GLASNIK MATEMATIČKI
Vol. 46(66)(2011), 367 – 383

AUTOMORPHISMS OF A MINIMAL NONABELIAN p-GROUP WITH p ODD I

János Kurdics
Nyíregyháza College, Hungary

Abstract. Description of automorphism groups of non-metacyclic minimal nonabelian finite p-groups with $p > 2$ in terms of generators and relations is provided. Furthermore, finite abelian groups with solvable automorphism groups are determined.

1. Introduction

At the end of their paper [1], Yakov Berkovich and Zvonimir Janko posed twenty problems, last of which was the following: Describe the automorphism groups of minimal nonabelian finite p-groups. The aim of this paper and its second part is to provide this description for odd primes p.

In the paper [2] G. Birkhoff gives a generator system for the group of automorphisms of a finite abelian p-group in a way that each of these generators has the effect of substitution of only one basis element. Hence, description of the automorphism group of an abelian finite p-group in terms of generators and relations is reduced to find the relations, which, given the structure invariants, is a complex but straightforward task. A deeper insight into the structure of automorphism groups of finite abelian p-groups reveals more on the structure of the automorphism groups studied, provided in paragraphs 2, 4 and 6. I know of no general information on the structure of the group of automorphisms except for elementary abelian p-groups.[1] As

2010 *Mathematics Subject Classification.* 20D45, 20F28.
Key words and phrases. Group, finite p-group, automorphism, minimal nonabelian group.

[1]Note added in proof: it has just come to my knowledge that certain parts of the results presented below concerning automorphism groups of finite Abelian groups agree with results by *M. Golasiński and G. Goncalves* in Math. Slovaca **58** (2008), 413–438 and by *C.J. Hiller and D.L. Rhea* in Amer. Math. Monthly **114** (2007), 917–922.

a byproduct of these investigations, finite abelian groups possessing solvable automorphism groups will be determined in the last paragraph.

By the result of L. Rédei [5] a finite p-group G ($p = 2$ included) is a minimal nonabelian group (that is, nonabelian with abelian maximal subgroups, A_1-group for short) if and only if either it is isomorphic to the quaternion group of order 8, or (A) has the presentation

$$\langle a, b \,|\, a^{p^m} = b^{p^n} = 1,\ a^b = a^{1+p^{m-1}} \rangle,$$

where $m \geq 2$, $n \geq 1$, $|G| = p^{m+n}$, or (B) has the presentation

$$\langle a, b \,|\, a^{p^m} = b^{p^n} = c^p = 1,\ [a, b] = c,\ [a, c] = 1,\ [b, c] = 1 \rangle,$$

where $|G| = p^{m+n+1}$ and all these groups are of class 2. In what follows, a generator system and generating relations will be determined for the group of automorphisms of 2-generated finite abelian p-groups with $p > 2$ in a way that each of the generator automorphisms has the effect of substitution of only one generator element. On this basis the group of automorphisms of any of the A_1-groups G of type (B) may be described as it will turn out that the group of outer automorphisms for each group G of type (B) is isomorphic to the group of automorphisms of the respective 2-generated finite abelian p-group.

Generally, an automorphism can be viewed as a substitution of generators satisfying the same relations. More precisely:

THEOREM 1.1. *Let the group H be finite, presented by*

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

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.

PROOF. If α is an automorphism of the group, then

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

is again a presentation of the same form as the presentation (*). Conversely, let $(g'_1, \ldots, g'_r)$ be an ordered r-tuple of generators of the group H satisfying all the relations $w_j(g'_1, \ldots, g'_r) = 1$. Then the mapping $g_i \mapsto g'_i$ between the generators extends to an isomorphism between the free groups over the alphabets $\{g_1, \ldots, g_r\}$ and $\{g'_1, \ldots, g'_r\}$, which maps the normal divisor generated by conjugates of the words $w_j(g_1, \ldots, g_r)$ onto the normal divisor generated by conjugates of the words $w_j(g'_1, \ldots, g'_r)$. That is, the mapping $g_i \mapsto g'_i$ between the generators determines an automorphism of the group H. □

2. The linear group $\mathrm{GL}(2,p)$

In what follows we shall frequently use fractional exponents, meant modulo the suitable prime power.

THEOREM 2.1. *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*

$$|\alpha| = p-1,\ |\beta| = p-1,\ |\gamma| = p,\ |\delta| = p, \tag{2.1}$$

$$\alpha^{-1}\beta\alpha = \beta, \qquad \alpha^{-1}\gamma\alpha = \gamma^t, \qquad \alpha^{-1}\delta\alpha = \delta^{\frac{1}{t}}, \tag{2.2}$$

$$\beta^{-1}\gamma\beta = \gamma^{\frac{1}{t}} \qquad \beta^{-1}\delta\beta = \delta^t, \qquad \gamma^{-1}\delta\gamma = \delta^{-1}\gamma^{-1}\delta, \tag{2.3}$$

$$\delta^u\gamma = \alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}}, \qquad \nu^2 = \alpha^{\frac{p-1}{2}}\beta^{\frac{p-1}{2}} \qquad \nu^{-1}\alpha\nu = \beta, \tag{2.4}$$

where $\frac{1}{t}$ is the multiplicative inverse of t modulo p, an integer between 1 and p, $1 \le u \le p-2$, $\frac{1}{u+1}$ 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.

