Quelques remarques sur les anneaux $\mathbb{Z}/n\mathbb{Z}$

Le contenu de cette note peut servir dans les leçons :

- Groupes finis. Exemples et applications.
- Groupe linéaire d'un e. v. de dimension finie E, sous-groupes de $\mathrm{GL}(E)$. Applications.
- Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- Anneaux principaux. Applications.
- Opérations élémentaires sur les lignes et les colonnes d'une matrice. Exemples et applications.
- Méthodes combinatoires, problèmes de dénombrement.

1 Structure de $\mathbb{Z}/n\mathbb{Z}$

1.1 Généralités

Sur le groupe abélien $\mathbb{Z}/n\mathbb{Z}$, il n'y a qu'une structure d'anneau possible. En effet, un produit ab est une somme $a + \cdots + a$ avec b termes, donc toute multiplication est une itération finie d'additions et la multiplication est déterminée par l'addition.

Dit autrement, la structure de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est déterminée par sa structure de groupe additif. Ceci se reflète aussi sur les éléments inversibles de l'anneau, qui sont les générateurs du groupe additif, et sur les idéaux, qui sont les sous-groupes additifs.

Un autre fait notable est que dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, comme d'ailleurs dans tout anneau fini A, les éléments non nuls sont soit inversibles, soit diviseurs de zéro. En effet, pour $x \in A \setminus \{0\}$, la multiplication par x donne un endomorphisme de groupe abélien $m_x : A \to A$. Si m_x est surjectif, alors 1 est dans l'image, donc il existe $y \in A$ tel que $xy = 1$ et x est inversible. Si m_x n'est pas surjectif, alors il n'est pas injectif (car A est fini) et donc il y a un élément non nul y dans le noyau. Alors, $xy = 0$ et x est un diviseur de zéro.

Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition en facteurs premiers de n. La structure algébrique de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est pour l'essentiel gouvernée par la décomposition en produit donnée par l'isomorphisme du théorème des restes chinois :

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$

et par la structure particulière des facteurs $\mathbb{Z}/p^\alpha\mathbb{Z}$.

1.2 Structure de $\mathbb{Z}/p^\alpha\mathbb{Z}$

Décrivons donc plus en détail l'anneau $A = \mathbb{Z}/p^\alpha\mathbb{Z}$. Une très bonne manière de se représenter les éléments de A est d'utiliser l'écriture en base p : pour tout $x \in A$, il existe des entiers uniques $0 \leq x_i \leq p-1$ tels que $x = x_0 + x_1 p + x_2 p^2 + \cdots + x_{\alpha-1} p^{\alpha-1}$. Si un élément de A est écrit ainsi, on a $x \in A^*$ ssi $x_0 \neq 0$, ou encore, ssi $x \notin (p)$. En particulier, on voit que si on note $\pi : \mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ la surjection canonique, alors x est inversible dans A si et seulement si $\pi(x)$ est inversible dans $\mathbb{Z}/p\mathbb{Z}$. (En général, si $f : R \to S$ est un morphisme d'anneaux commutatifs et unitaires, l'image d'un inversible est inversible, mais la réciproque n'est pas vraie.) De plus, l'idéal (p) est égal à l'idéal des éléments nilpotents, et on a $A = A^* \sqcup (p)$.

Par ailleurs, les idéaux de A forment une chaîne :

$$0 \subset (p^{\alpha-1}) \subset \cdots \subset (p^2) \subset (p) \subset A \ .$$

Ceci permet de définir la *valuation p-adique* d'un élément non nul $x \in A$ comme étant le plus grand entier $k \leq \alpha - 1$ tel que $x \in (p^k)$. On peut alors écrire $x = p^k u$, où u est inversible dans A, et cette écriture est unique.

2 Puissances dans $\mathbb{Z}/n\mathbb{Z}$

2.1 Puissances k-ièmes

Proposition : *Soient $k \geq 2$ et $n \geq 2$ deux entiers. Alors, l'application $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ d'élévation à la puissance k est bijective si et seulement si tous les facteurs premiers p de n sont de multiplicité 1 et tels que $p-1$ est premier avec k.*

Preuve : Notons $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ telle que $\varphi(x) = x^k$. Cette application est multiplicative. Soit $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ la décomposition en facteurs premiers de n. Par le théorème des restes chinois, on a un isomorphisme $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$. Si l'on décrit φ via cet isomorphisme, il est clair que $\varphi(x_1, \dots, x_r) = (x_1^k, \dots, x_r^k)$, de sorte que φ est bijective si et seulement si pour tout i, l'application d'élévation à la puissance k dans $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ est bijective. Ceci nous ramène au cas où $n = p^\alpha$.

