

Exercice 5.12 Soit K un groupe cyclique, soit H un groupe arbitraire et soient ϕ_1, ϕ_2 deux morphismes $K \rightarrow \text{Aut}(H)$. Si K est infini, supposons en plus que ϕ_1 et ϕ_2 sont injectifs. Supposons que $\phi_1(K)$ et $\phi_2(K)$ sont conjugués dans $\text{Aut}(H)$: i.e., il existe $\sigma \in \text{Aut}(H)$ tel que $\sigma\phi_1(K)\sigma^{-1} = \phi_2(K)$.

(a) Montrer qu'il existe $a \in \mathbf{Z}$ tel que $\sigma\phi_1(k)\sigma^{-1} = \phi_2(k)^a$ pour tout $k \in K$.

Solution. Soit x un générateur de K . Alors $\phi_2(x)$ est un générateur de $\phi_2(K) = \sigma\phi_1(K)\sigma^{-1}$ et comme $\sigma\phi_1(x)\sigma^{-1} \in \sigma\phi_1(K)\sigma^{-1}$, il existe $a \in \mathbf{Z}$ tel que $\sigma\phi_1(x)\sigma^{-1} = \phi_2(x)^a$. Maintenant si $k \in K$, $k = x^b$ est arbitraire, on a

$$\sigma\phi_1(x^b)\sigma^{-1} = (\sigma\phi_1(x)\sigma^{-1})^b = (\phi_2(x)^a)^b = \phi_2(x^b)^a. \quad \square$$

(b) Montrer que l'application $\psi: H \rtimes_{\phi_1} K \rightarrow H \rtimes_{\phi_2} K$ définie par

$$\psi((h, k)) = (\sigma(h), k^a)$$

est un morphisme.

Solution. Pour tout $h_1, h_2 \in H$, $k_1, k_2 \in K$ on a :

$$\begin{aligned} \psi((h_1, k_1)(h_2, k_2)) &= \psi((h_1\phi_1(k_1)(h_2), k_1k_2)) \\ &= (\sigma(h_1\phi_1(k_1)(h_2)), (k_1k_2)^a) \\ &= (\sigma(h_1)\sigma(\phi_1(k_1)(h_2)), (k_1k_2)^a) \\ &= (\sigma(h_1)\phi_2(k_1^a)(\sigma(h_2)), (k_1k_2)^a) \\ &= (\sigma(h_1), k_1^a)(\sigma(h_2), k_2^a) = \psi((h_1, k_1))\psi((h_2, k_2)). \end{aligned} \quad \square$$

(c) En construisant un inverse montrer que ψ est bijectif et conclure que les groupes $H \rtimes_{\phi_1} K$ et $H \rtimes_{\phi_2} K$ sont isomorphes.

Solution. D'abord supposons que K est fini, d'ordre n . On va montrer que dans (a) on peut choisir a de manière que de plus, $\text{pgcd}(a, n) = 1$. Soit $m = |\phi_1(K)|$ et notons que $m|n$. Notre but est de trouver $a' \in \mathbf{Z}$ tel que $a' \equiv a \pmod{m}$ et $\text{pgcd}(a', n) = 1$. Soient p_1, \dots, p_k les nombres premiers qui divisent n mais pas m . Par le théorème chinois, les congruences $a' \equiv a \pmod{m}$, $a' \equiv 1 \pmod{p_1 \cdots p_k}$ admettent une solution et celle-ci convient. Posons donc $a = a'$. Maintenant soit $b \in \mathbf{Z}$ tel que $ab \equiv 1 \pmod{n}$. Alors $k^{ab} = k$ pour tout $k \in K$.

Définissons l'application $\psi': H \rtimes_{\phi_2} K \rightarrow H \rtimes_{\phi_1} K$ par

$$\psi'((h, k)) = (\sigma^{-1}(h), k^b).$$

Un calcul direct montre que ψ' est un inverse de ψ et ψ est donc bijectif.

Supposons maintenant que ϕ_1 est injectif. L'argument de (a) nous donne qu'il existe $b \in \mathbf{Z}$ qui satisfait

$$\phi_1(k^b) = \sigma^{-1}\phi_2(k)\sigma \quad \text{pour tout } k \in K.$$

En composant cette identité avec celle pour a , on obtient que $\phi_1(k^{ab}) = \phi_1(k)$ pour tout $k \in K$. L'injectivité de ϕ_1 implique que $k^{ab} = k$ pour tout k et on peut conclure en définissant ψ' comme avant. \square

Remarque. L'exercice comme posé n'est pas tout à fait correct. Comme on l'a vu, le fait que a satisfasse (a) n'est pas suffisant pour que ψ soit un isomorphisme et il faut de plus supposer que $\text{pgcd}(a, |K|) = 1$. Ceci ne change en rien la conclusion finale que les groupes $H \rtimes_{\phi_1} K$ et $H \rtimes_{\phi_2} K$ sont isomorphes.