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

Extrait du rapport de jury

Il est attendu de construire rapidement $\mathbb{Z}/n\mathbb{Z}$, puis d'en décrire les éléments inversibles, les diviseurs de zéro et les idéaux. Ensuite, le cas où l'entier n est un nombre premier doit être étudié. La fonction indicatrice d'Euler ainsi que le théorème chinois et sa réciproque sont incontournables. Il est naturel de s'intéresser à la résolution des systèmes de congruences.
Les applications sont très nombreuses. Les candidates et candidats peuvent, par exemple, choisir de s'intéresser à la résolution d'équations diophantiennes (par réduction modulo n bien choisi) ou bien au cryptosystème `RSA`. Si des applications en sont proposées, l'étude des morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$ ou le morphisme de Frobenius peuvent figurer dans la leçon.
Pour aller plus loin, les candidates et candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, s'intéresser au calcul effectif des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$, au logarithme discret, ou à la transformée de Fourier rapide.

Présentation de la leçon

Je vais vous présenter la leçon 120 intitulée : "Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.". Lorsque l'on fait de l'arithmétique dans $\mathbb{Z}$ on s'intéresse rapidement à l'arithmétique modulaire, c'est-à-dire le reste d'un nombre modulo n. La puissance de l'arithmétique modulaire provient surtout des différentes structures de $\mathbb{Z}/n\mathbb{Z}$, (naturellement héritées de la structure de $\mathbb{Z}$) et c'est pourquoi on s'intéresse en partie autant à cet ensemble en temps que groupe, anneau et corps.
On s'intéresse tout d'abord à $\mathbb{Z}/n\mathbb{Z}$ en temps que groupe en commençant par le construire via les congruences puis en s'intéressant aux notions de groupe monogène et cyclique qui sont reliées au groupe $\mathbb{Z}/n\mathbb{Z}$ via le théorème 7. On continue ensuite en classifiant les groupes d'ordre p^2 et $2p$ ainsi qu'à une description des sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ et des groupes abéliens simples. Dans un deuxième point, on s'attarde sur la notion d'exposant d'un groupe en commençant par donner la définition d'un groupe d'exposant fini ainsi qu'un premier résultat. On donne ensuite deux résultats dans le cas particulier des groupes abéliens avant de montrer le théorème 22 qui nous sera utile dans la suite de cette leçon. Dans un dernier point, on s'intéresse à la structure des groupes abéliens finis avec tout d'abord le théorème de structure des groupes abéliens finis qui justifie que l'on s'intéresse tant aux groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ et qui possède énormément d'applications. En particulier, on tire de cette partie que tous les groupes abéliens finis vérifient la réciproque du théorème de Lagrange. De plus, le théorème de structure des groupes abéliens finis ainsi que l'étude des groupes cycliques $\mathbb{Z}/n\mathbb{Z}$ justifient que l'on connaît très bien n'importe quel groupe abélien fini en termes de structure interne.
Dans une deuxième partie on s'intéresse à $\mathbb{Z}/n\mathbb{Z}$ en temps qu'anneau en commençant par le construire puis en faisant le lien avec les idéaux de $\mathbb{Z}$. Dans un deuxième point on s'intéresse au théorème des restes chinois que l'on énonce dans le cas d'un anneau principal mais que l'on utilise en pratique dans $\mathbb{Z}$ pour résoudre des systèmes de congruence dans la majorité des cas. Ce théorème nous permet également d'avoir des isomorphismes d'anneaux entre différents $\mathbb{Z}/n\mathbb{Z}$. Enfin, on termine cette partie par l'étude du groupe des inversibles avec notamment la proposition 40 qui donne une caractérisation des inversibles ainsi que les théorèmes 45, 46 et 47 qui donnent des conditions de cyclicité de ce groupe puis les théorèmes d'Euler, de Fermat et de Wilson qui sont des tests de primalité pour les deux derniers.
Enfin on consacre une dernière partie à différentes applications. On commence tout d'abord avec le cryptage `RSA` qui est utilisé de nos jours en finance et pour protéger nos données bancaires. Cette méthode repose sur le fait qu'il est très difficile (à l'heure actuelle) de décomposer un très grand nombre en produit de deux nombres premiers. On continue avec le théorème de Dirichlet faible qui nous dit qu'il y a une infinité de nombres premiers d'une certaine forme donnée et que l'on complète par le théorème de Dirichlet (bien que sa démonstration ne soit pas du tout élémentaire !). On donne une troisième application avec l'anneau des entiers de Gauss où l'on donne des inversibles ainsi que le théorème des deux carrés et les éléments irréductibles de cet anneau. On

