Leçon 120 : Anneaux Z/nZ. Applications.

Développements :

Automorphismes de $\mathbb{Z}/n\mathbb{Z}$, Théorème des deux carrés (bof)

Bibliographie :

Rombaldi, Beruy, Combes, Perrin, Gozard, Demazure.

Rapport du jury :

Dans cette leçon, l'entier n n'est pas forcément un nombre premier. Il serait bon de connaître les idéaux de $\mathbb{Z}/n\mathbb{Z}$ et, plus généralement, les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. Il est nécessaire de bien maîtriser le lemme chinois et sa réciproque. S'ils le désirent, les candidats peuvent poursuivre en donnant une généralisation du lemme chinois lorsque deux éléments ne sont pas premiers entre eux, ceci en faisant apparaître le pgcd et le ppcm de ces éléments. Il faut bien sûr savoir appliquer le lemme chinois à l'étude du groupe des inversibles, et ainsi, retrouver la multiplicativité de l'indicatrice d'Euler. Toujours dans le cadre du lemme chinois, il est bon de distinguer clairement les propriétés de groupes additifs et d'anneaux, de connaître les automorphismes, les nilpotents et les idempotents. Enfin, il est indispensable de présenter quelques applications arithmétiques des propriétés des anneaux $\mathbb{Z}/n\mathbb{Z}$, telles que l'étude de quelques équations diophantiennes bien choisies. De même, les applications cryptographiques telles que l'algorithme RSA sont naturelles dans cette leçon. S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant au calcul effectif des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$.

1 Le groupe $\mathbb{Z}/n\mathbb{Z}$

1.1 Congruences et $\mathbb{Z}/n\mathbb{Z}$

Remarque 1. *Faire cette partie ou définir directement le groupe quotient ? regarder Minerve 2014*

Definition 2 (Romb p277)**.** *L'ensemble de toutes les classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$.*

Remarque 3. *C'est aussi le quotient de $\mathbb{Z}$ par $n\mathbb{Z}$ (distingué car $\mathbb{Z}$ est abélien.)*

Proposition 4 (Romb p278)**.** *Description de $\mathbb{Z}/n\mathbb{Z}$. Bijection avec les restes de la division euclidienne.*

Definition 5 (Romb p 277)**.** *Surjection canonique. C'est un morphisme d'anneaux.*

Exemple 6. *$\mathbb{Z}/2\mathbb{Z}$: 2 classes, les entiers pairs et impairs.*

1.2 Structure de groupe cyclique

Proposition 7 (Romb p4)**.** *$n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, distingué car $\mathbb{Z}$ est abélien, c'est donc un groupe. (A mettre ? Où ?)*

Proposition 8 (Romb p14)**.** *$\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme surjectif.*

Proposition 9 (Romb p279)**.** *$\mathbb{Z}/n\mathbb{Z}$ est un groupe cyclique d'ordre n.*

Proposition 10 (Romb p279)**.** *Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 11 (Romb p14)**.** *Un groupe monogène est isomorphe à $\mathbb{Z}$ ou à $\mathbb{Z}/n\mathbb{Z}$.*

Exemple 12 (Combes p59)**.** *Le groupe des racines nième de l'unité est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 13 (Romb p279)**.** *Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont cycliques d'ordre divisant n. Réciproquement pour tout diviseur de n, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d.*

Exemple 14. *Le sous-groupe d'ordre 2 de $\mathbb{Z}/4\mathbb{Z}$ est $2\mathbb{Z}/4\mathbb{Z} = \{0, 2\}$.*

Exemple 15 (Combes p62)**.** *Sous groupes de $\mathbb{Z}/20\mathbb{Z}$.*

Proposition 16 (Calais p151)**.** *$\mathbb{Z}/n\mathbb{Z}$ est simple si, et seulement si, n est premier.*

Proposition 17 (Romb p293)**.** *[Combes p71] Il y a exactement $pgcd(n, m)$ morphismes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.*

1.3 Générateurs et indicatrice d'Euler

Proposition 18 (Romb p281)**.** *$\pi(a)$ est un générateur du groupe $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a est premier avec n.*

Proposition 19 (Combes)**.** *Ordre d'un élément dans $\mathbb{Z}/n\mathbb{Z}$.*

Definition 20 (Romb p281)**.** *Fonction indicatrice d'Euler.*

Exemple 21. *$\phi(6)$, $\phi(10)$.*

Proposition 22 (Romb p281)**.** *$\phi(n)$ est le nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 23 (Romb p286)**.** *$\phi(p^\alpha)$.*

Proposition 24 (Romb p282)**.** *$n = \sum \phi(d)$.*

Application 25 (Perrin)**.** *Si K est un corps, tout sous-groupe fini de K^* est cyclique.*

1.4 Théorème de structure des groupes abéliens finis

Proposition 26. *Théorème de structure des groupes abéliens finis.*

Exemple 27 (Combes ?). $\mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z}$ *est isomorphe à* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$.

