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

Refs : [RB] Risler Boyer. Algèbre pour la L3 (Cal1) Calais, Théorie des groupes. [Ulm] Ulm, Théorie des groupes (Com1) Combes Algèbre [Per2] Perrin Algèbre. [Serre] Serre Cours d'Arithmétique. [FGNAP1] Oraux X-ens Algèbre 1

Devts : 26 (Sophie Germain)
97 (Chevalley Warning)
39 (Réciprocité)
57 (Dirichlet faible)

Notation : Par défaut, n désignera un entier, p un nombre premier, q une puissance (non nulle) de p.

I. Structure.

1) Structure de groupe.

[RB] 10 11

Rappel : Les sous groupes de $\mathbb{Z}$ sont les ensembles $n\mathbb{Z}$ où $n\in\mathbb{N}$. Ce sont aussi ses idéaux.

Prop-def 1 : Le groupe $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$. Le morphisme canonique $\pi : \mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ fait correspondre à $k\in\mathbb{Z}$ sa classe modulo n.
Deux entiers sont dits congrus modulo n si ils ont même image par π. (on notera $\cdot\equiv\cdot[n]$ cette relation).

Prop 2 Tout groupe monogène est isomorphe soit à $(\mathbb{Z},+)$ soit à $(\mathbb{Z}/n\mathbb{Z},+)$ pour un entier $n>0$ suivant son cardinal. ($\forall n\in\mathbb{N}^*$, $|\mathbb{Z}/n\mathbb{Z}|=n$).

(Cal1) 93

Ex 3 Le groupe $\mathbb{U}_n$ des racines n-ièmes de l'unité dans $\mathbb{C}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

[RB] 11

Prop 4 : Tout sous groupe d'un groupe cyclique est cyclique ; pour $n\geq 1$
. Tout sous groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique engendré par la classe d'un diviseur b de n, ce sous groupe est d'ordre $a=n/b$.
. Réciproquement, si $a>0$ divise n et $b:=n/a$, il existe un unique sous groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre a, engendré par la classe de b modulo n.

(Cal1) 93 98

Ex 5 : Sous groupes de $\mathbb{Z}/6\mathbb{Z}$: Les diviseurs de 6 sont 1, 2, 3, 6. Donc 4 sous groupes distincts

$\langle\bar 1\rangle=\mathbb{Z}/6\mathbb{Z}$ $\langle\bar 2\rangle=\{\bar 2,\bar 4,\bar 0\}$ $\langle\bar 3\rangle=\{\bar 0,\bar 3\}$ $\langle\bar 6\rangle=\{\bar 0\}$.
$\simeq\mathbb{Z}/6\mathbb{Z}$ $\simeq\mathbb{Z}/3\mathbb{Z}$ $\simeq\mathbb{Z}/2\mathbb{Z}$ $\simeq\mathbb{Z}/\mathbb{Z}$.

Def 6 : Soit $n\geq 1$, On appelle indicatrice d'Euler de n l'entier $\varphi(n)=\#\{k\in[\![1,n]\!] \mid k\wedge n=1\}$
avec $\varphi(1)=1$ par convention.

Prop 7 : Soit $k\in\mathbb{N}$, $\bar k$ engendre $(\mathbb{Z}/n\mathbb{Z},+)$ si et seulement si $k\wedge n=1$. En particulier, $\varphi(n)$ donne le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z},+)$.

Ex 8 $\varphi(6)=2$. Car les générateurs de $\mathbb{Z}/6\mathbb{Z}$ sont $\bar 1,\bar 5$.

Prop 9 : Pour $d\mid n$, $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(d)$ éléments d'ordre d.
- $n=\sum_{d\mid n}\varphi(d)$ (utile pour calculer les valeurs de φ).

Prop 10 : Les automorphismes du groupe de $\mathbb{Z}/n\mathbb{Z}$ sont les applications $\psi_k:\bar x\longmapsto k.\bar x$ pour $1\leq k\leq n$ avec $k\wedge n=1$.

