Théorie des groupes

Corrigé contrôle continu 1

12 Octobre 2015

Exercice 1 Énoncer et prouver la formule des indices.

Correction : Voir cours

Exercice 2 Répondre par « vrai » ou « faux »à la question suivante. *Répondre « vrai » implique que vous donniez une preuve complète et valide de l'assertion ; répondre « faux » implique que vous donniez une preuve complète et valide de la négation de l'assertion proposée*.

Soient G, H deux groupes non triviaux. Soit $\alpha\colon G \to \mathrm{Aut}(H)$ un morphisme de groupes. Le produit semi-direct $G \rtimes_\alpha H$ n'est pas un groupe simple.

Correction : Petite coquille : C'était $H \rtimes_\alpha G$.

Vrai.

$K = \{(h, e) \mid h \in H\}$ est toujours propre et distingué.

$\alpha(e) = Id_H$, donc K est isomorphe à H, donc est bien un sous-groupe propre.

Soient $(h_1, g_1) \in H \rtimes_\alpha G$, et $(h, e) \in K$.

$(h_1, g_1)(h, e)(h_1, g_1)^{-1} = (h_1\alpha(g_1)(h)\alpha(g_1)(\alpha(g_1^{-1})(h^{-1})), e) \in K$. Donc $K \lhd H \rtimes_\alpha G$.

Exercice 3 Soit G un groupe d'ordre 4. On suppose que G n'est pas cyclique.

1. Montrer que tous les éléments de G sont d'ordre 1 ou 2.
2. Montrer que G est abélien.
3. Montrer que G est isomorphe au produit direct de deux de ses sous-groupes.
4. En déduire la classification des groupes d'ordre 4. *Une classification est une liste de groupes non-isomorphes 2 à 2 telle que tout groupe d'ordre 4 soit isomorphe à un des groupes de cette liste.*

Correction :

1. Par le théorème de Lagrange, l'ordre d'un élément divise l'ordre du groupe, donc peut être 1,2 ou 4. Si G possède un élément d'ordre 4, cet élément engendre G, qui serait donc cyclique. Absurde. Donc l'ordre d'un élément est 1 ou 2.
2. Soient g et h dans G.
   $g.h \in G$, donc est d'ordre 1 ou 2. Dans tous les cas, $(g.h)^2 = e$. En multipliant à droite par $h^{-1}.g^{-1}$, on a $g.h = h^{-1}.g^{-1}$.
   h et g étant d'ordre 1 ou 2, ils sont leur propre inverse, d'où $g.h = h.g$.
3. Soient a, b et c les trois éléments distincts d'ordre 2 de G. On a :
   - $< a > \cap < b >= e$
   - $a.b = c$ (Une autre valeur pour ce produit serait absurde), donc $< a >< b >= G$.
   - G est abélien, donc les éléments de $< a >$ commutent avec ceux de $< b >$.
   On peut donc appliquer le théorème d'isomorphie à un produit direct pour écrire que $G \simeq < a > \times < b >$.
4. Soit G un groupe d'ordre 4. Distinguons deux cas :
   Si G est cyclique, il est isomorphe à $\mathbb{Z}/4\mathbb{Z}$.
   Sinon, on est dans le cas des premières questions, et g est isomorphe au produit de deux groupes d'ordre 2. Il n'y a à isomorphisme près qu'un seul groupe d'ordre 2, qui est $\mathbb{Z}/2\mathbb{Z}$. D'où $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
   A isomorphisme près, les seuls groupes d'ordre 4 sont donc $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 4 Soit G un groupe ayant exactement 2 sous-groupes propres (c'est à dire distincts de G et $\{e\}$).

1. Montrer que G est fini.
2. Montrer que G est monogène.
3. En déduire que G est cyclique d'ordre pq ou p^3 avec p et q des nombres premiers distincts.

