Feuille $n^0 1$
jeudi 9 janvier 2020
un peu d'arithmétique

Exercice 1 Soit $p > 3$ un nombre premier. Soient $s_1, ..., s_p$ les entiers tels que

$$P := (X-1)...(X-p+1) = X^{p-1} - s_1 X^{p-2} + ... - s_{p-2}X + s_{p-1} \quad .$$

a) Montrer que $P = X^{p-1} - 1 \bmod p$ et en déduire les relations :

$$s_{p-1} = -1 \bmod p, \ s_i = 0 \bmod p \text{ si } 1 \leq i < p-1$$

b) Montrer $s_{p-2} = 0 \bmod p^2$ (*indication : calculer* $P(p)$) et en déduire :

$$1^{-1} + 2^{-1} + ... + (p-1)^{-1} = 0 \bmod p^2 \quad .$$

Exercice 2 pgcd et ppcm Soient $m, n \in \mathbb{N}$. On pose $d = \mathrm{pgcd}(m,n)$ l'entier naturel tel que $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$. On pose $p = \mathrm{ppcm}(m,n)$, l'entier naturel tel que $p\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$.

On considère les morphismes de groupes :

$$x \longmapsto (x,x)$$

$$\mathbb{Z} \xrightarrow{f} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{g} \mathbb{Z}/m\mathbb{Z} + n\mathbb{Z}$$

$$(x,y) \longmapsto x - y$$

a) Montrer que $\mathrm{Im}\, f = \ker g$.

b) En déduire que $mn = pd$.

c) Cas particulier : en déduire que si $d = 1$ alors

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$k \bmod mn \mapsto (k \bmod m, \ k \bmod n)$$

est un isomorphisme (théorème des restes chinois).

d) En déduire que si m, n sont premiers entre eux, alors $\phi(mn) = \phi(m)\phi(n)$.

e) Trouver $P, Q \in \mathrm{SL}_2(\mathbb{Z})$ telles que :

$$P \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix} Q = \begin{pmatrix} d & 0 \\ 0 & p \end{pmatrix} .$$

En déduire un isomorphisme : $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 3 Matrices unimodulaires

a) Montrer que si $(a_1, ...a_n)$ sont premiers entre eux (dans leur ensemble) alors $(a_1, ..., a_n)$ est la première ligne d'une matrice $n \times n$ à coefficients entiers inversible.

$$\begin{pmatrix} a_1 & \cdots & a_n \\ \cdot & \cdots & \cdot \\ \vdots & & \vdots \\ \cdot & \cdots & \cdot \end{pmatrix}$$

Indication : commencer par le cas où $n = 2$, puis par récurrence considérer $d = \mathrm{pgcd}(a_2, .., a_n)$, poser $db_i = a_i$ si $2 \leq i \leq n$, appliquer l'hypothèse de récurrence à la ligne $(b_2, ..., b_n)$, choisir s, t tels que $sa_1 + td = 1$ et un bon signe $\pm$ tels que la matrice :

$$\begin{pmatrix} a_1 & db_2 & \cdots & db_n \\ 0 & \cdot & \cdots & \cdot \\ | & \vdots & & \vdots \\ 0 & \cdot & \cdots & \cdot \\ t & \pm sb_2 & \cdots & \pm sb_n \end{pmatrix}$$

soit de déterminant ± 1.

