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

Références : Gourdon Algèbre, Rombaldi, Perrin.

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

1.1 Structure de groupe cyclique

Définition 1. Les sous-groupes de $(\mathbb{Z},+)$ sont de la forme $n\mathbb{Z}$, $n \in \mathbb{N}^*$

Définition 2. On définit la congruence modulo n : Pour a,b dans $\mathbb{Z}$, $a \equiv b \ mod\ n$ ssi il existe k dans $\mathbb{Z}$ tel que $a = b + kn$ ssi $(b-a) \in n\mathbb{Z}$. C'est une relation d'équivalence sur $\mathbb{Z}$

Définition 3. On note $\mathbb{Z}/n\mathbb{Z}$ le quotient de $\mathbb{Z}$ par $n\mathbb{Z}$

Exemple 4. Cas triviaux pour n=0 et n=1

Proposition 5. *(Z/nZ,+) est un groupe cyclique à n éléments. Tout groupe cyclique d'ordre n lui est isomorphe. (Un groupe cyclique non-fini est isomorphe à Z).*

Proposition 6. *$\bar{k}$ est générateur dans (Z/nZ,+)* $\iff$ *$pgcd(k,n) = 1$*

Proposition 7. *On définit la fonction indicatrice d'Euler φ. Le nombre de générateur de (Z/nZ,+) est $\varphi(n)$.*

Proposition 8. *Si p est premier, on à $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$*

1.2 Sous-groupes de (Z/nZ,+)

Théorème 9.
- *Tout les sous-groupes de Sous-groupes de (Z/nZ,+) sont cycliques d'ordre d qui divise n.*
- *Réciproquement, si d est un diviseur de n, alors il existe un unique sous-groupe H d'ordre d de (Z/nZ,+) et on à son expression : $H =< \bar{q} >= \{\bar{x} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{x}^d = 1\}$ avec $q = \frac{n}{d}$. Les générateurs de H sont les $\{\bar{x} \in \mathbb{Z}/n\mathbb{Z} \mid o(\bar{x}) = d\}$*

Corollaire 10. *On note D_n l'ensemble des diviseurs positifs de n. On a $n = \sum_{d \in D_n} \varphi(d)$*

Exemple 11. $\mathbb{Z}/20\mathbb{Z}$ admet 4 sous-groupes distincts : $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/10\mathbb{Z}$

1.3 Structure des groupes abéliens finies

Lemme 12. *Tout caractère φ de $H \to \mathbb{C}^*$ avec H un sous-groupe de G se prolonge en un caractère de $H \to \mathbb{C}^*$*

Proposition 13. *Soit G un groupe. Il existe un élément d'ordre maximale dans G, son ordre est exactement le PPMC des éléments de G.*

Théorème 14 (Théorème de structure des groupes abéliens finis). *Il existe une suite d'entiers $(n_i)_i$ finis tel que $n_1|n_2|...|n_r$ $(n_1 > 1)$ et tel que G est isomorphe au produit de groupe cyclique $\prod_{i=1}^{r} \frac{\mathbb{Z}}{n_i\mathbb{Z}}$.*

2 Anneaux (Z/nZ,+,×)

2.1 Anneau et corps (Z/nZ,+,×)

Définition 15. (Z/nZ,+,×) est un anneau, on note $(\mathbb{Z}/n\mathbb{Z})^\times$ le groupe multiplicatif des éléments inversibles de Z/nZ.

Proposition 16. *Soit $n = \Pi_{i=1}^{r} p_i^{\alpha_i}$ sa décomposition en facteurs premiers. $\bar{k}$ est nilpotent dans (Z/nZ,+,×) si et seulement si le produit $p_1...p_r$ divise k.*

Proposition 17. *On a $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ ssi $pgcd(k,n) = 1$.Le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ est donc $\varphi(n)$*

