Leçon 120 Anneaux $\mathbb{Z}/n\mathbb{Z}$, applications

Dorian Cacitti-Holland

2020-2021

Références.

1. Algèbre et géométrie de Jean-Etienne Rombaldi
2. Eléments d'analyse et d'algèbre de Pierre Colmez
3. L'algèbre discrète de la transformation de Fourier de Gabriel Peyré
4. Cours d'algèbre de Daniel Perrin
5. Histoires hédonistes de groupes et de géométries tome 1 de Caldero et Germoni
6. Extension de corps de Josette Calais

Développements.

1. Théorème de structure des groupes abéliens finis
2. Loi de réciprocité quadratique
3. Critère d'irréductibilité d'Eisenstein

Table des matières

1 Point de vue groupe **2**
1.1 Lien avec les groupes cycliques 2
1.2 Caractères de $\mathbb{Z}/n\mathbb{Z}$ et groupes abéliens finis 2

2 Point de vue anneau **3**
2.1 Propriétés 3
2.2 Cyclicité du groupe des inversibles $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ 3
2.3 Restes chinois et systèmes de congruence 4

3 Point de vue corps **4**
3.1 Résidu quadratique modulo p 4
3.2 Construction des corps finis 5
3.3 Irréductibilité de polynômes 6

1 Point de vue groupe

1.1 Lien avec les groupes cycliques

(Chapitres 10.1, 10.2, 1.4 et 1.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
On considère $n \in \mathbb{Z}$ et G un groupe.

1. Définition : Soit $a, b \in \mathbb{Z}$, alors on dit que $a \equiv b[n]$ si $n \mid a - b$
2. Proposition : La relation de congruence module n est une relation d'équivalence sur $\mathbb{Z}$, on note les classes $\overline{a} = a + n\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient des classes
3. Corollaire : $\mathbb{Z}/n\mathbb{Z}$ est un groupe pour $\overline{a} + \overline{b} = \overline{a+b}$
4. Théorème : Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $\overline{k}$ avec $k \in [\![1, n-1]\!]$ premier avec n
5. Exemple : Les générateurs de $\mathbb{Z}/8\mathbb{Z}$ sont $\overline{1}, \overline{3}, \overline{5}, \overline{7}$
6. Définition : L'indicatrice d'Euler est $\varphi(n)$ le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$
7. Exemple : Si $n = p$ premier alors $\varphi(n) = n - 1$
8. Définition : On dit que G est monogène s'il existe $g \in G$ tel que $G = \langle g \rangle$, si de plus G est fini alors on dit que G est cyclique
9. Exemple : Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité est un groupe cyclique d'ordre n
10. Proposition : Si G cyclique d'ordre n alors $G \simeq \mathbb{Z}/n\mathbb{Z}$
11. Corollaire : Si $G = \langle g \rangle$ cyclique d'ordre n alors les générateurs de G sont les g^k où $k \in [\![1, n-1]\!]$ premier avec n
12. Théorème : Si G de cardinal premier p alors il existe $g \in G \backslash \{1\}$ d'ordre p et $k + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z} \longmapsto g^k \in G$ est isomorphisme de groupes, donc G est cyclique
13. Théorème : 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 il s'agit de $H = \langle \overline{a} \rangle = \{\overline{0}, \overline{a}, ..., (d-1)\overline{a}\}$ avec $q = \frac{n}{d}$
14. Théorème : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont tous cycliques d'ordre divisant n
15. Corollaire : Pour tout $d \mid n$, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$, il s'agit de $\left\langle \frac{n}{d}\overline{1} \right\rangle$

1.2 Caractères de $\mathbb{Z}/n\mathbb{Z}$ et groupes abéliens finis

(Chapitres 1.5 et 1.9 d'Algèbre et géométrie de Jean-Etienne Rombaldi, 0.3.2 et I.2.5 de Eléments d'analyse et d'algèbre de Pierre Colmez et VIII.1 de L'algèbre discrète de la transformation de Fourier de Gabriel Peyré)

On considère un groupe abélien fini G.

