Partiel Algèbre 1

Responsable : Mr O. DEBARRE

Important : vous avez droit de consulter le polycopié et d'utiliser sans démonstration ses résultats (sauf ceux des exercices ou des TD). Si vous voulez utiliser des résultats hors du cours, il faut les démontrer (sauf mention explicite du contraire).

Exercice 1. Soient p et q des nombres premiers vérifiant $p < q$ et $p \nmid q - 1$. Le but de cet exercice est de déterminer tous les groupes d'ordre p^2q. Soit G un tel groupe.

a) Montrer que G contient un unique p-Sylow ; on le notera P.

b) Montrer que G contient un unique q-Sylow ; on le notera Q.

c) Montrer que P et Q sont distingués dans G.

d) Montrer On pose $PQ := \{xy \mid x \in P,\ y \in Q\}$. Montrer $PQ = G$ (Indication : on pourra commencer par montrer que PQ est un sous-groupe de G).

e) Montrer $P \cap Q = \{e\}$.

f) En déduire que tout élément de P commute avec tout élément de Q.

g) En déduire que G est abélien.

h) Déterminer tous les groupes d'ordre p^2q (à isomorphisme près).

Exercice 2. Soient p et q des nombres premiers vérifiant $p < q$ et soit G un groupe d'ordre $p^m q^n$, avec $0 \leq m \leq 2$ et $n \geq 0$. Le but de cet exercice est de montrer que G est résoluble.

a) Si $m = 0$ ou $n = 0$, montrer que G est résoluble.

b) Si $m = 1$ et $n > 0$, montrer que G est résoluble (*Indication :* on pourra compter les q-Sylow de G).

c) Si $m = 2$ et $n > 0$, montrer que G n'est pas simple (*Indication :* on pourra compter les q-Sylow de G et, dans le cas $p = 2$ et $q = 3$, considérer l'action de G sur l'ensemble des 3-Sylow de G), puis que G est résoluble.

Exercice 3. Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbf{Q})$. On pose

$$H := \sum_{M \in G} M \cdot \mathbf{Z}^n \subset \mathbf{Q}^n.$$

a) Montrer que H est un groupe abélien libre de type fini. On note r son rang, c'est-à-dire l'entier r tel que $H \simeq \mathbf{Z}^r$.

b) Montrer $r \geq n$.

c) Montrer $r \leq n$.

d) En déduire que G est conjugué dans $\mathrm{GL}_n(\mathbf{Q})$ à un sous-groupe de $\mathrm{GL}_n(\mathbf{Z})$.

e) Soit p un nombre premier et soit $M \in \mathrm{GL}_n(\mathbf{Z})$ tel que $M^p = I_n$ et $M \equiv I_n \pmod 3$. Montrer $M = I_n$.

f) En déduire que n étant fixé, il n'y a qu'un nombre fini de classes d'isomorphisme de sous-groupes finis de $\mathrm{GL}_n(\mathbf{Q})$.

g) N'y a-t-il qu'un nombre fini de classes d'isomorphisme de sous-groupes finis de $\mathrm{GL}_n(\mathbf{R})$?

Corrigé du partiel Algèbre 1

Responsable : Mr O. DEBARRE

Exercice 1. *Soient p et q des nombres premiers vérifiant $p < q$ et $p \nmid q-1$. Le but de cet exercice est de déterminer tous les groupes d'ordre p^2q. Soit G un tel groupe.*

a) Montrer que G contient un unique p-Sylow ; on le notera P.

Le nombre de p-Sylow divise q, donc c'est 1 ou q. Comme il est $\equiv 1 \pmod p$ et que $p \nmid q-1$, il n'y a qu'un p-Sylow.

b) Montrer que G contient un unique q-Sylow ; on le notera Q.

Le nombre de q-Sylow divise p^2, donc c'est 1, p ou p^2. Comme il est $\equiv 1 \pmod q$ et que $p < q$, c'est 1 ou p^2. Si c'est p^2, q divise $p^2-1 = (p-1)(p+1)$, donc $q = p+1$, ce qui contredit $p \nmid q-1$.

c) Montrer que P et Q sont distingués dans G.

Comme P est l'unique p-Sylow, il est distingué dans G. De même pour Q.

d) On pose $PQ := \{xy \mid x \in P,\ y \in Q\}$. Montrer $PQ = G$ (Indication : on pourra commencer par montrer que PQ est un sous-groupe de G).