[Ulm]

Rq 11 : Cette correspondance donnera un isomorphisme, voir.

Ex 12 : $Aut(\mathbb{Z}/6\mathbb{Z})\simeq\mathbb{Z}/2\mathbb{Z}$ (groupe à deux éléments).

Appli 13 : Soit G un groupe abélien fini, il existe des entiers $d_1,\dots d_r$ tels que $d_1\mid d_2\dots\mid d_r$ et $G\simeq\mathbb{Z}/d_1\mathbb{Z}\times\dots\times\mathbb{Z}/d_r\mathbb{Z}$. Cette écriture est de plus unique.

Rq : Nécessite Ulm 22.

Ex 14 : Il existe exactement deux groupes d'ordre p^2 $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$.

Prop 15 : Pour $\alpha\geq 1$, on a $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$, en particulier $\varphi(p)=p-1$ et tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ en est un générateur.

2) Structure d'anneaux

[RB] 13-15

Prop 16 Pour $n\geq 1$, $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ est muni d'une structure d'anneau par $\bar x.\bar y:=\overline{xy}$.

Prop 17 Soit $n>1$ et $a\in\mathbb{Z}$, les conditions suivantes sont équivalentes
- $\bar a$ engendre $\mathbb{Z}/n\mathbb{Z}$ - $\bar a\in(\mathbb{Z}/n\mathbb{Z})^\times$

Ainsi le sous ensemble de $\mathbb{Z}/n\mathbb{Z}$ formé de ses générateurs est $(\mathbb{Z}/n\mathbb{Z})^\times$. (La correspondance de prop 10 donne alors un isomorphisme de groupes $Aut(\mathbb{Z}/n\mathbb{Z})\simeq(\mathbb{Z}/n\mathbb{Z})^\times$.)

Cor 18 : L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier. On note $\mathbb{F}_n$ le corps $\mathbb{Z}/n\mathbb{Z}$ dans ce cas.

Prop 19 (Euler) Soit a, n deux entiers non nuls avec $a\wedge n=1$. Alors $a^{\varphi(n)}\equiv 1[n]$.

Prop 20 (Fermat). Soit p premier et $a\in\mathbb{N}^*$ non divisible par p alors
$a^{p-1}\equiv 1[p]$.

Prop 21 (Wilson) Soit p premier, alors $(p-1)!\equiv -1[p]$.

[RB] 16. Théo 22 (Restes Chinois) Soit $n \in \mathbb{N}$ tel que $n = m_1 m_2$ avec $m_1 \wedge m_2 = 1$. L'application

$$\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}, \quad \bar{k}^{n} \longmapsto (\bar{k}^{m_1}, \bar{k}^{m_2})$$

est bien définie et est un isomorphisme d'anneaux.

Rq 23 : Ce résultat se généralise au cas d'un produit $m_1 \dots m_s$ de nombres premiers entre eux deux à deux.

Ex 24 : Résolution de systèmes de congruences : $x \in \mathbb{N}$ est solution de $\begin{cases} x \equiv 1 [3] \\ x \equiv 2 [4] \\ x \equiv 0 [5] \end{cases}$ si et seulement si $x = 10 + 60k$ avec $k \in \mathbb{Z}$.

Cor 25 : Soient $n, m \in \mathbb{N}$ premiers entre eux, on a $(\mathbb{Z}/nm\mathbb{Z})^\times \simeq (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ et donc $\varphi(nm) = \varphi(n)\varphi(m)$ (on dit que la fonction φ est multiplicative).

II Arithmétique.

1) Nombres premiers.

[Gou1] 34-35. Chiffrement RSA Étant donnés p et q premiers distincts et $n = pq$, c et d deux entiers tels que $cd \equiv 1 [\varphi(n)]$. Alors pour $t \in \mathbb{Z}$, on a $t^{cd} \equiv t [n]$. L'application $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ donnée par $\bar{t} \mapsto \bar{t}^c$ est la fonction de chiffrement, $\bar{t} \mapsto \bar{t}^d$ celle de déchiffrement. Le couple (n, c) forme une "clef publique" permettant à tous le chiffrement d'un message, que seule la connaissance de d permet de décoder. L'intérêt de ce système réside dans la difficulté à trouver p, q et donc $\varphi(n)$.