Exercice 4 Symbole de Legendre

Soit p un nombre premier impair. Si $x \in \mathbb{Z}$ st premier à p, on pose $\left(\frac{x}{p}\right) = 1$ si x est un carré $\mod p$, -1 sinon.

a) En considérant le morphisme de groupes :

$$\mathbb{F}_p^* \to \mathbb{F}_p^*,\ x \mapsto x^2 ,$$

déterminer le nombre de carrés dans $\mathbb{F}_p^*$ et en déduire que $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \mod p$

b) Montrer que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

c) On admet la loi de réciprocité quadatique :
Théorème. Si p, q premiers impairs distincts , alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \quad .$$

Par exemple : p est un carré $\bmod 5 \Leftrightarrow 5$ est un carré $\bmod p$.
Montrer que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$
Indication : on étend d'abord la loi de réciprocité quadratique aux symboles de Jacobi[†] *puis vérifier que :*

$$\left(\frac{2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p-2}\right)...$$

Exercice 5

a) Vérifier qu'il y a une infinité de nombres premiers $= -1 \bmod 4$. *Indication : si $p_1, ..., p_N$ sont des nombres premiers $= -1 \bmod 4$, alors considérer $4p_1....p_N - 1$ ...*
b) Vérifier qu'il y a une infinité de nombres premiers $= 1 \bmod 4$. *Indication : si $p_1, ..., p_N$ sont des nombres premiers $= 1 \bmod 4$, alors considérer $4(p_1....p_N)^2 + 1$ ...*
c) Vérifier que si p est un nombre premier, alors :

$$\mathbb{Z}[i]/p \simeq \begin{cases} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} & \text{si } p = 1 \bmod 4 \\ \mathbb{F}_{p^2} & \text{si } = p = -1 \bmod 4 \\ \mathbb{F}_2[X]/(X^2) & \text{si } p = 2 \end{cases}$$

d) En déduire que si p est un nombre premier impair, p est somme de deux carrés $\Leftrightarrow p = 1 \bmod 4$. *Indication : utiliser la factorisation dans l'anneau $\mathbb{Z}[i]$.*

†. **Symbole de Jacobi.** Si n, m sont des entiers. Si m est impair et si

$$m = p_1^{a_1}...p_k^{a_k}$$

où $k \geq 0$ et les p_i sont des nombres premiers impairs deux à deux distincts, on pose

$$\left(\frac{n}{m}\right) := \left(\frac{n}{p_1}\right)^{a_1} ... \left(\frac{n}{p_k}\right)^{a_k} \quad .$$

e) en déduire que si $n \in \mathbb{N}$, alors n est somme de deux carrés $\Leftrightarrow$ les facteurs premiers de n congrus à $-1 \bmod 4$ apparaissent avec un exposant pair dans sa décomposition. *Indications : vérifier d'abord que le produit de deux sommes de deux carrés est encore la somme de deux carrés. Si $n = a^2 + b^2 = (a + ib)(a - ib)$ avec $a, b \neq 0$, si $p|n$ et si $p = 3 mod 4$, vérifier que $p^2|n$ ...*

Exercice 6 le théorème des quatre carrés via les *quaternions d'Hurwitz* On note i, j, k les quaternions usuels : $ij = k$, $i^2 = j^2 = k^2 = -1$, $ij = -ji$, ...

On pose

$$\mathcal{O} := \{a+ib+jc+kd \,:\, a,b,c,d \in \mathbb{Z}\} \cup \{a+ib+jc+kd \,:\, a,b,c,d \in \frac{1}{2}+\mathbb{Z}\} \ .$$

a) Vérifier que $\mathcal{O}$ est un sous-anneau de H, et que si $x \in \mathcal{O}$, $N(x) \in \mathbb{Z}$.

b) Déterminer les 24 éléments inversibles : $\mathcal{O}^\times$.

c) Montrer que si $x \in \mathbb{H}$, il existe $\alpha \in \mathcal{O}$ tel que $N(\alpha - x) < 1$. En déduire que tout idéal à droite de $\mathcal{O}$ est principal.

d) Montrer que le produit d'entiers somme de 4 carrés est encore une somme de 4 carrés.

e) Soit p premier impair. Vérifier qu'il existe $a, b \in \mathbb{N}$ tels que $a^2 + b^2 = -1 \bmod p$. *Indication calculer le cardinal des ensembles*

$$\{x^2 \,:\, x \in \mathbb{Z}/p\mathbb{Z}\} \text{ et } \{-1 - y^2 \,:\, y \in \mathbb{Z}/p\mathbb{Z}\}$$

et en déduire que leur intersection n'est pas vide ...

