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. Donner la liste de tous les groupes abéliens d'ordre 500.

Exercice 2. Soit G un groupe fini d'ordre $2n$, avec n impair.

a) Montrer que G contient un élément d'ordre 2.

b) Montrer que l'image du morphisme injectif $G \hookrightarrow \mathfrak{S}_{2n}$ donné par le théorème de Cayley (ex. I.2.3 du poly) n'est pas contenue dans $\mathfrak{A}_{2n}$.

c) En déduire que G contient un sous-groupe distingué d'indice 2.

Exercice 3. a) Soit G un groupe fini simple. Écrivons $|G| = p^\alpha m$, avec $p \nmid m$, $m \geq 2$ et $\alpha \geq 1$, et notons s le nombre de ses p-Sylow. Montrer que $|G|$ divise $s!$.

b) Montrer qu'il n'existe pas de groupe simple de cardinal 10 000 000.

Exercice 4. a) Montrer que pour $n \geq 3$, le groupe dérivé $D(\mathrm{SL}(n, \mathbf{Z}))$ est $\mathrm{SL}(n, \mathbf{Z})$ (*Indication :* c'est une conséquence directe d'une propriété vue en cours).

b) Soit p un nombre premier. Montrer que la réduction modulo p des coefficients d'une matrice induit un morphisme de groupes $\mathrm{SL}(n, \mathbf{Z}) \to \mathrm{SL}(n, \mathbf{Z}/p\mathbf{Z})$ qui est surjectif (*Indication :* c'est une conséquence directe d'une propriété vue en cours).

On rappelle (inutile de le redémontrer) que le groupe $\mathrm{SL}(2, \mathbf{Z})$ *est engendré par les matrices* $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *et* $R := \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

c) Montrer que le groupe dérivé $D(\mathrm{SL}(2, \mathbf{Z}))$ est d'indice ≤ 12 dans $\mathrm{SL}(2, \mathbf{Z})$ (*Indication :* on pourra calculer S^2, S^4, R^3 et R^6).

d) Montrer que $\mathrm{SL}(2, \mathbf{Z})$ a un quotient d'ordre 2 et un quotient d'ordre 3.

e) En déduire que l'indice de $D(\mathrm{SL}(2, \mathbf{Z}))$ dans $\mathrm{SL}(2, \mathbf{Z})$ est 6 ou 12.

Exercice 5. a) Rappeler pourquoi chacun des groupes alternés $\mathfrak{A}_3$, $\mathfrak{A}_4$ et $\mathfrak{A}_5$ est un quotient d'un groupe $\mathrm{SL}(2, \mathbf{F}_p)$ pour un certain p.

b) Soit H un sous-groupe distingué d'un groupe fini G. Montrer que la collection de facteurs simples de G est la réunion de la collection des facteurs simples de H et de la collection des facteurs simples de G/H.

c) Montrer que pour $m \geq 6$, le groupe $\mathfrak{A}_m$ n'est un quotient d'aucun groupe $\mathrm{SL}(2, \mathbf{F}_p)$.

Exercice 6. Soit p un nombre premier. On considère le groupe G des bijections de $\mathbf{F}_p$ du type $x \mapsto ax + b$, avec $a \in \mathbf{F}_p^*$ et $b \in \mathbf{F}_p$. Il opère fidèlement sur l'ensemble $\mathbf{F}_p = \{0, \ldots, p-1\}$, ce qui en fait un sous-groupe de $\mathfrak{S}_p$.

a) Quel est le cardinal de G ?

b) On note $\tau \in G$ la translation $x \mapsto x + 1$. Quelle est la nature de la permutation de $\mathbf{F}_p$ correspondante ?

c) Quels sont les p-Sylow de G ?

d) Montrer que G opère transitivement sur $\mathbf{F}_p$.

e) Montrer que G est un groupe résoluble.

f) Soit g un élément de $\mathfrak{S}_p$ tel que $g\tau g^{-1} \in G$; montrer $g \in G$.

T.S.V.P.