Application 28 (Combes ?). *A isomorphisme près, il existe* 5 *groupes abéliens d'ordre* 48.

2 L'anneau $\mathbb{Z}/n\mathbb{Z}$

2.1 Structure d'anneau

Proposition 29 (Romb p279). *[Romb p250] Les idéaux de* $\mathbb{Z}$ *sont ses sous-groupes.*

Proposition 30 (Romb). $\mathbb{Z}/n\mathbb{Z}$ *est un anneau + structure de morphisme.*

Proposition 31. *Les idéaux de* $\mathbb{Z}/n\mathbb{Z}$ *sont principaux. Ainsi ; il est principal si et seulement si n est premier si et seulement si n est intègre. (ce sont les* $d\mathbb{Z}/n\mathbb{Z}$ *où* $d|n$ *par le théorème de correspondance des idéaux.*

2.2 Théorème chinois

Proposition 32 (Romb p284). *Théorème chinois.*

Exemple 33. $\mathbb{Z}/4\mathbb{Z}$ *n'est pas isomorphe comme anneau à* $(\mathbb{Z}/2\mathbb{Z})^2$.

Application 34 (Romb p289). *Système d'équations diophantiennes* $k = a_j[n_j]$

Exemple 35 (Romb p289).

Application 36 (Romb p289). $x = a_1[n_1], x = a_2[n_2]$ *avec* n_1 *et* n_2 *non premiers entre eux.*

Proposition 37 (Romb p296). $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *et* $\mathbb{Z}/pgcd(n,m)\mathbb{Z} \times \mathbb{Z}/ppcm(n,m)\mathbb{Z}$ *sont isomorphes.*

2.3 Eléments inversibles et groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$

Remarque 38. *Le théorème chinois est valable pour les inversibles.*

Proposition 39 (Romb p281). $\pi(a) \in (\mathbb{Z}/n\mathbb{Z})^*$ *si et seulement si a est premier avec n si et seulement si* $\pi(a)$ *est un générateur de* $\mathbb{Z}/n\mathbb{Z}$. *Donc* $card((\mathbb{Z}/n\mathbb{Z})^*) = \phi(n)$.

Proposition 40 (Romb p281). *Théorème d'Euler.*

Proposition 41 (Romb p282). *Petit théorème de Fermat.*

Application 42 (Demazuez p66). *Test de primalité de Fermat.*

Application 43. *Nombres de Carmichael.*

Proposition 44 (Romb p280). *[Combes p206]* $Aut(\mathbb{Z}/n\mathbb{Z})$ *est isomorphe à* $(\mathbb{Z}/n\mathbb{Z})^*$ *+ morphismes en exo.*

Proposition 45 (Romb p293). *Expression de* $\phi(n)$, ϕ *est multiplicative.*

Proposition 46 (Romb p293). $(\mathbb{Z}/n\mathbb{Z})^*$ *est cyclique si et seulement si* $n = 2, 4, p^\alpha, 2p^\alpha$.

Proposition 47 (Perrin). *Si p est premier et* $\alpha \geq 3$, $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \sim \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

2.4 Eléments nilpotents et idempotents

Proposition 48 (Beruy p489). *Les éléments nilpotents de* $\mathbb{Z}/n\mathbb{Z}$ *sont les k tels que* $n|k^r$ *pour un* $r \geq 1$. $\mathbb{Z}/n\mathbb{Z}$ *possède des éléments nilpotents non-nuls si et seulement si il existe p premier tel que* $p^2|n$.

Proposition 49 (Combes, Perrin ?, Beruy). *Soit* $n = p_1^{\alpha_1}..p_r^{\alpha_r} \in \mathbb{N}$. $x \in \mathbb{Z}/n\mathbb{Z}$ *est nilpotent si et seulement si* $x \in p_1..p_r\mathbb{Z}$.

Proposition 50. $x \in \mathbb{Z}/n\mathbb{Z}$ *est idempotent si et seulement si, pour tout* $i \in [1, ..r]$, $x = 0[p_i^{\alpha_i}]$ *ou* $x = 1[p_i^{\alpha_i}]$.

Corollaire 51. *Il y a donc exactement* $2r$ *éléments idempotents.*

Exemple 52. *Les idempotents de* $\mathbb{Z}/12\mathbb{Z}$ *sont* $0, 1, 4, 9$.

3 Le corps $\mathbb{Z}/p\mathbb{Z}$

3.1 Propriétés

Proposition 53 (Romb p324). $\mathbb{Z}/n\mathbb{Z}$ *est un corps si et seulement si* $\mathbb{Z}/n\mathbb{Z}$ *est intègre si et seulement si n est premier. On le note alors* F_n.

