120

ANNEAUX $\mathbb{Z}/n\mathbb{Z}$. APPLICATIONS.

Cadre : n sera un nombre entier strictement positif.

I STRUCTURE DE $\mathbb{Z}/n\mathbb{Z}$.

1 Le groupe $\mathbb{Z}/n\mathbb{Z}$.

Déf 1 : Congruence
Deux entiers $x, y \in \mathbb{Z}$ sont congrus modulo n (noté $x \equiv y\ [n]$) si $\exists k \in \mathbb{Z},\ x = y + kn$; c'est une relation d'équivalence ; on note $\bar{x}$ la classe de x.

Déf 2 : Quotient $\mathbb{Z}/n\mathbb{Z}$. ([RB], 1.4.1)
Les sous-groupes de $\mathbb{Z}$ sont les $k\mathbb{Z}$ où $k \in \mathbb{N}$;
On définit le groupe quotient $\mathbb{Z}/n\mathbb{Z}$, de morphisme canonique $\pi : \left| \begin{array}{c} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ x \mapsto \bar{x} \end{array} \right.$
$\mathbb{Z}/n\mathbb{Z}$ est abélien, cyclique, d'ordre n, d'éléments $\bar{0}, \bar{1}, \dots, \overline{n-1}$.

Prop 3 : ([RB], prop 1.33)
Tout groupe monogène est isomorphe à $(\mathbb{Z}, +)$ ou à un $(\mathbb{Z}/n\mathbb{Z}, +)$, où $n \in \mathbb{N}^*$.

Ex 4 : $\mathbb{U}_n = \{ e^{2ik\pi/n} \mid k \in \mathbb{Z} \}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Prop 5 : ([RB], prop 1.35)
Ici, $n \geq 2$; soit $d \in \mathbb{N}^*$ un diviseur de n.
Il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, il est engendré par $\frac{n}{d}$ et formé de l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ d'ordre divisant d.

Déf 6 : Indicatrice d'Euler ([RB], déf 1.40)
Si $n \geq 2$, on note $\varphi(n)$ le nombre de générateurs du groupe $\mathbb{Z}/n\mathbb{Z}$; $\varphi(1) = 1$.

Prop 7 : ([RB], prop 1.38)
Soit $n \geq 2$, $a \in \mathbb{Z}$.
On a : $a \wedge n = 1 \Leftrightarrow \bar{a}$ engendre $(\mathbb{Z}/n\mathbb{Z}, +)$

Coro 8 : ([RB], 1.4.2)
On en déduit : $\varphi(n) = \#\{ a \in [\![1, n]\!] \mid a \wedge n = 1 \}$;
Si p est premier et $\alpha \in \mathbb{N}^*$, alors $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Ex 9 : $\mathbb{Z}/6\mathbb{Z}$ possède 4 sous-groupes : $\{\bar{0}\}$, $\langle \bar{3} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \bar{2} \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ et lui-même
$\varphi(6) = 2$ et les générateurs de $\mathbb{Z}/6\mathbb{Z}$ sont $\bar{1}$ et $\bar{5}$.

Prop 10 : ([RB], prop 1.42)
Soit $d \in \mathbb{N}^*$, avec $d \mid n$.
$\mathbb{Z}/n\mathbb{Z}$ contient exactement $\varphi(d)$ éléments d'ordre d.

Coro 11 : ([RB], coro 1.43)
On en déduit : $\sum_{\substack{d \mid n \\ d > 0}} \varphi(d) = n$.

Prop 12 :
L'ensemble des automorphismes du groupe $\mathbb{Z}/n\mathbb{Z}$ est :
$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \{ \bar{k} \mapsto \overline{ak} \mid a \wedge n = 1,\ a \in [\![1, n]\!] \}$; on a : $\#\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \varphi(n)$.

