~~Anneau~~ $\mathbb{Z}/n\mathbb{Z}$ : Applications :

DVPT : Dirichlet faible
(Structure des groupes abéliens finis)

## I - Structure d'anneau et de groupe :

**Prop 1** - Les sous groupes de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ $n \in \mathbb{N}$ et sont tous distingués dans $\mathbb{Z}$

**Déf/prop 2** Soit $n \in \mathbb{N}$ : le quotient de $\mathbb{Z}$ par $n\mathbb{Z}$ est un groupe, noté $\mathbb{Z}/n\mathbb{Z}$ :

**Prop 3** $\forall n \in \mathbb{N}^*$ $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

est un groupe cyclique à $n$ éléments.

**Prop 4** Tout groupe cyclique d'ordre $n$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

**Ex 5** Un le groupe des racines $n$-ièmes de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$

**Prop 6** Pour $n \geq 2$ : tous les sous groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre d qui divisent $n$ ! Réciproquement, $\forall$ d diviseur de $n$, $\exists!$ sous groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d. C'est le groupe cyclique $\langle \overline{\frac{n}{d}} \rangle$

**Ex 7** $\mathbb{Z}/6\mathbb{Z}$ a 4 sous groupes :
$\langle \bar{1} \rangle = \mathbb{Z}/6\mathbb{Z}$ $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\} \simeq \mathbb{Z}/3\mathbb{Z}$
$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\} \simeq \mathbb{Z}/2\mathbb{Z}$ et $\langle \bar{6} \rangle = \{\bar{0}\}$

**Prop 8** Pour $n \geq 2$, il existe une unique structure d'anneau commutatif unitaire sur $\mathbb{Z}/n\mathbb{Z}$ telle que la surjection canonique $\pi_n$ soit un morphisme d'anneau.

**Remarque** : la loi $\cdot$ est définie par $\bar{a} \cdot \bar{b} = \overline{ab}$ $\forall (\bar{a}, \bar{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

## II - Éléments remarquables, indicatrice d'Euler, automorphismes :

**Prop 10** Soit $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ les propriétés suivantes sont équivalentes :
1) $\bar{a}$ est noté avec $n$
2) $\bar{a}$ est générateur de $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
3) $\bar{a}$ est inversible dans $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$

**Déf 11** Soit $n \in \mathbb{N}^*$, on appelle fonction d'Euler et on note $\varphi(n)$ le cardinal de l'ensemble $\{k \in [\![1, n]\!] \text{ et } k \text{ est premier avec } n\}$.

**Corollaire 12** $\forall n \in \mathbb{N}^*$ $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ où $(\mathbb{Z}/n\mathbb{Z})^\times$ désigne le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

**Exemple 13** pour $p$ un nombre 1er, $\varphi(p) = p-1$ et $\forall \alpha \in \mathbb{N}^*$ on a $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$

**Corollaire 14** $\mathbb{Z}/p\mathbb{Z}$ est un corps $\Leftrightarrow$ $p$ est premier

**Prop 15** $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ en particulier, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est un groupe abélien de cardinal $\varphi(n)$.

**Prop 16** Soit $n \geq 2$ et $a \in \mathbb{Z}$ alors $\bar{a}$ est un diviseur de $0 \Leftrightarrow a \wedge n \neq 1$ et $a$ et $n$ ne sont pas premiers entre eux.

Cx17 : dans $\mathbb{Z}/4\mathbb{Z}$ : $\bar{2}$ est un diviseur de 0 car $4 \mid 2$ et 2 et 4 ne sont pas premiers entre eux.

## III - Application de la structure de groupe :

**Thm 18** Soit $G$ un groupe abélien fini d'ordre $n \geq 2$. Il existe une unique suite d'entiers $q_1, \dots q_k$ tels que $q_1 \mid q_2 \mid q_3 \cdots \mid q_k$ et $G \simeq \mathbb{Z}/q_1\mathbb{Z} \times \cdots \times \mathbb{Z}/q_k\mathbb{Z}$

**Application 19** : Soit $G$ un $p$-groupe d'ordre $p^2$ : alors $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ (groupe cyclique)

## IV - Applications à l'arithmétique

### a) Théorème chinois et applications

**Thm 20** Soit $n, m \in \mathbb{N}^*$. Alors $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \iff n$ et $m$ sont premiers entre eux.

