Université de Lille - Sciences et Technologies
Master Mathématiques, Semestre 3 (2019-20)
Algèbre
Devoir Surveillé, 6/11/2019
Corrigé

Barême indicatif : 3+9+6+2. Les exercices sont autonomes et peuvent être traités dans un ordre arbitraire.

1. Quiz

On considère la matrice des vecteurs $(u_1, \dots, u_n)$ relativement à la base canonique $\underline{e} = (e_1, \dots, e_n)$ de $\mathbb{Z}^n$. Soit A cette matrice. D'après le théorème de la forme normale de Smith, on a des matrices inversibles $P, Q \in GL_n(\mathbb{Z})$ telles que :

$$A' = PAQ = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d_n \end{pmatrix}$$

avec $d_1 | d_2 | \cdots | d_n$, où on a éventuellement $d_{r+1} = \cdots = d_n = 0$ pour un entier $0 \leq r \leq n$. On a alors $\mathbb{Z}^n/\mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$ et $M = \mathbb{Z}^n/\mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n$ est fini si et seulement si on a aucun d_i tel que $d_i = 0$, ce qui revient à dire que $Det(A') \neq 0 \Leftrightarrow Det(A) \neq 0$, soit que les vecteurs $(u_1, \dots, u_n)$ forment une base de $\mathbb{R}^n$. On a alors $|\mathbb{Z}^n/\mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n| = d_1 d_2 \cdots d_n$. D'après le cours, on a la formule $d_1 d_2 \cdots d_n = \text{pgcd déterminants mineurs } n \times n \text{ de } A = \epsilon\, Det(A)$, avec $\epsilon \in \mathbb{Z}^\times$ (un facteur ± 1 qui correspond au facteur d'indétermination du pgcd dans $\mathbb{Z}$). On a donc au final :

$$|\mathbb{Z}^n/\mathbb{Z}u_1 + \cdots + \mathbb{Z}u_n| = |\, Det_{\underline{e}}(u_1, \dots, u_n)|.$$

2. Exercice

2.1) On a $0 \in \sqrt{0}$. Si $x, y \in \sqrt{0}$, alors il existe k et l tels que $x^k = 0$ et $y^l = 0$. On a alors d'après la formule du binôme

$$(x-y)^{k+l-1} = \sum_{i=0}^{l-1} (-1)^i \binom{k+l-1}{i} \underbrace{x^{k+l-1-i}}_{=0} y^i + \sum_{i=l}^{k+l-1} (-1)^i \binom{k+l-1}{i} x^{k+l-1-i} \underbrace{y^i}_{=0} = 0.$$

On a donc $x, y \in \sqrt{0} \Rightarrow x - y \in \sqrt{0}$. On a également $x^N = 0 \Rightarrow (ax)^N = a^N x^N = 0$ pour tout $a \in A$, d'où $x \in \sqrt{0} \Rightarrow ax \in \sqrt{0}$ $(\forall a \in A)$. Ceci prouve que $\sqrt{0}$ est un idéal de A.

2.2) S'il existe un idéal premier P tel que $x \notin P$, alors on a aussi $x^N = x \cdots x \notin P$, pour toute puissance x^N de x. Comme on a $0 \in P$, ceci implique $x^N \neq 0$. Donc $\exists P$ tel que $x \notin P$ implique $x \notin \sqrt{0}$. Par contraposée, on en déduit $x \in \sqrt{0} \Rightarrow x \in P$, quel que soit P premier.

2.3) On se donne un élément $s \in A$ tel que $s \notin \sqrt{0}$, c'est à dire tel que l'on a $s^N \neq 0$, $\forall N \in \mathbb{N}$. On note alors $\mathcal{C}$ l'ensemble des idéaux de A qui ne contiennent aucune puissance de s.

Soit I_α, $\alpha \in \Lambda$, un ensemble totalement ordonné (non vide) d'idéaux de $\mathcal{C}$. On poste $I = \bigcup_\alpha I_\alpha$. On a $0 \in I$. Si $x, y \in I$, alors il existe α tel que $x \in I_\alpha$ et il existe β tel que $y \in I_\beta$. On a soit $I_\alpha \subset I_\beta$, soit $I_\beta \subset I_\alpha$. On a dans le premier cas $x, y \in I_\beta \Rightarrow x - y \in I_\beta \Rightarrow x - y \in I$ et dans le second cas $x, y \in I_\alpha \Rightarrow x - y \in I_\alpha \Rightarrow x - y \in I$. D'où au final $x, y \in I \Rightarrow x - y \in I$. Si $x \in I$, alors il existe α tel que $x \in I_\alpha$ et alors on a $ax \in I_\alpha \Rightarrow ax \in I$ quel que soit $a \in A$. Ceci montre que I forme un idéal de A.

