GROUPES ET ANNEAUX 2
CORRIGÉ DU CONTRÔLE CONTINU N°2

Exercice 1. Soit G un groupe, $K \lhd G$ un sous-groupe distingué, et $H < G$ un sous-groupe.

(i) Montrer que $G = K \rtimes H \Leftrightarrow$ la projection canonique $\pi : G \to G/K$ se restreint à un isomorphisme entre H et G/K.

(ii) Montrer que, si $G = K \rtimes H$, alors tout sous-groupe $K < L < G$ vérifie $L = K \rtimes (H \cap L)$.

Solution. On rappelle que $G = K \rtimes H$ signifie $K \cap H = \{e\}$ et $KH = G$.

(i) $\Rightarrow$) Par définition, $\ker \pi = K$. Comme, par hypothèse, $K \cap H = \{e\}$, on déduit que la restriction de π à H est injective. De plus, comme chaque élément de G est de la forme kh avec $k \in K$ et $h \in H$, il suit que la restriction de π à H est surjective.

$\Leftarrow$) Si $h \in K \cap H$, alors $\pi(h) = hK = eK$, et puisque la restriction de la projection canonique $\pi : G \to G/K$ à H est injective, alors $h = e$. Cela montre que $K \cap H = \{e\}$. Ensuite, pour tout $g \in G$, comme la restriction de $\pi : G \to G/K$ à H est surjective, il existe $h \in H$ tel que $\pi(g) = \pi(h)$. On déduit que $Kg = Kh$, donc il existe $k \in K$ tel que $g = kh$. Cela montre que $KH = G$.

(ii) Comme $K \lhd G$ et $K < L$, on déduit que $K \lhd L$. Montrons alors que la projection canonique $\pi : L \to L/K$ se restreint à un isomorphisme entre $H \cap L$ et L/K. Comme $K \cap H = \{e\}$, alors $\ker \pi \cap (H \cap L) = K \cap H \cap L \subset K \cap H = \{e\}$, et on déduit que la restriction de π à $H \cap L$ est injective. De plus, tout $\ell \in L$ est de la forme $\ell = kh$ avec $k \in K$ et $h \in H$, ce qui implique que $h = k^{-1}\ell \in H \cap L$. Il suit que la restriction de π à $H \cap L$ est surjective. □

Exercice 2. Soit I un idéal d'un anneau A.

(i) Montrer que, si I est un idéal premier, alors, pour tout idéaux I_1 et I_2 de A, on a que $I_1 I_2 \subset I$ implique $I_1 \subset I$ ou $I_2 \subset I$.

(ii) Montrer que, si I n'est pas un idéal premier, alors ils existent deux idéaux $I_1 \neq I \neq I_2$ de A satisfaisant $I_1 I_2 \subset I \subset I_1 \cap I_2$.

Solution. On rappelle que $I \subset A$ est premier si et seulement si, pour tout $x, y \in A$, on a que $xy \in I$ implique $x \in I$ ou $y \in I$.

(i) Supposons $I_1 I_2 \subset I$, et montrons que $I_1 \not\subset I \Rightarrow I_2 \subset I$. Soit $x \in I_1 \smallsetminus I$. Pour tout $y \in I_2$, on a $xy \in I_1 I_2 \subset I$. Comme I est premier, on déduit que $y \in I$.

(ii) Comme I n'est pas premier, alors il existent $x, y \in A \smallsetminus I$ tels que $xy \in I$. Si on pose $I_1 := (x) + I$ et $I_2 := (y) + I$, alors

$$\begin{aligned} I_1 I_2 &= \left\{ \sum_{i=1}^{n} (a_i x + b_i)(c_i y + d_i) \;\middle|\; n \in \mathbb{N}, a_i, b_i \in A, c_i, d_i \in I \right\} \\ &= \left\{ \sum_{i=1}^{n} a_i c_i xy + a_i d_i x + b_i c_i y + b_i d_i \;\middle|\; n \in \mathbb{N}, a_i, b_i \in A, c_i, d_i \in I \right\}. \end{aligned}$$

Alors $I_1 I_2 \subset I$, car I absorbe la multiplication. De plus, $I \subset (x) + I$ et $I \subset (y) + I$, donc $I \subset I_1 \cap I_2$. □

Exercice 3. Soit G un groupe d'ordre 150. En utilisant les théorèmes de Sylow, montrer que G n'est pas simple (on rappelle que, par définition, un groupe G est simple si ses seuls sous-groupes distingués sont $\{e\}$ et G).

Solution. Pour commencer, on remarque que $|G| = 150 = 2 \cdot 3 \cdot 5^2$. Soit alors $\mathrm{Syl}_5(G)$ l'ensemble des 5-Sylows de G, et soit $n_5 = |\mathrm{Syl}_5(G)|$. D'après les théorèmes de Sylow, on sait que :

(*i*) G agit transitivement (par conjugaison) sur $\mathrm{Syl}_5(G)$;

(*ii*) $n_5 \mid 2 \cdot 3 = 6$;

(*iii*) $n_5 \equiv 1 \pmod 5$.

Cela implique que $n_5 \in \{1, 6\}$. Étudions donc ces deux cas. D'une part, si $n_5 = 1$, alors $\mathrm{Syl}_5(G) = \{P_5\}$ et $P_5 \lhd G$. Comme $|P_5| = 5^2 = 25$, on trouve ainsi un sous-groupe distingué de G non trivial. D'autre part, si $n_5 = 6$, alors on obtient une action $\rho : G \to \mathfrak{S}_{\mathrm{Syl}_5(G)} \cong \mathfrak{S}_6$. Mais $|G| = 150 \not| \, 720 = 6! = |\mathfrak{S}_6|$. Donc ρ ne peut pas être injectif. Il ne peut pas être trivial non plus, car l'action de G sur $\mathrm{Syl}_5(G)$ est transitive. On déduit alors que $\{e\} \neq \ker \rho \neq G$, et comme $\ker \rho \lhd G$, on peut conclure. □

Exercice 4. Construire un corps avec exactement 27 éléments. *Indication :* Utiliser le fait que, si $\Bbbk$ est un corps, alors, pour tout polynôme $P(X) \in \Bbbk[X]$ de degré $n > 0$, l'anneau $A = \Bbbk[X]/(P(X))$ est un espace vectoriel de dimension n sur $\Bbbk$, et que A est un corps si et seulement si $P(X)$ est irréductible.

Solution. Comme vu en TD, un polynôme $P(X) \in \Bbbk[X]$ de degré $n \in \{2, 3\}$ est irréductible dans $\Bbbk[X]$ si et seulement si il n'a pas de racines dans $\Bbbk$. Il suffit alors de trouver un polynôme $P(X) \in \mathbb{F}_3[X]$ de degré 3 qui n'admet aucune racine dans $\mathbb{F}_3$. Si on considère par exemple $P(X) = X^3 - X + 1$, alors

$$0^3 - 0 + 1 = 1, \qquad 1^3 - 1 + 1 = 1, \qquad 2^3 - 2 + 1 \equiv 1 \pmod 3,$$

donc $P(X)$ n'a pas de racines dans $\mathbb{F}_3$. □