Soit H un sous-groupe résoluble *de $\mathfrak{S}_p$ qui opère transitivement sur $\{0, \dots, p-1\}$. Le but de la fin de l'exercice est de montrer que H est conjugué à un sous-groupe de G.*

Soit $H = H_0 \rhd H_1 \rhd \cdots \rhd H_r = \{e\}$ une suite de sous-groupes emboîtés où chaque groupe H_i/H_{i+1} est abélien d'ordre premier.

g) Montrer que les groupes $H_0, \dots, H_{r-1}$ agissent transitivement sur $\mathbf{F}_p$, puis que H_{r-1} est d'ordre p.

h) Soit τ' un générateur de H_{r-1}. Montrer qu'il existe $g \in \mathfrak{S}_p$ tel que $\tau' = g\tau g^{-1}$.

i) Conclure $H \leq gGg^{-1}$ (*Indication :* on pourra utiliser f)).

Corrigé du partiel Algèbre 1

Responsable : Mr O. DEBARRE

Exercice 1. *Donner la liste de tous les groupes abéliens d'ordre 500.*

Un tel groupe s'écrit de façon unique comme $\mathbf{Z}/d_1\mathbf{Z} \times \cdots \times \mathbf{Z}/d_r\mathbf{Z}$, avec $1 < d_1 \mid \cdots \mid d_r$ et $d_1 \cdots d_r = 500$. En particulier, $d_1^r \mid 500 = 2^2 5^3$ et $r \leq 3$. Si $r = 3$, $d_1 = 5$ et on obtient $(\mathbf{Z}/5\mathbf{Z})^2 \times \mathbf{Z}/20\mathbf{Z}$ et $\mathbf{Z}/5\mathbf{Z} \times (\mathbf{Z}/10\mathbf{Z})^2$. Si $r = 2$, soit $d_1 = 2$ et on obtient $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/250\mathbf{Z}$, soit $d_1 = 5$ et on obtient $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/100\mathbf{Z}$, soit $d_1 = 10$ et on obtient $\mathbf{Z}/10\mathbf{Z} \times \mathbf{Z}/50\mathbf{Z}$. Si $r = 1$, obtient $\mathbf{Z}/500\mathbf{Z}$, soit au total 6 groupes différents.

Exercice 2. *Soit G un groupe fini d'ordre $2n$, avec n impair.*

a) Montrer que G contient un élément d'ordre 2.

Cela résulte des théorèmes de Sylow. On peut aussi adapter la démonstration du lemme de Cauchy (exerc. I.2.11) : si G ne contient élément d'ordre 2, $G - \{e\}$ est réunion disjoint des parties $\{g, g^{-1}\}$, qui ont toutes 2 éléments, donc son cardinal est impair ; contradiction.

b) Montrer que l'image du morphisme injectif $G \hookrightarrow \mathfrak{S}_{2n}$ donné par le théorème de Cayley (ex. I.2.3) n'est pas contenue dans $\mathfrak{A}_{2n}$.

Soit $g \in G$ d'ordre 2. La permutation de G associée est produit de n transpositions à supports disjoints, dont la signature est $(-1)^n = -1$.

c) En déduire que G contient un sous-groupe distingué d'indice 2.

On prend l'image inverse de $\mathfrak{A}_{2n}$ par $G \hookrightarrow \mathfrak{S}_{2n}$.

Exercice 3. *a) Soit G un groupe fini simple. Écrivons $|G| = p^\alpha m$, avec $p \nmid m$, $m \geq 2$ et $\alpha \geq 1$, et notons s le nombre de ses p-Sylow. Montrer que $|G|$ divise $s!$.*

Le groupe G opère transitivement sur l'ensemble à s éléments de ses p-Sylow. Si $s = 1$, il y a un seul p-Sylow ; il est distingué donc égal à G puisque celui-ci est simple ; cela contredit $m \geq 2$. Si $s > 1$, le noyau de l'application $G \to \mathfrak{S}_s$ donnée par l'action est distinct de G, donc est trivial puisque G est simple. Donc G est un sous-groupe de $\mathfrak{S}_s$ et son cardinal divise $s!$.

b) Montrer qu'il n'existe pas de groupe simple de cardinal 10 000 000.