Pour toute puissance s^N de s, on a en outre $I_\alpha \in \mathcal{C} \Rightarrow s^N \notin I_\alpha$ quel que soit I_α. Donc $s^N \notin I$. Donc on a aussi $I \in \mathcal{C}$. Et comme on a clairement $I_\alpha \subset I$, ceci montre que toute famille totalement ordonnée d'idéaux de $\mathcal{C}$ possède un majorant dans $\mathcal{C}$, donc que $\mathcal{C}$ est inductif.

On note que $\mathcal{C}$ est non vide, car on a $s \notin \sqrt{0} \Rightarrow s^N \neq 0\,(\forall N) \Rightarrow 0 \in \mathcal{C}$. D'après le lemme de Zorn il s'ensuit que $\mathcal{C}$ possède un élément maximum, c'est à dire qu'il existe un idéal $P_0 \in \mathcal{C}$ qui ne possède pas de majorant strict dans $\mathcal{C}$.

Pour $x \notin P_0$, on a $P_0 \subset_{\neq} P_0 + Ax$ car $x \in P_0 + Ax \setminus P_0$. Il s'ensuit que $P_0 + Ax \notin \mathcal{C}$, c'est à dire, il existe un puissance s^k de s telle que $s^k \in P_0 + Ax$. Pour $y \notin P_0$, on a de même $P_0 \subset_{\neq} P_0 + Ay \Rightarrow P_0 + Ay \notin \mathcal{C}$, c'est à dire, il existe une puissance s^l de s telle que $s^l \in P_0 + Ax$. On écrit alors $s^k = p + ax$, avec $p \in P_0$, $a \in A$, et $s^l = q + bx$, avec $q \in P_0$, $b \in A$. On a alors :

$$s^{k+l} = (p+ax)(q+by) = \underbrace{pq + pby + axq}_{\in P_0} + abxy \Rightarrow s^{k+l} \in P_0 + Axy,$$

d'où $P_0 + Axy \notin \mathcal{C}$, ce qui implique que l'inclusion $P_0 \subset P_0 + Axy$ est stricte. Comme on a l'implication $x'y' \in P_0 \Rightarrow Ax'y' \subset P_0 \Rightarrow P_0 + Ax'y' = P_0$, pour tout couple $x', y' \in A$, on a par contraposée $P_0 \subset_{\neq} P_0 + Axy \Rightarrow xy \notin P_0$. On a au final $x, y \notin P_0 \Rightarrow xy \notin P_0$, ce qui prouve que P_0 est un idéal premier.

On déduit de cette analyse qu'il existe un idéal premier P_0 tel que $P_0 \in \mathcal{C}$, soit tel que $s^N \notin P_0$ pour toute puissance s^N de s. En particulier $s \notin P_0$.

2.4) On a "$s \in \sqrt{0} \Rightarrow s \in P\,(\forall P \in \mathcal{P})$" d'après la question 2.2 et "$s \notin \sqrt{0} \Rightarrow \exists P \in \mathcal{P}$ tel que $s \notin P$" d'après la question 2.3. Ceci montre que l'on a l'identité $\sqrt{0} = \bigcap_{P \in \mathcal{P}} P$.

3. Exercice

Soit p un nombre premier impair. Soit $(\mathbb{Z}/p\mathbb{Z})^{\times 2}$ le sous groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ constitué des éléments x tels qu'il existe un élément $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $x = y^2$ (le sous groupe des carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$).

3.1) Soit $\phi : (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ le morphisme de groupes tel que $\phi(x) = x^2$. On a $x \in \ker\phi \Leftrightarrow \phi(x) = x^2 = \bar{1} \Leftrightarrow$ "x est racine de $P(X) = X^2 - 1$". Or $P(X) = X^2 - 1$ a au plus deux racines (polynômes de degré 2 sur un corps $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$) et $P(X) = (X-1)(X+1)$ montre que $P(X)$ a en fait exactement deux racines qui sont $\bar{1}$ et $-\bar{1}$. Donc $\ker\phi = \{\bar{1}, -\bar{1}\}$.

