120

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

Soit $n\in\mathbb{N}^*$, $p\in\mathbb{N}$ premier et G groupe. Soit $a\in\mathbb{N}^*$, $b\in\mathbb{Z}$.
Soit $q := p^\alpha$.

I] Le groupe $\mathbb{Z}/n\mathbb{Z}$

1] Structure de groupe cyclique

I.4

Définition 1: 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.

X.1

Proposition 2: Les $n\mathbb{Z}$ sont les seuls sous-groupes de $(\mathbb{Z};+)$.

Proposition 3: Les applications $\pi_n : \begin{array}{l}\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\\ k\mapsto \bar{k}\end{array}$ sont des morphismes de groupes surjectifs.

I.1

Proposition 4: Soit G groupe monogène.
Alors: (1) Si G est infini, alors il est isomorphe à $(\mathbb{Z};+)$.
(2) Si G est cyclique d'ordre n, alors il est isomorphe à $(\mathbb{Z}/n\mathbb{Z};+)$.

X.1 [Rom]

Exemple 5: Le groupe μ_n des racines n-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Théorème 6: Pour $n\geq 2$, tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre divisant n.

Théorème 7: L'application $\sigma : \begin{array}{l}(\mathbb{Z}/n\mathbb{Z})^\times \to Aut(\mathbb{Z}/n\mathbb{Z})\\ x\mapsto \left[\begin{array}{l}\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}\\ y\mapsto xy\end{array}\right]\end{array}$ est un isomorphisme.

2] Générateurs et indicatrice d'Euler

X.2

Théorème 8: Soit $a\in\mathbb{Z}$.
Alors: $\bar{a}\in(\mathbb{Z}/n\mathbb{Z})^\times$ ssi $a\wedge n=1$
ssi $\bar{a}$ est générateur de $(\mathbb{Z}/n\mathbb{Z};+)$

[Rom]

Définition 9: On appelle fonction indicatrice d'Euler la fonction qui associe à tout $n\in\mathbb{N}^*$ le nombre $\varphi(n)$ d'entiers dans $[\![1;n]\!]$ premiers avec n.

Exemple 10: $\varphi(1)=1$; $\varphi(3)=2$; $\varphi(9)=6$

X.2

Remarque 11: Le théorème nous donne alors que $\varphi(n)$ est le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z};+)$ ou encore le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}$

X.3 [Rom]

Lemme 12: $\forall \alpha\in\mathbb{N}^*$, $\forall p\in\mathbb{N}$, p premier $\Rightarrow \varphi(p^\alpha)=(p-1)p^{\alpha-1}$

Théorème 13: Soit $n=\prod_{i=1}^{r} p_i^{\alpha_i}$ décomposition en facteurs premiers.
Alors: $\varphi(n)=\prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i-1) = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$

X.2

Théorème 14: $\forall n\geq 2$, $n=\sum_{d\mid n}\varphi(d)$

II] L'anneau $\mathbb{Z}/n\mathbb{Z}$

1] Groupe multiplicatif

X.1

Théorème 15: Pour $n\geq 2$, il existe une unique structure d'anneau commutatif unitaire sur $\mathbb{Z}/n\mathbb{Z}$ telle que la surjection canonique π_n soit un morphisme d'anneaux.

X.2 [Rom]

Définition 16: Pour $n\geq 2$, on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 17: (d'Euler) $\forall a\in\mathbb{Z}$, $a\wedge n=1 \Rightarrow a^{\varphi(n)}\equiv 1\,[n]$

Corollaire 18: (petit théorème de Fermat) Soit $a\in\mathbb{Z}$, $a\wedge p=1$.
Alors: $a^{p-1}\equiv 1\,[p]$

[FGN A1 1]

Théorème 19: (de Sophie Germain) Soit p premier impair tel que $q:=2p+1$ est premier.
Alors: $\nexists (x;y;z)\in\mathbb{Z}^3 \mid \begin{cases} xyz\not\equiv 0\,[p]\\ x^p+y^p+z^p=0\end{cases}$

2] Restes chinois et systèmes de congruences

X.3 [Rom]

Lemme 20: Soit $(n_j)_{j=1}^{r}\in\mathbb{N}\setminus\{0;1\}^r$.
Alors: (1) Si $n_1;\dots;n_r$ sont deux à deux premiers entre eux,
alors: $PPCM(n_1;\dots;n_r)=\prod_{j=1}^{r} n_j$
(2) Sinon, $PPCM(n_1;\dots;n_r)<\prod_{j=1}^{r} n_j$

X.3 [Rom]

Théorème 21: (des restes chinois) Soit $(n_j)_{j=1}^r \in (\mathbb{N}\setminus\{0,1\})^r$, $n=\prod_{j=1}^r n_j$.