Remarque 54. *Pour* $s \geq 2$, $\mathbb{Z}/p^s\mathbb{Z}$ *n'est pas un corps, bien qu'il existe des corps à* p^s *éléments.*

Theoreme 55 (Romb p324). *Théorème de Wilson.*

Proposition 56. F_p *est de caractéristique p.*

Application 57 (Perrin). *Tout corps fini K de caractéristique p est un* F_p*-espace vectoriel. Si on note r sa dimension, il est de cardinal* $q = p^r$ *. Le groupe additif de K est alors isomorphe à* $(\mathbb{Z}/p\mathbb{Z})^r$ *, et son groupe multiplicatif à* $\mathbb{Z}/(p^{r-1})\mathbb{Z}$.

Proposition 58. *K est cyclique (pour le théorème de structure).*

Proposition 59. *Irréductibilité des polynômes cyclotomiques. (Ici ?)*

Proposition 60. *Théorème de Sophie Germain.*

Proposition 61. *Théorème de Chevaley Warning et EGZ.*

3.2 Polynômes irréductibles sur F_p

Bof.

3.3 Carrés et sommes de carrés

Remarque 62. *Prendre $q = p$...*

Definition 63 (Perrin p74)**.** *F_q^2, F_q^{*2}.*

Proposition 64 (Perrin p74)**.** *Pour $p = 2$, $F_q^2 = F_q$.*
Sinon, cardinaux.

Proposition 65 (Perrin p75)**.** *$x \in F_q^{*2} si et seulement si x^{(p-1)/2} = 1$.*

Theoreme 66 (Romb p428)**.** *1. Nombre de carrés et de non carrés.*

2. *Les carrés de F_q^* sont les racines de $X^{(q-1)/2} - 1$ et les non carrés sont les racines de $X^{(q-1)/2} + 1$.*

Corollaire 67 (Romb p428)**.** *1. -1 est un carré dans F_q^* si et seulement si q est congru à 1 modulo 4.*

2. *Le produit de deux carrés ou de deux non carrés est un carré. Le produit d'un carré et d'un non carré est un non carré.*
3. *Pour tout $a, b \in F_q^*$ et tout $c \in F_q$, il existe $x, y \in F_q$ tels que $c = ax^2 + by^2$.*

Application 68. *Classification des formes quadratiques.*

Application 69 (Perrin p76)**.** *Il existe une infinité de nombres premiers de la forme $4m + 1$.*

Definition 70 (Romb p429)**.** *[Gozard p155] Symbole de Legendre.*

Proposition 71. *Le symbole de Legendre est une fonction multiplicative.*

Proposition 72. $(\frac{x}{p}) = x^{\frac{p-1}{2}}$.

Exemple 73 (Gozard p155)**.** $(\frac{-1}{p}), (\frac{2}{p})$

Theoreme 74. *Loi de réciprocité quadratique.*

Remarque 75. *La loi de réciprocité quadratique, les symboles pour -1 et 2 et la division euclidienne, permettent de calculer les symboles de Legendre.*

Exemple 76 (Gozard p156)**.** $(\frac{23}{59} = -1$.

Corollaire 77. *L'équation $x^2 + 59y = 23$ n'a pas de solutions.*

Proposition 78. *Théorème des deux carrés.*

4 Applications

4.1 Critères de divisibilités

Bof
Voir Combes

4.2 Irréductibilité des polynômes

Proposition 79 (Perrin p76)**.** *Critère d'Eisenstein.*

Exemple 80 (Perrin p76)**.** *$X^{p-1} + ... + X + 1$ est irréductible sur $\mathbb{Z}$.*

Proposition 81 (Perrin p76)**.** *Critère de réduction.*

Exemple 82 (Perrin p77)**.** *$3X^3 + 17X - 11$ est irréductible dans $\mathbb{Z}[X]$ et dans $\mathbb{Q}[X]$.*

Contre exemple 83 (Perrin)**.** *$X^4 + 1$ est réductible dans $F_p[X]$ pour tout p premier, mais irréductible dans $\mathbb{Z}[X]$ et $Q[X]$.*

4.3 Cryptographie RSA

Proposition 84 (Demazure)**.** *[Gourdon p34-35] Soient p, q deux nombres premiers distincts. Soit $n = pq$, soient c, d tels que $cd = 1[\phi(n)]$. Les applications $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définies par $c : x \to x^c$ et $d : x \to x^d$ sont respectivement appelées fonction de chiffrement et de déchiffrement. On a $c \circ d = d \circ c = Id$. On peut ainsi transmettre des messages cryptés à l'aide de la clé publique (n, c) et de la clé privée d.*