1. Théorème : Un groupe abélien si et seulement si toutes ses représentations irréductibles sont de degré 1
2. Théorème : La table de caractères de $\mathbb{Z}/n\mathbb{Z}$ est une matrice de Vandermonde associée à une racine n-ième primitive de l'unité et ses puissances successives

3. Définition : L'exposant de G est l'entier $N(G) = PPCM(o(g), g \in G)$
4. Exemple : Si $G = \mathbb{Z}/9\mathbb{Z}$ alors $N(G) = 3$
5. Définition : Un caractère de G est un morphisme de groupe de G dans $\mathbb{C}^*$, et on note $\hat{G}$ l'ensemble des caractères sur G
6. Exemple : Le morphisme $g \in G \longmapsto 1 \in \mathbb{C}^*$ est la caractère trivial
7. Proposition : Soit H sous-groupe de G et χ caractère de H, alors χ peut se prolonger en un caractère sur G
8. Lemme : $\hat{G}$ est un groupe et G et $\hat{\hat{G}}$ sont isomorphismes
9. Proposition : G et $\hat{G}$ ont le même exposant
10. Théorème : Il existe $g \in G$ d'ordre $N(G)$
11. Théorème de structure des groupes abéliens finis : $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times ...\mathbb{Z}/d_r\mathbb{Z}$ avec $d_{i+1} \mid d_i$

2 Point de vue anneau

2.1 Propriétés

(Chapitres 10.2 et 11.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Théorème : $\mathbb{Z}/n\mathbb{Z}$ est un anneau avec $\overline{a} \times \overline{b} = \overline{ab}$
2. Corollaire : $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux
3. Définition : $(\mathbb{Z}/n\mathbb{Z})^\times$ est le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$
4. Exemple : $(\mathbb{Z}/3\mathbb{Z})^\times = \{\overline{1}, \overline{2}\} \sim \mathbb{Z}/2\mathbb{Z}$
5. Théorème : Soit $a \in \mathbb{Z}$, alors $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $a \wedge n = 1$ si et seulement si $\overline{a}$ est générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$
6. Théorème d'Euler : Soit $a \in \mathbb{Z}$ premier avec n, alors $a^{\varphi(n)} \equiv 1[n]$
7. Corollaire : Théorème de Fermat : Soit $p \in \mathbb{N}$ premier et $a \in \mathbb{Z}$ premier avec p, alors $a^{p-1} \equiv 1[p]$, donc pour $b \in \mathbb{Z}$, $b^p \equiv b[p]$
8. Théorème : n est premier si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps
9. Exemple : $\mathbb{Z}/7\mathbb{Z}$ est un corps mais pas $\mathbb{Z}/9\mathbb{Z}$

2.2 Cyclicité du groupe des inversibles $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$

(Chapitre 10.5 d'Algèbre et géométrie de Jean-Etienne Rombaldi)
Soit $p \in \mathcal{P}$.

1. Lemme : Soit d divisant $p-1$, alors il y a $\varphi(d)$ éléments d'ordre d dans $(\mathbb{Z}/p\mathbb{Z})^\times$
2. Théorème : $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique
3. Exemple : $(\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/4\mathbb{Z}$
4. Théorème : Si p impair, soit $\alpha \in [\![2, +\infty[\![$, alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique
5. Corollaire : Soit $n \in \mathbb{N}^*$, alors $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = 2, 4, p^\alpha, 2p^\alpha$ avec $p \in \mathcal{P}$ impair et $\alpha \in \mathbb{N}^*$

2.3 Restes chinois et systèmes de congruence

(Chapitre 8.3 d'Algèbre et géométrie de Jean-Etienne Rombaldi)