Ex 13 :
Les automorphismes de $\mathbb{Z}/4\mathbb{Z}$ sont Id et $\alpha : \left| \begin{array}{ccc} \bar{0} & \mapsto & \bar{0} \\ \bar{1} & \mapsto & \bar{3} \\ \bar{2} & \mapsto & \bar{2} \\ \bar{3} & \mapsto & \bar{1} \end{array} \right.$. $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$

Thm 14 : Groupes abéliens finis ([Com], 3.6)
Soit G un groupe abélien fini d'ordre $n \geq 2$;
Il existe un unique k-uplet $(d_1, \dots, d_k) \in \mathbb{N}^k$ tel que $d_1 | d_2 | \dots | d_k$ et $G \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z}$.

Ex 15 : Les groupes abéliens d'ordre 24 sont $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/6\mathbb{Z}$

2 L'anneau $\mathbb{Z}/n\mathbb{Z}$.

Prop 16 : ([RB], 1.4.2)
$n\mathbb{Z}$ est en fait un idéal de l'anneau $\mathbb{Z}$; dès lors, on munit $\mathbb{Z}/n\mathbb{Z}$ de $\bar{a}.\bar{b} = \overline{ab}$ et $\mathbb{Z}/n\mathbb{Z}$ est un anneau.

Prop 17 : Inversibles de $\mathbb{Z}/n\mathbb{Z}$ ([RB], prop 1.38)
On a, pour $a \in \mathbb{Z}$: $a \wedge n = 1 \Leftrightarrow \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$
Par conséquent : $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ et $\#(\mathbb{Z}/n\mathbb{Z})^\times = \varphi(n)$.

Thm 18 : ([RB], coro 1.39)
$\mathbb{Z}/n\mathbb{Z}$ est un corps $\Leftrightarrow n$ est premier

Rq 19 : Si $\alpha \geq 2$, et si p est premier, $\mathbb{F}_{p^\alpha} \simeq \mathbb{Z}/p^\alpha\mathbb{Z}$ car $p^\alpha - 1 > \varphi(p^\alpha)$.
Plus précisément $(\mathbb{F}_{p^\alpha})^\times \simeq \mathbb{Z}/(p^\alpha - 1)\mathbb{Z}$.

Thm 20 : Lemme chinois ([Per], prop I.6.1)
Si m et n sont des entiers premiers entre eux, on a l'isomorphisme d'anneaux : $\left| \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ \bar{r} & \longmapsto & (\hat{r}, \dot{r}) \end{array} \right.$ où $\bar{r}$ (resp. $\hat{r}$, $\dot{r}$) désigne la classe de r modulo mn (resp. m, n).

C-Ex 21 : $\mathbb{Z}/4\mathbb{Z} \not\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Ex 22 : ([RB], ex 1.52)
On a, pour $x \in \mathbb{Z}$: $x \equiv 159\ [247] \Leftrightarrow \begin{cases} x \equiv 3\ [13] \\ x \equiv 7\ [19] \end{cases}$.

Coro 23 : ([Per], prop I.7.4)
1) Si $m \wedge n = 1$, alors $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ et $\varphi(mn) = \varphi(m)\varphi(n)$.
2) Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ où les p_i sont premiers, distincts et où $\alpha_i \in \mathbb{N}^*$,
Alors $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})$ et $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$.

Lem 24 : ([Per], lem I.7.7)
Soit $\alpha \in \mathbb{N}^*$, p premier impair ; on a $(1+p)^{p^\alpha} = 1 + \lambda p^{\alpha+1}$ où $\lambda \in \mathbb{N}^*$, $\lambda \wedge n = 1$.

Prop 25: ([Per], prop I.7.6)
Soit $\alpha \in \mathbb{N}^*$, p premier impair ; on a $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

Lem 26: ([Per], lem I.7.11)
Soit $\alpha \in \mathbb{N}^*$, on a : $5^{2^\alpha} = 1 + \lambda . 2^{\alpha+2}$ avec λ impair.

Prop 27: ([Per], prop I.7.10)
On a $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$, $(\mathbb{Z}/4\mathbb{Z})^\times = \{\bar{1}, \bar{3}\}$ et pour $\alpha \geq 3$, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.
On peut alors décrire le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.