Nombres de Carmichael. Réciproque fausse de la prop 20 (Fermat). Un nombre $n \geq 2$ est dit de Carmichael s'il n'est pas premier et si $\forall a \in \mathbb{Z}$, $a^n \equiv a [n]$. Le plus petit tel nombre est 561. Il existe une infinité de nombres de Carmichael.

[FGNAe1] 167 Théo 26 (Sophie Germain) Si $p \neq 2$ est tel que $2p+1$ soit premier, alors pour $(x, y, z) \in \mathbb{Z}^3$, $x^p + y^p + z^p = 0$ entraîne $xyz \equiv 0 [p]$. DVP

Théo 27 (Chevalley Warning) Soit p premier et $n \geq 1$. Soient $P_1, \dots, P_r$ dans $\mathbb{F}_p[X_1, \dots, X_n]$ tels que $\sum_{i \leq r} \deg_{tot}(P_i) < n$ et $V = \bigcup P_i^{-1}\{0\}$, alors $\operatorname{card} V \equiv 0 [p]$. DVP

2) Carrés et sommes de carrés.

[Perr] 73-75 Rappel : Si $q = p^n$ est une puissance de p, il existe un unique corps $\mathbb{F}_q$ à q éléments. Réciproquement, le cardinal d'un corps fini est toujours une puissance d'un nombre premier p (ce corps est alors une extension de $\mathbb{F}_p$).

Def 28 On pose $(\mathbb{F}_q)^2 = \{ y \in \mathbb{F}_q \mid \exists x \in \mathbb{F}_q \mid x^2 = y \}$ l'ensemble des carrés de $\mathbb{F}_q$ et $(\mathbb{F}_q^*)^2 = \mathbb{F}_q^{*} \cap \mathbb{F}_q$

Prop 29 : Si $q = p^n$, on a
- Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$ - Si $p > 2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|(\mathbb{F}_q^*)^2| = \frac{q-1}{2}$.

Prop 30 : Si $q = p^n$ et $p > 2$, on a $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$

Cor 31 : Sous les mêmes hypothèses, -1 est un carré dans $\mathbb{F}_q$ si et seulement si q est congru à 1 modulo 4.

Appli 32 Il existe une infinité de nombres premiers de la forme $4k+1$.

[Serre] 14-16 Def 33 : Soit p premier > 2. On dit que $a \in \mathbb{N}$ est résidu quadratique modulo n si $\bar{a}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Ex 34 : a est un résidu quadratique modulo 6 si et seulement si $a \equiv 0, 1, 3, 4 [6]$.

Def 35 : Soit p premier > 2 et $a \in \mathbb{N}$, on définit le symbole de Legendre de a par $\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } x \in \mathbb{F}_p^{*2} \\ -1 \text{ si } x \notin \mathbb{F}_p^{*2} \\ 0 \text{ si } x = 0 \end{cases}$ (ne dépend que de $\bar{a}^p$)

Rq 36 : L'entier $\left(\frac{a}{p}\right)$ a la même classe modulo p que $a^{\frac{p-1}{2}}$.

Prop 37 : Pour $x, y \in \mathbb{F}_p^*$ on a $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$. Le symbole de Legendre donne un morphisme $\mathbb{F}_p^* \longrightarrow \{\pm 1\}$.

Théo 38 (Réciprocité quadratique) Soient p et q deux nombres premiers distincts impairs. On a

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

DVP

[Serre] 17.

Ex39 Calcul de symbole de Legendre :

$$\left(\frac{29}{43}\right)=\left(\frac{43}{29}\right)=\left(\frac{14}{29}\right)=\left(\frac{2}{29}\right)\left(\frac{7}{29}\right)=-\left(\frac{7}{29}\right)=-\left(\frac{29}{7}\right)=-\left(\frac{1}{7}\right)=-1.$$

Prop40 : On a $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$. On peut toujours calculer le symbole de Legendre $\left(\frac{p}{q}\right)$ par réduction et division euclidienne.