parle ensuite de la caractéristique d'un anneau et le lien avec le sous-corps premier ainsi qu'une application avec les corps finis où l'on montre qu'ils existent et que leur cardinal est une puissance d'un nombre premier. On donne une avant-dernière application dans le cas des anneaux factoriels avec les critères d'irréductibilité d'Eisenstein et de réduction qui sont surtout utilisés dans le cas de $\mathbb{Z}$ et de la réduction modulo $\mathbb{F}_p$ comme le montrent les exemples 74 et 76. Enfin, on donne une dernière application en revenant sur les corps finis avec la loi de réciprocité quadratique. On commence par donner des rappels concernant les carrés dans un corps fini avant de donner la définition du symbole de Legendre ainsi que les théorèmes de Frobenius-Zolotarev et de réciprocité quadratique.

Plan général

Cours détaillé

I Le groupe $(\mathbb{Z}/n\mathbb{Z}, +_n)$

Dans toute cette partie, on considère un groupe $(G, *)$ (noté G par la suite) et de neutre e_G.

I.1 Construction et premières propriétés

Définition 1 : Congruence [Berhuy, p.30] :
On considère $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$.
On dit que a et b sont **congrus modulo** n lorsqu'il existe un entier k tel que $a = b + kn$.

Lemme 2 : [Berhuy, p.30]
Soit $n \in \mathbb{N}$.
$*$ La relation de congruence modulo n est une relation d'équivalence.
$*$ De plus, pour tous $a, a', b, b' \in \mathbb{Z}$ tels que $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ on a :

$$a + b \equiv a' + b'\ [n],\ -a \equiv -a'\ [n] \text{ et } ab \equiv a'b'\ [n]$$

Puisque la relation de congruence est une relation d'équivalence sur $\mathbb{Z}$, on note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient.

Proposition 3 : [Berhuy, p.32]
Soit $n \in \mathbb{N}$.
La loi $+_n : \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) & \longmapsto & \overline{a} +_n \overline{b} = \overline{a+b} \end{array} \right.$ confère à $\mathbb{Z}/n\mathbb{Z}$ une structure de groupe dont l'élément neutre est $\overline{0}$ et l'opposé de $\overline{a}$ est $\overline{-a}$.

Proposition 4 : [Berhuy, p.32]
Pour tout $n \in \mathbb{N}^*$, le groupe $\mathbb{Z}/n\mathbb{Z}$ possède n éléments qui sont $\overline{0}, \overline{1}, ..., \overline{n-1}$.

Définition 5 : Groupe monogène/cyclique [Berhuy, p.154] :
On dit que le groupe G est :
$*$ **monogène** lorsqu'il est engendré par un unique élément.
$*$ **cyclique** lorsqu'il est monogène et fini.

Exemple 6 : [Berhuy, p.154]
$*$ Le groupe $\mathbb{Z}$ est monogène mais non cyclique.
$*$ Pour tout entier naturel $n \geq 1$, le groupe $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n.

Théorème 7 : [Berhuy, p.154]
∗ Tout groupe monogène infini est isomorphe à $\mathbb{Z}$.
∗ Tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En particulier, deux groupes cycliques sont isomorphes si, et seulement si, ils ont le même ordre.

Corollaire 8 : [Berhuy, p.155]
Soit p un nombre premier.
Si G est d'ordre p, alors G est cyclique et $G \cong \mathbb{Z}/p\mathbb{Z}$.

