Plan détaillé 120 $\mathbb{Z}/n\mathbb{Z}$

I) $\mathbb{Z}/n\mathbb{Z}$ en tant que groupe :

A) Définitions et premières propriétés : $n \in \mathbb{N}^*$

Déf 1 : congruence modulo n

Déf 2 : classe d'un entier relatif a, et $\mathbb{Z}/n\mathbb{Z}$

THM 3 : $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \overline{n-1}\}$ groupe abélien de cardinal n, en bijection avec les restes possibles de la div. eucli par n.

Rem 4 : $\mathbb{Z}/n\mathbb{Z}$ est le quotient du groupe $(\mathbb{Z}, +)$ par le sous-groupe (distingué) $n\mathbb{Z}$.

Prop 5 : $\mathbb{Z}/n\mathbb{Z}$ cyclique, engendré par $\bar{1}$.

THM 6 : Par G groupe monogène. Si G infini, $G \simeq (\mathbb{Z}, +)$
G fini, $|G| = n$, $G \simeq (\mathbb{Z}/n\mathbb{Z}, +)$ cyclique

[ROM] p. 277 - 278

[ROM] p. 14 - 15

Ex 7 : $U_n = \{e^{\frac{2ik\pi}{n}} \mid k \in [\![0, n-1]\!]\} \simeq (\mathbb{Z}/n\mathbb{Z}, +)$ via $\bar{k} \mapsto e^{\frac{2ik\pi}{n}}$

Prop 7 : Un groupe de cardinal p premier est cyclique, donc isom. à $\mathbb{Z}/p\mathbb{Z}$

B) Sous-groupes et structure :

THM 8 : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre $d \mid n$
- $\forall d \mid n$, $\exists ! H < \mathbb{Z}/n\mathbb{Z}$ d'ordre d, $H = \langle \frac{\bar{n}}{d} \rangle$
- exemples

[ROM] p. 279

Prop 9 : Les générateurs de $\mathbb{Z}/n\mathbb{Z}$ sont les $\bar{k}$ tq $k \wedge n = 1$

THM 10 : (Structure des groupes abéliens finis) : Gabélien fini
$\exists !$ suite d'entiers $(n_k)_{1 \le k \le r}$ tq $n_1 \ge 2$, $n_1 \mid n_2 \mid \dots \mid n_k$ et $G \simeq \prod_{k=1}^{r} \mathbb{Z}/n_k\mathbb{Z}$ (3)

Ex 11 : $12 = 2^2 \cdot 3$ Les sous-groupes d'ordre 12 sont (à isom. près)
$\mathbb{Z}/12\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ (ou autre ex)

[ROM] p. 279

[ROM] p. 279

[ROM] p. 281

[ROM] p. 286

[ROM] p. 220 - 220

Dév 1

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

A) Structure et théorème des restes chinois

DÉF 12 : déf de $\mathbb{Z}/n\mathbb{Z}$ comme quotient de l'anneau $\mathbb{Z}$ avec l'idéal $n\mathbb{Z}$
↳ $\mathbb{Z}/n\mathbb{Z}$ a une structure d'anneau.

[ROM] p. 278

Rem 13 : $\mathbb{Z}/n\mathbb{Z}$ pas intègre en général ex : $\mathbb{Z}/6\mathbb{Z}$

Prop 14 : Si n non premier, $\mathbb{Z}/n\mathbb{Z}$ possède des diviseurs de 0, ce sont les éléments non nuls, non premiers avec n...
~~les $\bar{k}$ tel que $k \in [\![2, n-1]\!]$, $k \mid n$.~~

[ROM] p. 284

THM 15 : $\bar{a}$ inversible $\Leftrightarrow a \wedge n = 1 \Leftrightarrow$ $\bar{a}$ générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$

Prop 16 : Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont exactement ses sous-groupes $\frac{n}{d}(\mathbb{Z}/n\mathbb{Z})$ d|n.

THM 17 : $\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow$ n premier

THM 18 : (Le thm des restes chinois) avec r termes + mettre expression de Ψ^{-1}...
~~Cor 19 : passage aux inversibles~~.

[ROM] p. 284

Ex 19 : ...

Cor 20 : $n, m \ge 2$, $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/(n \wedge m)\mathbb{Z} \times \mathbb{Z}/(n \vee m)\mathbb{Z}$

[ROM] p. 256

B) Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$:

Déf 21 : $(\mathbb{Z}/n\mathbb{Z})^\times$

Cor 22 : corollaire du thm Chinois

Déf 23 : $\varphi(n)$ ← ind. Euler

THM 24 : (Euler) $a^{\varphi(n)} \equiv 1 \ [n]$, $(a \wedge n = 1)$.

