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

Soit $n \in \mathbb{N}^*$. On notera $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ et $\mathcal{P}$ l'ensemble des nombres premiers.
Soit $p \in \mathcal{P}$, G un groupe, $a \in \mathbb{N}^*$, $b \in \mathbb{Z}$ et $q = p^n$.

I Le groupe $(\mathbb{Z}_n, +)$

A Structure de groupe cyclique

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 : on dit que G est cyclique.

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

Proposition 3 : Les applications $\pi_n : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}_n \\ k & \mapsto & \overline{k} \end{array}$ sont des morphismes de groupes surjectifs.

Proposition 4 : Soit G un groupe monogène. S'il est infini, il est alors isomorphe à $(\mathbb{Z}, +)$, s'il est cyclique d'ordre n, il est isomorphe à $(\mathbb{Z}_n, +)$.

Exemple 5 : $\mathbb{Z}_n \simeq U_n$ avec $\begin{array}{ccc} \mathbb{Z}_n & \to & U_n \\ \overline{k} & \mapsto & e^{2i\frac{k\pi}{n}} \end{array}$

Théorème 6 : Pour $n \geq 2$ tous les sous groupes de $\mathbb{Z}_n$ sont cycliques d'ordre qui divise n. Réciproquement pour tout d diviseur de n, il existe un unique sous groupe de $\mathbb{Z}_n$ d'ordre d, c'est le sous groupe cyclique $H = \langle \frac{n}{d}\overline{1} \rangle$.

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

B Générateurs et indicatrice d'Euler

Théorème 8 : Soit $a \in \mathbb{Z}$. On a équivalence entre :
i) $\overline{a}$ est inversible dans $\mathbb{Z}_n$,
ii) a est premier avec n,
iii) $\overline{a}$ est un générateur du groupe cyclique $(\mathbb{Z}_n, +)$.

Définition 9 : On appelle fonction indicatrice d'Euler, la fonction qui associe à tout entier naturel non nul n, le nombre $\varphi(n)$ d'entiers compris entre 1 et n qui sont premiers avec n (pour $n = 1$ on a $\varphi(1) = 1$).

Exemple 10 : $\varphi(1) = 1$, $\varphi(3) = 2$, $\varphi(9) = 6$, $\varphi(p) = p - 1$.

Remarque 11 : Le théorème nous donne alors que $\varphi(n)$ est le nombre de générateurs de $(\mathbb{Z}_n, +)$ autrement le nombre d'inversible de $\mathbb{Z}_n$.

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

Théorème 13 : Soit $n = \prod_{i=1}^{\wedge} p_i^{\alpha_i}$ décomposition en facteurs premiers, alors :

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

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

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

A Groupe multiplicatif

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

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

Théorème 17 (Euler) : Pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1 \ [n]$

Corollaire 18 (petit théorème de Fermat) : Soit $p \in \mathcal{P}$, pour tout entier relatif a premier avec p on a $a^{p-1} \equiv 1 \ [p]$ et pour tout entier a, on a $a^p \equiv a \ [p]$.

Développement (Sophie - Germain)
Soit p premier impair tel que $q = 2p + 1$ est premier
Alors $\nexists (x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 [p]$ et $x^p + y^p + z^p = 0$

B Restes chinois et systèmes de congruences

Lemme 19 : Soient $(m_i)_{i \in [\![1,n]\!]}$ une suite de $n \geq 2$ entiers naturels distincts de 0 et 1.
i) Si les entiers $m_1, \dots, m_n$ sont deux à deux premiers entre eux bien ppcm est $\prod_{i=1}^{\wedge} m_i$
ii) Si on a $\mathrm{ppcm}(m_1, \dots, m_n) < \prod_{i=1}^{\wedge} m_i$

Exemple 20 : $\exists X \exists Y$ $4 = 12 < 2 \cdot 3 (= 6)$, $2 \wedge 3 \wedge 4 = 1$ ne suffit pas.

Théorème 21 (chinois) Soient $(m_i)_{1\le i\le n}$ une suite de $n\ge 2$ entiers naturels distincts de 0 et 1 et $m = m_1 \cdots m_n$.
Les entiers $m_1, \dots, m_n$ sont deux à deux premiers entre eux ssi $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$. Dans ce cas

$$\psi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \quad \Pi_m(k) \longmapsto (\Pi_{m_1}(k), \dots, \Pi_{m_n}(k))$$

(où on a noté Π_{m_i} la surjection canonique Π_{m_i}) est un isomorphisme d'anneaux d'inverse :

$$\psi^{-1} : \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \quad (\Pi_{m_1}(a_1), \dots, \Pi_{m_n}(a_n)) \longmapsto \Pi_m\left(\sum_{j=1}^{n} a_j u_j \frac{m}{m_j}\right)$$

où $(u_j)_{1\le j\le n}$ suite d'entiers relatifs telle que $\sum_{j=1}^{n} u_j \frac{m}{m_j} = 1$

Application 22 : L'équation diophantienne $ax \equiv b\,[m]$ a des solutions entières si et seulement si $\operatorname{pgcd}(a,m) \mid b$. Dans ce cas, l'ensemble des solutions est $S = \{x' + km' \mid k \in \mathbb{Z}\}$ où x' est une solution particulière de $a'x \equiv 1\,[m']$ avec $b = \operatorname{pgcd}(a,m)b'$ et $m = \operatorname{pgcd}(a,m)m'$ et $a = \operatorname{pgcd}(a,m)a'$.

