(Extrait du partiel 2007)
Corrigé.

On considère un groupe cyclique $A = \langle a \rangle$ engendré par un élément a d'ordre 11 et un groupe cyclique $B = \langle b \rangle$ engendré par un élément b d'ordre 5. Les groupes A et B sont notés multiplicativement.

a) Montrer qu'il existe un automorphisme f du groupe A tel que $f(a) = a^4$. Quel est l'ordre de f dans le groupe $Aut(A)$? Montrer qu'il existe un homomorphisme $\phi : B \to Aut(A)$ tel que $\phi(b) = f$.

Montrer de même qu'il existe un homomorphisme $\psi : B \to Aut(A)$ tel que, si l'on pose $g = \psi(b)$, on ait $g(a) = a^5$.

Trouver un automorphisme β du groupe B tel que $\phi = \psi \circ \beta$.

A est un groupe cyclique engendré par a. Donc, pour tout élément x du groupe A, il existe un unique endomorphisme de A qui envoie a sur x. Notons f l'endomorphisme qui envoie a sur a^4. Par ailleurs, a est d'ordre 11. Comme 4 et 11 sont premiers entre eux, a^4 est aussi un générateur de A. Donc, l'homomorphisme de groupes f de A dans A défini par $f(a) = a^4$ est surjectif, et comme A est un groupe fini, c'est un automorphisme de A.

L'ordre de f est le plus petit entier $k > 0$ tel que $f^k = Id_A$, c'est donc le plus petit entier $k > 0$ tel que $f^k(a) = a$. Or, on a $f^2(a) = f(f(a)) = f(a^4) = (a^4)^4 = a^{4^2}$. Plus généralement, on montre, par une récurrence immédiate, que pour tout entier $k \geq 1$, on a $f^k(a) = a^{4^k}$. On en déduit que l'ordre de f dans le groupe $Aut(A)$ est le plus petit entier $k \geq 1$ tel que $a^{4^k} = a$. Or $a^{4^k} = a \Leftrightarrow 4^k = 1 \bmod 11$, donc l'ordre de f est l'ordre de $\overline{4}$ dans le groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^\times$. L'ordre de f est donc 5 car, dans $\mathbb{Z}/11\mathbb{Z}$, on a $\overline{4}^2 = \overline{16} = \overline{5}$, $\overline{4}^3 = \overline{4} \times \overline{5} = \overline{20} = \overline{9}$, $\overline{4}^4 = \overline{9} \times \overline{4} = \overline{36} = \overline{3}$ et $\overline{4}^5 = \overline{4} \times \overline{3} = \overline{12} = \overline{1}$.

Puisque $B = \langle b \rangle$ est un groupe cyclique d'ordre 5 et que f est un élément d'ordre 5 du groupe $Aut(A)$, il existe un unique homomorphisme de groupes $\phi : B \to Aut(A)$ tel que $\phi(b) = f$.

On peut appliquer le raisonnement précédent à a^5 au lieu de a^4. En effet, d'une part, 5 est premier avec 11, et, d'autre part, l'ordre de $\overline{5}$ dans le groupe multiplicatif $(\mathbb{Z}/11\mathbb{Z})^\times$ est encore 5 (en effet, on a $\overline{5} = \overline{4}^2$, or $\overline{4}$ est d'ordre 5, et 2 est premier avec 2). Il existe donc un unique homomorphisme $\psi : B \to Aut(A)$ tel que, si l'on pose $g = \psi(b)$, on ait $g(a) = a^5$.

Un endomorphisme β de B est défini par la donnée de $\beta(b) = b^k$, où $0 \leq k \leq 4$. C'est un automorphisme si et seulement si b^k est un générateur de B, c'est-à-dire, si et seulement si $k \neq 0$. Comme B est engendré par b, légalité $\phi = \psi \circ \beta$ est équivalente à $\phi(b) = (\psi \circ \beta)(b)$. Or $\phi(b) = f$, et $(\psi \circ \beta)(b) = \psi(b^k) = \psi(b)^k = g^k$. On cherche donc k tel que $1 \leq k \leq 4$ et $f = g^k$. Maintenant, comme A est engendré par a, l'égalité $f = g^k$ est équivalente à $f(a) = g^k(a)$, c'est-à-dire à $a^4 = a^{5^k}$, ou encore à $\overline{4} = \overline{5}^k$ dans $\mathbb{Z}/11\mathbb{Z}$. Or $\overline{5}^3 = \overline{125} = \overline{4}$, on obtient donc la solution (unique) $k = 3$. En résumé, l'automorphisme β de B défini par $\beta(b) = b^3$ vérifie la condition $\phi = \psi \circ \beta$.

b) On considère les produits semi-directs $G = A \rtimes_\phi B$ et $H = A \rtimes_\psi B$. On note respectivement $*_\phi$ et $*_\psi$ la multiplication dans G et la multiplication dans H. Pour $(x, y) \in A \times B$ et $(x', y') \in A \times B$, rappeler la définition des produits $(x, y) *_\phi (x', y')$ et $(x, y) *_\psi (x', y')$ (on notera ϕ_y et ψ_y les images respectives de y par ϕ et par ψ).

Démontrer que l'application $\alpha : (x, y) \to (x, \beta(y))$ est un isomorphisme du groupe G sur le groupe H.

Par définition, on a $(x, y) *_\phi (x', y') = (x\phi_y(x'), yy')$ et $(x, y) *_\psi (x', y') = (x\psi_y(x'), yy')$. On a donc, d'une part,

$$\alpha((x, y) *_\phi (x', y')) = \alpha(x\phi_y(x'), yy') = (x\phi_y(x'), \beta(yy'))$$

et d'autre part,

$$\alpha((x, y)) *_\psi \alpha((x', y')) = (x, \beta(y)) *_\psi (x', \beta(y')) = (x\psi_{\beta(y)}, \beta(y)\beta(y'))$$

Les deux résultats obtenus sont égaux car la relation $\phi = \psi \circ \beta$ entraîne que $\phi_y = \psi_{\beta(y)}$ et on a $\beta(yy') = \beta(y)\beta(y')$. Ainsi, on a $\alpha((x, y) *_\phi (x', y')) = \alpha((x, y)) *_\psi \alpha((x', y'))$, ce qui prouve que α est un homomorphisme de groupes. Par ailleurs, l'application α est bijective, d'inverse: $(x, y) \to (x, \beta^{-1}(y))$, donc α est un isomorphisme de G vers H.