Développement 1 : [cf. BERHUY]

Proposition 9 : [Berhuy, p.194]
Soit p un nombre premier.
Si G est d'ordre p^2, alors $G \cong \mathbb{Z}/p^2\mathbb{Z}$ ou $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Proposition 10 : [Berhuy, p. 310]
Soit p un nombre premier supérieur ou égal à 3.
Si G est d'ordre $2p$, alors G est isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ ou à D_{2p}.

Théorème 11 : [Berhuy, p.155]
Si G est un groupe cyclique d'ordre n, alors pour tout diviseur positif d de n, il existe un unique sous-groupe H_d d'ordre d de G et ce sous-groupe est cyclique.
De plus, si x_0 est un générateur de G, on a alors les égalités :

$$H_d = \left\langle x_0^{\frac{n}{d}} \right\rangle = \left\{ x \in G \text{ tq } x^d = e_G \right\}$$

Remarque 12 :
On a ici un cas où la réciproque du théorème de Lagrange est vraie !

Corollaire 13 : [Berhuy, p.156]
Pour tout $n \in \mathbb{N}^*$ et tout diviseur positif d de n, il y a $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$.

Théorème 14 : [Berhuy, p.161]
Les groupes abéliens simples sont exactement les $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier.

Théorème 15 : [Rombaldi, p.15]
Soit $n \in \mathbb{N}$.
Tout groupe d'ordre n est cyclique si, et seulement si, n et $\varphi(n)$ sont premiers entre eux

I.2 Lien avec l'exposant

Définition 16 : Groupe d'exposant fini [Berhuy, p.344] :
On dit que G est **d'exposant fini** lorsqu'il existe un entier $n \in \mathbb{N}^*$ tel que pour tout $x \in G$, $x^n = e_G$.
Dans ce cas, on appelle **exposant de** G le plus petit entier $n \in \mathbb{N}^*$ vérifiant cette propriété et on le note $\exp(G)$.

Lemme 17 : [Berhuy, p.344]
Si G est un groupe d'exposant fini, alors $\exp(G) = \text{PPCM}(\{o(x),\ x \in G\})$.
De plus, si G est fini, on a $\exp(G)$ qui divise $\text{Card}(G)$.

Exemple 18 : [Berhuy, p.345]
∗ Si G est cyclique d'ordre n, alors $\exp(G) = n$.
∗ On a $\exp(D_4) = 4$ et $\exp(\mathfrak{S}_3) = 6$.

Proposition 19 : [Berhuy, p.345]
Si G est un groupe abélien d'exposant fini, alors il existe un élément $x \in G$ d'ordre $\exp(G)$.

Corollaire 20 : [Berhuy, p.345]
Si G est un groupe abélien fini, alors on a l'équivalence :

$$(\exp(G) = \text{Card}(G)) \iff (G \text{ cyclique})$$

Remarque 21 : [Berhuy, p.346]
L'ensemble $\mathfrak{S}_3$ montre que les deux résultats précédents sont faux si G n'est pas supposé abélien.

Théorème 22 : [Berhuy, p.346]
Soit $\mathbb{K}$ un corps commutatif quelconque.
Tout sous-groupe fini de $\mathbb{K}^\times$ est cyclique.

I.3 Structure des groupes abéliens finis

Dans toute cette sous-partie, on suppose que G est d'ordre fini et abélien.

Théorème 23 : Théorème de structure [ADMIS] [Berhuy, p.358] :
Il existe des entiers $d_1, ..., d_s \geq 2$ vérifiant $d_1 | d_2 | ... | d_s$ et tels que $G \cong \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$.
De plus, la suite d'entiers $(d_1, ..., d_s)$ est unique, et ne dépend que de la classe d'isomorphisme de G.

Définition 24 : Facteurs invariants [Berhuy, p.361] :
Les entiers $d_1, ..., d_s$ fournis par le théorème précédent sont appelés les **facteurs invariants de** G.