f) En utilisant que l'idéal $p\mathcal{O} + (1 + ai + bj)\mathcal{O}$ est principal, obtenir une factorisation non triviale :

$$p = xy$$

avec $x, y \in \mathcal{O}$ non inversibles.

g) Montrer que $p = N(x) = N(y)$.

h) Si $x \in \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$, c'est terminé, si $x \in \frac{1}{2}(1 + i + j + k) + \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}k$, choisir $\epsilon = \frac{\pm 1 \pm i \pm j \pm k}{2}$ (avec les bons signes !) tel que $x + \epsilon \in 2\mathbb{Z} + 2\mathbb{Z}i + 2\mathbb{Z}j + 2\mathbb{Z}k$; Vérifier alors que

$$p = N(z\bar{\epsilon} - 1) \ .$$

Exercice 7 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

a) Montrer que $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/(\mathrm{pgcd}(n,m))\mathbb{Z}$ et *(pour ceux qui connaissent)* que $\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\mathrm{pgcd}(m,n)$.

b) Montrer que $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$. Quel est l'ordre des groupes suivants : $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z},+)$ (p premier), $\mathrm{Aut}(\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}))$ et $\mathrm{Aut}(\mathrm{Aut}(\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z})))$?

c) Soit p un nombre premier ($p \neq 2$), montrer que pour tout entier $k \geq 1$, il existe un entier $\lambda \geq 1$, premier avec p, et tel que

$$(1+p)^{p^k} = 1 + \lambda p^{k+1}$$

En déduire que pour tout $n \geq 1$ on a $(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}$.

d) En montrant que pour tout $k \geq 1$, $5^{2^k} = 1 + \lambda 2^{k+2}$ avec λ un entier impair, en déduire pour $n \geq 2$ l'isomorphisme

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$$

e) Donner la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$. Pour quelles valeurs de n est-il cyclique ?

Exercice 8 Soit p un nombre premier.

a) Déterminer l'ordre du groupe $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.

b) Montrer que $\mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, $(a_{i,j}) \mapsto (a_{i,j} \bmod p)$ est un morphisme surjectif. En déduire l'ordre du groupe $\mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$.

c) Montrer que pour tout entier $n > 0$, le groupe $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ est d'ordre

$$n^4 \prod_{p|n} \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)$$

Exercice 9 Le groupe $\mathbb{Z}^{\mathbb{N}}$ n'est pas un groupe abélien libre

a) Soit M un $\mathbb{Z}-$module libre. Soit $N \leq M$. Alors N aussi est un $\mathbb{Z}-$module libre. *Indication : soit $(e_i)_{i\in I}$ une base de M. Soit $(J, \mathscr{B})$ un élément maximal de l'ensemble des couples tels que $J \subseteq I$ et $\mathscr{B}$ est une base de $N_J := M \cap \langle e_j \ : \ j \in J\rangle$ (ça existe par le lemme de Zorn ...) ; montrer que $J = I$.*

b) Supposons par l'absurde que $A := \mathbb{Z}^{\mathbb{N}}$ a une base $(e_i)_{i\in I}$. Justifier que I n'est pas dénombrable.

c) On note $B = \{(x_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \ : \ \lim_n v_2(x_n) = +\infty\}$ où $v_2(x)$ est le plus grand exposant k tel que $2^k | x$. Vérifier que $A \to B$, $(x_n) \mapsto (2^n x_n)_n$ est injective et en déduire que B est libre avec une base non dénombrable.

d) Montrer que $B/2B$ est engendré par une famille dénombrable ... et conclure !