II ARITHMÉTIQUE DANS $\mathbb{Z}$

1 Nombres premiers

Thm 28: Test de primalité d'Euler-Fermat ([FG], exo 3.1)
1) Si $a \in \mathbb{Z}$, $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1 [n]$
Ainsi, si p est premier et si $a \wedge p = 1$, alors $a^p \equiv a [p]$.
2) Soient $a \in \mathbb{N}^*$, $n \in \mathbb{N}$ $(n \geq 2)$ tels que $a^{n-1} \equiv 1 [n]$ et $a^x \not\equiv 1 [n]$ pour tout x diviseur strict de $n-1$.
Alors n est premier.

Ex 29: $(1035^{125})^{5642} \equiv 9 [17]$ ([RB], exo 1.12)

Appli 30: Chiffrement RSA ([Gou], prob 1.1)
Soient p et q premiers distincts ; $c, d \in \mathbb{Z}$ tels que $cd \equiv 1 [\varphi(n)]$, où $n = pq$.
Alors $\forall t \in \mathbb{Z}$, $t^{cd} \equiv t [n]$.
→ On veut transmettre le message $t \in \mathbb{Z}/n\mathbb{Z}$, qu'on chiffre par l'application $g : \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ t & \mapsto & t^c \end{array} \right.$, appelée fonction de chiffrement.
→ (n, c) constitue la clé publique et d la clé secrète.
→ Connaissant d, on obtient $f : \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ t & \mapsto & t^d \end{array} \right.$, appelée fonction de déchiffrement, car $f \circ g(t) = t$.
→ La sécurité du système RSA vient du fait qu'il est très difficile de déterminer d à partir de (n, c).

Déf 31: Nombres pseudo-premiers ([Gou], prob 1.2)
Soit $a \in \mathbb{N}$, $a \geq 2$; on dit que $n \in \mathbb{N}$ est pseudo-premier en base a (noté pp-a) si n n'est pas premier et si $a^{n-1} \equiv 1 [n]$.

Prop 32: ([Gou], prob 1.2)
Si p est premier impair avec $p \nmid a(a^2-1)$
Alors $\frac{a^{2p}-1}{a^2-1}$ est pp-a. Ainsi il existe une infinité de nombres pp-a.

Déf 33: Nombres de Carmichael ([Gou], prob 1.2)
Un entier $n \geq 2$ est appelé nombre de Carmichael si n n'est pas un nombre premier et si $\forall a \in \mathbb{Z}$, $a^n \equiv a [n]$ (en particulier, pour tout a premier avec n, n est pp-a).

Thm 34: Korselt ([Gou], prob 1.2)
Soit $n \geq 2$, on a l'équivalence :
n est de Carmichael $\Leftrightarrow \begin{cases} n \text{ est composé, sans facteur carré} \\ \forall p \text{ facteur premier de } n,\ (p-1) \mid (n-1) \end{cases}$

Ex 35: 561 est un nombre de Carmichael. ([Gou], prob 1.2).

Thm 36: Wilson ([FG], exo 3.2)
Soit $n \geq 2$; on a : n est premier $\Leftrightarrow (n-1)! \equiv -1 [n]$

Thm 37: Sophie Germain ([XENSAR1], exo 4.39)
Soit p un nombre premier impair tel que $2p+1$ soit impair.
Alors il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 [p]$ et $x^p + y^p + z^p = 0$.

DÉVELOPPEMENT N°1.