Le cardinal est $2^7 5^7$. Prenons $p = 5$. Par le théorème de Sylow, le nombre s de 5-Sylow divise 2^7, donc est 1, 2, 4, 8, 16, 32, 64 ou 128. Il est aussi > 1 et $\equiv 1 \pmod 5$, donc c'est 16. Mais $2^7 5^7$ ne divise pas 16! puisque la puissance maximale de 5 qui divise ce dernier est 3.

Exercice 4. *a) Montrer que pour $n \geq 3$, le groupe dérivé $D(\mathrm{SL}(n, \mathbf{Z}))$ est $\mathrm{SL}(n, \mathbf{Z})$.*

Il suffit d'utiliser le fait que pour $n \geq 3$, toute matrice élémentaire est un commutateur (§ II.2.2) et que ces matrices élémentaires engendrent $\mathrm{SL}(n, \mathbf{Z})$ (th. I.4.2).

b) Soit p un nombre premier. Montrer que la réduction modulo p des coefficients d'une matrice induit un morphisme de groupes $\mathrm{SL}(n, \mathbf{Z}) \to \mathrm{SL}(n, \mathbf{Z}/p\mathbf{Z})$ qui est surjectif.

Si $M \in \mathrm{SL}(n, \mathbf{Z})$, le déterminant de sa réduction modulo p est encore 1 car l'expression du déterminant est la même quel que soit le corps. La réduction modulo p d'un produit est bien le produit des réductions car l'expression du produit de deux matrices est la même quel que soit le corps.

Toute matrice élémentaire $I_n + E_{ij}$ de $\mathrm{SL}(n, \mathbf{Z}/p\mathbf{Z})$ est l'image de la matrice $I_n + E_{ij} \in \mathrm{SL}(n, \mathbf{Z})$. Comme les matrices élémentaires engendrent $\mathrm{SL}(n, \mathbf{Z}/p\mathbf{Z}) = \mathrm{SL}(n, \mathbf{F}_p)$ (th. II.2.2), le morphisme est surjectif.

c) Montrer que le groupe dérivé $D(\mathrm{SL}(2, \mathbf{Z}))$ est d'indice ≤ 12 dans $\mathrm{SL}(2, \mathbf{Z})$.

On calcule $S^2 = R^3$ et $S^4 = R^6 = I_2$. Tout élément de $\mathrm{SL}(2, \mathbf{Z})/D(\mathrm{SL}(2, \mathbf{Z}))$ s'écrit donc comme la classe de $S^a R^b$, avec $0 \leq a \leq 1$ et $0 \leq b \leq 5$, soit au plus 12 éléments.

d) Montrer que $\mathrm{SL}(2, \mathbf{Z})$ a un quotient d'ordre 2 et un quotient d'ordre 3.

Il a un quotient d'ordre 2, via $\mathrm{SL}(2, \mathbf{Z}) \twoheadrightarrow \mathrm{SL}(2, \mathbf{Z}/2\mathbf{Z}) \simeq \mathfrak{S}_3 \twoheadrightarrow \{\pm 1\}$ et un quotient d'ordre 3 via $\mathrm{SL}(2, \mathbf{Z}) \twoheadrightarrow \mathrm{SL}(2, \mathbf{Z}/3\mathbf{Z}) \twoheadrightarrow \mathrm{PSL}(2, \mathbf{Z}/3\mathbf{Z}) \simeq \mathfrak{A}_4 \twoheadrightarrow \mathbf{Z}/3\mathbf{Z}$, donc son indice est divisible par 6.

e) En déduire que l'indice de $D(\mathrm{SL}(2, \mathbf{Z}))$ dans $\mathrm{SL}(2, \mathbf{Z})$ est 6 ou 12.

Les quotients de la question précédente sont abéliens, donc ce sont aussi des quotients de $\mathrm{SL}(2, \mathbf{Z})/D(\mathrm{SL}(2, \mathbf{Z}))$. Le cardinal de ce groupe est donc divisible par 2 et par 3 (on peut montrer que c'est 12 ; voir note 5 du poly).