1. Lemme : Soit $a_1, ..., a_r$ éléments deux à deux premiers entre eux dans $\mathbb{Z}$ et pour tout k dans $[\![1, r]\!], b_k := \prod_{\substack{i=1 \\ i \neq k}}^{r} a_i$ alors les $b_1, ..., b_r$ sont premiers entre eux dans leur ensemble
2. Théorème des restes chinois : Avec les notations du lemme précédent, en notant de plus $a := \prod_{k=1}^{r} a_k$ et les surjections canoniques $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/a\mathbb{Z}$ et $\pi_k : \mathbb{Z} \longrightarrow \mathbb{Z}/a_k\mathbb{Z}$ pour $k \in [\![1, r]\!]$, l'application $\varphi : \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/a_1\mathbb{Z} \times ... \times \mathbb{Z}/a_r\mathbb{Z} \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$ est un morphisme d'anneaux surjectif, en particulier φ induit un isomorphisme d'anneaux $\overline{\varphi} : \begin{array}{ccc} \mathbb{Z}/a\mathbb{Z} & \longrightarrow & \mathbb{Z}/a_1\mathbb{Z} \times ... \times \mathbb{Z}/a_r\mathbb{Z} \\ \pi(x) & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array}$ d'inverse $\overline{\varphi}^{-1} : \begin{array}{ccc} \mathbb{Z}/a_1\mathbb{Z} \times ...\mathbb{Z}/a_r\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \\ (\pi_1(x_1), ..., \pi_r(x_r)) & \longmapsto & \pi\left(\sum_{k=1}^{r} x_k u_k b_k\right) \end{array}$ avec $(u_1, ..., u_r) \in \mathbb{Z}^r$ tel que $1 = \sum_{k=1}^{r} u_k b_k$
3. Application : On considère le système de congruences $\left\{ \begin{array}{rcl} x & \equiv & a[n] \\ x & \equiv & b[m] \end{array} \right.$ d'inconnue $x \in \mathbb{Z}$ et de paramètres $(a, b, n, m) \in \mathbb{Z}^4$ avec n et m premiers entre eux, alors il existe une solution $x \in \mathbb{Z}$ (unique modulo nm) de ce système
4. Exemple : Le système $\left\{ \begin{array}{rcl} x & \equiv & 2[4] \\ x & \equiv & 3[5] \\ x & \equiv & 1[9] \end{array} \right.$ a pour ensemble de solutions $\{838 + 180k, k \in \mathbb{Z}\}$ car on a la relation de Bézout entre 4,5 et 9 : $1 = 1 \times 5 \times 9 + 11 \times 4 \times 9 - 22 \times 4 \times 5$

3 Point de vue corps

3.1 Résidu quadratique modulo p

(Chapitres 13.6 et 13.7 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.d du Cours d'algèbre de Daniel Perrin et V.C de Histoires hédonistes de groupes et de géométries de Caldero et Germoni)

Soit p premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1. Théorème : Il existe $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non carrés dans $\mathbb{F}_p^*$
2. Théorème de caractérisation des carrés : Si $p > 2$ premier, soit $x \in \mathbb{F}_p$, alors x est un carré dans $\mathbb{F}_p^*$ si et seulement si $x^{\frac{p-1}{2}} = 1$
3. Corollaire : -1 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv 1[4]$
4. Application : Il existe une infinité de nombre premiers $p \equiv 1[4]$

5. Définition : On dit que a non multple de p est un résidu quadratique modulo p si $\overline{a}$ est un carré dans $\mathbb{F}_p^*$ et on note $\left(\frac{a}{p}\right) = 1$ si a est résidu quadratique et $\left(\frac{a}{p}\right) = -1$ sinon, appelé symbole de Legendre
6. Exemple : $4^2 \equiv 1[5]$, donc 4 est un résidu quadratique modulo 5
7. Proposition : Soit $a \in \mathbb{F}_p^*$, alors $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)[p]$ et $a \in \mathbb{F}_p^* \longmapsto \left(\frac{a}{p}\right) \in \{-1, 1\}$ est l'unique morphisme de groupes non trivial
8. Exemple : $2^{\frac{5-1}{2}} = 2^2 = 4 \equiv -1[5]$, donc 2 n'est pas un résidu quadratique modulo 5
9. Corollaire : Si $n = \pm\prod_{i=1}^{r} p_i^{\alpha_i}$ alors $\left(\frac{n}{p}\right) = (\pm 1)^{\frac{p-1}{2}} \prod_{i=1}^{r} \left(\frac{p_i}{p}\right)^{\alpha_i}$
10. Proposition : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
11. Lemme : Soit $a \in \mathbb{F}_p^*$, alors $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$
12. Théorème : Loi de réciprocité quadratique : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
13. Exemple : $\left(\frac{219}{383}\right) = 1$ donc 219 est un résidu quadratique modulo 383

