Automorphisms of a non-metacyclic minimal nonabelian p-group, p odd

J. Kurdics kurdics@nyf.hu

Nyíregyháza College, Hungary

23-28 August 2010, Bedlewo (Poland)

Problem: (Y. Berkovich and Z. Janko 2009) Describe the automorphism groups of minimal nonabelian finite p-groups.

Theorem

(L. Rédei 1947) A finite p-group G is a minimal nonabelian group if and only if either it is isomorphic to the quaternion group of order 8, or (A) has the presentation $\langle a, b \mid a^{p^m} = b^{p^n} = 1,\ a^b = a^{1+p^{m-1}} \rangle$, *where* $m \geq 2$, $n \geq 1$, $|G| = p^{m+n}$, *or (B) has the presentation* $\langle a, b \mid a^{p^m} = b^{p^n} = c^p = 1,\ [a, b] = c,\ [a, c] = 1,\ [b, c] = 1 \rangle$, *where* $|G| = p^{m+n+1}$.

Theorem

Let the group H be finitely presented by

$$\langle g_1, \ldots, g_r \,|\, w_1(g_1, \ldots, g_r), \ldots, w_s(g_1, \ldots, g_r)\rangle.$$

Then there is a bijective correspondence between automorphisms of the group H and ordered r-tuples $({g'}_1, \ldots, {g'}_r)$ of elements generating the group H for which all the relations $w_j({g'}_1, \ldots, {g'}_r) = 1$ hold.

Theorem

Consider the linear group $GL(2, p)$ *as the automorphism group of the elementary abelian group* $\langle a\rangle \times \langle b\rangle$ *of type* $C_p \times C_p$. *Let the automorphism* α *be induced by the substitution* $a \mapsto a^t$ *with* t *primitive root modulo* p $(1 < t < p)$ *and* $b \mapsto b$; *the automorphism* β *by the substitution* $a \mapsto a$, $b \mapsto b^t$; *the automorphism* γ *by the substitution* $a \mapsto ab$, $b \mapsto b$; *the automorphism* δ *by the substitution* $a \mapsto a$, $b \mapsto ab$; *and set* $\nu = \delta\gamma^{-1}\delta$. *Then the linear group* $GL(2, p)$ *is presented with generators* α, β, γ *and* δ, *and with generating relations* $|\alpha| = p - 1,\ |\beta| = p - 1,\ |\gamma| = p,\ |\delta| = p,\ \alpha^{-1}\beta\alpha = \beta,\ \alpha^{-1}\gamma\alpha = \gamma^t,\ \alpha^{-1}\delta\alpha = \delta^{\frac{1}{t}},\ \beta^{-1}\gamma\beta = \gamma^{\frac{1}{t}}\ \beta^{-1}\delta\beta = \delta^t,\ \gamma^{-1}\delta\gamma = \delta^{-1}\gamma^{-1}\delta,\ \delta^u\gamma = \alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}},\ \nu^2 = \alpha^{\frac{p-1}{2}}\beta^{\frac{p-1}{2}}\ \nu^{-1}\alpha\nu = \beta$ *where* $\frac{1}{t}$ *is the multiplicative inverse of* t *modulo* p, *an integer between 1 and* p, $1 \leq u \leq p - 2$, $\frac{1}{u+1}$ *is the multiplicative inverse of* $u + 1$ *modulo* p, *an integer between 1 and* p, *and* $t^i \equiv u + 1($mod $p)$ *with* i *an integer between 1 and* p.

Theorem

Consider the automorphism group $Aut(G)$ *with*
$G = \langle a, b \,|\, a^p = b^p = c^p = 1,\ [a, b] = c,\ [a, c] = 1,\ [b, c] = 1\rangle$.
Let the automorphisms α, β, γ *and* δ *be defined analogously as in Theorem 3; the automorphism* η *by the substitution* $a \mapsto ac$, $b \mapsto b$*; the automorphism* θ *by the substitution* $a \mapsto a$, $b \mapsto bc$*; and set* $\nu = \delta\gamma^{-1}\delta$*. Then the group of inner automorphisms is* $Inn(G) = \langle \eta, \theta\rangle$*, the factor-group* $Aut(G)/\,Inn(G)$ *of outer automorphisms is isomorphic to the linear group* $GL(2, p)$*. Furthermore, the automorphism group* $Aut(G)$ *is presented with generators* α, β, γ, δ, η, θ*, and with generating relations*