Corollaire 25 : [Berhuy, p.362]
Deux groupes abéliens finis sont isomorphes si, et seulement si, ils ont les mêmes facteurs invariants.

Exemple 26 : [Berhuy, p.363]
$*$ Si $G = \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, alors $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$.
$*$ Il y a exactement 3 groupes abéliens d'ordre 120 (à l'isomorphisme près).

Corollaire 27 :
Pour tout diviseur d de l'ordre de G, il existe un sous-groupe de G d'ordre d.

Théorème 28 : [ADMIS] [Berhuy, p.364]
Si G est un groupe abélien de type fini, alors il existe des entiers naturels r, s et des entiers $d_1, ..., d_s \geq 2$ vérifiant $d_1|d_2|...|d_s$ tels que $G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \mathbb{Z}/d_i\mathbb{Z}$.
De plus, l'entier r et la suite d'entiers $(d_1, ..., d_s)$ sont uniques.

II L'anneau $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$

II.1 Construction et premières propriétés

Proposition 29 : [Berhuy, p.30]
Soit $n \in \mathbb{N}$.
La loi $\times_n : \left| \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ (\overline{a}, \overline{b}) & \longmapsto & \overline{a} \times_n \overline{b} = \overline{a \times b} \end{array} \right.$ confère à $(\mathbb{Z}/n\mathbb{Z}, +_n)$ une structure d'anneau dont l'élément neutre est $\overline{1}$.

Proposition 30 : [Berhuy, p.405]
Tout idéal de $\mathbb{Z}$ est de la forme $n\mathbb{Z}$, avec $n \in \mathbb{Z}$.
L'anneau $\mathbb{Z}/n\mathbb{Z}$ est alors le quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$.

Proposition 31 : [Berhuy, p.460]
Les idéaux premiers et maximaux de $\mathbb{Z}$ coïncident et sont les $p\mathbb{Z}$, avec p un nombre premier.

Corollaire 32 : [Berhuy, p.33]
On a les équivalences suivantes :

L'anneau $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$ est un corps $\iff$ n est un nombre premier
$\iff$ L'anneau $(\mathbb{Z}/n\mathbb{Z}, +_n, \times_n)$ est intègre

II.2 Le théorème des restes chinois

Dans toute cette sous-partie, on considère un anneau $(A, +, \times)$ principal.

Développement 2 : [cf. ROMBALDI]

Lemme 33 : [Rombaldi, p.249]
Soient $a_1, ..., a_r$ des éléments deux à deux premiers entre eux de A.
Si l'on pose pour tout $j \in [\![1; r]\!]$, $b_j = \prod_{\substack{i=1 \\ i \neq j}}^{r} a_j$, alors les b_j sont premiers entre eux dans leur ensemble.

Théorème 34 : Théorème des restes chinois [Rombaldi, p.249] :
Soient $a_1, ..., a_r$ des éléments de A deux à deux premiers entre eux.
L'application :

$$\varphi : \left| \begin{array}{ccc} A & \longrightarrow & \prod_{i=1}^{r} A/(a_i) \\ x & \longmapsto & (\pi_1(x), ..., \pi_r(x)) \end{array} \right.$$

est un morphisme d'anneaux surjectif de noyau $\left(\prod_{i=1}^{r} a_i\right)$.

On a donc en particulier :

$$A \Big/ \left(\prod_{i=1}^{r} a_i\right) = \prod_{i=1}^{r} A/(a_i)$$

Exemple 35 : [Rombaldi, p.291]
Le système d'équations diophantiennes :

$$(S) \begin{cases} k \equiv 2 & [4] \\ k \equiv 3 & [5] \\ k \equiv 1 & [9] \end{cases}$$

possède pour solution particulière $k_0 = 118$ et l'ensemble des solutions à ce système d'équations diophantiennes est $\{118 + 180n,\ n \in \mathbb{Z}\}$.