Exemple 23 : Les solutions de $\begin{cases} x \equiv 2\,[4] \\ x \equiv 3\,[5] \\ x \equiv 1\,[9] \end{cases}$ sont $S = \{118 + 180k \mid k \in \mathbb{Z}\}$.

III Le corps $(\mathbb{Z}/m, +, \times)$

A Résidus quadratiques modulo p.

Théorème 24 : m est premier si et seulement $\mathbb{Z}/m$ est un corps.

Théorème 25 : 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 un carré dans $\mathbb{F}_p^*$ si et seulement si p est congru à 1 modulo 4.

Définition 27 : On dit que un entier k non multiple de p est un résidu quadratique modulo p si k est un carré dans $\mathbb{F}_p^*$.
Pour $a \in \mathbb{F}_p^*$ on note $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{sinon} \end{cases}$ le symbole de Legendre.

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

Théorème 29 : L'application $\begin{aligned} \mathbb{F}_p^* &\longrightarrow \{-1,1\} \\ a &\longmapsto \left(\frac{a}{p}\right) \end{aligned}$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ vers $\{-1,1\}$.

De plus pour tout $a \in \mathbb{F}_p^*$, on a $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$ dans $\mathbb{F}_p^*$.

Exemple 30 : $2^{\frac{5-1}{2}} = 4 \equiv -1\,[5]$ donc 2 n'est pas un résidu quadratique modulo 5.

Corollaire 31 : si $m = \pm \prod_{i=1}^{n} p_i^{\alpha_i}$ alors $\left(\frac{m}{p}\right) = (\pm 1)^{\frac{p-1}{2}} \prod_{i=1}^{n} \left(\frac{p_i}{p}\right)^{\alpha_i}$

Proposition 32 : on a $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Théorème 33 : (Loi de réciprocité quadratique) Pour tout nombre premier impair $q \neq p$ on a : $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right)$

Exemple 34 : $\left(\frac{219}{383}\right) = 1$ donc 219 est un résidu quadratique modulo 383.

B Construction de corps finis.

Notation 35 : On note $\mathcal{U}_m(p)$ l'ensemble de tous les polynômes unitaires irréductibles de degré m dans $\mathbb{F}_p[X]$ et $I_m(p)$ le cardinal de $\mathcal{U}_m(p)$.

Théorème 36 : Pour tout $P \in \mathcal{U}_m(p)$, le quotient $\mathbb{F}_p[X]/(P)$ est une $\mathbb{F}_p$-algèbre de dimension m de base $(\overline{X}^k)_{0\le k\le m-1}$ et c'est un corps fini de cardinal p^m.

Exemple 37 : Pour tout $\lambda \in \mathbb{F}_p$, le polynôme $P(X) = X - \lambda$ est unitaire de degré 1 donc irréductible dans $\mathbb{F}_p[X]$ donc $I_1(p) = p$. Tous ces corps $\mathbb{F}_p[X]/(X-\lambda)$ sont isomorphes à $\mathbb{F}_p$.

Lemme 38 : Tout diviseur irréductible de $X^{p^m} - X$ dans $\mathbb{F}_p[X]$ est de degré divisant m.
Réciproquement, tout diviseur d de m, $P \in \mathcal{U}_d(p)$ divise $X^{p^m} - X$.

Théorème 39 : Le polynôme $X^{p^m} - X$ est sans facteur carré dans $\mathbb{F}_p[X]$ et sa décomposition en facteurs irréductibles :

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

Théorème 40 : À isomorphisme près, il n'existe qu'un seul corps à p^n éléments, c'est le corps $\mathbb{F}_{p^n} = \mathbb{F}_p[X]/(P)$ où $P \in \mathcal{U}_n(p)$.

Exemple 41 : $\mathbb{F}_2 = \mathbb{Z}/2$, $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+1)$

C Irréductibilité des polynômes

Théorème 42 (critère d'Eisenstein)
Soit $P \in \mathbb{Z}[X]$, $P = \sum_0^n a_i X^i$ et p premier tel que :
i) $p \nmid a_n$
ii) $\forall i \in [\![0, n-1]\!]$ $p \mid a_i$
iii) $p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{Q}[X]$. Si de plus $c(P) = 1$ alors P est aussi irréductible dans $\mathbb{Z}[X]$

Application 43 : pour p premier, le polynôme $X^{p-1} + \dots + X + 1$ est irréductible sur $\mathbb{Z}[X]$

Théorème 44 : Soit $p \in \mathcal{P}$, $P = \sum_0^n a_i X^i \in \mathbb{Z}[X]$ et $\overline{P}$ sa réduction modulo p telle que $\overline{a_n} \neq 0$
Alors $\overline{P}$ est irréductible sur $\mathbb{Z}_p$ et P est irréductible sur $\mathbb{Q}$.

Exemple 45 : pour p premier, $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

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

Théorème 47 : $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$ avec $\Phi_d(X) = \prod_{\omega \in \mathbb{U}_d^\times} (X - \omega)$

Développement : Φ_n est à coefficients entiers, unitaire et irréductible dans $\mathbb{Z}[X]$.

Changer le dvlpt, prendre le critère d'Eisenstein au lieu des dvlpt sur les pol cyclotomiques

Références :

Rombaldi Mathématiques pour l'agrégation Algèbre et géométrie.

D. Perrin Cours d'Algèbre.

Francinou XENS algèbre 1 2007.

X. G Algèbre.