Correction : Notons H_1 et H_2 les deux sous-groupes propres de G

1. Pour tout x dans G, $ordre(x)$ est fini. Sinon, $< x >$ serait isomorphe à $\mathbb{Z}$ et admettrait une infinité de sous-groupes disjoints. Ce qui est absurde.
   On a que $G = \cup_{x \in G} < x >$. Comme G a exactement 4 sous-groupes, il s'agit d'une union d'au plus 4 ensembles finis, donc G est fini.
2. On note $r = min\left\{i \mid \exists (x_1, x_2, \ldots, x_i) \in G^i, G =< x_1, x_2, \ldots, x_i >\right\}$. r est donc le cardinal minimal d'une famille génératrice, et existe bien car G est fini.
   Montrons que $r = 1$.
   On suppose que $r \geq 2$:
   Soit $X = \{x_1, x_2, \ldots, x_r\}$ un ensemble générateur minimal. Pour tout i, $< x_i >$ est propre. En effet, si $< x_i >= G$, alors $r = 1$, ce qui est absurde. Si $< x_i >= \{e\}$, alors $X \setminus \{x_i\}$ est un ensemble générateur de G, ce qui est absurde par minimalité de r.
   — Si $r \geq 3$, tous les $< x_i >$ étant propres, ils sont soit H_1 soit H_2. Donc au moins 2 d'entre eux sont les mêmes. Donc au moins un des x_i est une puissance d'un x_j avec $j \neq i$. Donc $X \setminus \{x_i\}$ est un ensemble générateur de G, ce qui est absurde par minimalité de r.
   — Donc $r = 2$. On alors que $< x_1 > \neq < x_2 >$. On pose $y = x_1 x_2$. $< y >$ est propre (sinon on contredit la minimalité de r). Donc $< y >=< x_1 >$ ou $< y >=< x_2 >$.
   Si $< y >=< x_1 >$, on a $x_1 x_2 = x_1^k$ avec $k \neq 0$, et $x_2 = x_1^{k-1} \in < x_1 >$, ce qui est absurde. De même, si $< y >=< x_2 >$, on a $x_1 \in < x_2 >$, ce qui est absurde.
   Notre hypothèse est donc fausse, d'où $r = 1$, ce qui signifie que g est monogène.
3. Soit g tel que $G =< g >$. On note n l'ordre de G. Soit $n = \prod_{i=1}^{s} p_i^{\alpha_i}$ une décomposition de n en facteurs premiers. (avec les $\alpha_i \geq 1$)
   — Si $s \geq 3$, alors les sous-groupes $< g^{n/p_1} >$, $< g^{n/p_2} >$, $< g^{n/p_3} >$ sont trois sous-groupes propres d'ordre distincts (respectivement d'ordres p_1, p_2 et p_3), donc sont distincts. Absurde. Donc $s < 3$.
   — Si $s = 2$, alors $n = p^{\alpha_1} q^{\alpha_2}$. Supposons que $\alpha_1 \geq 2$. Alors $< g^p >$, $< g^{p^2} >$ et $< g^q >$ sont trois sous-groupes propres d'ordre distincts (respectivement d'ordres pq,q et p). Absurde. Donc $\alpha_1 = 1$. Par symétrie, on a aussi $\alpha_2 = 1$, et donc $n = pq$.
   — Si $s = 1$, $n = p^\alpha$.
   On ne peut pas avoir $\alpha = 1$, car $\mathbb{Z}/p\mathbb{Z}$ n'a pas de sous-groupe propre.
   Si $\alpha = 2$, G ne contient qu'un sous-groupe propre, qui est $< g^p >$. En effet, si H est un sous-groupe propre, il ne peut contenir un élément g^k avec k premier avec p^2 car ce sont des générateurs de G. Donc H contient un élément g^{kp} avec $k \neq 0$, donc contient tout $< g^p >$.
   Si $\alpha > 3$, alors $< g^p >$, $< g^{p^2} >$ et $< g^{p^3} >$ sont trois sous-groupes propres distincts.
   D'où $n = p^3$.
   On a donc bien montré que les seules possibilités pour G sont d'être cycliques d'ordre pq ou p^3 avec p et q des nombres premiers distincts.