2 Résidus quadratiques

Ici, p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps noté $\mathbb{F}_p$; $\mathbb{F}_p^2 := \{x \in \mathbb{F}_p \mid \exists y \in \mathbb{F}_p,\ x = y^2\}$ et $\mathbb{F}_p^{*2} := \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Prop 38: ([Per], prop III.2.10-11)
- Si $p = 2$, $\mathbb{F}_p^2 = \mathbb{F}_p$.
- Si $p > 2$, $\#\mathbb{F}_p^2 = \frac{p+1}{2}$, $\#\mathbb{F}_p^{*2} = \frac{p-1}{2}$ et $x \in \mathbb{F}_p^{*2} \Leftrightarrow x^{\frac{p-1}{2}} = 1$

Appli 39: ([Com], exo 12.14)
Soient $a, b, c \in \mathbb{F}_p$ avec $a, b \neq 0$.
L'équation $ax^2 + by^2 = c$ admet des solutions $(x, y) \in \mathbb{F}_p^2$.

Ex 40: Résolution de $x^2 + xy + 8y^2 \equiv 10 [13]$. ([Com], exo 12.14)

Coro 41: ([Per], coro III.2.13)
On a, pour $p > 2$: $(-1) \in \mathbb{F}_p^2 \Leftrightarrow p \equiv 1 [4]$.

Appli 42: ([Com], exo 12.7.1)
Si $p \equiv 3 [4]$, alors l'équation $x^2 + y^2 = pz^2$ a pour seule solution $(0,0,0)$ dans $\mathbb{Z}^3$.

Appli 43: ([Per], appli III.2.16)
Il existe une infinité de nombres premiers de la forme $4n+1$, $n \in \mathbb{N}$.

Thm 44: des deux carrés ([Per], thm II.6.6)
p est somme de deux carrés $\Leftrightarrow p = 2$ ou $p \equiv 1 [4]$.

Déf 45: Symbole de Legendre. ([Goz], déf XII.18).
Quand p est impair, on définit, pour $x \in \mathbb{F}_p$: $\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \in \mathbb{F}_p^{*2} \\ 0 \text{ si } x = 0 \\ -1 \text{ sinon} \end{cases}$.
On a donc $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ dans $\mathbb{F}_p$.

Thm 46: Réciprocité quadratique ([Goz], thm XII.25)
Soient p, q premiers impairs distincts.
On a : $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Ex 47: 17 n'est pas un carré dans $\mathbb{F}_{41}$. ([Goz], ex XII.28)

Appli 48: ([Gou], sujet 1.2)
Soit $p > 5$. 5 est un carré dans $\mathbb{F}_p \Leftrightarrow p \equiv \pm 1 [10]$
Il existe une infinité de nombres premiers de la forme $10n-1$, $n \in \mathbb{N}$.

Thm 49: Frobenius-Zolotarev ([OA], exo 5.4)
Soit p premier impair, $n \geq 2$ et $u \in GL_n(\mathbb{F}_p)$.
On a : $\varepsilon(u) = \left(\frac{\det u}{p}\right)$.

Appli 50: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ pour p premier impair.

III POLYNÔMES IRRÉDUCTIBLES

1 Irréductibilité dans $\mathbb{Z}/p\mathbb{Z}[X]$

Thm 51: ([Goz], thm VII.24)
Soit p premier, et π un polynôme irréductible de $\mathbb{F}_p[X]$.
Alors $\mathbb{F}_p[X]/(\pi)$ est un corps, à $p^{\deg \pi}$ éléments.

Thm 52: ([Goz], thm VII.27)
Soit p premier, $n \in \mathbb{N}^*$;
Pour $j \in \mathbb{N}^*$, on note $I(p,j)$ l'ensemble des polynômes irréductibles de $\mathbb{F}_p[X]$ de degré j.
Alors $X^{p^n} - X = \prod_{d|n} \prod_{Q \in I(p,d)} Q(X)$, dans $\mathbb{F}_p[X]$

Coro 53: ([Goz], déf VII.28)
On en déduit : $p^n = \sum_{d|n} d \, \#I(p,d)$.

Ex 54: Dans $\mathbb{F}_2[X]$, on a : $X^{2^3} - X = X(X+1)(X^3+X+1)(X^3+X^2+1)$ ([Goz], ex VII.30)

Thm 55: ([Per], thm III.3.9)
Soit $P \in \mathbb{F}_p[X]$, de degré $n \in \mathbb{N}^*$.
Alors P est irréductible dans $\mathbb{F}_p[X] \Leftrightarrow$ P est sans racine dans les extensions de $\mathbb{F}_p$ de degré inférieur à $\frac{n}{2}$.

