*$. On appelle $m^{\text{ème}}$ polynôme cyclotomique le polynôme :*

$$\Phi_{m,\mathbb{Q}}(X)=\prod_{\zeta\in\mu_n^*(\mathbb{C})}(X-\zeta)$$

Proposition 53. *On a $X^m-1=\prod_{d|m}\Phi_{d,\mathbb{Q}}(X)$.*

Remarque 54. Cette formule permet de calculer $\Phi_{m,\mathbb{Q}}$ par récurrence.

Exemple 55. On a $\Phi_{1,\mathbb{Q}}(X)=X-1$, $\Phi_{2,\mathbb{Q}}(X)=X+1$, $\Phi_{4,\mathbb{Q}}(X)=X^2+1$, $\Phi_{8,\mathbb{Q}}(X)=X^4+1$.

On a $\Phi_{p,\mathbb{Q}}(X)=\frac{X^p-1}{X-1}=1+X+\cdots+X^{p-1}$ pour tout p premier.

Proposition 56. *Pour tout $n\in\mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X)\in\mathbb{Z}[X]$.*

Théorème 57.
Pour tout $n\in\mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X)$ est irréductible dans $\mathbb{Q}[X]$.

Théorème 58. *(Wedderburn)*
Tout corps fini est commutatif.