GROUPES ET ANNEAUX 2
CORRIGÉ DE L'EXAMEN DU 24 MAI 2024

Exercice 1 (2+4 pts)**.** Soit $H < G$ un sous-groupe d'un groupe G. On considère l'action par translation à gauche de G sur l'ensemble G/H.

(i) Montrer que, pour tout $g \in G$, le stabilisateur $\mathrm{st}(gH)$ coïncide avec gHg^{-1}.

(ii) Soit $H' < G$ un autre sous-groupe de G. Montrer que les G-ensembles G/H et G/H' sont isomorphes si et seulement si H et H' sont conjugués.

Solution. (i) $g' \in \mathrm{st}(gH) \Leftrightarrow g'gH = gH \Leftrightarrow g'gHg^{-1} = gHg^{-1} \Leftrightarrow g' \in gHg^{-1}$.

(ii) Montrons que $G/H \cong G/H' \Leftrightarrow \exists\, g \in G \; gHg^{-1} = H'$.

($\Leftarrow$) $G/H' = G/gHg^{-1} = G/\,\mathrm{st}(gH) \cong \mathrm{orb}(gH) = G/H$ grâce au point (i).

($\Rightarrow$) Soit $\varphi : G/H \to G/H'$ un isomorphisme, et soit $gH = \varphi^{-1}(H')$. Montrons que $gHg^{-1} = H'$.

($\supset$) $\forall\, h' \in H' \; \varphi(h'gH) = h'\varphi(gH) = h'H' = H' = \varphi(gH)$. Comme φ est injectif, alors $\forall\, h' \in H' \; h'gH = gH$. En particulier, $\forall\, h' \in H' \;\; \exists\, h \in H \; h'g = gh$. De manière équivalente, $\forall\, h' \in H' \;\; \exists\, h \in H \; h' = ghg^{-1}$. Cela signifie que $gHg^{-1} \supset H'$.

($\subset$) $\forall\, h \in H \; H' = \varphi(gH) = \varphi(ghH) = \varphi(ghg^{-1}gH) = ghg^{-1}H'$. De manière équivalente, $\forall\, h \in H \; ghg^{-1} \in H'$. Cela signifie que $gHg^{-1} \subset H'$. ☐

Exercice 2 (4+2+2 pts)**.** Soit A un anneau. Par définition, le *nilradical de* A est le sous-ensemble $\mathrm{N}(A) = \{x \in A \mid \exists\, m \in \mathbb{N} \; x^m = 0\} \subset A$, et le *radical de Jacobson de* A est le sous-ensemble $\mathrm{J}(A) = \{x \in A \mid \forall\, a \in A \; 1 - ax \in A^\times\} \subset A$.

(i) Montrer que $\mathrm{N}(A)$ et $\mathrm{J}(A)$ sont des idéaux de A.

(ii) Montrer que, si $I \subset A$ est un idéal premier, alors $\mathrm{N}(A) \subset I$.

(iii) Montrer que, si $I \subset A$ est un idéal maximal, alors $\mathrm{J}(A) \subset I$.

Solution. On rappelle que, afin de montrer qu'un sous-ensemble I d'un anneau A est un idéal, il suffit de montrer qu'il n'est pas vide, qu'il est clos par l'addition, et qu'il absorbe la multiplication. En effet, la dernière propriété implique en particulier que I est un sous-groupe additif, car il absorbe la multiplication par $-1 \in A$.

(i) Tout d'abord, $0^1 = 0$, donc $0 \in \mathrm{N}(A)$. Ensuite, si $x, y \in \mathrm{N}(A)$, alors ils existent $m, n \in \mathbb{N}$ tels que $x^m = 0$ et $y^n = 0$. Par conséquent,

$$(x+y)^{m+n-1} = \sum_{k=0}^{m+n-1} \binom{m+n-1}{k} x^{m+n-k-1} y^k = 0,$$

car $k < n$ implique $m+n-k-1 \geqslant m$, donc $x+y \in \mathrm{N}(A)$. Pour terminer, si $a \in A$ et $x \in \mathrm{N}(A)$, alors il existe $m \in \mathbb{N}$ tel que $x^m = 0$. Cela implique $(ax)^m = a^m x^m = 0$, donc $ax \in \mathrm{N}(A)$.

Tout d'abord, $1 - a \cdot 0 = 1 \in A^\times$ pour tout $a \in A$, donc $0 \in \mathrm{J}(A)$. Ensuite, si $x, y \in \mathrm{J}(A)$, alors $1 - ax, 1 - by \in A^\times$ pour tout $a, b \in A$. Par conséquent,

$$1 - a(x+y) = (1 - ax) - ay = (1 - ax)\left(1 - \frac{a}{(1 - ax)} y\right) \in A^\times$$

pour tout $a \in A$, donc $x + y \in \mathrm{J}(A)$. Pour terminer, si $a \in A$ et $x \in \mathrm{J}(A)$, alors $1 - bx \in A^\times$ pour tout $b \in A$. Cela implique $1 - abx \in A^\times$ pour tout $b \in A$, donc $ax \in \mathrm{J}(A)$.

