120

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

I) Les groupes $(\mathbb{Z}/n\mathbb{Z},+)$

A] Construction de $(\mathbb{Z}/n\mathbb{Z},+)$

Soient $n\in\mathbb{N}$ et $n\mathbb{Z}=\{nq \mid q\in\mathbb{Z}\}$.

Prop 1: Les groupes $n\mathbb{Z}$ sont les seuls sous-groupes (et idéaux) de $\mathbb{Z}$.

Def 2: $a,b\in\mathbb{Z}$ sont dits congrus modulo n si $(a-b)\in n\mathbb{Z}$. On note $a\equiv b\,[n]$.

[1]

Prop 3: Ceci définit une relation d'équivalence sur $\mathbb{Z}$. On note $\mathbb{Z}/n\mathbb{Z}$ le quotient.

Prop-def 4: Soit $n\in\mathbb{N}^*$. On définit sur $\mathbb{Z}/n\mathbb{Z}$: $\bar a+\bar b=\overline{a+b}$. Alors $\mathbb{Z}/n\mathbb{Z}$ est un groupe abélien d'ordre n muni de cette loi.

Rem 5: $\{\bar 0;\bar 1;\dots;\overline{n-1}\}$ forme une classe de représentants de $(\mathbb{Z}/n\mathbb{Z},+)$

B] Groupes cycliques et sous-groupes

Def 6: Un groupe G est cyclique si il est fini et engendré par un élément.

Prop 7: Les groupes $(\mathbb{Z}/n\mathbb{Z},+)$ sont les seuls groupes cycliques à isomorphisme près.

Ex 8: Si $\mathbb{U}_n=\{z\in\mathbb{C}\mid z^n=1\}$ alors $\mathbb{U}_n\simeq\mathbb{Z}/n\mathbb{Z}$.

[1]

Prop 9: Les sous-groupes $(\mathbb{Z}/n\mathbb{Z},+)$ sont cycliques d'ordre divisant n. Réciproquement, si $d\mid n$, il existe un unique sous-groupe d'ordre d de $(\mathbb{Z}/n\mathbb{Z},+)$.

Prop 10: Pour tout $k\in\mathbb{Z}$, l'ordre de $\bar k$ dans $(\mathbb{Z}/n\mathbb{Z},+)$ est $\frac{n}{n\wedge k}$

Cor 11: $\bar k$ engendre $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $n\wedge k=1$.

Def 12: On définit l'indicatrice d'Euler $\varphi(n)$ comme le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z},+)$. [1]

Cor 13: $\forall n\in\mathbb{N}^*$, $n=\sum_{d\mid n}\varphi(d)$

Prop 14: Soient $p\in\mathbb{N}^*$ premier et $\alpha\in\mathbb{N}^*$. Alors $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

C] Structure des groupes abéliens finis

Soit G un groupe abélien fini. Si $x\in G$, $o(x)$ désignera son ordre.

Lem 15: Soit $a\in G$ d'ordre maximal dans G. Alors $\forall y\in G/\langle a\rangle$, $\exists x\in G \mid \bar x=y$ et $o(x)=o(y)$.

Thm 16: Il existe des entiers $q_1\mid q_2\mid\dots\mid q_k\in\mathbb{N}^*$ uniques tels que $G\simeq\prod_{i=1}^{k}\mathbb{Z}/q_i\mathbb{Z}$. Ce sont les facteurs invariants de G. [2]

Ex 17: $\mathbb{Z}/60\mathbb{Z}\times\mathbb{Z}/72\mathbb{Z}\simeq\mathbb{Z}/12\mathbb{Z}\times\mathbb{Z}/360\mathbb{Z}$.

App 18: Il existe $a\in G$ d'ordre le ppcm des ordres des éléments de G.

App 19: Soit $|G|=\prod_{i=1}^{k}p_i^{\alpha_i}$ sa décomposition en facteurs premiers. Pour tout $d\mid |G|$, il existe un sous-groupe de G d'ordre d. En particulier, pour $i\in[\![1;k]\!]$, il existe $H_i\leq G$ d'ordre $p_i^{\alpha_i}$ qui est en plus unique et $G\simeq\prod_{i=1}^{k}H_i$. Ce sont les composantes primaires de G.