Soit $x \in \mathbb{Z}/p^\alpha\mathbb{Z}$. Si x est inversible, alors $\varphi(x)$ est inversible, c'est-à-dire qu'il n'est pas dans (p). Si x n'est pas inversible, il est dans (p) et donc $\varphi(x) = x^k$ est dans (p^k). (Pour le dire autrement, l'application φ multiplie la valuation p-adique par k de sorte que les éléments de l'image ont une valuation multiple de k.) On voit donc que si $\alpha \geq 2$, l'élément $p \in A$ n'est pas dans l'image de φ. Donc $\alpha = 1$ si φ est bijectif.

L'application φ envoie 0 sur 0 et sa restriction à $(\mathbb{Z}/p\mathbb{Z})^*$ est un morphisme de groupes multiplicatifs. Il reste à voir quand celui-ci est bijectif. Or $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$ et φ

s'identifie, comme endomorphisme du groupe additif $\mathbb{Z}/(p-1)\mathbb{Z}$, à la multiplication par k. Celle-ci est bijective ssi k est premier à $p-1$. □

2.2 Carrés

Le résultat précédent dit que l'application d'élévation au carré ($k=2$) dans $\mathbb{Z}/n\mathbb{Z}$ n'est bijective que lorsque $n=2$. Donc en général, les carrés forment un sous-ensemble strict, que l'on va dénombrer, généralisant le résultat correspondant pour $\mathbb{Z}/p\mathbb{Z}$ avec p premier. Ici encore, en utilisant le théorème chinois, le nombre de carrés est le produit des nombres de carrés dans des anneaux $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. Ceci nous ramène au cas où $n=p^\alpha$ et nous citerons le résultat dans ce cas. Nous ne traiterons que le cas où $p \geq 3$, mais le cas où $p=2$ se traite de la même manière (la seule différence provenant de la structure du groupe des inversibles).

Lemme : *Soit p un nombre premier impair et $\alpha \geq 1$ un entier.*
(i) Le cardinal de $(\mathbb{Z}/p^\alpha\mathbb{Z})^{*2}$, ensemble des carrés des éléments inversibles de $\mathbb{Z}/p^\alpha\mathbb{Z}$, est égal à $p^{\alpha-1}\frac{p-1}{2}$.
(ii) Soit i un entier tel que $i \leq \alpha$. Alors, la multiplication par p^i induit une injection de groupes abéliens $\mathbb{Z}/p^{\alpha-i}\mathbb{Z} \hookrightarrow \mathbb{Z}/p^\alpha\mathbb{Z}$ et l'image de $(\mathbb{Z}/p^{\alpha-i}\mathbb{Z})^{*2}$ est égale à $p^i(\mathbb{Z}/p^\alpha\mathbb{Z})^{*2}$.
(iii) Le cardinal de $p^i(\mathbb{Z}/p^\alpha\mathbb{Z})^{*2}$ est égal à $p^{\alpha-i-1}\frac{p-1}{2}$.

Preuve : (i) Comme p est impair, on a $(\mathbb{Z}/p^\alpha\mathbb{Z})^* \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$ et l'élévation au carré s'identifie à la multiplication par 2 dans $\mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$. Comme 2 divise $p-1$, l'image est donc le sous-groupe strict engendré par 2, d'indice 2. Donc le cardinal de $(\mathbb{Z}/p^\alpha\mathbb{Z})^{*2}$ est $p^{\alpha-1}\frac{p-1}{2}$.

(ii) Il est immédiat de voir que le noyau de la multiplication par p^i de $\mathbb{Z}/p^\alpha\mathbb{Z}$ dans lui-même est égal à l'idéal engendré par $p^{\alpha-i}$, d'où la première assertion. On peut décrire cette application ainsi : à $x = x_0 + x_1 p + \cdots + x_{\alpha-i-1}p^{\alpha-i-1}$ on associe $p^i x = p^i(x_0 + x_1 p + \cdots + x_{\alpha-i-1}p^{\alpha-i-1})$. L'image de $(\mathbb{Z}/p^{\alpha-i}\mathbb{Z})^{*2}$ est $p^i(\mathbb{Z}/p^{\alpha-i}\mathbb{Z})^{*2}$. C'est aussi $p^i(\mathbb{Z}/p^\alpha\mathbb{Z})^{*2}$, puisque dans l'écriture $p^i(x_0 + x_1 p + \cdots + x_{\alpha-1}p^{\alpha-1})^2$ les termes $x_j p^j$ avec $j \geq \alpha - i$ sont annulés par p^i.

