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

Rombaldi
Dreveton, Lhabouz
Ulmer (dev 2)

Dans toute cette leçon, on considère $n \geq 2$.

Définition 0.1 On définit $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence pour la relation $a \sim b \iff n$ divise $b-a$.

Théorème 0.2 On a $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$. Cet ensemble est de cardinal n et est en bijection avec les restes possibles dans la division euclidienne par n.

Théorème 0.3 Il existe une unique structure d'anneau commutatif unitaire sur $\mathbb{Z}/n\mathbb{Z}$ telle que π_n, la surjection canonique, soit un morphisme d'anneaux.

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

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

Proposition 1.1 Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique. De plus, tout groupe cyclique à n éléments est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Exemples 1.2
- $(\{-1, 1\}, \cdot) \simeq (\mathbb{Z}/2\mathbb{Z}, +)$
- $\{\mathrm{id}, (1\,2\,3), (1\,3\,2)\} \simeq (\mathbb{Z}/3\mathbb{Z}, +)$

Théorème 1.3 Tous les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre qui divise n. Réciproquement, pour tout diviseur d de n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, il s'agit de $\langle \bar{q} \rangle$ où $q = \frac{n}{d}$.

Proposition 1.4 Pour tout diviseur d de n, le sous-groupe d'ordre d est l'ensemble des éléments de $\mathbb{Z}/n\mathbb{Z}$ dont l'ordre divise d et les générateurs de ce sous-groupe sont les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$.

2. Le groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$

Théorème 1.5 Soit $a \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :
- $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$
- a est premier avec n
- $\bar{a}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$

Définition 1.6 On appelle fonction indicatrice d'Euler la fonction $\varphi : n \in \mathbb{N} \longmapsto \#\{m \in [\![1, n-1]\!] \mid m \wedge n = 1\}$

Exemple 1.7
Soit p un nombre premier alors $\varphi(p) = p-1$

Remarque 1.8 D'après le théorème précédent, $\varphi(n)$ est le nombre de générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ et le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$.

Conséquence 1.9 Pour tout $a \in \mathbb{Z}$ tel que $a \wedge n = 1$, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Corollaire 1.10 (Fermat) Soient p un nombre premier et $a \in \mathbb{Z}$. Alors, si $a \wedge p = 1$ on a $a^{p-1} \equiv 1 \pmod{p}$, et quelque soit a, $a^p \equiv a \pmod{p}$.

Proposition 1.11 On note $\mathcal{D}_n$ l'ensemble des diviseurs positifs de n alors $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

Proposition 1.12 On a : $((\mathbb{Z}/n\mathbb{Z})^*, \cdot) \simeq (\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ)$.

3. Structure des groupes abéliens finis

Lemme 1.13 Soit H un sous-groupe de G abélien fini. Tout caractère χ de $\hat{H}$ se prolonge en un caractère de $\hat{G}$.

Proposition 1.14 (structure des groupes abéliens finis) Soit G un groupe abélien fini non trivial. Il existe alors $r \geq 1$ et $n_1, \dots, n_r \geq 2$ vérifiant $n_i \mid n_{i+1}$, tels que $G \simeq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}$. De plus, il y a unicité des entiers r et $n_1, \dots, n_r$.

II. $\mathbb{Z}/n\mathbb{Z}$ en tant qu'anneau

1. Propriétés

Proposition 2.1 L'anneau $\mathbb{Z}/n\mathbb{Z}$ possède un stathme.

Remarque 2.2 Toutefois, $\mathbb{Z}/n\mathbb{Z}$ n'est pas nécessairement euclidien car il n'est pas forcément intègre.

Exemple 2.3
dans $\mathbb{Z}/6\mathbb{Z}$, $\bar{2}.\bar{3} = \bar{0}$ mais $\bar{2} \neq \bar{0}$ et $\bar{3} \neq \bar{0}$

Théorème 2.4 (chinois) Soient $(n_j)_{1\leq j\leq r}$ une famille de $r \geq 2$ entiers naturels distincts de 0 et de 1, et $n = \prod_{j=1}^{r} n_j$. Les entiers n_j sont premiers entre eux deux à deux si et seulement si $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$. Le cas échéant, l'application $\varphi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_r\mathbb{Z}$, $\pi_n(k) \longmapsto (\pi_1(k), \dots, \pi_r(k))$ est un isomorphisme d'anneaux d'inverse $\varphi^{-1} : (\pi_{j}(k))_j \longmapsto \pi_n\left(\sum_{i=1}^{r} a_i u_i \frac{n}{n_i}\right)$ où $(u_j)_j$ vérifie $\sum_{i=1}^{r} u_i \frac{n}{n_i} = 1$.

développement 1

Application 2.5
Une armée compte environ 800 soldats.
On demande aux soldats de se ranger par tas de 9 puis 10 puis 11. Il y a un reste de 6 puis 9 puis 8.
Alors l'armée compte 789 soldats.

Application 2.6 Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ alors $\varphi(n) = \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

Corollaire 2.7 Si $n_1, \dots, n_r$ sont premiers entre eux deux à deux, on a alors l'isomorphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^* \simeq (\mathbb{Z}/n_1\mathbb{Z})^* \times \dots \times (\mathbb{Z}/n_r\mathbb{Z})^*$.

2. Cas où n est premier

Proposition 2.8 Un nombre p est premier si et seulement si $\varphi(p) = p - 1$.

Théorème 2.9 L'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier. De plus, le cas échéant, $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Proposition 2.10 Soit $\mathbb{K}$ un corps de caractéristique p. Notons ϕ le morphisme de Frobenius alors $\phi(x) = x$ si et seulement si $x \in \mathbb{Z}/p\mathbb{Z}$.

III. Applications

1. Équations diophantiennes

Remarque 3.1 On part d'une équation diophantienne dont on suppose qu'il existe une solution. On peut utiliser la réduction modulo n (pour un n bien choisi) pour aboutir à une contradiction.

Exemples 3.2
- $x^3 + 5 = 117y^3$ n'a pas de solutions entières (réduction modulo 9)
- $x^3 + y^3 + z^3 = 4$ ou 5 n'a pas de solutions entières (réduction modulo 9)

Lemme 3.3 L'anneau des entiers de Gauss $\mathbb{Z}[i]$ est euclidien.

Proposition 3.4 Un nombre premier p est somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1\ [4]$.

développement 2

2. Polynômes

Théorème 3.5 (Critère d'Eisenstein) Soit $P = a_n X^n + \dots + a_1 X + a_0 \in \mathbb{Z}[X]$ et soit p un nombre premier. On suppose que :
- $p \nmid a_n$
- $\forall k \in [\![0, n-1]\!]$, $p \mid a_k$
- $p \nmid a_0^2$

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

Application 3.6 Les polynômes cyclotomiques $\Phi_{p^n}(X) = \Phi_p(X^{p^{n-1}})$ sont irréductibles dans $\mathbb{Q}[X]$.