Ex 56: X^4+X+1 est irréductible dans $\mathbb{F}_2[X]$. ([Per], ex III.3.10)

2 Irréductibilité dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$

Prop 57: ([Per], III.3)
Soit $P \in \mathbb{Z}[X]$; on a :
P est irréductible dans $\mathbb{Z}[X] \Leftrightarrow$ P est irréductible dans $\mathbb{Q}[X]$ et de contenu 1.

Thm 58: Eisenstein ([Per], thm III.3.2)
Soit $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ et soit p un nombre premier.
On suppose : 1) $p \nmid a_n$
2) $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$
3) $p^2 \nmid a_0$
Alors P est irréductible dans $\mathbb{Q}[X]$.

Ex 59: Soit p un nombre premier. ([Per], appli III.3.4)
Alors $X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Z}[X]$.

Thm 60: Réduction ([Per], thm III.3.5)
Soit p un nombre premier; $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ et $\overline{P}$ la réduction de P modulo $p\mathbb{Z}$.
On suppose que $\overline{a_n} \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$.
Alors, si $\overline{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$,
Alors P est irréductible dans $\mathbb{Q}[X]$.

Ex 61: $123X^3 + 456X^2 + 7X - 89$ est irréductible dans $\mathbb{Z}[X]$ ([Per], lem III.3.8)
Pour p premier, $X^p - X - 1$ est irréductible dans $\mathbb{F}_p[X]$ donc dans $\mathbb{Z}[X]$

Rmq 62: ([Per], prop III.3.11)
Le polynôme X^4+1 est irréductible dans $\mathbb{Z}[X]$, mais réductible dans $\mathbb{F}_p[X]$ pour tout p premier.
Il met ainsi en évidence que le théorème de réduction peut être mis en défaut.

3 Polynômes cyclotomiques

Déf 63: Polynôme cyclotomique. ([Per], déf III.4.3)
Soit $n \in \mathbb{N}^*$,
On note $\Phi_n = \prod_{\xi \in \mu_n^*} (X - \xi)$ le $n^{\text{ième}}$ polynôme cyclotomique sur $\mathbb{C}$,
où $\mu_n^* = \left\{ \exp\left(\frac{2ik\pi}{n}\right) \mid k \in \mathbb{Z}, \, k \wedge n = 1 \right\}$ est l'ensemble des racines primitives $n^{\text{èmes}}$ de l'unité.

Prop 64: ([Per], prop. III.4.4)
On a : $X^n - 1 = \prod_{d|n} \Phi_d$, où $n \in \mathbb{N}^*$.

Thm 65: ([Gou], prob 2.9)
D'une part, $\forall n \in \mathbb{N}^*$, $\Phi_n \in \mathbb{Z}[X]$.
D'autre part, $\forall n \in \mathbb{N}^*$, Φ_n est irréductible dans $\mathbb{Z}[X]$.

DÉVELOPPEMENT N°2

Références :
[RB] : J.J. Risler, P. Boyer — Algèbre pour la licence 3 — Dunod, 2006.
[Com] : F. Combes — Algèbre & Géométrie — Bréal, 1998.
[Per] : D. Perrin — Cours d'algèbre — Ellipses, 1996.
[FG] : S. Francinou, H. Gianella — Exercices de mathématiques pour l'agrégation, Algèbre 1 — Masson, 1997.
[Gou] : X. Gourdon — Algèbre — Ellipses, 2009.
[XENSAlg1] : S. Francinou, H. Gianella, S. Nicolas — Oraux X-ENS Algèbre 1 — Cassini, 2014
[Goz] : I. Gozard — Théorie de Galois — Ellipses, 2009.
[OA] : V. Beck, J. Malick, G. Peyré — Objectif Agrégation — H&K, 2005.