(iii) D'après (ii) le cardinal de $p^i(\mathbb{Z}/p^\alpha\mathbb{Z})^{*2}$ est égal à celui de $(\mathbb{Z}/p^{\alpha-i}\mathbb{Z})^{*2}$, d'où le résultat d'après (i). □

Proposition : *Si p est un nombre premier impair, le nombre de carrés dans $A = \mathbb{Z}/p^\alpha\mathbb{Z}$ est égal à*

$$1 + \frac{p-1}{2}(p + p^3 + \cdots + p^{2\beta-1})$$

si $\alpha = 2\beta$ est pair, et

$$1 + \frac{p-1}{2}(1 + p^2 + \cdots + p^{2\beta})$$

si $\alpha = 2\beta + 1$ est impair.

Preuve : Si $x \in A$ est non nul, il s'écrit de manière unique sous la forme $x = p^i u$ avec $0 \leq i \leq \alpha - 1$ et $u \notin (p)$, c'est-à-dire u inversible dans A. Il est clair que x est un carré si

et seulement si i est pair et u est un carré. En d'autres termes, l'ensemble des carrés non nuls dans A est

$$A^{*2} \sqcup p^2A^{*2} \sqcup p^4A^{*2} \sqcup \cdots \sqcup p^{2\beta-2}A^{*2} \quad \text{si } \alpha = 2\beta \text{ est pair,}$$

$$A^{*2} \sqcup p^2A^{*2} \sqcup p^4A^{*2} \sqcup \cdots \sqcup p^{2\beta}A^{*2} \quad \text{si } \alpha = 2\beta+1 \text{ est impair.}$$

En utilisant le lemme qui donne le cardinal de $p^{2k}A^{*2}$ et en tenant compte du fait que $0 \in A$ est un carré, on trouve que le nombre de carrés dans A est

$$1 + p^{2\beta-1}\frac{p-1}{2} + p^{2\beta-3}\frac{p-1}{2} + \cdots + p\frac{p-1}{2}$$

si $\alpha = 2\beta$, et l'expression similaire si α est impair. □

Références : Je ne connais de référence ni pour la description de l'application d'élévation à la puissance k-ième, ni pour le calcul du nombre de carrés de $\mathbb{Z}/n\mathbb{Z}$.

3 Matrices à coefficients dans $\mathbb{Z}/n\mathbb{Z}$

Soit $r \geq 1$ un entier. Dans ce paragraphe, nous nous intéressons aux groupes linéaires $\mathrm{GL}_r(\mathbb{Z}/n\mathbb{Z})$ et $\mathrm{SL}_r(\mathbb{Z}/n\mathbb{Z})$. Nous utiliserons les remarques simples qui suivent.

Si $f : A \to B$ est un morphisme d'anneaux commutatifs et unitaires, il y a une application $\mathrm{M}_r(A) \to \mathrm{M}_r(B)$ entre les ensembles de matrices carrées de taille r, notée encore f pour simplifier, obtenue en associant à une matrice $M = (m_{i,j})$ la matrice $f(M) = (f(m_{i,j}))$. Puisque f est un morphisme d'anneaux et que l'addition et la multiplication des matrices s'expriment par des additions et des multiplications entre les coefficients des matrices, cette application $f : \mathrm{M}_r(A) \to \mathrm{M}_r(B)$ est un morphisme d'anneaux. Puisque le déterminant d'une matrice est lui aussi un polynôme en les coefficients de la matrice, on a $\det(f(M)) = f(\det(M))$. Il en découle que f induit des morphismes de groupes $\mathrm{GL}_r(A) \to \mathrm{GL}_r(B)$ et $\mathrm{SL}_r(A) \to \mathrm{SL}_r(B)$.

