Anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Applications.

Février Hugo Liard Thibault

12 avril 2012

1 Structure

1.1 Définition et premières propriétés

- Si $n \in \mathbb{N}$, $n\mathbb{Z}$ est un sous groupe de $(\mathbb{Z}, +)$. Or $(\mathbb{Z}, +)$ est commutatif donc $n\mathbb{Z}$ est un sous groupe distingué de $\mathbb{Z}$. Ainsi on peut définir le groupe quotient $\frac{\mathbb{Z}}{n\mathbb{Z}}$.
- $\mathbb{Z}$ est un anneau commutatif unitaire et $n\mathbb{Z}$ un idéal de $\mathbb{Z}$ donc il existe sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$ une unique structure d'anneau qui fasse de $\pi : \mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ un morphisme d'anneaux.

Proposition 1 *Soit $s \in \mathbb{Z}$, les propriétés suivantes sont équivalentes :*

1. *s premier avec n*
2. *$\overline{s}$ générateur du groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$*
3. *$\overline{s} \in (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$ groupe des éléments inversibles pour la multiplication de l'anneau $\frac{\mathbb{Z}}{n\mathbb{Z}}$*

Definition 1 (la fonction d'Euler) *On appelle fonction d'Euler et on note $\varphi(n)$ le nombre d'entiers x tels que $1 \leq x \leq n$ et x premier avec n.*

Remarque 1

- $\varphi(n) = |(\frac{\mathbb{Z}}{n\mathbb{Z}})^*|$
- *Si p premier, $\varphi(p) = p - 1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ avec $\alpha \in \mathbb{N}^*$*
- *On peut retrouver $\varphi(p) = p - 1$ en utilisant (p premier) $\Leftrightarrow$(L'anneau $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est un corps)*

Proposition 2 *Tout sous-groupe de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est cyclique et pour tout diviseur d de n, il existe un unique sous groupe H_d de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ d'ordre d.*

Application 1 *Détermination des sous groupes de $\frac{\mathbb{Z}}{20\mathbb{Z}}$*

Théorème 1 (chinois) *Soit m et n deux entiers non nuls premiers entre eux. Les anneaux $(\frac{\mathbb{Z}}{m\mathbb{Z}}) \times (\frac{\mathbb{Z}}{n\mathbb{Z}})$ et $\frac{\mathbb{Z}}{mn\mathbb{Z}}$ sont isomorphes.*

1.2 Les automorphismes de $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +)$

L'identité est l'unique automorphisme de $(\frac{\mathbb{Z}}{n\mathbb{Z}}, +, \times)$.

Proposition 3 *On a un isomorphisme $Aut(\frac{\mathbb{Z}}{n\mathbb{Z}}) \simeq (\frac{\mathbb{Z}}{n\mathbb{Z}})^*$. En particulier, $Aut(\frac{\mathbb{Z}}{n\mathbb{Z}})$ est un groupe abélien de cardinal $\varphi(n)$.*

Proposition 4 *Soit n un entier, $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec les p_i premiers distincts et les α_i dans $\mathbb{N}^*$.*

1. *on a un isomorphisme d'anneaux :*

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \prod_{i=1}^{r} \frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}$$

2. *On a un isomorphisme de groupes :*

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \simeq \prod_{i=1}^{r} \left(\frac{\mathbb{Z}}{p_i^{\alpha_i}\mathbb{Z}}\right)^*$$

3. on a

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

Lemme 1 *Si p est un nombre premier on a un isomorphisme*

$$\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \simeq \frac{\mathbb{Z}}{(p-1)\mathbb{Z}}$$

Proposition 5 *Si p est un nombre premier ≥ 3 et α un entier ≥ 2 on a :*

$$\left(\frac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^* \simeq \frac{\mathbb{Z}}{\varphi(p^\alpha)\mathbb{Z}} \simeq \frac{\mathbb{Z}}{p^{\alpha-1}(p-1)\mathbb{Z}}$$

Proposition 6 *On a $(\frac{\mathbb{Z}}{2\mathbb{Z}})^* = \{1\}$, $(\frac{\mathbb{Z}}{4\mathbb{Z}})^* = \{1, -1\} \simeq \frac{\mathbb{Z}}{2^\alpha\mathbb{Z}}$ Pour $\alpha \geq 3$ on a $(\frac{\mathbb{Z}}{2^\alpha\mathbb{Z}})^* \simeq \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^{\alpha-2}\mathbb{Z}}$*

Application 2 (Premier développement) *Détermination des groupes d'ordre pq avec $p < q$ premiers.*

Exemple 1 *Si $p = 2$ il y a deux groupes d'ordre $2q$ non isomorphes qui sont : $\frac{\mathbb{Z}}{2q\mathbb{Z}}$ et le groupe diédral D_q*

2 Arithmétique

Definition 2 *Deux entiers $x \in \mathbb{Z}$ et $y \in \mathbb{Z}$ sont dits congrus modulo n si il existe k appartenant à $\mathbb{Z}$ tel que $y = x + kn$. Cette relation notée $x \equiv y \pmod{n}$ est la relation d'équivalence associée à l'idéal $n\mathbb{Z}$.*

