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

1) Les générateurs de $\mathbb{Z}/n\mathbb{Z}$

Déf-Prop: • Soient $x, y \in \mathbb{Z}$. On dit que x et y sont congrus modulo n (noté $x \equiv y\,[n]$) ssi $\exists\, k \in \mathbb{Z} \,/\, x - y = kn$. C'est une relation d'équivalence.
• On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence.
On note $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

Prop: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif

Prop: $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique à n éléments.
Etudions ses générateurs.

Prop: Soit $k \in \mathbb{Z}$ et $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ sa classe. Les propriétés suivantes sont équivalentes: (i) $\overline{k}$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$
(ii) $k \wedge n = 1$
(iii) k est inversible mod n, i.e. $\exists\, k' \in \mathbb{Z} \,/\, kk' \equiv 1\,[n]$

Rem: Sous le (iii), l'inverse de k peut se calculer avec une relation de Bezout.

Prop: Pour chaque entier $d \geq 1$ avec $d | n$, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d : c'est le sous-groupe cyclique engendré par la classe de $\frac{n}{d}$ dans $\mathbb{Z}/n\mathbb{Z}$

Ex: Les générateurs de $\mathbb{Z}/6\mathbb{Z}$ sont $\overline{1}$ et $\overline{5}$, et le sous-groupe de $\mathbb{Z}/6\mathbb{Z}$ d'ordre 3 est le groupe G engendré par $\overline{2}$: $G = \{\overline{2}, \overline{4}, \overline{0}\}$

Rem: Cette propriété s'applique de façon plus générale à un groupe cyclique d'ordre n.

Prop: Soit G un groupe abélien fini d'ordre $n \geq 2$. Alors $\exists!\, q_1, \dots, q_k$ tels que $\forall i \in [\![1;k]\!]$, $q_i \geq 2$, $q_i | q_{i+1}$ (si $i \neq 1$) et $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \dots \times \mathbb{Z}/q_k\mathbb{Z}$

2) Morphismes de groupes

Prop (Lemme chinois) Soient p et q des entiers ≥ 2.
Si $p \wedge q = 1$, l'application $f : \mathbb{Z}/pq\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$
définie par: $\forall k \in \mathbb{Z}$, $f(\overline{k}_{[pq]}) = (\overline{k}_{[p]}, \overline{k}_{[q]})$
est un isomorphisme d'anneaux.

Rem: Si $p \wedge q \neq 1$, $\mathbb{Z}/pq\mathbb{Z}$ n'a pas d'élément d'ordre pq.

Prop: Soit G un groupe et $a \in G$ ($a^n = 1$). Il existe un unique morphisme de groupes $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ tel que $f(\overline{1}) = a$.
Il est défini par: $\forall \overline{k} \in \mathbb{Z}/n\mathbb{Z}$, $f(\overline{k}) = a^k$

Rem: $\mathbb{Z}/n\mathbb{Z}$ est, à isomorphisme près, l'unique groupe cyclique à n éléments.

Appl: $G = \mathbb{Z}/m\mathbb{Z}$, $m \in \mathbb{N}^*$. Il existe alors $m \wedge n$ morphismes de groupes $f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$.
Si $m \wedge n = 1$ c'est le morphisme nul ($f(k) = 0 \ \forall k \in \mathbb{Z}/n\mathbb{Z}$)

Ex: Les morphismes de groupes $\mathbb{Z}/6\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z}$ sont f_1, f_2, f_3 avec
$f_1(\overline{1}_{[6]}) = \overline{0}_{[15]}$, $f_2(\overline{1}_{[6]}) = \overline{5}_{[15]}$, $f_3(\overline{1}_{[6]}) = \overline{10}_{[15]}$

Prop: Les automorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont les applications $x \longmapsto kx$ avec $k \in [\![1;n]\!] \,/\, k \wedge n = 1$.