3.2) On a $(\mathbb{Z}/p\mathbb{Z})^{\times 2} = \operatorname{im}\phi$ et $|\operatorname{im}\phi| = |(\mathbb{Z}/p\mathbb{Z})^\times|/|\ker\phi| = (p-1)/2$. Donc $|(\mathbb{Z}/p\mathbb{Z})^{\times 2}| = (p-1)/2$.

3.3) On a $\phi(x^{(p-1)/2}) = x^{2(p-1)/2} = x^{p-1} = \bar{1}$ d'après le petit théorème de Fermat. Donc $x^{(p-1)/2} \in \ker\phi \Rightarrow x^{(p-1)/2} \in \{\bar{1}, -\bar{1}\}$.

Si $x \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}$, c'est à dire s'il existe $y \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $x = y^2$, alors on a encore $x^{(p-1)/2} = y^{2(p-1)/2} = y^{p-1} = \bar{1}$.

3.4) Le résultat de la question précédente montre que les éléments de $(\mathbb{Z}/p\mathbb{Z})^{\times 2}$ sont racines du polynôme $Q(X) = X^{(p-1)/2} - 1$. Comme ce polŷnôme, de degré $(p-1)/2$, possède au plus $(p-1)/2$ racines dans $\mathbb{Z}/p\mathbb{Z}$, et que l'on a vu que $|(\mathbb{Z}/p\mathbb{Z})^{\times 2}| = (p-1)/2$, on en conclut que les éléments de $(\mathbb{Z}/p\mathbb{Z})^{\times 2}$ sont exactement les racines de $Q(X) = X^{(p-1)/2} - 1$.

Si $x \notin (\mathbb{Z}/p\mathbb{Z})^{\times 2}$, on a donc $Q(x) = x^{(p-1)/2} - 1 \neq 0$ et donc $x^{(p-1)/2} \neq 1$ ce qui implique $x^{(p-1)/2} = -1$ d'après la question 3.3.

On en conclut que l'on a $x^{(p-1)/2} = 1$ si x est un carré dans $(\mathbb{Z}/p\mathbb{Z})^\times$ et $x^{(p-1)/2} = -1$ sinon.

4. Exercice

4.1) Soit p un nombre premier impair. On a soit $p \equiv 1 (\mathrm{mod}\, 4)$ soit $p \equiv 3 (\mathrm{mod}\, 4)$. Dans le premier cas, si on écrit $p = 1 + 4k$, avec $k \in \mathbb{N}$, alors on obtient $(-1)^{(p-1)/2} = (-1)^{2k} = 1$. Dans le second cas, si on écrit $p = 3 + 4k$, avec $k \in \mathbb{N}$, alors on obtient $(-1)^{(p-1)/2} = (-1)^{1+2k} = -1$. On a donc $p \equiv 1 (\mathrm{mod}\, 4) \Rightarrow (-1)^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p)$ et $p \equiv 3 (\mathrm{mod}\, 4) \Rightarrow (-1)^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$, ce qui

montre (d'après le résultat de l'exercice précédent) que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $p \equiv 1 (\mathrm{mod}\, 4)$.

4.2) On suppose que l'ensemble des nombres premiers p tels que $p \equiv 1 (\mathrm{mod}\, 4)$ est fini. Soit alors p_0 le plus grand de ces nombres. Soit p_1 un nombre premier tel $p_1 | 1 + (p_0!)^2$. On a alors $-1 \equiv (p_0!)^2 (\mathrm{mod}\, p_1)$ ce qui montre que -1 est un carré dans $\mathbb{Z}/p_1\mathbb{Z}$, et donc $p_1 \leq p_0$ par maximalité de p_0. Mais alors on a $p_1 | (p_0!)^2$ et p_1 ne peut divisier $1+(p_0!)^2$. On aboutit donc à une contradiction.

Donc il y a un nombre infini de nombres premiers p tels que $p \equiv 1 (\mathrm{mod}\, 4)$, c'est à dire tels que $p = 1 + 4k$, pour un entier $k \in \mathbb{N}$.

— Fin du devoir —