Exemple 36 : [Berhuy, p.471]
L'inverse de l'isomorphisme $\varphi : \mathbb{Z}/48\mathbb{Z} \longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ est :

$$\varphi^{-1} : \left| \begin{array}{ccc} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} & \longrightarrow & \mathbb{Z}/48\mathbb{Z} \\ (\widehat{a_1}, \dot{a_2}, \widetilde{a_3}) & \longmapsto & \overline{28a_1 + 21a_2 + 36a_3} \end{array} \right.$$

Théorème 37 : [Berhuy, p.485]
Soient $m_1, ..., m_r$ des entiers naturels non nuls premiers entre eux deux à deux.
Le morphisme des projections $f : \mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$ est surjectif et de noyau $(m_1...m_r)$.
En particulier, on a l'isomorphisme $\mathbb{Z}/m_1...m_r\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_r\mathbb{Z}$.

Corollaire 38 : [Berhuy, p.485]
Soit n un entier naturel supérieur ou égal à 2.
Si $n = \prod_{i=1}^{r} p_i^{m_i}$ (décomposition en facteur premiers), alors on a l'isomorphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times ... \times \mathbb{Z}/p_r^{m_r}\mathbb{Z}$.

II.3 Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$

Proposition 39 : [Rombaldi, p.282]
Soit n un entier naturel non nul.
Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est isomorphe à $\mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z})$.

Proposition 40 : [Rombaldi, p.283]
Soient a un entier relatif et n un entier naturel non nul.
$\overline{a}$ est un générateur du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, l'entier relatif a est premier avec n (ou encore si, et seulement si, $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$).

Remarque 41 :
On retrouve le fait que $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est un nombre premier.

Lemme 42 : [Berhuy, p.488]
Pour tout entier naturel $n \geq 2$, on a $\mathrm{Card}\left((\mathbb{Z}/n\mathbb{Z})^\times\right) = \varphi(n)$.

Lemme 43 : [Berhuy, p.488]
$*$ Soient n, m deux entiers naturels supérieurs ou égaux à 2.
Si m et n sont premiers entre eux, alors $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.
$*$ Soit $n \geq 2$ un entier naturel.
Si $\prod_{i=1}^{r} p_i^{m_i}$ est la décomposition en facteurs premiers de n, alors on a l'isomorphisme de groupes $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{m_1}\mathbb{Z})^\times \times ... \times (\mathbb{Z}/p_r^{m_r}\mathbb{Z})^\times$.

Corollaire 44 : [Berhuy, p.489]
$*$ Pour $m, n \geq 2$ des entiers naturels premiers entre eux, on a $\varphi(nm) = \varphi(n)\varphi(m)$.
$*$ Pour tout nombre premier p et tout entier $m \in \mathbb{N}$, on a $\varphi(p^m) = p^m - p^{m-1}$.
$*$ Soit $n \geq 2$ un entier naturel.
Si $\prod_{i=1}^{r} p_i^{m_i}$ est la décomposition en facteurs premiers de l'entier n, alors on a $\varphi(n) = \prod_{i=1}^{r} \left(p_i^{m_i} - p_i^{m_i - 1}\right)$.

Théorème 45 : [Rombaldi, p.292]
Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique et isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.

Théorème 46 : [Rombaldi, p.292]
Si p est un nombre premier impair et α un entier supérieur ou égal à 2, alors le groupe multiplicatif $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est cyclique.

Théorème 47 : [Rombaldi, p.294] [ADMIS]
Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si, et seulement si, $n = 2, 4, p^\alpha$ ou $2p^\alpha$ avec p premier impair et $\alpha \geq 1$.

Théorème 48 : Théorème d'Euler [Rombaldi, p.283] :
Soit n un entier naturel non nul.
Pour tout entier relatif a premier avec n, on a $a^{\varphi(n)} \equiv 1\ [n]$.

Théorème 49 : Petit théorème de Fermat [Rombaldi, p.284] :
Soient p un nombre premier et a un entier relatif.
Si a est premier avec p, alors on a $a^{p-1} \equiv 1\ [p]$.

Théorème 50 : Théorème de Wilson [Gourdon, p.11] :
Un entier $p \geq 2$ est un nombre premier si, et seulement si, $(p-1)! \equiv -1\ [p]$.