Exercice 10 À propos du dual de $\mathbb{Z}^{\mathbb{N}}$

a) On note ϵ_n la suite qui vaut 1 en position n et 0 ailleurs.
Montrer que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{(\mathbb{N})}, \mathbb{Z}) \simeq \mathbb{Z}^{\mathbb{N}}$, $\phi \mapsto (\phi(\epsilon_n))_{n\in\mathbb{N}}$.

b) Montrer que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{(\mathbb{N})}, \mathbb{Z})$ est injective. *Indication : soit ϕ dans le noyau, montrer que $\phi((2^n a_n)_n) = 0$ pour toute suite (a_n), puis montrer que si (x_n) est une suite quelconque, alors $x_n = 2^n a_n + 3^n b_n$ pour tout n et pour certains entiers a_n, b_n ...*

c) Montrer que si a est un entier, si $k \geq 0$, alors il existe un unique $(a_n)_{0\leq n\leq k} \in \{0,1\}^{k+1}$ tel que $a = a_0 + ... + a_k 2^k \bmod 2^{k+1}$. On appelle $(a_n)_{n\in\mathbb{N}}$ la décomposition de a en base binaire. Par exemple donner la décomposition de -1.

d) Montrer que la décomposition en base binaire d'un entier se termine par que des 1 ou par que des 0.

e) Soit $\phi \in \mathrm{Hom}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$. On pose $\lambda_n = \phi(\epsilon_n)$. On choisit une suite $a = (\pm 2^{s_n})_n$ où la suite s_n est strictement croissante (d'entiers) $\pm 2^{s_n}\lambda_n \geq 0$ et $2^{s_n} > 2^{1+s_{n-1}}|\lambda_n|$ pour tout n.
Montrer que $f(a) = 2^{s_0}|\lambda_0| + ... + 2^{s_n}|\lambda_n| \bmod 2^{s_{n+1}}$ pour tout n. En utilisant la décomposition binaire de l'entier $f(a)$, montrer que $\lambda_n = 0$ pour n assez grand.

f) Pour un groupe abélien G, on pose $G^\vee := \mathrm{Hom}(G, \mathbb{Z})$. Montrer que $(\mathbb{Z}^{\mathbb{N}})^\vee \simeq \mathbb{Z}^{(\mathbb{N})}$ et $(\mathbb{Z}^{(\mathbb{N})})^\vee \simeq \mathbb{Z}^{\mathbb{N}}$. En particulier :

$$(\mathbb{Z}^{\mathbb{N}})^{\vee\vee} \simeq \mathbb{Z}^{\mathbb{N}} \text{ et } (\mathbb{Z}^{(\mathbb{N})})^{\vee\vee} \simeq \mathbb{Z}^{(\mathbb{N})}$$

les duaux ne sont pas isomorphes mais l'isomorphisme avec le bidual est respecté.

Exercice 11 Montrer :

$$\begin{tikzcd}
\text{euclidien} \arrow[r, Rightarrow] & \text{principal} \arrow[r, Rightarrow] \arrow[l, Rightarrow, bend left, "/" marking, "\mathbb{R}[X,Y]/(X^2+Y^2+1)^{\ddagger}"] & \text{factoriel} \arrow[r, Rightarrow] \arrow[l, Rightarrow, bend left, "/" marking, "\mathbb{Z}[X]^{\S}"] & \text{intégralement clos} \arrow[l, Rightarrow, bend left, "/" marking, "\mathbb{Z}[i\sqrt{5}]^{\P}"]
\end{tikzcd}$$

‡. *cf. Exercices d'algèbre de Francinou et Gianella, §2.23*

§. par exemple, si p est premier et si $n \in \mathbb{N}$, alors l'idéal $(p, X)^n$ est engendré par $n+1$ polynômes mais non moins

¶. les éléments $2, 3, 1 \pm i\sqrt{5}$ sont irréductibles non associés et $2\times 3 = (1+i\sqrt{5})\times(1-i\sqrt{5})$