Corollaire 18. *Z/nZ est un corps (à p éléments) ssi n=p premier.*

Application 19. *En arithmétique :*
- *Théorème d'Euler : $k^{\varphi(n)} \equiv 1 \pmod{n}$ si pgcd(k,n)=1.*
- *Théorème de Fermat : $a^p \equiv a[p]$ pour a qcq et p premier, et si pgcd(a,p)=1, on à $a^{p-1} \equiv 1 \pmod{p}$*
- *Théorème de Wilson : p est premier ssi $(p-1)! \equiv -1 \pmod{p}$*

Théorème 20. *Les idéaux de (Z/nZ,+,×) sont les sous-groupes additifs de (Z/nZ,+).*

Théorème 21. *L'application*

$$\begin{aligned} \sigma : \quad & (\mathbb{Z}/n\mathbb{Z})^\times \to Aut((\mathbb{Z}/n\mathbb{Z},+)) \\ & x \mapsto \sigma(x) \end{aligned} \tag{1}$$

est un isomorphisme de $(\mathbb{Z}/n\mathbb{Z})^\times$ *dans Aut((Z/nZ,+)) avec*

$$\sigma(x): \begin{array}{l} (\mathbb{Z}/n\mathbb{Z},+) \to (\mathbb{Z}/n\mathbb{Z},+) \\ y \mapsto xy \end{array} \quad (2)$$

Théorème 22. *Si p est premier,* $(\mathbb{Z}/p\mathbb{Z})^\times$ *est cyclique d'ordre p-1.*

Théorème 23. *Si p est premier impair et si* α *est plus grand que 3, on à* $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ *est cyclique d'ordre* $p^{\alpha-1}(p-1)$.

2.2 Le théorème chinois

Théorème 24 (Théorème chinois). — $(n_1,...n_r)$ *sont premiers entre eux deux à deux, ssi* $\mathbb{Z}/(n1...n_r)\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}$. *On donne l'isomorphisme correspondant et son inverse !.*

Application 25. *Multiplicativité de la fonction indicatrice d'Euler.*

Application 26. *Résolution d'un système d'équation diophantienne grâce à la réciproque de l'application introduite dans le théorème chinois*

Exemple 27. Un exemple simple, on cherche k tel que $k \equiv 2[4]$ et $k \equiv [5]$. L'ensemble solution est $\{18+20j, j \in \mathbb{N}\}$

3 Applications

3.1 Arithmétique et équations diophantiennes

Proposition 28. *Soit* $n = a_d a_{d-1}...a_0$ *son écriture en base 10. On réduit n modulo 2,3,5,7,11 en fonction de son écriture en base 10 =¿* ***Pas de source***

Théorème 29 (Equation diophantienne de degré 2). *On considère l'équation* $ax+by=c$, *avec a,b et c trois entiers relatifs.*
Cette équation admet des solutions $\iff$ $a \wedge b$ *divise c.*
Dans ce cas, l'ensemble des solutions est les couples $(x,y) = (x_0,y_0) + \frac{k}{a \wedge b}(b,-a$ *avec* $k \in \mathbb{Z}$, *avec* (x_0,y_0) *une solution particulière de l'équation (donnée par l'algorithme d'Euclide étendue).*

Exemple 30. — Pour l'équation $3x+2y=5$, l'ensemble des solutions est $(5,-5)+k\times(2,-3)$, pour $k \in \mathbb{Z}$.
— L'équation $12x+8y=5$ n'admet pas de solutions.

Théorème 31. *On s'intéresse à l'équation de congruence* $ax \equiv b \pmod n$, *avec* $n>1$, *a un entier naturel et b un entier relatif.*

- *Si b=1, cette équation à des solutions* $\iff$ $\bar{a}$ *est inversible dans* $\frac{\mathbb{Z}}{n\mathbb{Z}}$ $\iff$ *a est premier avec n.*
  Dans ce cas, l'ensemble des solutions est x_0+kn, *où* x_0 *est une solution particulière de* $ax \equiv 1 \pmod n$
- *Si b est qcq et* $a \wedge n = 1$. *Alors* $u_0 = bx_0$ *est une solution particulière avec* x_0 *solution de* $ax \equiv 1 \pmod n$. *L'ensemble des solutions de* $ax \equiv b \pmod n$ *est alors* $\{u_0+kn | k \in \mathbb{Z}\}$.
- *Le cas général : l'équation* $ax \equiv b \pmod n$ *admet des solutions* $\iff$ $\delta = a \wedge n | b$.
  Dans ce cas, les solutions sont les entiers de la forme : $\frac{b}{\delta}x'_0 + k\frac{n}{\delta}$ *avec* $k \in \mathbb{Z}$ *et* x'_0 *une solution particulière de l'équation* $\frac{a}{\delta}x \equiv \frac{b}{\delta} \pmod{\frac{n}{\delta}}$