Si $x, x' \in P$ et $y, y' \in Q$, on a

$$(xy)(x'y')^{-1} = xyy'^{-1}x'^{-1} = (xx'^{-1})(x'yy'^{-1}x'^{-1}).$$

Comme $Q \lhd G$, on a $x'yy'^{-1}x'^{-1} \in Q$, et ce produit est donc dans PQ. Comme PQ contient e, c'est donc bien un sous-groupe de G. Il contient bien sûr P et Q.

Par le théorème de Lagrange, son ordre est divisible par celui de P, c'est-à-dire p^2 et par celui de Q, c'est-à-dire q, donc par p^2q. Comme G est d'ordre p^2q, on en déduit $PQ = G$.

e) Montrer $P \cap Q = \{e\}$.

L'ordre du groupe $P \cap Q$ doit diviser les ordres des groupes P et Q, c'est-à-dire p^2 et q. C'est donc 1.

f) En déduire que tout élément de P commute avec tout élément de Q.

Si $x \in P$ et $y \in Q$, alors $xyx^{-1} \in Q$ car $Q \lhd G$, donc $[x,y] = xyx^{-1}y^{-1} \in Q$. De même, $[x,y] \in P$. Par e), on en déduit $[x,y] = e$, donc x et y commutent.

g) En déduire que G est abélien.

On a vu en cours que P et Q sont abéliens. Par d), tout élément de G peut s'écrire xy, avec $x \in P$ et $y \in Q$. Par f), on a

$$xyx'y' = xx'yy' = x'xy'y = x'y'xy.$$

Le groupe G est donc abélien.

h) Déterminer tous les groupes d'ordre p^2q.

Les groupes d'ordre p^2q sont abéliens par g) ; d'après le cours, ils sont isomorphes soient à $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/pq\mathbf{Z}$, soit à $\mathbf{Z}/p^2q\mathbf{Z}$.

Exercice 2. *Soient p et q des nombres premiers vérifiant $p < q$ et soit G un groupe d'ordre p^mq^n, avec $0 \leq m \leq 2$ et $n \geq 0$. Le but de cet exercice est de montrer que G est résoluble.*

a) Si $m = 0$ ou $n = 0$, montrer que G est résoluble.

Si $m = 0$ ou $n = 0$, le groupe G est un p-groupe ; il est donc résoluble par le cours.

*b) Si $m = 1$ et $n > 0$, montrer que G est résoluble (*Indication : *on pourra compter les q-Sylow de G).*

Le nombre de q-Sylow divise p, donc c'est 1 ou p. Comme il est $\equiv 1 \pmod q$ et que $p < q$, c'est 1. Il y a un unique q-Sylow S ; il est donc distingué dans G. Le groupe S est un q-groupe et le quotient G/S est un p-groupe ; ils sont donc résolubles par le cours. De nouveau par le cours, G est résoluble.

*c) Si $m = 2$ et $n > 0$, montrer que G n'est pas simple (*Indication : *on pourra compter les q-Sylow de G et, dans le cas $p = 2$ et $q = 3$, considérer l'action de G sur l'ensemble des 3-Sylow de G), puis que G est résoluble.*

Le nombre n_q de q-Sylow divise p^m, donc c'est 1, p ou p^2. Comme il est $\equiv 1 \pmod q$ et que $p < q$, c'est 1 ou p^2.

Si $n_q = 1$, on conclut comme en b).

Si $n_q = p^2$, on a $m = 2$ et $q \mid p^2-1 = (p-1)(p+1)$ et $q = p+1$, donc $p = 2$ et $q = 3$ et $|G| = 4 \cdot 3^n$. Le groupe G agit transitivement par conjugaison sur l'ensemble à 4 éléments des 3-Sylow de G. On en déduit un morphisme non trivial $G \to \mathfrak{S}_4$.

Si ce morphisme est injectif, on a $4 \cdot 3^n \leq 4!$, donc $G \xrightarrow{\sim} \mathfrak{S}_4$, qui n'est pas simple. Sinon, le noyau est un sous-groupe distingué propre de G, qui n'est donc pas simple.

On en déduit par récurrence sur $|G|$ que G est résoluble, puisque, si $N \lhd G$, les ordres de N et de G/N peuvent aussi s'écrire $p^m q^n$, avec $0 \leq m \leq 2$ et $n \geq 0$.

Exercice 3. *Soit G un sous-groupe fini de $\mathrm{GL}_n(\mathbf{Q})$. On pose*

$$H := \sum_{M \in G} M \cdot \mathbf{Z}^n \subset \mathbf{Q}^n.$$

a) Montrer que H est un groupe abélien libre de type fini. On note r son rang, c'est-à-dire l'entier r tel que $H \simeq \mathbf{Z}^r$.