Alors: $n_1,\dots,n_r$ sont premiers entre eux ssi $\mathbb{Z}/n\mathbb{Z}$ et $\prod_{j=1}^r \mathbb{Z}/n_j\mathbb{Z}$ sont isomorphes.

Dans ce cas, $\psi: \begin{array}{l} \mathbb{Z}/n\mathbb{Z} \to \prod_{j=1}^r \mathbb{Z}/n_j\mathbb{Z} \\ k \mapsto (\pi_{n_1}(k),\dots,\pi_{n_r}(k)) \end{array}$ est un isomorphisme d'anneaux d'inverse $\psi^{-1}: \begin{array}{l} \prod_{j=1}^r \mathbb{Z}/n_j\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ (a_1,\dots,a_r) \mapsto \pi_n\left(\sum_{j=1}^r a_j u_j \frac{n}{n_j}\right) \end{array}$

avec $(u_j)_{j=1}^r \in \mathbb{Z}^r$ telle que $\sum_{j=1}^r u_j \frac{n}{n_j} = 1$

X.4

Application 22: L'équation diophantienne $ax\equiv b[n]$ a des solutions entières ssi $a\wedge n \mid b$.

Dans ce cas, l'ensemble des solutions est: $S=\{b'x_0'+kn' \mid k\in\mathbb{Z}\}$.

où x_0' est solution particulière de $a'x\equiv 1[n']$ avec $b=(a\wedge n)b'$.

et $n=(a\wedge n)n'$.

Exemple 23: Les solutions de $\begin{cases} x\equiv 2[4] \\ x\equiv 3[5] \\ x\equiv 1[3] \end{cases}$ sont: $\{838+180k \mid k\in\mathbb{Z}\}$

III] Le corps $\mathbb{Z}/p\mathbb{Z}$

1] Résidus quadratiques modulo p

XIII.5

Théorème 24: n est premier ssi $\mathbb{Z}/n\mathbb{Z}$ est un corps

Théorème 25: (caractérisation des carrés) Les carrés de $\mathbb{F}_p^*$ sont les racines de $X^{\frac{p-1}{2}}-1$ et les non-carrés sont les racines de $X^{\frac{p-1}{2}}+1$.

Corollaire 26: -1 est carré dans $\mathbb{F}_p^*$ ssi $p\equiv 1[4]$

XIII.6 [Rom]

Définition 27: On dit que $k\in\mathbb{Z}$ tel que $p\nmid k$ est un résidu quadratique modulo p si $\bar{k}$ est un carré dans $\mathbb{F}_p^*$.

Pour $a\in\mathbb{F}_p^*$, on note $\left(\frac{a}{p}\right)=\begin{cases} 1 \text{ si } a \text{ est carré dans } \mathbb{F}_p^* \\ -1 \text{ sinon} \end{cases}$ le symbole de Legendre.

Exemple 28: $4^2\equiv 1[5]$ donc 4 est résidu quadratique modulo 5 et $\left(\frac{4}{5}\right)=1$.

XIII.6 [Rom]

Théorème 29: L'application $\begin{array}{l} \mathbb{F}_p^* \to \{\pm 1\} \\ a \mapsto \left(\frac{a}{p}\right) \end{array}$ est l'unique morphisme de groupes non-trivial de $\mathbb{F}_p^*$ dans $\{\pm 1\}$.

[Isen]

Définition 30: Une matrice de dilatation de $GL_n(\mathbb{K})$ est de la forme $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \\ & & & \lambda \end{pmatrix}$ avec $\lambda\in\mathbb{K}^*$ dans une certaine base.

Soit H hyperplan de E $\mathbb{K}$-ev et G son supplémentaire $E=H\oplus G$.

La dilatation f de base H, direction G, rapport $\lambda\in\mathbb{K}^*$ est telle que: $\forall h,u\in H\times G$, $f(h+u)=h+\lambda u$.

Lemme 31: Soit $\mathbb{K}$ corps à ≥ 3 éléments, V un $\mathbb{K}$-ev.

Alors: les dilatations engendrent $GL(V)$.

Théorème 32: (de Frobenius-Zolotarev) Soit p premier impair, V un $\mathbb{F}_p$-espace vectoriel de dimension n.

Alors: $\forall u\in GL(V)$, $\varepsilon(u)=\left(\frac{\det(u)}{p}\right)$.

2] Construction de corps finis

XIII.4 [Rom]

Notation 33: On note $\mathcal{U}_n(p)$ l'ensemble des polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$.

Théorème 34: $\forall P\in\mathcal{U}_n(p)$, $\mathbb{F}_p[X]/(P)$ est une $\mathbb{F}_p$-algèbre de dimension n de base $\{\bar{X}^k\}_{k=0}^{k=n-1}$. C'est un corps fini à p^n éléments.