Rem 25 : On retrouve le petit thm de Fermat

Prop 26 : propriétés sur $\varphi(n)$ ... (bcp)

THM 26 : $(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ)$

THM 27 : $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclique, p premier

THM 28 : $(\mathbb{Z}/n\mathbb{Z})^\times$ cyclique ssi ...
- [Zemor]
- [Rom]
- [Perrin]

Dév 1

Plan détaillé [120] suite

III) Cas particulier n premier et applications

A) Étude de carrés dans $\mathbb{F}_p$

Déf 29 : $\mathbb{F}_p^2$ ($\mathbb{F}_p^{*2}$ ss-groupe de $\mathbb{F}_p^*$)

Prop 30 : • Si $p=2$, $\mathbb{F}_p^2 = \mathbb{F}_p$

• $p>2$, $|\mathbb{F}_p^*| = p-1$, $|\mathbb{F}_p^2| = \frac{p+1}{2}$

• $\mathbb{F}_p^{*2} = \{x \in \mathbb{F}_p \mid x^{\frac{p-1}{2}} = 1\}$

Cor 31 : $-1 \in \mathbb{F}_p^2 \iff p \equiv 1 [4]$

Rem 32 Ces 2 prop sont vraies dans un corps fini $\mathbb{F}_q$, $q = p^m$

Cor 32 : ∃ une infinité de nbres 1er de la forme $4k+1$

→ $p \geq 3$ premier.

Déf 33 : Symbole de Legendre sur $\mathbb{F}_p^*$ et étendu sur $\mathbb{F}_p$

Rem 34 $\forall a \in \mathbb{F}_p^*$ le nbre de sol de $ax^2 = 1$ est $\left(\frac{a}{p}\right)+1 = \begin{cases} 2 \text{ si } a \text{ carré dans } \mathbb{F}_p^* \\ 0 \text{ sinon} \end{cases}$

Prop 35 : • $\forall a \in \mathbb{F}_p^*$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ dans $\mathbb{F}_p^*$

• $\left|\begin{array}{ccc} \mathbb{F}_p^* & \to & \{+1,-1\} \\ a & \mapsto & \left(\frac{a}{p}\right) \end{array}\right.$ morphisme de groupes

THM 36 : loi de réciprocité quadratique (11) (Dev 2)

Ex 37 : Calcul de $\left(\frac{23}{59}\right) = \ldots = -1$ (ou autre)

B) Équations diophantiennes : $n \geq 2$, $a \in \mathbb{N}^*$, $b \in \mathbb{Z}$

But : Résoudre dans $\mathbb{Z}$: $ax \equiv b [n]$. (*)

Prop 38 : • Si $b=1$, l'équation a des solutions (ssi) $a \wedge n = 1$

Pour $x_0 \in \mathbb{Z}$ une solution, $S = \{x_0 + kn \mid k \in \mathbb{Z}\}$

⌞ • Si $a \wedge n = 1$, $b \in \mathbb{Z}$ $S = \{bx_0 + kn \mid k \in \mathbb{Z}\}$ où x_0 est une solution particulière de $ax \equiv 1 [n]$

THM 39 : L'équation diophantienne (*) a des solutions (dans $\mathbb{Z}$) (ssi) $S := a \wedge n \mid b$

Dans ce cas, $S = \{b'x_0' + kn' \mid k \in \mathbb{Z}\}$ où $\begin{cases} a = Sa' \\ b = Sb' \\ n = Sn' \end{cases}$, x_0' solut° part de $a'x \equiv 1 [n']$

Ex 40 : Résolution de $\begin{cases} k \equiv 2 [4] \\ k \equiv 3 [5] \\ k \equiv 1 [3] \end{cases}$

C) Irréductibilité de polynômes :

[PER] p.86

THM 41 : Irréductibilité avec réduction mod un idéal 1er

Rem : En général pour $\mathbb{Z}[X]$ et $I = (p)$, premier ⇝ on se place dans $\mathbb{Z}/p\mathbb{Z}$

THM 42 : Eisenstein

Ex 43 : $X^3 + 462X^2 + 2433X - 676911 \in \mathbb{Z}[X]$ irréductible

[PER] p.82 (ou) [GOZ] p.93 (ou) [ROM] p.428

[PER] p.89 – 92

DEF 44 : Φ_n polyn. cyclotomique + rem $\deg(\Phi_n) = \varphi(n)$

PROP 45 : $X^n - 1 = \prod_{d|n} \Phi_d$

THM 46 : $\Phi_n \in \mathbb{Z}[X]$ irréductible dans $\mathbb{Q}[X]$ et $\mathbb{Z}[X]$ (Dév 2 ?)

[ROM] p.434

[GOZ] p. 155

[ROM] p. 288