Exercice 5. *a) Rappeler pourquoi chacun des groupes alternés $\mathfrak{A}_3$, $\mathfrak{A}_4$ et $\mathfrak{A}_5$ est un quotient d'un groupe $\mathrm{SL}(2, \mathbf{F}_p)$ pour un certain p.*

On a vu en cours que le groupe $\mathfrak{A}_3 = \mathbf{Z}/3\mathbf{Z}$ est un quotient de $\mathrm{PSL}(2, \mathbf{F}_3) = \mathfrak{A}_4$ (par le groupe de Klein), donc de $\mathrm{SL}(2, \mathbf{F}_3)$; on a aussi $\mathfrak{A}_4 \simeq \mathrm{PSL}(2, \mathbf{F}_3)$ et $\mathfrak{A}_5 \simeq \mathrm{PSL}(2, \mathbf{F}_5)$.

b) *Soit H un sous-groupe distingué d'un groupe fini G. Montrer que la collection de facteurs simples de G est la réunion de la collection des facteurs simples de H et de la collection des facteurs simples de G/H.*

Soit $G/H = K_0 \rhd K_1 \rhd \cdots \rhd K_r = \{e\}$ une suite de composition pour le groupe G/H. On la remonte en une suite de composition $G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = H$ avec $G_i/H = K_i$, donc $K_i/K_{i+1} = (G_i/H)/(G_{i+1}/H) \simeq G_i/G_{i+1}$. On complète par une suite de composition $H = H_0 \rhd H_1 \rhd \cdots \rhd H_s = \{e\}$, d'où une suite de composition

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_r = H = H_0 \rhd H_1 \rhd \cdots \rhd H_s = \{e\}$$

dont les facteurs simples sont les K_i/K_{i+1}, puis les H_j/H_{j+1}.

c) *Montrer que pour $m \geq 6$, le groupe $\mathfrak{A}_m$ n'est un quotient d'aucun groupe* $\mathrm{SL}(2, \mathbf{F}_p)$.

Si on a une surjection $\mathrm{SL}(2, \mathbf{F}_p) \twoheadrightarrow \mathfrak{A}_m$, comme $\mathfrak{A}_m$ est simple, c'est un facteur simple de $\mathrm{SL}(2, \mathbf{F}_p)$ par b). De plus, pour des raisons de cardinaux, on a $p \geq 7$.

Pour $p \geq 7$, regardons les facteurs simples de $\mathrm{SL}(2, \mathbf{F}_p)$: on a une suite

$$\mathrm{SL}(2, \mathbf{F}_p) \rhd Z(\mathrm{SL}(2, \mathbf{F}_p)) = \{\pm I_2\} \rhd \{I_2\}$$

dont les quotients (simples) sont $\mathrm{PSL}(2, \mathbf{F}_p)$ et $\mathbf{Z}/2\mathbf{Z}$.

Donc, par b), la seule possibilité est que $\mathfrak{A}_m$ soit isomorphe à $\mathrm{PSL}(2, \mathbf{F}_p)$. En comparant les cardinaux, on obtient $m! = p(p^2-1)$, donc $p \mid m!$ et $p \leq m$. Si $p = m$, on a $(p-2)! = p+1$ et on trouve facilement que $p = m = 5$; si $p+1 = m$, on obtient $(p-2)! = 1$ et $p = 3$, $m = 4$; si $p+2 \leq m$, c'est impossible.

Exercice 6. *Soit p un nombre premier. On considère le groupe G des bijections de $\mathbf{F}_p$ du type $x \mapsto ax+b$, avec $a \in \mathbf{F}_p^*$ et $b \in \mathbf{F}_p$. Il opère fidèlement sur l'ensemble $\mathbf{F}_p = \{0, \ldots, p-1\}$, ce qui en fait un sous-groupe de $\mathfrak{S}_p$.*

a) Quel est le cardinal de G ?

C'est $p(p-1)$.

b) On note $\tau \in G$ la translation $x \mapsto x+1$. Quelle est la nature de la permutation de $\mathbf{F}_p$ correspondante ?

C'est le p-cycle $(0, \ldots, p-1)$.

c) Quels sont les p-Sylow de G ?

Un de ces p-Sylow est $\langle\tau\rangle$. Ils sont tous conjugués, mais $\langle\tau\rangle$ est distingué, donc c'est le seul.

d) Montrer que G opère transitivement sur $\mathbf{F}_p$.