PROOF. Clearly, the group $\mathrm{GL}(2,p)$ is of order $(p^2-1)(p^2-p)$. The relations (2.1) and (2.2_1) are easy to see. Since

$$\alpha^{-1}\gamma\alpha(a) = \alpha^{-1}\gamma(a^t) = \alpha^{-1}(a^tb^t) = ab^t, \qquad \alpha^{-1}\gamma\alpha(b) = b,$$

we have the relation (2.2_2). Furthermore,

$$\alpha^{-1}\delta\alpha(a) = \alpha^{-1}\delta(a^t) = \alpha^{-1}(a^t) = a,$$
$$\alpha^{-1}\delta\alpha(b) = \alpha^{-1}\delta(b) = \alpha^{-1}(ab) = a^{\frac{1}{t}}b,$$

therefore the relation (2.2_3) holds. In an analogous manner we obtain the relations (2.3_1) and (2.3_2). Further,

$$\gamma^{-1}\delta\gamma(a) = \gamma^{-1}\delta(ab) = \gamma^{-1}(a^2b) = (ab^{-1})^2b = a^2b^{-1},$$
$$\gamma^{-1}\delta\gamma(b) = \gamma^{-1}\delta(b) = \gamma^{-1}(ab) = a.$$

On the other hand,

$$\delta^{-1}\gamma^{-1}\delta(a) = \delta^{-1}(ab^{-1}) = a(a^{-1}b)^{-1} = a^2b^{-1} = \gamma^{-1}\delta\gamma(a),$$
$$\delta^{-1}\gamma^{-1}\delta(b) = \delta^{-1}\gamma^{-1}(ab) = \delta^{-1}(a) = a = \gamma^{-1}\delta\gamma(a),$$

and we have the relation (2.3_3). For $1 \le u \le p-2$ we see

$$\delta^u\gamma(a) = a^{u+1}b, \quad \delta^u\gamma(b) = a^ub.$$

On the other hand, let $t^i \equiv u+1 \pmod p$. Then

$$\alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}}(a) = \alpha^i\beta^{-i}(ab^{u+1}) = \alpha^i(ab) = a^{u+1}b = \delta^u\gamma(a),$$

$$\alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}}(b) = \alpha^i\beta^{-i}\gamma^{u+1}(a^{\frac{u}{u+1}}b) =$$

$$\alpha^i\beta^{-i}(a^{\frac{u}{u+1}}b^{u+1}) = \alpha^i(a^{\frac{u}{u+1}}b) = a^ub = \delta^u\gamma(b).$$

The relation (2.4_1) follows.

We prove now that the four automorphisms generate the whole linear group. The subgroup $A = \langle \alpha, \beta\rangle$ is elementary abelian of order $(p-1)^2$, and elements of this subgroup map a to an a-power and b to a b-power, while nonidentity automorphisms in the subgroup $\langle\gamma\rangle$ do not. Hence $A \cap \langle\gamma\rangle = \{1\}$, and by the relations (2.2_2) and (2.3_1), the subgroup $B = \langle A, \gamma\rangle$ is the semidirect product $A \ltimes \langle\gamma\rangle$ of order $p(p-1)^2$, of index $p+1$. Since

$$\alpha^i\beta^j\gamma^k(a) = a^{t^i}b^{t^jk}$$

$(0 \le i \le p-2,\ 0 \le j \le p-2,\ 0 \le k \le p-1)$ equals a only if $i = 0$, $k = 0$, we see that nonidentity automorphisms in the subgroup $\langle\delta\rangle$ are not in the subgroup B, and the subgroup $\langle B, \delta\rangle$ is of order $p^2(p-1)^2$ at least. But the greatest proper divisor of $(p^2-1)(p^2-p)$ is $\frac{p+1}{2}p(p-1)^2$, which is less than $p^2(p-1)^2$, and these four automorphisms generate the whole linear group $\mathrm{GL}(2,p)$ (clearly, by Dickson's theorem [3, Theorem 2.8.4] the matrices corresponding to the automorphisms γ and δ generate the special linear group, and the determinants of the matrices corresponding to the powers α^i take all the $p-1$ values).