II) Les anneaux $(\mathbb{Z}/n\mathbb{Z},+,\times)$

A] Construction et inversibles

Prop-def 20: On définit sur $\mathbb{Z}/n\mathbb{Z}$: $\bar x\times\bar y=\overline{xy}$. Alors [1]

[1] $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.

Prop 21: Soit $a \in \mathbb{Z}$. $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$.

Cor 22: $\forall n \in \mathbb{N}^*$, $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

Cor 23: $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier. On le note alors $\mathbb{F}_n$.

App 24: (Théorème de Wilson) $n \in \mathbb{N}^*$ est premier si et seulement si $(n-1)! \equiv -1 [n]$.

Thm 25: (d'Euler) $\forall a \in \mathbb{Z}$, $a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 [n]$

App 26: Si $p \in \mathbb{N}^*$ est premier, $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

B] Théorème d'isomorphisme chinois

[4] **Thm 27**: Soient $n_1, \dots, n_r$ 2 à 2 premiers entre eux, et $n = \prod_{i=1}^{r} n_i$. Alors
$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \\ x & \longmapsto & (x \bmod n_i\mathbb{Z})_{1 \le i \le r} \end{array}$$
est un isomorphisme.

Rem 28: Si on connait $u_1, \dots, u_r \in \mathbb{Z}$ tels que $\sum_{i=1}^{r} u_i \frac{n}{n_i} = 1$ (qu'on peut trouver avec l'algorithme d'Euclide) on peut donner sa bijection réciproque ψ.

App 29: L'unique solution du système d'équation $x \equiv a_i [n_i]$ $\forall i \in [\![1, r]\!]$, $a_i \in \mathbb{Z}$, modulo n est $\psi(x)$

Ex 30: L'ensemble des solutions de $\begin{cases} x \equiv 2 [4] \\ x \equiv 3 [5] \end{cases}$ est $\{18 + 20j \mid j \in \mathbb{Z}\}$.

Cor 31: Avec les mêmes notations que Thm 27:
$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^{r} (\mathbb{Z}/n_i\mathbb{Z})^\times$

App 32: $\forall n, m \in \mathbb{N}^*$, $n \wedge m = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m)$

Rem 33: Couplé avec Prop 14, ceci permet de déterminer entièrement φ.

C] Étude des carrés dans $\mathbb{F}_p$

Soit $p \in \mathbb{N}^*$ premier.

[1] **Def 34**: On note $\mathbb{F}_p^2 = \{x^2 \mid x \in \mathbb{F}_p\}$ l'ensemble des carrés de $\mathbb{F}_p$ et $\mathbb{F}_p^{*2} = \mathbb{F}_p^2 \cap \mathbb{F}_p^*$.

Prop 35: Si $p = 2$, $\mathbb{F}_p^2 = \mathbb{F}_p$. Si $p > 2$, on a $|\mathbb{F}_p^2| = \frac{p+1}{2}$ et $|\mathbb{F}_p^{*2}| = \frac{p-1}{2}$.

On considère $p > 2$.

Thm 36: $\forall x \in \mathbb{F}_p^*$, $x \in \mathbb{F}_p^{*2} \Leftrightarrow x^{\frac{p-1}{2}} = 1$.

Cor 37: $(-1) \in \mathbb{F}_p \Leftrightarrow p \equiv 1 [4]$

App 38: Il existe une infinité de nombres premiers de la forme $4n+1$, $n \in \mathbb{N}^*$.

Def 39: Soit $x \in \mathbb{Z}$. On définit son symbole de Legendre modulo p par: $\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \in \mathbb{F}_p^{*2} \\ 0 \text{ si } x = 0 \\ -1 \text{ si } x \notin \mathbb{F}_p^2 \end{cases}$

Prop 40: $\forall x \in \mathbb{F}_p$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$. En particulier, $x \in \mathbb{F}_p^* \longmapsto \left(\frac{x}{p}\right) \in \{\pm 1\}$ est un morphisme de groupes.

Soit $q > 2$ premier, $q \neq p$.