III Applications

III.1 Le cryptage RSA

Proposition 51 : [Gourdon, p.36]
Soient p et q deux nombres premiers distincts, $n = pq$ et c et d deux entiers tels que $cd \equiv 1\ [\varphi(n)]$.
Pour tout $t \in \mathbb{Z}$, on a $t^{cd} \equiv t\ [n]$.

Remarque 52 : [Gourdon, p.37]
Le couple (n, c) est appelé **clef publique** et l'entier d est appelé **clef secrète**.

La sécurité de ce système repose sur le fait que connaissant la clef publique, il est très difficile de déterminer d : un moyen consiste par exemple à factoriser n pour trouver p et q, ce qui est encore impossible à réaliser lorsque p et q sont grands, typiquement (pour l'année 2020) de l'ordre de 150 à 200 chiffres.

Ainsi, tout le monde peut chiffrer mais seuls ceux connaissant la clef secrète peuvent déchiffrer. Ce système de chiffrement est apparu en 1976, il est appelé RSA (du nom des inventeurs Rivest, Shamir et Adleman) et est couramment utilisé aujourd'hui car il est extrêmement robuste. Son apparition explique l'intérêt que l'on porte aujourd'hui aux algorithmes de factorisation et de primalité.

III.2 Le théorème de Dirichlet faible

Théorème 53 : Théorème de Dirichlet faible [Gourdon, p.99] :
Soit $n \in \mathbb{N}$.
Il existe une infinité de nombres premiers $p \in \mathcal{P}$ tels que $p \equiv 1\ [n]$.

Corollaire 54 : [Gourdon, p.14]
Il existe une infinité de nombres premiers de la forme $4k-1$ et $6k-1$ pour $k \in \mathbb{N}^*$.

Théorème 55 : Théorème de Dirichlet [Gourdon, p.14] [ADMIS] :
Soient a, b deux entiers naturels non nuls.
Si $\text{PGCD}(a,b) = 1$, alors il existe une infinité de nombres premiers de la forme $ak+b$ avec $k \in \mathbb{N}^*$.

III.3 Le théorème des deux carrés

Dans toute cette sous-partie, on pose $\Sigma = \{n \in \mathbb{N} \text{ tq } n = a^2 + b^2,\ a, b \in \mathbb{N}\}$, $\mathcal{P}$ l'ensemble des nombres premiers (au sens usuel) et une application (qui est multiplicative) $N : a + ib \longmapsto a^2 + b^2$ définie de $\mathbb{Z}[i]$ dans $\mathbb{N}$.

Définition 56 : L'anneau $\mathbb{Z}[i]$ [Perrin, p.56] :
On appelle **anneau** $\mathbb{Z}[i]$ l'anneau : $\mathbb{Z}[i] = \left\{a + ib,\ (a,b) \in \mathbb{Z}^2\right\}$ muni de l'addition et de la multiplication usuelles.

Remarque 57 :
$\mathbb{Z}[i]$ reste un anneau intègre car inclus dans $\mathbb{C}$, cependant les nombres premiers (au sens usuel) qui sont somme de deux carrés ne sont plus irréductibles dans $\mathbb{Z}[i]$ (par exemple $5 = (2+i)(2-i)$).

Proposition 58 : [Perrin, p.56]
$\mathbb{Z}[i]^\times = \{-1; 1; -i; i\}$.

Proposition 59 : [Perrin, p.56]
L'ensemble Σ est stable par multiplication.

Proposition 60 : [Perrin, p.57]
L'anneau $\mathbb{Z}[i]$ est euclidien pour le stathme N.

