Partiel Algèbre 1

Responsable : O. DEBARRE

Important : vous avez droit de consulter le polycopié et d'utiliser sans démonstration ses résultats (mis pas ceux des exercices ou des TD, sauf mention explicite du contraire).

Exercice 1. Soit n un entier > 0 et soit p un nombre premier $> n/2$. Soit G un sous-groupe de $\mathfrak{S}_n$ opérant transitivement sur l'ensemble $\{1, \dots, n\}$ et contenant une transposition et un p-cycle. Le but de l'exercice est de montrer $G = \mathfrak{S}_n$.

Si $a, b \in \{1, \dots, n\}$, on écrit $a \sim b$ si $a = b$, ou si $a \neq b$ et que la transposition (ab) est dans G.

a) Montrer que $\sim$ est une relation d'équivalence sur l'ensemble $\{1, \dots, n\}$.

b) Si $a \sim b$ et $g \in G$, montrer $g(a) \sim g(b)$.

c) Montrer que toutes les classes d'équivalence pour $\sim$ ont le même cardinal r et que $r \geqslant 2$.

d) Soit s le nombre de classes d'équivalence pour $\sim$. Montrer $n = rs$ et $r \geqslant p$. Conclure.

Exercice 2. Soit G un groupe. On dit qu'un sous-groupe K de G est *caractéristique* si, pour tout automorphisme f de G, on a $f(K) = K$.

a) Montrer que tout sous-groupe caractéristique de G est distingué dans G.

b) Montrer que le groupe de Klein $(\mathbf{Z}/2\mathbf{Z})^2$ a un sous-groupe distingué qui n'est pas caractéristique.

c) Montrer que le groupe dérivé $D(G)$ est un sous-groupe caractéristique de G.

d) Soit H un sous-groupe caractéristique de G et soit K un sous-groupe caractéristique de H. Montrer que K est un sous-groupe caractéristique de G.

e) Soit G un groupe résoluble fini non trivial. Montrer qu'il existe un p-sous-groupe abélien non trivial caractéristique de G.

Exercice 3. a) Soient A et B des groupes abéliens finis. On suppose que pour chaque entier m, le nombre d'éléments de A d'ordre m est égal au nombre d'éléments de B d'ordre m. Montrer que les groupes A et B sont isomorphes.

b) Montrer par un exemple que la conclusion de a) ne subsiste pas si on ne suppose plus l'un des groupes finis A et B abélien (on pourra utiliser le groupe des matrices 3×3 unipotentes triangulaires supérieures à coefficients dans $\mathbf{F}_3$).

Exercice 4. a) Soient H et K des sous-groupes distingués d'un groupe fini G. On suppose que les ordres $|H|$ et $|K|$ sont premiers entre eux. Montrer que $HK := \{hk \mid h \in H, k \in K\}$ est un sous-groupe de G isomorphe à $H \times K$.

b) Montrer que tout groupe d'ordre 35 est cyclique.

c) Soit N un sous-groupe distingué d'un groupe fini G, soit p un nombre premier divisant $|N|$ et soit S un p-sous-groupe de Sylow de N. Si S est distingué dans N, montrer qu'il est aussi distingué dans G.

Dans toute la suite, on note G un groupe d'ordre 105 et, pour chaque $p \in \{3, 5, 7\}$, on note n_p le nombre de p-sous-groupes de Sylow de G.

d) Quelles sont, selon le théorème de Sylow, les valeurs possibles de n_3, n_5 et n_7 ?

e) Montrer qu'on a $n_5 = 1$ ou $n_7 = 1$.

f) Montrer que G contient un sous-groupe N d'ordre 35.

g) Montrer que N est distingué dans G.

h) En déduire $n_5 = n_7 = 1$.

i) Montrer que G est isomorphe à un produit $H \times \mathbf{Z}/5\mathbf{Z}$, où H est un sous-groupe de G d'ordre 21.

j) Montrer qu'il n'y a, à isomorphisme près, que deux groupes d'ordre 105 (*on pourra utiliser sans démonstration les résultats du TD sur le produit semi-direct*).

Corrigé du partiel Algèbre 1

Responsable : Mr O. DEBARRE

Exercice 1. *Soit n un entier > 0 et soit p un nombre premier $> n/2$. Soit G un sous-groupe de $\mathfrak{S}_n$ opérant transitivement sur l'ensemble $\{1, \dots, n\}$ et contenant une transposition et un p-cycle. Le but de l'exercice est de montrer $G = \mathfrak{S}_n$.*

Si $a, b \in \{1, \dots, n\}$, on écrit $a \sim b$ si $a = b$, ou si $a \neq b$ et que la transposition (ab) est dans G.

a) Montrer que $\sim$ est une relation d'équivalence sur l'ensemble $\{1, \dots, n\}$.