3.2 Construction des corps finis

(Chapitres 13.4 d'Algèbre et géométrie de Jean-Etienne Rombaldi, III.2.b du Cours d'algèbre de Daniel Perrin et 4.3 de Extensions de corps de Josette Calais)

On considère $q = p^n$ avec $p \in \mathbb{N}$ premier.

1. Définition : On note $U_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p) = |U_n(p)|$
2. Proposition : Soit $P \in U_n(p)$, alors $\mathbb{F}_p[X]/(P)$ est un $\mathbb{F}_p$-espace vectoriel de dimension n et est un corps de cardinal $q = p^n$
3. Exemple : $\forall \lambda \in \mathbb{F}_p, X - \lambda \in U_1(p)$ donc $I_1(p) = p$ et tous ces corps $\mathbb{F}_p[X]/(X - \lambda)$ sont isomorphes à $\mathbb{F}_p$
4. Exemple : Comme $P = X^2 + \lambda X + \mu$ est irréductible si et seulement si sans racines, $I_2(p) = \frac{p(p-1)}{2}$
5. Lemme : En notant $P_n = X^{p^n} - X = X^q - X$, tout diviseur irréductible de P_n dans $\mathbb{F}_p[X]$ est de degré divisant n, réciproquement pour tout diviseur d de n, tout polynôme $P \in U_n(d)$ divise P_n
6. Théorème : P_n est sans facteur carré dans $\mathbb{F}_p[X]$ et on a la décomposition en irréductibles $P_n = \prod_{d|n} \prod_{P \in U_d(p)} P$
7. Théorème : A isomorphisme près, il existe un unique corps à $q = p^n$ éléments, on le note $\mathbb{F}_p$, il s'agit de $\mathbb{F}_p[X]/(P)$ avec $P \in U_n(p)$, et du corps de décomposition de P_n sur $\mathbb{F}_p$
8. Exemple : $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}, \mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + 1)$

3.3 Irréductibilité de polynômes

(Chapitres II.4.a et III.3 du Cours d'Algèbre de Daniel Perrin et 2.2 d'Algèbre de Xavier Gourdon)

1. Lemme : Soit $P, Q \in \mathbb{Z}[X]$, $\overline{P}, \overline{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$ leurs images par la surjection canonique prolongée et $p \in \mathbb{N}$ premier, si $P \mid Q$ alors $\overline{P} \mid \overline{Q}$
2. Théorème : Critère d'irréductibilité d'Eisenstein : Soit $P = a_n X^n + ... + a_0 \in \mathbb{Z}[X]$ et p premier tels que p ne divise pas a_n, $\forall i \in [\![0, n-1]\!], p \mid a_i$ et p^2 ne divise pas a_0, alors P est irréductible dans $\mathbb{Q}[X]$, si de plus P est primitif alors P est irréductible dans $\mathbb{Z}[X]$
3. Exemple : $X^4 + 15X + 10$ est irréductible
4. Exemple : $P = X^{p-1} + ... + X + 1$ est irréductible car $P(X+1)$ vérifie le critère précédent
5. Théorème : Critère d'irréductibilité modulo p : Soit p premier, $P \in \mathbb{Z}[X]$ et $\overline{P} \in \mathbb{Z}/p\mathbb{Z}[X]$ sa réduction modulo p, si $\overline{a}_n \neq 0$ et $\overline{P}$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$, alors P est irréductible sur $\mathbb{Z}$
6. Exemple : $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$ donc sur $\mathbb{Z}$
7. Remarque : La réciproque est fausse, par exemple $P = X^2 - 2X - 1$ est irréductible dans $\mathbb{Z}[X]$ mais réductible dans $\mathbb{F}_2[X]$