Exemple 35: $\forall\lambda\in\mathbb{F}_p$, $(X-\lambda)\in\mathcal{U}_1(p)$ et $\mathbb{F}_p[X]/(X-\lambda)$ est isomorphe à $\mathbb{F}_p$.

(2) $X^2+\lambda X+\mu\in\mathcal{U}_2(p)$ ssi il n'a pas de racines dans $\mathbb{F}_p$.

Lemme 36: Tout diviseur irréductible de $X^{p^n}-X$ dans $\mathbb{F}_p[X]$ est de degré divisant n. Réciproquement, tout diviseur $d\mid n$, $P\in\mathcal{U}_d(p)$ divise $X^{p^n}-X$.

Théorème 37: $X^{p^n}-X$ est sans facteurs carrés dans $\mathbb{F}_p[X]$ et:

$$X^{p^n}-X=\prod_{d\mid n}\prod_{P\in\mathcal{U}_d(p)} P$$

[Isa]

<u>Proposition 38</u>: L'application $S: \begin{array}{rcl}\mathbb{F}_q[X] & \to & \mathbb{F}_q[X] \\ Q & \mapsto & Q^q\end{array}$ est un $\mathbb{F}_q$-endomorphisme de $\mathbb{F}_q[X]$.

<u>Lemme 39</u>: Soit $\mathbb{L}$ une extension de corps de $\mathbb{F}_q$ et $x \in \mathbb{L}$

<u>Alors</u>: $x^q = x$ <u>ssi</u> $x \in \mathbb{F}_q$

<u>Théorème 40</u>: (des restes chinois) Soit $P_1; \dots; P_r \in \mathbb{F}_q[X]^r$ premiers entre eux et $P = \prod_{j=1}^{r} P_j$

<u>Alors</u>: $\begin{array}{rcl}\mathbb{F}_q[X]/\langle P \rangle & \to & \prod_{j=1}^{r} \mathbb{F}_q[X]/\langle P_j \rangle \\ Q \bmod (P) & \mapsto & (Q \bmod (P_1); \dots; Q \bmod (P_r))\end{array}$ est un isomorphisme de $\mathbb{F}_q$-algèbres.

<u>Théorème 41</u>: (de Berlekamp) Soit $P \in \mathbb{F}_q[X]$ sans facteurs carrés et $P = \prod_{i=1}^{r} P_i$ sa décomposition en produit d'irréductibles.

<u>Alors</u>: (1) Si $r = 1$, <u>alors</u> P est irréductible

(2) Sinon, il existe $a \in \mathbb{F}_q$ et $V \in \mathbb{F}_q[X]$ tel que $PGCD(P, V-a)$ est un facteur non-trivial de P.

III.3

3) Irréductibilité des polynômes

<u>Théorème 42</u>: (critère d'Eisenstein) Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ et p premier tel que:

(i) $p \nmid a_n$

(ii) $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$

(iii) $p^2 \nmid a_0$

<u>Alors</u>: P est irréductible dans $\mathbb{Q}[X]$

Si de plus, $c(P) = 1$, <u>alors</u> P est aussi irréductible dans $\mathbb{Z}[X]$.

[Per]

<u>Exemple 43</u>: Pour p premier, le polynôme $X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}$

<u>Théorème 44</u>: (critère d'irréductibilité modulo p) Soit p premier, $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ et $\overline{P}$ sa réduction modulo p telle que $\overline{a_n} \neq 0$.

<u>Alors</u>: $\overline{P}$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$ et P est irréductible sur $\mathbb{Q}$.

III.3 [Per]

<u>Exemple 45</u>: (1) Le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irréductible sur $\mathbb{Z}$ de réduction modulo 2 : $X^3 + X + 1$ qui est irréductible sur $\mathbb{F}_2$.

(2) Pour p premier, $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

III.4

<u>Notation 46</u>: On note $\mu_n^\times = \{z \in \mathbb{C}^* \mid \forall p \wedge n = 1, p < n \Rightarrow z^p \neq 1 \text{ et } z^n = 1\}$ l'ensemble des racines primitives n-ièmes de l'unité.

<u>Théorème 47</u>: $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ avec $\Phi_d(X) = \prod_{\xi \in \mu_n^\times} (X - \xi)$

<u>Théorème 48</u>: Φ_n est à coefficients entiers, unitaire et irréductible dans $\mathbb{Z}[X]$.

Références :

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie - Rombaldi

[FGNAl1] Exercices de mathématiques oraux X-ENS Algèbre 1 - Francinou

[Isen] L'oral à l'agrégation de mathématiques - Isenmann

[Per] Cours d'algèbre - Perrin