Cette relation est clairement réflexive et symétrique. Pour montrer qu'elle est transitive, il suffit de prendre a, b et c distincts avec (ab) et (bc) dans G, et de montrer que (ac) est aussi dans G. Cela résulte de l'égalité $(ac) = (bc)(ab)(bc)$.

b) Si $a \sim b$ et $g \in G$, montrer $g(a) \sim g(b)$.

Si $a = b$, c'est évident. Si $a \neq b$, cela résulte de $(g(a)g(b)) = g(ab)g^{-1}$.

c) Montrer que toutes les classes d'équivalence pour $\sim$ ont le même cardinal r et que $r \geqslant 2$.

Si $a \in \{1, \dots, n\}$, l'application $b \mapsto g(b)$ envoie la classe d'équivalence de a sur celle de $g(a)$. Cette application est bijective puisque son inverse est $c \mapsto g^{-1}(c)$. Les classes d'équivalence de a et de $g(a)$ ont donc le même cardinal. Comme G opère transitivement, toutes les classes d'équivalence ont le même cardinal, r. Si G contient la transposition (ab), la classe de a contient b, donc $r \geqslant 2$.

d) Soit s le nombre de classes d'équivalence pour $\sim$. Montrer $n = rs$ et $r \geqslant p$. Conclure.

Soit X l'ensemble des classes d'équivalence. Son cardinal est s et on a $n = rs$ par c). Comme G opère sur X (en envoyant la classe de a sur celle de $g(a)$; c'est bien défini par b)), on a un morphisme de groupes $u : G \to \mathrm{Bij}(X)$. Le cardinal $s!$ de $\mathrm{Bij}(X)$ n'est pas divisible par p (puisque $s = n/r \leqslant n/2 < p$), donc le p-cycle σ de G est dans le noyau de u. Pour tout $a \in \{1, \dots, n\}$, on a donc $\sigma(a) \sim a$, donc $r \geqslant p > n/2$. On en déduit $r = n$: il y a une seule classe d'équivalence, donc G contient toutes les transpositions et $G = \mathfrak{S}_n$.

Exercice 2. *Soit G un groupe. On dit qu'un sous-groupe K de G est* caractéristique *si, pour tout automorphisme f de G, on a $f(K) = K$.*

a) Montrer que tout sous-groupe caractéristique de G est distingué dans G.

Il suffit d'appliquer la définition aux automorphismes de conjugaison $f(x) = gxg^{-1}$.

b) Montrer que le groupe de Klein $(\mathbf{Z}/2\mathbf{Z})^2$ a un sous-groupe distingué qui n'est pas caractéristique.

L'application qui échange les deux facteurs est un automorphisme du groupe, mais elle ne laisse pas invariant $(\mathbf{Z}/2\mathbf{Z}) \times \{0\}$, qui est pourtant distingué puisque $(\mathbf{Z}/2\mathbf{Z})^2$ est abélien.

c) Montrer que le groupe dérivé $D(G)$ est un sous-groupe caractéristique de G.

La preuve est dans le polycopié : si f est un automorphisme de G, on a $f([g, g']) = [f(g), f(g')]$ pour tous $g, g' \in G$. L'image par f d'un commutateur est donc un commutateur, d'où $f(D(G)) \subset D(G)$. On obtient l'inclusion inverse en remplaçant f par f^{-1}.

d) Soit H un sous-groupe caractéristique de G et soit K un sous-groupe caractéristique de H. Montrer que K est un sous-groupe caractéristique de G.

Soit f un automorphisme de G. Puisque H est caractéristique dans G, on a $f(H) = H$, donc f induit par restriction un automorphisme $f|_H$ de H. Comme K est caractéristique dans H, on a $f|_H(K) = K$, donc $f(K) = K$. Cela montre que K est caractéristique dans G.

e) Soit G un groupe résoluble fini non trivial. Montrer qu'il existe un p-sous-groupe abélien non trivial caractéristique de G.