Ex: $\mathrm{Aut}(\mathbb{Z}/6\mathbb{Z}) = \{f_0, f_1\}$ où $f_0(\overline{1}) = \overline{1}$ et $f_1(\overline{1}) = \overline{5}$

II Le groupe $((\mathbb{Z}/n\mathbb{Z})^*, \times)$

1. Etude du groupe

Déf: On appelle $(\mathbb{Z}/n\mathbb{Z})^*$ le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Rem: $(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} \,/\, k \wedge n = 1\} = \{$générateurs de $\mathbb{Z}/n\mathbb{Z}\}$.

Déf: On appelle indicatrice d'Euler de l'entier n ($n \in \mathbb{N}$), noté $\varphi(n)$, l'entier $|(\mathbb{Z}/n\mathbb{Z})^*| = |\{x \in [\![1;n]\!] \,/\, n \wedge x = 1\}|$

Prop: • Soient p premier et $\alpha \in \mathbb{N}^*$.
Alors $\varphi(p) = p - 1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$
• Si m, n entiers tels que $m \wedge n = 1$. Alors $\varphi(mn) = \varphi(m)\varphi(n)$

Rem: On a un isomorphisme de groupes $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$
En particulier, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien de cardinal $\varphi(n)$.

Prop: Soit $n \geq 2$. Soit $k \in \mathbb{Z} \,/\, k \wedge n = 1$. Alors $k^{\varphi(n)} \equiv 1\,[n]$

Cor 1 (Fermat) Soit p premier. Alors $\forall x \in \mathbb{Z}$, $x^p \equiv x\,[p]$

Cor 2 (Wilson) Soit $n \geq 2$. Alors n premier $\Longleftrightarrow (n-1)! \equiv -1\,[n]$

Ex: Le chiffre des unités de 27^{1995} est 3.

2) Cryptographie RSA à clé publique

On choisit p, q deux nombres premiers très grands

Soit $N = pq$. Alors $\varphi(N) = (p-1)(q-1)$

Soit d entier tel que $d \wedge \varphi(N) = 1$

La clé publique est (N, d), mais p et q sont secrets.

On pose alors la fonction de codage $f : \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/N\mathbb{Z}$, $x \longmapsto x^d$

Pour décoder, on calcule l'inverse e de d modulo $\varphi(N)$ et on observe que $f^{-1}(y) = y^e$ $\forall y \in \mathbb{Z}/N\mathbb{Z}$. En effet, $a^{\varphi(N)} \equiv 1 [N]$ $\forall a \in \mathbb{Z}$ donc dans $\mathbb{Z}/N\mathbb{Z}$, $a^{de} = a\, a^{de-1} = a^{\varphi(N)k} = a$ $(de \equiv 1 [\varphi(N)])$

3) Équations diophantiennes

- $ax \equiv b [n]$, $n \geqslant 2$, $a \wedge n = 1$
  $a \in (\mathbb{Z}/n\mathbb{Z})^*$ donc l'ensemble des solutions est $\{a^{-1}b + kn, k \in \mathbb{Z}\}$
  Ex: L'ensemble des entiers x tels que $36 / 7x+11$ est $\{19+36k, k \in \mathbb{Z}\}$
- $\begin{cases} x \equiv a[n] \\ x \equiv b[p] \end{cases}$, $n \wedge p = 1$
  $\exists u, v \in \mathbb{Z} / nu + pv = 1$
  Soit $\alpha = pv$ et $\beta = nu$
  L'ensemble des solutions est alors $\{\alpha a + \beta b + knp, k \in \mathbb{Z}\}$
  Ex: L'ensemble des solutions du système $\begin{cases} x \equiv 3[8] \\ x \equiv 2[21] \end{cases}$ est $\{-61 + 168k, k \in \mathbb{Z}\}$
- Théorème de Sophie Germain
  Soit p un nombre premier impair tel que $q = 2p+1$ soit premier
  Alors il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 [p]$ et $x^p + y^p = z^p$.

4) Cyclicité de $(\mathbb{Z}/n\mathbb{Z})^*$

Prop: Un morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ existe ssi m/n.
Dans ce cas, il est unique.