Theorem

$|\alpha| = p-1,\ |\beta| = p-1,\ |\gamma| = p,\ |\delta| = p,\ \alpha^{-1}\beta\alpha = \beta,\ \alpha^{-1}\gamma\alpha = \eta^{-\frac{t-1}{2}}\gamma^{t},\ \alpha^{-1}\delta\alpha = \delta^{\frac{1}{t}},$
$\beta^{-1}\gamma\beta = \gamma^{\frac{1}{t}},\ \beta^{-1}\delta\beta = \theta^{-\frac{t-1}{2}}\delta^{t},\ \gamma^{-1}\delta\gamma = \delta^{-1}\gamma^{-1}\delta,$
$\delta^{u}\gamma = \alpha^{i}\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}}\theta^{-\frac{u}{u+1}},\ \nu^{2} = \eta\theta\alpha^{\frac{p-1}{2}}\beta^{\frac{p-1}{2}}\ \nu^{-1}\alpha\nu = \beta,\ \eta^{p} = 1,\ \theta^{p} = 1,\ \eta\theta = \theta\eta,\ \alpha^{-1}\eta\alpha = \eta,\ \alpha^{-1}\theta\alpha = \theta^{\frac{1}{t}},\ \beta^{-1}\eta\beta = \eta^{\frac{1}{t}},\ \beta^{-1}\theta\beta = \eta,\quad \gamma^{-1}\eta\gamma = \eta,\quad \gamma^{-1}\theta\gamma = \theta\eta,\ \delta^{-1}\eta\delta = \theta\eta,\quad \delta^{-1}\theta\delta = \theta,$ *where* $\frac{1}{t}$ *is the multiplicative inverse of* t *modulo* p*, an integer between 1 and* p*,* $1 \leq u \leq p-2$*,* $\frac{1}{u+1}$ *is the multiplicative inverse of* $u+1$ *modulo* p*, an integer between 1 and* p*, and* $t^{i} \equiv u+1 \pmod p$ *with* i *an integer between 1 and* p*.*

Theorem

Consider the automorphism group $Aut(C_{p^m} \times C_{p^m})$ $(m > 1)$ of the abelian group $\langle a \rangle \times \langle b \rangle$ of type $C_{p^m} \times C_{p^m}$. Let the automorphism α be induced by the substitution $a \mapsto a^t$ with t primitive root modulo p^m $(1 < t < p^m)$ and $b \mapsto b$; the automorphism β by the substitution $a \mapsto a$, $b \mapsto b^t$; the automorphism γ by the substitution $a \mapsto ab$, $b \mapsto b$; the automorphism δ by the substitution $a \mapsto a$, $b \mapsto ab$; and set $\nu = \delta\gamma^{-1}\delta$. Then the automorphism group $Aut(C_{p^m} \times C_{p^m})$ is of order $p^{4m-3}(p^2-1)(p-1)$, and is presented with generators α, β, γ and δ, and with generating relations

Theorem

$|\alpha| = \varphi(p^m),\ |\beta| = \varphi(p^m),\ |\gamma| = p^m,\ |\delta| = p^m,\ \alpha^{-1}\beta\alpha = \beta,\ \alpha^{-1}\gamma\alpha = \gamma^t,\ \alpha^{-1}\delta\alpha = \delta^{\frac{1}{t}},\ \beta^{-1}\gamma\beta = \gamma^{\frac{1}{t}},\ \beta^{-1}\delta\beta = \delta^t,\ \gamma^{-1}\delta\gamma = \delta^{-1}\gamma^{-1}\delta,\ \delta^u\gamma = \alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}},\ \nu^2 = \alpha^{\frac{\varphi(p^m)}{2}}\beta^{\frac{\varphi(p^m)}{2}},\ \nu^{-1}\alpha\nu = \beta,$
$\delta^{vp-1}\gamma = \alpha^j\beta^{-j}\gamma^{vp-1}\delta^{\frac{vp}{1-vp}}\nu$, *where* $\frac{1}{t}$ *is the multiplicative inverse of* t *modulo* p^m; $1 \leq u \leq p^m - 2$, $\gcd(u+1, p) = 1$, $\frac{1}{u+1}$ *is the multiplicative inverse of* $u+1$ *modulo* p^m, $t^i \equiv u + 1 \pmod{p^m}$; $0 \leq v \leq p^{m-1} - 1$, $t^j \equiv vp - 1 \pmod{p^m}$, $\frac{1}{1-vp}$ *is the multiplicative inverse of* $1 - vp$ *modulo* p^m; *and* $\frac{1}{t}$, i, j, $\frac{1}{u+1}$ *and* $\frac{1}{1-vp}$ *are integers between 1 and* p^m. *Moreover, there is an epimorphism* $Aut(C_{p^m} \times C_{p^m}) \to GL(2, p)$ *with a p-group kernel.*

Theorem

Consider the automorphism group $Aut(G)$ *with*
$G = \langle a, b \mid a^{p^m} = b^{p^m} = c^p = 1,\ [a, b] = c,\ [a, c] = 1,\ [b, c] = 1\rangle$,
$m > 1$. *Then the factor-group* $Aut(G)/\,Inn(G)$ *of outer automorphisms is isomorphic to the group* $Aut(C_{p^m} \times C_{p^m})$.