Par c) et d), $G_m := D^m(G)$ est caractéristique dans G pour tout m. Si n est tel que $H = D_n(G) \neq \{e\}$ et $D_{n+1}(G) = \{e\}$, le groupe H est abélien non trivial. Si p est un diviseur premier de $|H|$, le groupe H a un unique p-Sylow, qui est donc caractéristique dans H, et aussi dans G par d). C'est le sous-groupe de G cherché.

Exercice 3. *a) Soient A et B des groupes abéliens finis. On suppose que pour chaque entier m, le nombre d'éléments de A d'ordre m est égal au nombre d'éléments de B d'ordre m. Montrer que les groupes A et B sont isomorphes.*

Il suffit de reprendre la preuve du cours. En se limitant au sous-groupe $T_p(A)$ des éléments dont l'ordre est une puissance de p, on est ramené à montrer que dans l'écriture $T_p(A) = \mathbf{Z}/p^{\alpha_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{\alpha_s}\mathbf{Z}$, où $\alpha_1 \leqslant \cdots \leqslant \alpha_s$, les α_j sont complètement déterminés par A.

Considérons, pour chaque entier $i > 0$, le sous-groupe $T_{p,i} = \{x \in A \mid p^i x = 0\}$ de $T_p(A)$. On a $|T_{p,i}| = \prod_{\alpha_j \leqslant i} p^{\alpha_j} \prod_{\alpha_j > i} p^j$ et en particulier $|T_{p,i+1}/T_{p,i}| = p^{\mathrm{Card}\{j \mid \alpha_j > i\}}$. On récupère ainsi les exposants α_j à partir des sous-groupes $T_{p,i}$, complètement déterminés par les nombres d'éléments de A d'ordre donné, puisque $T_{p,i} = \bigsqcup_{0 \leqslant j \leqslant i} \{x \in A \mid \mathrm{ord}(x) = p^j\}$.

b) Montrer par un exemple que la conclusion de a) ne subsiste pas si on ne suppose plus l'un des groupes finis A et B abélien (on pourra utiliser le groupe des matrices 3×3 unipotentes triangulaires supérieures à coefficients dans $\mathbf{F}_3$).

Le groupe (non abélien) A des matrices 3×3 unipotentes triangulaires supérieures à coefficients dans $\mathbf{F}_3$ est d'ordre 3^3. Une telle matrice s'écrit $M = I_3 + N$, avec $N^3 = 0_3$, donc $M^3 = I_3 + 3N + 3N^2 = I_3$, puisqu'on est en caractéristique 3. Tout élément de A autre que I_3 est d'ordre 3 ; il y a donc 26 éléments d'ordre 3 et un élément d'ordre 1. Ces nombres sont les mêmes pour le groupe $B = (\mathbf{Z}/3\mathbf{Z})^3$, qui n'est pourtant pas isomorphe à A, puisque B est abélien.

Exercice 4. *a) Soient H et K des sous-groupes distingués d'un groupe fini G. On suppose que les ordres $|H|$ et $|K|$ sont premiers entre eux. Montrer que $HK := \{hk \mid h \in H, k \in K\}$ est un sous-groupe de G isomorphe à $H \times K$.*

L'ordre du groupe $H \cap K$ divise les ordres de H et K, donc $H \cap K$ est trivial. Si $h \in H$ et $k \in K$, on a $[h,k] = (hkh^{-1})k^{-1} \in K$ et de même, $[h,k] = h(kh^{-1}k^{-1}) \in H$, donc $[h,k] = e$ et $hk = kh$. Ceci entraîne que l'application $H \times K \to HK$, $(h,k) \mapsto hk$ est un isomorphisme de groupes.

b) Montrer que tout groupe d'ordre 35 est cyclique.

Le théorème de Sylow entraîne que dans un tel groupe G, il y a un unique 5-Sylow S_5 et un unique 7-Sylow S_7. Ils sont tous les deux distingués dans G et la question précédente entraîne $G \simeq S_5 \times S_7 \simeq \mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/7\mathbf{Z} \simeq \mathbf{Z}/35\mathbf{Z}$.

c) Soit N un sous-groupe distingué d'un groupe fini G, soit p un nombre premier divisant $|N|$ et soit S un p-sous-groupe de Sylow de N. Si S est distingué dans N, montrer qu'il est aussi distingué dans G.

Comme S est distingué dans N, c'est le seul p-Sylow de N. Pour tout $g \in G$, on a $gSg{-}1 \leq gNg^{-1} = N$ et $|gSg{-}1| = |S|$, de sorte que gSg^{-1} est un p-Sylow de N. C'est donc S, ce qui montre que S est distingué dans G.