Lem 41: [DEV 1] Soit $a \in \mathbb{F}_p^*$. L'équation $ax^2 = 1$ admet $1 + \left(\frac{a}{p}\right)$ solutions dans $\mathbb{F}_p$.

Thm 42: (loi de réciprocité quadratique) On a
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

App 43: Ceci permet de calculer certains symboles de Legendre.

[2] **Thm 44**: (des deux carrés) Soit $p \in \mathbb{N}^*$ premier. p est somme de deux carrés si et seulement si $p = 2$ ou $p \equiv 1 [4]$.

Rem 45: Ce théorème permet de décrire les sommes de deux carrés dans $\mathbb{N}$ via la décomposition en facteurs premiers.

III) Polynômes irréductibles

A] Polynômes sur $\mathbb{F}_p[X]$

On note $U_n(p)$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_p[X]$ et $I_n(p)$ son cardinal.

[1]

Prop 46 : Pour tout $P \in U_n(p)$, $\frac{\mathbb{F}_p[X]}{(P)}$ est un corps de cardinal p^n. On le note $\mathbb{F}_{p^n}$.

Nous allons montrer réciproquement que tout corps s'obtient ainsi.

Lem 47 : Tout diviseur irréductible divisant $X^{p^n}-X$ est de degré divisant n. Réciproquement, $\forall d \mid n$, $\forall P \in U_d(p)$, $P \mid (X^{p^n}-X)$.

Thm 48 : Dans $\mathbb{F}_p[X]$: $X^{p^n}-X = \prod_{d \mid n} \prod_{P \in U_d(p)} P$

Cor 49 : $n I_n(p) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$ où μ est la fonction de Möbius.

App 50 : $\forall n \in \mathbb{N}^*$, $U_n(p) \neq \emptyset$.

App 51 : Tout corps fini est isomorphe à un corps de la même forme que dans Prop 46.

B] Polynômes cyclotomiques

[1]

Def 52 : $\xi \in \mathbb{U}_n$ est dite primitive si $\mathbb{U}_n = \langle \xi \rangle$.

Ex 53 : $e^{\frac{2i\pi}{n}}$ est primitive dans $\mathbb{U}_n$.

On note $\mathbb{U}_n^*$ l'ensemble des racines primitives.

Def 54 : On définit le n-ème polynôme cyclotomique par $\Phi_n(X) = \sum_{\xi \in \mathbb{U}_n^*} (X-\xi)$.

Lem 55 : (DEV2) $\forall n \in \mathbb{N}^*$, $X^n-1 = \prod_{d \mid n} \Phi_d(X)$ et $\Phi_n \in \mathbb{Z}[X]$

App 50 : (Théorème de progression arithmétique faible de Dirichlet) Il existe une infinité de nombres premiers congrus à 1 modulo n.

C] Critère d'irréductibilité sur $\mathbb{Q}[X]$

[2]

Thm 57 : (Critère d'Eisenstein) Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. Si il existe $p \in \mathbb{N}^*$ premier tel que $p \mid a_k$ $\forall k \in [\![0;n-1]\!]$, $p \nmid a_n$ et $p^2 \nmid a_0$, alors P est irréductible sur $\mathbb{Q}[X]$.

App 58 : X^n-2 est irréductible sur $\mathbb{Q}[X]$ $\forall n \in \mathbb{N}^*$.

App 59 : Si $p \in \mathbb{N}^*$ est premier, Φ_p est irréductible sur $\mathbb{Z}[X]$.

Thm 60 : (de réduction) Avec les mêmes notations, si $\overline{P} \in \mathbb{F}_p[X]$ est l'image de P, que $cd(P) \not\equiv 0\ [p]$ et que $\overline{P}$ est irréductible sur $\mathbb{F}_p[X]$, alors P l'est aussi sur $\mathbb{Q}[X]$.

App 61 : $X^3+462X^2+2433X-67691$ est irréductible sur $\mathbb{Z}[X]$.

Références:

- Algèbre et géométrie, Rambaldi [1]
- Cours d'algèbre, Perrin [2]
- Algèbre, Gourdon [3] (pas utilisé)
- Algèbre et géométrie, Combes [4]