Lemme 61 : [Perrin, p.57]
Soit $p \in \mathcal{P}$.
Les assertions suivantes sont équivalentes :
$*$ $p \in \Sigma$. $*$ L'élément p n'est pas irréductible dans $\mathbb{Z}[i]$.
$*$ On a $p = 2$ ou $p \equiv 1\ [4]$

Théorème 62 : Théorème des deux carrés [Perrin, p.58] :
Soit $n = \prod_{p \in \mathcal{P}} p^{v_p(n)} \in \mathbb{N}$.
$n \in \Sigma$ si, et seulement si, pour tout $p \in \mathcal{P}$ vérifiant $p \equiv 3\ [4]$, l'entier $v_p(n)$ est pair.

Proposition 63 : [Perrin, p.58]
Les irréductibles de $\mathbb{Z}[i]$ sont, aux éléments inversibles près :
$*$ Les entiers premiers $p \in \mathbb{N}$ tels que $p \equiv 3\ [4]$.
$*$ Les entiers de Gauss $a + ib$ dont la norme est un nombre premier.

III.4 Caractéristique d'un anneau et corps finis

Dans toute cette sous-partie, on considère $\mathbb{K}$ un corps commutatif quelconque.

Définition 64 : Sous-corps premier [Perrin, p.72] :
On appelle **sous-corps premier de** $\mathbb{K}$ le plus petit sous-corps de $\mathbb{K}$ (contenant l'élément $1_\mathbb{K}$).

On considère le morphisme d'anneaux :

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ n & \longmapsto & n \cdot 1_\mathbb{K} \end{array} \right.$$

Le noyau de φ est un idéal de $\mathbb{Z}$ et par le premier théorème d'isomorphisme, on a $\mathbb{Z}/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi) \subseteq \mathbb{K}$, donc $\operatorname{Ker}(\varphi)$ est un idéal premier de $\mathbb{Z}$ de la forme $p\mathbb{Z}$ avec $p \in \mathcal{P} \cup \{0\}$.

Définition 65 : Caractéristique d'un corps [Perrin, p.72] :
On appelle **caractéristique de** $\mathbb{K}$ le nombre $p \in \mathcal{P} \cup \{0\}$ qui est le générateur de $\operatorname{Ker}(\varphi)$ et on le note $\text{car}(\mathbb{K})$.

Proposition 66 : [Perrin, p.73]
Si $\text{car}(\mathbb{K}) > 0$, alors l'application $F : \left| \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & x^p \end{array} \right.$ est un morphisme de corps.
De plus, si $\mathbb{K}$ est fini, alors c'est un automorphisme et si $\mathbb{K} = \mathbb{F}_p$, alors c'est l'identité.

Proposition 67 : [Perrin, p.72]
$*$ $\text{car}(\mathbb{K}) = 0$ si, et seulement si, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$.
$*$ $\text{car}(\mathbb{K}) > 0$ si, et seulement si, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Proposition 68 : [Perrin, p.72]
Soient p un nombre premier et $\mathbb{K}$ un corps fini.
Si $\mathbb{K}$ est de caractéristique p, alors $\mathbb{K}$ a pour cardinal une puissance de p.

Exemple 69 :
Il n'existe pas de corps de cardinal 6 mais de cardinal 7 oui (par exemple $\mathbb{Z}/7\mathbb{Z}$).

Théorème 70 : [Perrin, p.73]
Soient p un nombre premier et $n \in \mathbb{N}^*$.
Si l'on pose $q = p^n$, alors il existe un corps commutatif $\mathbb{K}$ à q éléments (c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$).
En particulier, $\mathbb{K}$ est unique à isomorphisme près et on le note $\mathbb{F}_q$.

Exemple 71 :
On peut construire un corps à 4 éléments de deux manières :
∗ En tant que corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$.
∗ Grâce à l'isomorphisme $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1)$.

Théorème 72 : [Rombaldi, p.292]
Soit p un nombre premier.
Le groupe multiplicatif $\mathbb{F}_p^*$ est un groupe cyclique et isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$.

III.5 Irréductibilité de certains polynômes

Dans toute cette sous-partie, on considère un anneau $(A, +, \times)$ factoriel.