Dans toute la suite, on note G un groupe d'ordre 105 et, pour chaque $p \in \{3,5,7\}$, on note n_p le nombre de p-sous-groupes de Sylow de G.

d) Quelles sont, selon le théorème de Sylow, les valeurs possibles de n_3, n_5 et n_7 ?

On a $n_3 = 1$ ou 7, $n_5 = 1$ ou 21, et $n_7 = 1$ ou 15.

e) Montrer qu'on a $n_5 = 1$ ou $n_7 = 1$.

Sinon, on a $n_5 = 21$ et $n_7 = 15$. Deux 5-Sylow s'intersectent trivialement, donc on a $4 \times 21 = 84$ éléments d'ordre 5 et de même, $6 \times 15 = 90$ éléments d'ordre 7. Comme $84 + 90 > |G|$, c'est impossible.

f) Montrer que G contient un sous-groupe N d'ordre 35.

Si $n_5 = 1$, le 5-Sylow S_5 est distingué et G/S_5 est d'ordre 21, donc contient un 7-Sylow, dont l'image inverse dans G est d'ordre 35. De même, si $n_7 = 1$, le 7-Sylow S_7 est distingué et G/S_7 est d'ordre 15, donc contient un 5-Sylow, dont l'image inverse dans G est d'ordre 35.

g) Montrer que N est distingué dans G.

Cela résulte du fait que son indice est le plus petit nombre premier divisant $|G|$. Dans le cas présent, on peut facilement le redémontrer : on a un morphisme de groupes $u : G \to \mathrm{Bij}(G/N)$ qui envoie g sur la bijection $g'N \mapsto gg'N$ de l'ensemble à 3 éléments G/N. Si $g \in \mathrm{Ker}(u)$, on a en particulier $gN = N$ donc $g \in N$; donc $\mathrm{Ker}(u) \subset N$. D'autre part, l'indice de $\mathrm{Ker}(u)$, qui est > 1, divise $|\mathrm{Bij}(G/N)| = 6$ et $|G| = 105$, donc c'est 3 et $N = \mathrm{Ker}(u)$ est distingué dans G.

h) En déduire $n_5 = n_7 = 1$.

Comme N est abélien (question b)), un 5-Sylow de N est distingué dans N donc dans G (question c)), de sorte que $n_5 = 1$. On montre de la même façon $n_7 = 1$.

i) Montrer que G est isomorphe à un produit $H \times \mathbf{Z}/5\mathbf{Z}$, où H est un sous-groupe de G d'ordre 21.

On vient de montrer qu'il y a un unique 5-Sylow S_5 et un unique 7-Sylow S_7, tous les deux distingués dans G et cycliques. Si S_3 est un 3-Sylow, $H = S_3S_7$ est donc un sous-groupe de G d'ordre 21. Il agit par conjugaison sur le sous-groupe distingué S_5, ce qui induit un morphisme de groupes $H \to \mathrm{Aut}(S_5) \simeq \mathbf{Z}/4\mathbf{Z}$ qui est trivial pour des raisons de cardinaux. Cela signifie que tout élément de H commute avec tout élément de S_5. Comme dans la question a), cela entraîne que l'application $H \times S_5 \to G$, $(h,s) \mapsto hs$ est un isomorphisme.

j) Montrer qu'il n'y a, à isomorphisme près, que deux groupes d'ordre 105.

Il suffit de montrer qu'il n'y a, à isomorphisme près, que deux groupes d'ordre 21. Le théorème de Sylow entraîne que dans un tel groupe H, il y a un unique 7-Sylow S_7 (distingué) et, soit un unique 3-Sylow, auquel cas le groupe est isomorphe à $\mathbf{Z}/21\mathbf{Z}$ par a), soit 7 3-Sylow. Si S_3 est l'un d'eux, on a $H \simeq S_7 \rtimes S_3$, où le produit semi-direct est défini par un morphisme $\mathbf{Z}/3\mathbf{Z} \simeq S_3 \to \mathrm{Aut}(S_7) \simeq \mathbf{Z}/6\mathbf{Z}$. L'image d'un tel morphisme est unique (engendrée par la classe de 2) et il y a deux tels morphismes : l'un envoie $\bar{1}$ sur $\bar{2}$, l'autre $\bar{1}$ sur $\bar{4}$. Le second est le composé du premier par l'automorphisme $x \mapsto 2x$ de $\mathbf{Z}/3\mathbf{Z}$. Les produits semi-directs sont donc isomorphes.