Ex41 : L'équation $x^2+59y=23$ n'a pas de solutions entières.

[Perrin] 57.

Théo42 (Deux carrés)

Un nombre premier p est somme de deux carrés si et seulement si $p\equiv 1[4]$ ou $p=2$.

II. Applications aux polynômes.

1) Irréductibilité des polynômes de $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$

Prop43 : Soit $P,Q\in\mathbb{F}_p[X]$. On a

- $(P+Q)^p=P^p+Q^p$ - $(P(X))^p=P(X^p)$

[Perrin] 51.

Def44 : On définit le contenu de $P=\sum_{k=0}^{n}a_kX^k$ par $c(P)=\text{pgcd}(a_0\dots a_n)$.

Un polynôme P est dit primitif si on a $c(P)=1$

Prop45 : Si P,Q sont deux polynômes de $\mathbb{Z}[X]$, alors $c(PQ)=c(P)c(Q)$.

Prop46 : Les polynômes irréductibles de $\mathbb{Z}[X]$ sont

- Les polynômes constants, irréductibles dans $\mathbb{Z}$ (les nombres premiers)
- Les polynômes de degré ≥ 1, primitifs et irréductibles dans $\mathbb{Q}[X]$.

[Perrin] 77.

Théo47 (Critère d'Eisenstein)

Soit $P=\sum_{k=0}^{n}a_kX^k\in\mathbb{Z}[X]$ et p un nombre premier tel que

$-p\nmid a_n$ $-p\mid a_i\ \forall i\leq n-1$. $-p^2\nmid a_0$

Alors P est irréductible dans $\mathbb{Z}[X]$.

Appli48 $X^{p-1}+\dots+1$ est irréductible sur $\mathbb{Z}[X]$.

[Perrin] 77

Théo49 (Réduction)

Soit $P=\sum_{k=0}^{n}a_kX^k\in\mathbb{Z}[X]$ et $\overline{P}$ son image dans $\mathbb{F}_p[X]$, si $a_n\not\equiv 0[p]$.

et $\overline{P}$ est irréductible sur $\mathbb{F}_p$ alors P est irréductible sur $\mathbb{Q}$

Ex50 : $P(X)=X^3+2014X^2+2015X-13$ est irréductible sur $\mathbb{Z}$.

Si p est premier, X^p-X-1 est irréductible sur $\mathbb{Z}$,

2) Polynômes cyclotomiques.

[Perrin] 8082

Def51 : Soit $n\in\mathbb{N}^*$, on définit $\phi_n\in\mathbb{C}[X]$ le $n$ième polynôme cyclotomique par

$$\phi_n(X)=\prod_{\xi\in\mu_n^*}(X-\xi).$$

ou $\mu_n^*\subset\mathbb{C}$ désigne les racines primitives n-ème de l'unité.

Rq52 : ϕ_n est unitaire de degré $\varphi(n)$.

Prop53 : $\forall n\in\mathbb{N}^*$, $X^n-1=\prod_{d\mid n}\phi_d(X)$.

Ex54 : $\phi_1=X-1$. $\phi_2=X+1$ $\phi_5=X^4+X^3+X^2+X+1$, $\phi_p=\sum_{k=0}^{p-1}X^k$.

Prop55 : Pour $n\in\mathbb{N}$, ϕ_n est à coefficients dans $\mathbb{Z}[X]$ et est irréductible.

[FGN1] 119

Lemme56 : Soit $a\in\mathbb{Z}$ et p premier tel que

$-p\mid\phi_n(a)$ $-p\nmid\phi_d(a)$ pour $d\mid n$ et $d<n$.

Alors p est congru à 1 modulo n

Théo57 (Dirichlet faible)

Pour $n\geq 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.

DVP