Le groupe abélien H est engendré par les $M \cdot e_i$, où $(e_1, \ldots, e_n)$ est la base canonique de $\mathbf{Z}^n$, $1 \leq i \leq n$ et M décrit G. Il est donc de type fini. Comme c'est un sous-groupe de $\mathbf{Q}^n$, il ne contient pas d'élément d'ordre fini autre que 0, donc il est libre par le cours.

b) Montrer $r \geq n$.

Comme H contient $\mathbf{Z}^n$, il est de rang $\geq n$.

c) Montrer $r \leq n$.

Si d est un entier non nul tel que dM soit à coefficients entiers pour tout $M \in G$, on a $H \subset \frac{1}{d}\mathbf{Z}^n \simeq \mathbf{Z}^n$, donc $r \leq n$.

d) En déduire que G est conjugué dans $\mathrm{GL}_n(\mathbf{Q})$ à un sous-groupe de $\mathrm{GL}_n(\mathbf{Z})$.

Soit $\mathscr{B} = (a_1, \ldots, a_n)$ une base de H. C'est aussi une base de $\mathbf{Q}^n$; soit $P \in \mathrm{GL}_n(\mathbf{Q})$ la matrice de passage de la base canonique vers $\mathscr{B}$. On a ainsi $H = P \cdot \mathbf{Z}^n$. Si $M \in G$, on a $M \cdot H \subset H$ et de même $M^{-1} \cdot H \subset H$, donc $M \cdot H = H$. Ceci entraîne

$$M \cdot P \cdot \mathbf{Z}^n = P \cdot \mathbf{Z}^n,$$

c'est-à-dire $P^{-1}MP \in \mathrm{GL}_n(\mathbf{Z})$. La conjugaison par P^{-1} envoie donc G isomorphiquement sur un sous-groupe de $\mathrm{GL}_n(\mathbf{Z})$.

e) Soit p un nombre premier et soit $M \in \mathrm{GL}_n(\mathbf{Z})$ tel que $M^p = I_n$ et $M \equiv I_n \pmod 3$. Montrer $M = I_n$.

Écrivons $M = I_n + 3^m N$, avec $m \geq 1$ et $N \in \mathscr{M}_n(\mathbf{Z})$ telle que $N \not\equiv 0_n \pmod 3$, et développons :

$$I_n = M^p = (I_n + 3^m N)^p = I_n + p3^m N + \frac{p(p-1)}{2} 3^{2m} N^2 + \cdots + 3^{pm} N^p.$$

Cela entraîne $3^m \mid pN$, donc $p = 3$ et $m = 1$. On écrit la même formule

$$I_n = I_n + 9N + 27N^2 + 27N^3,$$

qui mène encore à une contradiction. Donc $N = 0$.

f) En déduire que n étant fixé, il n'y a qu'un nombre fini de classes d'isomorphisme de sous-groupes finis de $\mathrm{GL}_n(\mathbf{Q})$.

Par d), tout sous-groupe fini de $\mathrm{GL}_n(\mathbf{Q})$ est conjugué (donc isomorphe) à un sous-groupe fini G de $\mathrm{GL}_n(\mathbf{Z})$. Montrons que la restriction à G du morphisme $\varphi : \mathrm{GL}_n(\mathbf{Z}) \to \mathrm{GL}_n(\mathbf{Z}/3\mathbf{Z})$ obtenu par réduction modulo 3 des coefficients des matrices est injectif. Soit m l'ordre d'un élément M de $\ker(\varphi)$. Si $m \neq 1$, soit p un nombre premier divisant m. On a alors $(M^{m/p})^p = I_n$ et $(M^{m/p})^p \equiv I_n \pmod 3$. La question e) entraîne $M^{m/p} = I_n$, ce qui contredit la définition de l'ordre. On a donc $m = 1$ et $M = I_n$. La restriction $\varphi|_G$ est donc injective. Le groupe G est alors isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbf{Z}/3\mathbf{Z})$ qui, étant fini, n'a qu'un nombre fini de sous-groupes.

g) N'y a-t-il qu'un nombre fini de classes d'isomorphisme de sous-groupes finis de $\mathrm{GL}_n(\mathbf{R})$?

Non : il existe des sous-groupes finis de $\mathrm{GL}_2(\mathbf{R})$ (donc aussi de $\mathrm{GL}_n(\mathbf{R})$) d'ordre arbitrairement grand, comme les groupes diédraux D_m.