(*ii*) Si $x \in \mathrm{N}(A)$, alors il existe $m \in \mathbb{N}$ tel que $x^m = 0$. Comme I est premier, A/I est intègre, donc $(x+I)^m = x^m + I = I$ implique $x \in I$.

(*iii*) Si $x \notin I$, alors $x + I \in (A/I)^\times$, car A/I est un corps. Il existe donc $y \in A$ tel que $(x+I)(y+I) = xy + I = 1 + I$. On a alors qu'il existe $y \in A$ tel que $1 - xy \in I$. Mais $I \cap A^\times = \varnothing$, car I est maximal, donc $x \notin \mathrm{J}(A)$. □

Exercice 3 (2+4+4+2 pts)**.** Soit G un groupe d'ordre 255. Le but de cet exercice est de montrer que G est cyclique.

(*i*) Montrer que G admet un sous-groupe distingué $K \lhd G$ d'ordre 17.

(*ii*) Montrer que G admet un sous-groupe $H < G$ d'ordre 15. *Indication :* montrer que G admet un sous-groupe d'ordre 3 et un d'ordre 5, et que l'un des deux est forcement distingué.

(*iii*) Montrer que $G \cong K \times H$. *Indication :* montrer d'abord que $G = K \rtimes H$, et ensuite que l'action par conjugaison de H sur K est triviale.

(*iv*) Montrer que tout groupe H d'ordre 15 est cyclique.

Solution. Soit $\mathrm{Syl}_p(G)$ l'ensemble des p-Sylows de G pour tout $p \in \mathbb{N}$ premier, et soit $n_p = |\mathrm{Syl}_p(G)|$.

(*i*) D'après les théorèmes de Sylow, on sait que $n_{17} \mid 15$ et $n_{17} \equiv 1 \pmod{17}$, donc $n_{17} = 1$. En d'autres termes, G admet un unique 17-Sylow K, qui est distingué et d'ordre 17.

(*ii*) D'après les théorèmes de Sylow, on sait que $n_3 \mid 85$ et $n_3 \equiv 1 \pmod 3$, donc $n_3 \in \{1, 85\}$. Similairement, $n_5 \mid 51$ et $n_5 \equiv 1 \pmod 5$, donc $n_5 \in \{1, 51\}$. Si $n_3 = 85$, alors G contient $2 \cdot 85 = 170$ éléments d'ordre 3 distincts. Si $n_5 = 51$, alors G contient $4 \cdot 51 = 204$ éléments d'ordre 5 distincts. Ces deux conditions ne peuvent pas être satisfaites au même temps, car $170 + 204 > 255 = |G|$. Soit donc P un 3-Sylow, et Q un 5-Sylow. Comme $|P \cap Q| \mid \mathrm{pgcd}(|P|, |Q|) = \mathrm{pgcd}(3,5) = 1$, alors le sous-groupe $H = PQ$ satisfait

$$|H| = \frac{|P||Q|}{|P \cap Q|} = \frac{3 \cdot 5}{1} = 15.$$

(*iii*) Comme avant, $|K \cap H| \mid \mathrm{pgcd}(|K|, |H|) = \mathrm{pgcd}(17, 15) = 1$, ce qui implique $K \cap H = \{e\}$. De plus,

$$|KH| = \frac{|K||H|}{|K \cap H|} = \frac{17 \cdot 15}{1} = 255,$$

donc $KH = G$. On déduit que $G = K \rtimes H$.

H agit par conjugaison sur K. Comme il s'agit d'une action par homomorphisme, on obtient un morphisme de groupes

$$\begin{aligned} \rho : H &\to \mathrm{Aut}(K) \\ h &\mapsto h\_h^{-1} \end{aligned}$$

Comme $|\mathrm{Aut}(K)| = 16$, et comme $\mathrm{pgcd}(|H|, |\mathrm{Aut}(K)|) = \mathrm{pgcd}(15, 16) = 1$, cette action est triviale, c'est-à-dire $hkh^{-1} = k$ pout tout $h \in H$ et $k \in K$. En d'autres termes,

$$\begin{aligned} K \times H &\to G \\ (k, h) &\mapsto kh \end{aligned}$$

est un isomorphisme de groupes.

(*iv*) Comme 3 et 5 sont deux nombres premiers avec $3 < 5$ et $5 \not\equiv 1 \pmod 3$, l'Exercice 6 du TD3 (ou alors le Théorème 2.6.7 du cours) nous permet de conclure. □