Par ailleurs, dans le cas où l'anneau des coefficients des matrices est un anneau produit, il est clair que $\mathrm{M}_r(A \times B) \simeq \mathrm{M}_r(A) \times \mathrm{M}_r(B)$, $\mathrm{GL}_r(A \times B) \simeq \mathrm{GL}_r(A) \times \mathrm{GL}_r(B)$ et $\mathrm{SL}_r(A \times B) \simeq \mathrm{SL}_r(A) \times \mathrm{SL}_r(B)$. Pour étudier $\mathrm{GL}_r(\mathbb{Z}/n\mathbb{Z})$ et $\mathrm{SL}_r(\mathbb{Z}/n\mathbb{Z})$, utilisant le théorème des restes chinois on est ramené au cas où $n = p^\alpha$.

3.1 Nombre d'éléments de $\mathrm{GL}_r(\mathbb{Z}/n\mathbb{Z})$ et $\mathrm{SL}_r(\mathbb{Z}/n\mathbb{Z})$

Proposition : *On a* $|\mathrm{GL}_r(\mathbb{Z}/p^\alpha\mathbb{Z})| = p^{(\alpha-1)r^2}(p^r-1)(p^r-p)\dots(p^r-p^{r-1})$.

Preuve : Commençons par le cas $\alpha = 1$. Dans ce cas, l'anneau de coefficients est le corps $k = \mathbb{Z}/p\mathbb{Z}$. Une matrice est dans $\mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$ ssi ses vecteurs colonnes forment une base. Le premier vecteur doit être non nul, il y a donc $p^r - 1$ façons de le choisir. Le deuxième vecteur ne doit pas être dans la droite engendrée par le premier, il y a donc $p^r - p$ façons de le choisir. En continuant ainsi, on trouve $|\mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})| = (p^r-1)(p^r-p)\dots(p^r-p^{r-1})$.

Passons au cas général. On notera $\mathbb{Z}/p^\alpha\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, $x \mapsto \overline{x}$ le morphisme de réduction. Rappelons-nous que x est inversible ssi $\overline{x}$ est inversible (voir 1.2). Nous allons

voir que le morphisme induit $\nu : \mathrm{GL}_r(\mathbb{Z}/p^\alpha\mathbb{Z}) \to \mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$ est surjectif. En effet, si $M \in \mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$ et qu'on considère une matrice $N \in \mathrm{M}_r(\mathbb{Z}/p^\alpha\mathbb{Z})$ obtenue en relevant de manière arbitraire les coefficients de M, on a $\overline{\det(N)} = \det(M)$ qui est inversible. Donc $\det(N)$ est inversible, i.e. $N \in \mathrm{GL}_r(\mathbb{Z}/p^\alpha\mathbb{Z})$ et N est un antécédent pour M. On regarde maintenant le noyau $H = \ker(\nu)$. C'est l'ensemble des matrices $\mathrm{Id} + N$ où N est à coefficients dans $p(\mathbb{Z}/p^\alpha\mathbb{Z}) \simeq \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$. Comme les matrices ont r^2 coefficients, on trouve $|H| = (p^{\alpha-1})^{r^2}$. Finalement $|\mathrm{GL}_r(\mathbb{Z}/p^\alpha\mathbb{Z})| = |\mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})|.|H|$ et ceci donne le résultat annoncé. □

Proposition : *On a* $|\mathrm{SL}_r(\mathbb{Z}/p^\alpha\mathbb{Z})| = p^{(\alpha-1)(r^2-1)}(p^r-1)(p^r-p)\dots(p^r-p^{r-2})p^{r-1}$.

Preuve : On considère le morphisme déterminant $\det : \mathrm{GL}_r(\mathbb{Z}/p^\alpha\mathbb{Z}) \to (\mathbb{Z}/p^\alpha\mathbb{Z})^*$. Il est surjectif, car tout $x \in (\mathbb{Z}/p^\alpha\mathbb{Z})^*$ est le déterminant d'une matrice de dilatation diagonale $(x, 1, \dots, 1)$. Il s'ensuit que le cardinal du noyau, le groupe spécial linéaire, est

$$|\mathrm{SL}_r(\mathbb{Z}/p^\alpha\mathbb{Z})| = \frac{|\mathrm{GL}_r(\mathbb{Z}/p^\alpha\mathbb{Z})|}{p^{\alpha-1}(p-1)} \ .$$

Compte tenu de la proposition précédente, ceci mène au résultat annoncé. □

Références : Le calcul du cardinal de $\mathrm{GL}_r(\mathbb{Z}/p\mathbb{Z})$ et d'autres groupes linéaires sur les corps finis est fait dans Perrin [P]. Le calcul du cardinal de $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ peut être trouvé dans [FGN2], exercice 3.23 (lire la fin de la correction).