Theorem

Consider the automorphism group $Aut(C_{p^m} \times C_{p^n})$ $(m > n > 0)$ *of the abelian group* $\langle a \rangle \times \langle b \rangle$ *of type* $C_{p^m} \times C_{p^n}$. *Let the automorphism* α *be induced by the substitution* $a \mapsto a^t$ *with* t *primitive root modulo* p^m $(1 < t < p^m)$ *and* $b \mapsto b$; *the automorphism* β *by the substitution* $a \mapsto a$, $b \mapsto b^t$, *notice that* t *is a primitive root modulo* p^n *also; the automorphism* γ *by the substitution* $a \mapsto ab$, $b \mapsto b$; *the automorphism* δ *by the substitution* $a \mapsto a$, $b \mapsto a^{p^{m-n}}b$. *Then the automorphism group* $Aut(C_{p^m} \times C_{p^n})$ *is of order* $p^{m+3n-2}(p-1)^2$, *and is presented with generators* α, β, γ *and* δ, *and with generating relations*

Theorem

$|\alpha| = \varphi(p^m)$, $|\beta| = \varphi(p^n)$, $|\gamma| = p^n$, $|\delta| = p^n$, $\alpha^{-1}\beta\alpha = \beta$, $\alpha^{-1}\gamma\alpha = \gamma^t$, $\alpha^{-1}\delta\alpha = \delta^{\frac{1}{t}}$, $\beta^{-1}\gamma\beta = \gamma^{\frac{1}{t}}$, $\beta^{-1}\delta\beta = \delta^t$, $\delta^u\gamma = \alpha^i\beta^{-i}\gamma^{up^{m-n}+1}\delta^{\frac{u}{up^{m-n}+1}}$, where $\frac{1}{t}$ is the multiplicative inverse of t modulo p^n, an integer between 1 and p^n, $1 \leq u \leq p^n - 1$, $\frac{1}{up^{m-n}+1}$ is the multiplicative inverse of $up^{m-n}+1$ modulo p^n, an integer between 1 and p^n, and $t^i \equiv up^{m-n}+1 \pmod{p^m}$ with i an integer between 1 and p^m. Moreover, there is a homomorphism $Aut(C_{p^m} \times C_{p^n}) \to GL(2,p)$ with a p-group kernel and a metabelian image. In particular, the group $Aut(C_{p^m} \times C_{p^n})$ is solvable.

Theorem

Consider the automorphism group $Aut(G)$ *with* $G = \langle a, b \,|\, a^{p^m} = b^{p^n} = c^p = 1,\ [a, b] = c,\ [a, c] = 1,\ [b, c] = 1\rangle$, $m > n > 0$. *Then the factor-group* $Aut(G)/\,Inn(G)$ *of outer automorphisms is isomorphic to the group* $Aut(C_{p^m} \times C_{p^n})$.

Relax the asssumption that the prime p is odd.

Theorem

Let A be a finite abelian group, p a prime divisor of its order and P the primary component belonging to the prime p. The automorphism group $Aut(A)$ is solvable if and only if the following statements are satisfied:

(i) *For $p = 2$ the primary component P is of type either C_{2^k}, $C_{2^k} \times C_{2^k}$ or $C_{2^{k_1}} \times C_{2^{k_2}} \times \cdots \times C_{2^{k_r}}$ with $k_1 \geq k_2 \geq \cdots \geq k_r > 0$ $(r > 1)$ such that an exponent k may appear at most twice in the orders of the direct cyclic factors;*

(ii) *For $p = 3$ the primary component P is of type either C_{3^k}, $C_{3^k} \times C_{3^k}$ or $C_{3^{k_1}} \times C_{3^{k_2}} \times \cdots \times C_{3^{k_r}}$ with $k_1 \geq k_2 \geq \cdots \geq k_r > 0$ $(r > 1)$ such that an exponent k may appear at most twice in the orders of the direct cyclic factors;*

(iii) *For $p \geq 5$ the primary component P is of type either C_{p^k}, or $C_{p^{k_1}} \times C_{p^{k_2}} \times \cdots \times C_{p^{k_r}}$ with $k_1 > k_2 > \cdots > k_r > 0$ $(r > 1)$.*