Application 32. *Cryptographie RSA*

3.2 Irreductibilité de polynômes dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$

Proposition 33. *Soit p premier.*
- *Soit A et B dans* $\mathbb{Z}[X]$, *alors* $(A+B)^p = \bar{A}^p + \bar{B}^p$ *dans* $\mathbb{F}_p[X]$.
- *Si A est dans* $\mathbb{Z}[X]$ *et* $B = A^p$, *alors on à l'égalité dans* $\mathbb{F}_p[X]$ *:* $\bar{B}(X) = \bar{A}(X^p)$

Définition 34. Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. On appelle contenu de P l'entier c(p)=pgcd$(a_0,...,a_n)$.

Proposition 35. — $c(PQ) = c(P)c(Q)$ *pour deux polynômes de* $\mathbb{Z}[X]$
- *Soit P un polynôme de* $\mathbb{Z}[X]$, *de degré* >1. *P est irreductible dans* $\mathbb{Z}[X]$ *ssi P est de contenu 1 et P est irreductible dans* $\mathbb{Q}[X]$
- *Si P,Q sont deux polynômes unitaires de* $\mathbb{Q}[X]$ *tel que le produit PQ soit dans* $\mathbb{Z}[X]$, *alors P et Q sont dans* $\mathbb{Z}[X]$

Théorème 36 (Critère d'irreductibilité d'Eisenstein). *Soit* $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ *et p un nombre premier. On suppose que* $p|a_i \forall i \in \{0,...,n-1\}$, *p ne divise pas* a_n *et* p^2 *ne divise pas* a_0. *Alors P est un polynôme irreductible de* $\mathbb{Z}[X]$

Application 37. $P(X)=X^n-p$ *est irreductible dans* $\mathbb{Q}[X]$, *pour tout entier naturel n.*

Théorème 38 (Réduction modulo p). *Réduction modulo p. Soit* $P=\sum_{i=0}^{n} a_k X^k$ *non constant dans* $\mathbb{Z}[X]$, *p premier,* $\bar{P} = \sum_{i=0}^{n} \bar{a_k} X^k$. *Si p ne divise pas* a_n *et* $\bar{P}$ *est irreductible dans* $\mathbb{F}_p[X]$, *alors P est irreductible dans* $\mathbb{Q}[X]$

Application 39. *Le polynôme* $X^3 + 462X^2 + 2433X - 67691$ *est irreductible sur* $\mathbb{Z}[X]$ *(et donc sur* $\mathbb{Q}[X]$*.*

3.3 Polynômes cyclotomiques

Définition 40. On définit le nème polynôme cyclotomique Φ_n tout en introduisant les racines nèmes primitives de l'unité. Le degré de Φ_n est $\varphi(n)$

Théorème 41. *On a* $X^n - 1 = \Pi_{d|n}\Phi_d(X)$ *et* $\Phi_n(X)$ *est unitaire dans* $\mathbb{Z}[X]$

Application 42 (Progression arithmétique de Dirichlet)**.** *Soit* a, n *tel que* $a \wedge n = 1$*. Alors il existe une infinité de nombres premiers tel que* $p \equiv a \pmod{n}$

Théorème 43. *Pour tout entier naturel n plus grand que 1,* Φ_n *est irreductible dans* $\mathbb{Q}[X]$*, donc dans* $\mathbb{Q}[X]$

Application 44. *Degré de l'extension cyclotomique. Soit* ω *une racine nème première de l'unité, on a* $[\mathbb{Q}(\omega) : \mathbb{Q}] = \phi(n)$