Definition 3 *On note $\overline{x}$ la classe d'un entier x dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Ainsi $\frac{\mathbb{Z}}{n\mathbb{Z}} = \{\overline{0}, \ldots, \overline{n-1}\}$.*

Théorème 2 (Fermat) *Soit $p \geq 2$ un nombre premier, alors $\forall a \in \mathbb{Z}$ $a^p \equiv a \pmod{p}$ et $\forall a \in \mathbb{Z}$ $a^{p-1} \equiv 1 \pmod{p}$ si p ne divise pas a.*

Théorème 3 (Wilson) *Un entier $p \geq 2$ est un nombre premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$.*

Proposition 7 (Euler-Fermat) *Soit $n \geq 2$ entier, pour tout $k \in \mathbb{Z}$, premier avec n, on a $k^{\varphi(n)} \equiv 1 \pmod{n}$.*

Application 3 (du théorème chinois) *Le système*

$$\begin{cases} x \equiv 2 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{9} \end{cases}$$

a pour solution $\{x = 118 + K180$ où $K \in \mathbb{Z}\}$

Application 4 (Les carrés de F_q)

Notations :

- F_q *est le corps à* q *éléments*[1]
- $F_q^2 = \{x \in F_q \exists y \in F_q, x = y^2\}$
- $F_q^{\star 2} = F_q^2 \cap F_q^\star$

Proposition 8 *On suppose* $p > 2$. *Alors on a :*

$$x \in F_q^{\star 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$$

Corollaire 1 *Soit* p *un nombre premier,* $p > 2$ *et posons* $q = p^n$, $n \in \mathbb{N}^*$. *Alors,* -1 *est un carré dans* F_q *si et seulement si* q *est congru à* 1 *modulo* 4.

Application : $\mathbb{Z}[i]$ *et le théorème des deux carrés*

3 Applications

3.1 Décomposition cyclique d'un groupe abélien

Proposition 9 *Soit* G *un groupe abélien fini d'ordre* $n \geq 2$, *il existe des entiers* $q_1 \geq 2$, q_2 *multiple de* q_1, $\ldots$, q_k *multiple de* q_{k-1}, *uniques, tels que* G *soit isomorphe à* $(\frac{\mathbb{Z}}{q_1\mathbb{Z}}) \times \cdots \times (\frac{\mathbb{Z}}{q_k\mathbb{Z}})$.

La suite $q_1, \ldots, q_k$ *est appelée les invariants de* G

Application 5 *On peut déterminer à isomorphisme près les structures possibles pour un groupe abélien d'ordre* 600.

3.2 Irréductibilité des polynômes

Théorème 4 (réduction) *Soient* A *un anneau factoriel et* $K = Frac(A)$. *Soit* I *un idéal premier de* A *et* $B = \frac{A}{I}$ *qui est un anneau intègre de corps de fractions* L. *Soit* $P(X) = a_n X^n + \cdots + a_0$ *un polynôme de* $A[X]$ *et* $\overline{P}$ *sa réduction modulo* I. *On suppose* $\overline{a_n} \neq 0$ *dans* B.
Alors, si $\overline{P}$ *est irréductible sur* B *ou sur* L, *le polynôme* P *est irréductible sur* K.

Application 6 *Le polynôme* $X^3 + 462X^2 + 2433X - 67691$ *est irréductible sur* $\mathbb{Z}$ *car* $X^3 + X + 1$ *est irréductible sur* $\frac{\mathbb{Z}}{2\mathbb{Z}}$.

3.3 Polynômes cyclotomiques

Definition 4 $\forall n \in \mathbb{N}$, *on note* $\mathbb{U}_n = \{e^{\frac{2ik\pi}{n}} / k \in \mathbb{Z}\} \subset \mathbb{C}$. *On dit qu'un élément* $x \in \mathbb{U}_n$ *est une racine primitive* n*-ième de l'unité si* x *engendre le groupe* $(\mathbb{U}_n, \times)$.

Definition 5 *On note* Π_n *l'ensemble des racines primitives* n*-ième de l'unité.*

Definition 6 *On définit le polynôme cyclotomique d'indice* n *par* $\phi_n(X) = \prod_{\xi \in \Pi_n}(x - \xi)$.

1. Le nombre q est toujours une puissance d'un nombre premier p

Théorème 5 (deuxiÃ¨me dÃ©veloppement) *$\phi_n(X)$ est irréductible sur $\mathbb{Z}$.*

Corollaire 2 *Si ξ est une racine primitive n-ième de l'unité dans un corps de caractéristique nulle alors son polynôme minimal sur $\mathbb{Q}$ est ϕ_n et on a*

$$[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$$

3.4 Equations diophantiennes

Definition 7
On appelle équation diophantienne une équation $\rho(X, Y, Z) = 0$ où les inconnues X, Y, Z sont des entiers et où ρ est un polynôme de plusieurs variables, à coefficients entiers.

Exemple 2

- *Triplet pythagoricien : $x^2 + y^2 = z^2$*
- *Fermat : $x^4 + y^4 = z^4$*
- *Identité de Bezout : $ax + by = c$ avec $(a, b, c) \in \mathbb{Z}^3$*

Parmi ces 3 exemples seul Fermat n'a pas de solution non trivial.