Prop: Soit $n \in \mathbb{N}^*$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec les p_i premiers distincts et $\alpha_i \in \mathbb{N}^*$

1) On a un isomorphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$

2) On a un isomorphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})^*$

Regardons la structure de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ pour p premier.

Prop: Soit p premier impair et $\alpha \geqslant 1$. Alors $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/\varphi(p^\alpha)\mathbb{Z}$ [DVP1]

Prop: $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, $(\mathbb{Z}/4\mathbb{Z})^* = \{1, -1\} \simeq \mathbb{Z}/2\mathbb{Z}$
Pour $\alpha \geqslant 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$

Cor: $(\mathbb{Z}/n\mathbb{Z})^*$ cyclique $\Longleftrightarrow n \in \{1,2,4\} \cup \bigcup_{\substack{q \text{ premier impair} \\ \alpha \in \mathbb{N}^*}} (\{q^\alpha\} \cup \{2q^\alpha\})$

III Les carrés dans $\mathbb{Z}/p\mathbb{Z}$

Prop: Soit $n \geqslant 2$. Alors $\mathbb{Z}/n\mathbb{Z}$ est un corps $\Longleftrightarrow n$ est premier

Dans la suite, on note le corps $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ (p premier)

1) Symbole de Legendre

Déf: Soit $a \in \mathbb{Z}$ et p premier. On dit que a est un carré mod p si $\exists x \in \mathbb{Z} / x^2 \equiv a[p]$.
Ex: 1 est un carré mod p ($\forall p$ premier) car $1^2 \equiv 1 [p]$

Prop: Soit p un nombre premier. L'ensemble des carrés de $\mathbb{F}_p^*$ est un sous-groupe (multiplicatif) qui a $\frac{p-1}{2}$ éléments. Dans $\mathbb{F}_p^*$, il y a $\frac{p-1}{2}$ carrés et $\frac{p-1}{2}$ non-carrés.

Déf: On définit le symbole de Legendre pour $a \in \mathbb{Z}$ et $p \neq 2$ premier comme:
$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0 [p] \\ 1 \text{ si } a \text{ est un carré non nul mod } p \\ -1 \text{ si } a \text{ n'est pas un carré mod } p. \end{cases}$$

Prop: Soient $a, b \in \mathbb{Z}$
(i) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
(ii) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} [p]$
(iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ donc -1 est un carré mod $p \Longleftrightarrow p \equiv 1[4]$
-1 n'est pas un carré mod $p \Longleftrightarrow p \equiv 3[4]$
(iv) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ donc 2 est un carré mod $p \Longleftrightarrow p \equiv \pm 1 [8]$
2 n'est pas un carré mod $p \Longleftrightarrow p \equiv \pm 3 [8]$

Thm (Loi de réciprocité quadratique)

Soient p, q premiers impairs distincts

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

Ex: $\left(\frac{220}{71}\right) = \left(\frac{7}{71}\right) = -\left(\frac{71}{7}\right) = -\left(\frac{1}{7}\right) = -1$ (71 est premier)

Donc 220 n'est pas un carré mod 71

Thm (Frobenius-Zolotarev) [DVP 2]

Soient p premier impair et V un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

Alors pour tout $u \in GL(V)$, on a

$$\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$$

2) Symbole de Jacobi

Soit $N = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ impair. Le symbole de Jacobi est donné par:

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\cdots\left(\frac{a}{p_r}\right)^{\alpha_r}$$

Prop (i) Si N est premier, on retrouve le symbole de Legendre.

Soient N, M impairs, et $a, b \in \mathbb{Z}$

(ii) $\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right)$ et $\left(\frac{a}{N}\right) = 0 \Longleftrightarrow a \wedge N > 1$

(iii) $\left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}$ et $\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$

(iv) $\left(\frac{M}{N}\right) = (-1)^{\frac{(N-1)(M-1)}{4}}\left(\frac{N}{M}\right)$

Rem: Le symbole de Jacobi ne caractérise pas les carrés modulo N.

En revanche, si $\left(\frac{a}{N}\right) = -1$, alors a n'est pas un carré modulo N.