Proposition 73 : Critère d'irréductibilité d'Eisenstein [Perrin, p.76] :
Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$.
S'il existe un élément irréductible p tel que :
∗ p ne divise pas a_n. ∗ Pour tout $i \in [\![0; n-1]\!]$, p divise a_i.
∗ p^2 ne divise pas a_0.
alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple 74 :
Les polynômes $X^n - 2$ et $X^4 - 6X^3 + 3X^2 - 12X + 3$ sont irréductibles dans $\mathbb{Q}[X]$.

Proposition 75 : Critère de réduction [Perrin, p.77] :
Soient I un idéal premier de A et $P \in A[X]$ unitaire.
Si $\overline{a}_n \neq 0$ dans A/I et si $\overline{P}$ est irréductible sur A/I ou $\mathrm{Frac}(A/I)$, alors le polynôme P est irréductible sur $\mathrm{Frac}(A)$.

Exemple 76 : [Perrin, p.77]
Le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Q}[X]$ par le critère de réduction.

III.6 La loi de réciprocité quadratique

Théorème 77 : [Rombaldi, p.427]
∗ Il y a $\frac{q-1}{2}$ carrés et $\frac{q-1}{2}$ non carrés dans $\mathbb{F}_q^*$.
∗ Les carrés de $\mathbb{F}_q^*$ sont les racines de $X^{\frac{q-1}{2}} - 1$ et les non carrés sont les racines de $X^{\frac{q-1}{2}} + 1$.

Corollaire 78 : [Rombaldi, p.427]
∗ Le produit de deux carrés ou de deux non carrés de $\mathbb{F}_q^*$ est un carré et le produit d'un carré et d'un non carré est un non carré.
∗ -1 est un carré dans $\mathbb{F}_q^*$ si, et seulement si, q est congru à 1 modulo 4.

Définition 79 : Symbole de Legendre [Rombaldi, p.428] :
Pour tout $a \in \mathbb{F}_q^*$, on appelle **symbole de Legendre** l'entier :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{sinon} \end{cases}$$

Théorème 80 : [Rombaldi, p.428]
Pour tout $a \in \mathbb{F}_p^*$, on a $a^{\frac{p-1}{2}} = \overline{\left(\frac{a}{p}\right)}$ dans $\mathbb{F}_p^*$ et l'application $a \longmapsto \left(\frac{a}{p}\right)$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ dans $\{-1; 1\}$.

Corollaire 81 : [Rombaldi, p.429]
Soient $n \in \mathbb{N}^*$ et p un nombre premier impair.
L'application :

$$\Psi : \left| \begin{array}{ccc} \mathrm{GL}_n(\mathbb{F}_p) & \longrightarrow & \{-1; 1\} \\ A & \longmapsto & \left(\frac{\det(A)}{p}\right) \end{array} \right.$$

est l'unique morphisme de groupes non trivial de $\mathrm{GL}_n(\mathbb{F}_p)$ dans $\{-1; 1\}$.

Théorème 82 : Théorème de Frobenius-Zolotarev [Rombaldi, p.430] :
Soient $n \in \mathbb{N}^*$ et p un nombre premier impair.
Pour tout $A \in \mathrm{GL}_n(\mathbb{F}_p)$ on a $\varepsilon(A) = \left(\frac{\det(A)}{p}\right)$.

Théorème 83 : Loi de réciprocité quadratique [Rombaldi, p.434] :
Pour tous nombres $p, q \in \mathcal{P}$ impairs distincts, $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Remarques sur le plan

— Il faut savoir calculer des inverses et résoudre des équations dans $\mathbb{Z}/n\mathbb{Z}$.

— On peut également s'intéresser aux carrés dans $\mathbb{Z}/n\mathbb{Z}$ ainsi qu'à la résolution d'équations.

Liste des développements possibles

— Classification des groupes d'ordre p^2 et $2p$.

— Théorème des restes chinois + application.

Bibliographie

— Grégory Berhuy, *Algèbre : le grand combat*.

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et Géométrie*.

— Xavier Gourdon, *Les maths en tête, Algèbre et Probabilités*.

— Daniel Perrin, *Cours d'algèbre*.