Étant donnés $x, y \in \{0, \ldots, p-1\}$, on a $\tau^{y-x}(x) = y$.

e) Montrer que G est un groupe résoluble.

Le groupe $\langle\tau\rangle$ est abélien distingué et le quotient est isomorphe à $(\mathbf{F}_p^*, \times)$, abélien, donc G est résoluble.

f) Soit g un élément de $\mathfrak{S}_p$ tel que $g\tau g^{-1} \in G$; montrer $g \in G$.

On écrit $g\tau g^{-1}(x) = ax+b$ avec $a \neq 0$; alors, $(g\tau g^{-1})^{p-1}(x) = a^{p-1}x + (a^{p-2} + \cdots + a + 1)b$. On a $a^{p-1} = 1$; si $a \neq 1$, on a aussi $a^{p-2} + \cdots + a + 1 = \frac{a^{p-1}-1}{a-1} = 0$, donc $g\tau^{p-1}g^{-1} = (g\tau g^{-1})^{p-1} = \mathrm{Id}$ et $\tau^{p-1} = \mathrm{Id}$, absurde.

On a donc $a = 0$ et $g\tau g^{-1} = \tau^b$ pour un certain b. Mais on peut aussi utiliser c) : le groupe $\langle g\tau g^{-1}\rangle$ est un p-Sylow, donc c'est $\langle\tau\rangle$ et $g\tau g^{-1} \in \langle\tau\rangle$.

On a donc $g(x+1) = g\tau(x) = \tau^b g(x) = g(x) + b$, et $g(x) = g(0) + bx$, donc $g \in G$.

Soit H un sous-groupe résoluble *de $\mathfrak{S}_p$ qui opère transitivement sur $\{0, \ldots, p-1\}$. Soit $H = H_0 \rhd H_1 \rhd \cdots \rhd H_r = \{e\}$ une suite de sous-groupes emboîtés où chaque groupe H_i/H_{i+1} est abélien d'ordre premier.*

g) Montrer que les groupes $H_0, \ldots, H_{r-1}$ agissent transitivement sur $\mathbf{F}_p$, puis que H_{r-1} est d'ordre p.

On montre par récurrence sur i que H_i agit transitivement. Si c'est le cas avec $i \leq r-1$, prenons $x, y \in \mathbf{F}_p$; il existe $g \in H_i$ avec $y = gx$. On a $H_{i+1}y = H_{i+1}gx = g(g^{-1}H_{i+1}g)x = gH_{i+1}x$ (puisque $H_{i+1} \lhd H_i$), donc les H_{i+1}-orbites ont toutes même cardinal. Comme la réunion disjointes des orbites est $\mathbf{F}_p$, ce cardinal divise p, et il est > 1 puisque $H_{i+1} \neq \{e\}$ (on a supposé $i \leq r-1$) et que G opère fidèlement. Ces orbites ont donc cardinal p, ce qui signifie que H_{i+1} agit transitivement.

Le groupe H_{r-1} est d'ordre premier ; mais il opère transitivement sur un ensemble de cardinal p, donc $p \mid |H_{r-1}|$ et il y a égalité.

h) Soit τ' un générateur de H_{r-1}. Montrer qu'il existe $g \in \mathfrak{S}_p$ tel que $\tau' = g\tau g^{-1}$.

Les permutations τ et τ' sont des p-cycles. Elles sont donc conjuguées dans $\mathfrak{S}_p$.

i) Conclure $H \leq gGg^{-1}$.

Montrons par récurrence descendante sur i que $H_i \leq gGg^{-1}$.

On a $H_{r-1} = \langle\tau'\rangle < gGg^{-1}$. Supposons $H_i \leq gGg^{-1}$ et soit $h \in H_{i-1}$; comme $\tau' \in H_i$ et $H_i \lhd H_{i-1}$, on a $h\tau'h^{-1} \in H_i \leq gGg^{-1}$, donc $g^{-1}hg\tau(g^{-1}hg)^{-1} = g^{-1}h\tau'h^{-1}g \in G$. Le f) donne $g^{-1}hg \in G$, donc $h \in gGg^{-1}$. On a bien montré $H_{i-1} \leq gGg^{-1}$.