Ex 21 : $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \simeq \mathbb{Z}/35\mathbb{Z}$ mais $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique

**Thm 21** Soit $m_1, \dots m_r \geq 1$ des entiers premiers entre eux 2 à 2. Alors (équivalence des Bombalai) $\mathbb{Z}/m_1 \cdots m_r\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \mathbb{Z}/m_r\mathbb{Z}$

**Corollaire 22** Soit $n \geq 2$ $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ sa décomposition en facteurs premiers. Alors $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$

Ex 23 : $\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

Appli 24 : sous les mêmes hypothèses que le corollaire 22 : $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{k} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$ et donc $\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}) = n \prod_{i=1}^{k} (1 - 1/p_i)$

Appli 25 Le système de congruence :
$x \equiv 1\ [3]$
$x \equiv 2\ [4]$
$x \equiv -1\ [7]$
admet des solutions. Elles sont données par $x \equiv 34\ [84]$

### b) Tests de primalité :

**Thm 26 (Fermat)** Soit $p \geq 2$ un nombre ier : alors $\forall a \in \mathbb{Z}$ : $a^p \equiv a \mod p$ et si $p \nmid a$ $a^{p-1} \equiv 1\ [p]$

**Thm 27 (Wilson)** Soit $p \geq 2$. $p$ est premier $\iff (p-1)! \equiv -1 \mod p$.

**Thm 28 : (RSA)** Soit $p$ et $q$ distincts et $n = pq$ et $c, d$ deux entiers tels que $cd \equiv 1\ [\varphi(n)]$ Alors $\forall t \in \mathbb{Z}$ : $t^{cd} \equiv t \mod n$.

Appli 29 : le couple $(n, c)$ est rendu public et on peut encoder un message $t \in \mathbb{Z}/n\mathbb{Z}$ en renvoyant $t^c$. Pour décoder le message, il faut ensuite le mettre à la puissance $d$ donc seuls ceux qui connaissent $d$ peuvent décoder le message.

**Thm 30** : Soit $n \geq 2$ tel que $\forall a \in \mathbb{Z}$ $a^{n-1} \equiv 1 \mod n$ et $\forall q \mid n-1$ $a^{(n-1)/q} \not\equiv 1\ [n]$ alors $n$ est ier.

## V - Application à l'irréductibilité de polynômes sur $\mathbb{Z}$ et $\mathbb{Q}$

**Def 31** Soit $P \in \mathbb{Z}[X]$ ou $P \in \mathbb{Q}[X]$, $P(X) = a_0 + \cdots + a_n X^n$. On appelle contenu de $P$ et on note $c(P) = \text{pgcd}(a_0, \cdots a_n)$

**Lemme 32** : le produit de 2 polynômes primitifs (ie de contenu $\pm 1$) est primitif

**Prop 33** $\forall P, Q$ $c(PQ) = c(P)c(Q)$

**Prop 34** Les polynômes irréductibles de $\mathbb{Z}[X]$ sont :
- les irréductibles de $\mathbb{Z}$
- les polynômes primitifs de degré $\geq 1$, irréductibles sur $\mathbb{Q}$

Ex 35 $P(X) = 2X + 4$ n'est pas irréductible sur $\mathbb{Z}$.

**Prop 36** Soit $p$ un entier premier et $P \in \mathbb{Z}[X]$ de contenu 1, de coefficient dominant non divisible par $p$. Alors si $\bar{P} \in \mathbb{Z}/p\mathbb{Z}[X]$ est irréductible, $P$ est irréductible sur $\mathbb{Z}$.

Ex 37 $X^3 + 4X^2 + 2X + 33$ $X - 67691$ est irréductible sur $\mathbb{Z}$ (en réduisant mod 2)

**Thm 38** Soit $P \in \mathbb{Z}[X]$ $P(X) = a_n X^n + \dots + a_0$ et $p$ premier on suppose :
- $p \nmid a_n$
- $p \mid a_i \quad \forall i \in [\![0, n-1]\!]$
- $p^2 \nmid a_0$

Alors $P$ irréductible sur $\mathbb{Q}$

**Ex 39.** $P(X) = 5X^4 + 6X + 2$ est irréductible sur $\mathbb{Q}$

**Def 40** Soit $\Phi_n = \prod_{\substack{k \in [\![1,n]\!] \\ pgcd(k,n)=1}} (X - e^{\frac{2ik\pi}{n}})$ le $n$-ième polynome cyclotomique, défini $\forall n \geq 2$. et $\Phi_1 = X - 1$

**Prop 41.** $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$

**Prop 42.** $\forall n \in \mathbb{N}^* : \Phi_n \in \mathbb{Z}[X]$

**Lemme 43** Soit $a \in \mathbb{Z}$ et $p$ ner tel que $p \mid \Phi_n(a)$ et tel que $p \nmid \Phi_d(a)$ $\forall d$ diviseur strict de $n$. Alors $p \equiv 1 \bmod n$

**Thm 44 (Dirichlet faible)** pour $n \geq 1$, $\exists$ une infinité de nombres ners de la forme $kn+1$ avec $k$ entier