3.2 Surjection $\mathrm{SL}_r(\mathbb{Z}) \to \mathrm{SL}_r(\mathbb{Z}/n\mathbb{Z})$

On peut se poser la question de savoir si toute matrice inversible à coefficiens dans $\mathbb{Z}/n\mathbb{Z}$ peut être relevée en une matrice inversible à coefficients dans $\mathbb{Z}$. Mais ceci est presque tout le temps faux, pour la raison que le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est plus gros que le groupe des inversibles de $\mathbb{Z}$: il est clair qu'une matrice de $\mathrm{GL}_r(\mathbb{Z}/n\mathbb{Z})$ de déterminant inversible, mais distinct de ± 1, ne peut pas être relevée dans $\mathrm{GL}_r(\mathbb{Z})$. Le théorème suivant est donc assez surprenant :

Théorème : *Le morphisme de réduction* $\mathrm{SL}_r(\mathbb{Z}) \to \mathrm{SL}_r(\mathbb{Z}/n\mathbb{Z})$ *est surjectif.*

Preuve : On fait une récurrence sur r. Comme $\mathrm{SL}_1(\mathbb{Z}) \simeq \mathrm{SL}_1(\mathbb{Z}/n\mathbb{Z}) \simeq 1$, le résultat est clair pour $r = 1$. Supposons-le vrai pour l'entier $r-1$, et soit $A \in \mathrm{M}_r(\mathbb{Z})$ une matrice carrée telle que $\det(A) \equiv 1\ (n)$. D'après le théorème des invariants de similitude, il existe deux matrices U, V dans $\mathrm{GL}_r(\mathbb{Z})$ telles que UAV est une matrice diagonale, d'éléments $a_1, \dots, a_m$. Posons $b = a_2 \dots a_m$ et considérons les matrices

$$W = \begin{pmatrix} b & 1 & & & \\ b-1 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \ X = \begin{pmatrix} 1 & -a_2 & & & \\ 0 & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \ A' = \begin{pmatrix} 1 & 0 & & & \\ 1-a_2 & a_1a_2 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}.$$

Comme $a_1 b = \det(A) \equiv 1\ (n)$, on voit que $WUAVX \equiv A'\ (n)$. Par l'hypothèse de récurrence, la matrice carrée de taille $(r-1, r-1)$ en bas à droite de A' se relève en une matrice $C \in \mathrm{SL}_{r-1}(\mathbb{Z})$. On vérifie alors facilement que

$$B = U^{-1}W^{-1} \left(\begin{array}{c|c} 1 & 0 \\ \hline 1-a_1 & \\ & C \\ 0 & \end{array}\right) X^{-1}V^{-1}$$

est une matrice dans $\mathrm{SL}_r(\mathbb{Z})$ qui relève A. □

Remarques et références : Ce théorème est une jolie application du théorème des invariants de similitude, sous forme matricielle. La démonstration donnée ici est la reproduction fidèle de celle que l'on trouve en pages 20-21 du livre de Shimura [Shi]. Dans le cas $r = 2$, la preuve du théorème se trouve aussi dans [FGN2], exercice 3.23, p. 204, et dans le livre d'Hellegouarch [H], chapitre 5, § 3, p. 295.

Une des raisons de l'importance de ce théorème provient de l'étude des *groupes fuchsiens* et des *sous-groupes de congruence de* $\mathrm{SL}_2(\mathbb{Z})$ tels que le sous-groupe :

$$\Gamma(n) = \ker\left(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})\right) .$$

Ce groupe intervient dans l'étude des formes modulaires, qui sont l'un des ingrédients de la preuve du théorème de Fermat. Vous trouverez plus de détails sur tout cela dans le livre d'Hellegouarch [H].

Références

[FGN2] S. Francinou, H. Gianella, S. Nicolas, *Exercices de Mathématiques Oraux X-ENS, Algèbre 2*, Cassini.

[H] Y. Hellegouarch, *Invitation aux Mathématiques de Fermat-Wiles*, Masson, 1997.

[P] D. Perrin, *Cours d'Algèbre*, Ellipses.

[Shi] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Forms*, Princeton University Press, 1971.