IV Polynômes sur $\mathbb{F}_p[X]$

1) Irréductibilité

Prop: Soient $P, Q \in \mathbb{F}_p[X]$. Alors $P^p + Q^p = (P+Q)^p$ et $(P(X))^p = P(X^p)$

Ex: Dans $\mathbb{F}_5[X]$, $(X^2+3X-1)^5 = X^{10}+3X^5-1$

Prop: (Critère d'irréductibilité d'un polynôme sur $\mathbb{Q}[X]$)

Soit $P \in \mathbb{Z}[X]$ de degré non nul. Soit p un nombre premier qui ne divise pas le coefficient dominant de P.

Si la réduction de P modulo p est un polynôme irréductible de $\mathbb{F}_p[X]$, alors P est irréductible sur $\mathbb{Q}[X]$.

Ex: X^3+X^2+4X+1 est irréductible sur $\mathbb{Q}[X]$ (avec $p=2$)

2) Cyclotomie

Déf: Une racine n-ième de l'unité est un élément ζ de $\mathbb{C}$ tel que $\zeta^n = 1$.

Soit μ_n l'ensemble de ces éléments.

• Soit $\mu_n^* = \{\zeta \in \mu_n \,/\, \zeta^d \neq 1 \ \forall d < n\}$. Un élément de μ_n^* est appelé une racine n-ième primitive de l'unité.

Prop: • μ_n est un groupe cyclique d'ordre n, donc $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$

• Comme tout $\zeta \in \mu_n^*$ est un générateur de μ_n, il y a $\varphi(n)$ éléments de μ_n^*.

Déf: On appelle n-ième polynôme cyclotomique Φ_n le polynôme

$$\Phi_n(X) = \prod_{\zeta \in \mu_n^*}(X-\zeta)$$

Rem: Φ_n est unitaire, de degré $\varphi(n)$

Prop: $X^n - 1 = \prod_{d|n}\Phi_d(X)$

Rem: • $n = \sum_{d|n}\varphi(d)$

• On peut alors calculer Φ_n par récurrence avec $\Phi_n(X) = \dfrac{X^n-1}{\prod_{d|n,\, d\neq n}\Phi_d(X)}$

On sait déjà que $\Phi_1(X) = X-1$

Alors $\Phi_2(X) = X+1$, $\Phi_3(X) = X^2+X+1, \ldots$

App: (Thm de Wedderburn) Tout corps fini est commutatif.

Prop: $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$, et Φ_n est irréductible sur $\mathbb{Z}[X]$.

Φ_n est toujours irréductible sur $\mathbb{Q}[X]$, mais ce n'est pas forcément le cas dans $\mathbb{F}_p[X]$.

Ex: $\Phi_8 = X^4+1$ est réductible sur tous les $\mathbb{F}_p[X]$, p premier.

Thm: Soit $n \in \mathbb{N}^*$. Les propriétés suivantes sont équivalentes:

(i) $\exists p$ premier avec $p \wedge n = 1$ / Φ_n est irréductible sur $\mathbb{F}_p[X]$.

(ii) $(\mathbb{Z}/n\mathbb{Z})^*$ est cyclique.

Prop: Si $p \nmid n$, Φ_n est réductible sur $\mathbb{F}_p$ sauf, éventuellement, si on a $p=2$ et $n = 2q^\alpha$, q premier impair.

Rem: Il n'y a pas de propriété pour $p=2$ et $n=2q^\alpha$. En effet, Φ_6 est irréductible sur $\mathbb{F}_2$, mais Φ_{14} est réductible sur $\mathbb{F}_2$.

Références

[COM] Combes, Algèbre et géométrie

[HIN] Hindry, Arithmétique

[LIR] Liret, Arithmétique

[OBJ] Beck-Malick-Peyré, Objectif agrégation (pour le thm de Frobenius-Zolotarev)

[PER] Perrin, Cours d'algèbre

[XENS] Francinou-Gianella-Nicolas, Oraux X-ENS, algèbre 1 (pour le thm de Sophie Germain)