The automorphism ν maps a to b^{-1} and b to a. We see that elements of the set $\cup_{i=0}^{p-1} B\delta^i$ map a to an element a^jb^k with j relatively prime to p so the cosets $B\delta^i$ $(0 \le i \le p-1)$ and $B\nu$ are all distinct. There remained to show that these are all the cosets, using relations only. For this aim we need the remaining two relations (2.4_2) and (2.4_3), which are immediate, and imply that, in fact, the automorphisms α, γ and δ generate the whole linear group (remarked already above). By the relation (2.2_3) $B\delta^u\alpha = B\delta^{\frac{u}{t}}$, and by the relations (2.4_2)–(2.4_3) $B\nu\alpha = B\nu$ (clearly, by the relations (2.2_1)–(2.3_2) the automorphism $\alpha\beta$ is central). By the relations (2.4_1) $B\delta^u\gamma = B\delta^{\frac{u}{u+1}}$ $(1 \le u \le p-2)$, by the relation (2.3_3) $\delta^{-1}\gamma = \gamma^{-1}\nu^{-1}$ so $B\delta^{-1}\gamma = B\nu$ and $B\nu\gamma = B\delta$. Again by the relation (2.3_3) $\nu\delta = \gamma^{-1}\nu$ and hence $B\nu\delta = B\nu$. Hence there are no more cosets, the elements δ^i, ν $(i = 0, \dots, p-1)$ form a right transversal to the subgroup B, and the relations (2.1)–(2.4) determine the group operation completely. □

In the course of the proof a permutation representation has been given by means of the relations on the right cosets of the subgroup B (with core the center $\langle\alpha\beta\rangle$).

3. The case of the group $G = \langle a, b \,|\, a^{p^m} = b^{p^n} = c^p = 1,\ [a,b] = c,\ [a,c] = 1,\ [b,c] = 1\rangle$ with $m = n = 1,\ |G| = p^3$

Theorem 3.1. *Consider the automorphism group $Aut(G)$ (with G as in the title). 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 $a \mapsto a$, $b \mapsto ab$; the automorphism η by the substitution $a \mapsto ac$, $b \mapsto b$; and 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*

$$|\alpha| = p-1,\ |\beta| = p-1,\ |\gamma| = p,\ |\delta| = p, \tag{3.1}$$

$$\alpha^{-1}\beta\alpha = \beta, \qquad \alpha^{-1}\gamma\alpha = \eta^{-\frac{t-1}{2}}\gamma^t, \qquad \alpha^{-1}\delta\alpha = \delta^{\frac{1}{t}}, \tag{3.2}$$

$$\beta^{-1}\gamma\beta = \gamma^{\frac{1}{t}}, \qquad \beta^{-1}\delta\beta = \theta^{-\frac{t-1}{2}}\delta^t, \qquad \gamma^{-1}\delta\gamma = \delta^{-1}\gamma^{-1}\delta, \tag{3.3}$$

$$\delta^u\gamma = \alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}}\theta^{-\frac{u}{u+1}}, \quad \nu^2 = \eta\theta\alpha^{\frac{p-1}{2}}\beta^{\frac{p-1}{2}}, \quad \nu^{-1}\alpha\nu = \beta, \tag{3.4}$$

$$\eta^p = 1,\ \theta^p = 1,\ \eta\theta = \theta\eta, \quad \alpha^{-1}\eta\alpha = \eta,\ \alpha^{-1}\theta\alpha = \theta^{\frac{1}{t}},\ \beta^{-1}\eta\beta = \eta^{\frac{1}{t}}, \tag{3.5}$$

$$\beta^{-1}\theta\beta = \eta, \quad \gamma^{-1}\eta\gamma = \eta, \quad \gamma^{-1}\theta\gamma = \theta\eta, \quad \delta^{-1}\eta\delta = \theta\eta, \quad \delta^{-1}\theta\delta = \theta, \tag{3.6}$$

where $\frac{1}{t}$ is the multiplicative inverse of t modulo p, an integer between 1 and p, $1 \le u \le p-2$, $\frac{1}{u+1}$ 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.

Proof. Clearly, the group G is of exponent p now with centre $\langle c\rangle$. Let $G = \langle a', b' \,|\, a'^p = b'^p = 1,\ [a',b'] = c',\ [a',c'] = 1,\ [b',c'] = 1\rangle$ be another presentation. Obviously, for the generators a' and b' we may choose any two noncommuting elements of order p, so there are $(p^3-p)(p^3-p^2) = p^2(p^2-1)(p^2-p)$ choices, which coincides with the order of the automorphism group. Notice that $(p^2-1)(p^2-p)$ is the order of the linear group $\mathrm{GL}(2,p)$.

Put $C = \langle c\rangle$, then the factor-group G/C is elementary abelian of order p^2. The automorphisms α, β, γ and δ act on the factor-group G/C, the induced automorphisms may be viewed as elements of the linear group $\mathrm{GL}(2,p)$ of order $(p^2-1)(p^2-p)$. Hence the group $\langle\alpha, \beta, \gamma, \delta\rangle$ maps homomorphically into the group $\mathrm{GL}(2,p)$ (cf. [4, I.4.3.Satz]). The generating relations (3.1)–(3.4) for the group $\mathrm{Aut}(G)$ are identical to the relations (2.1)–(2.4) of Theorem 2.1 of the previous section but the relations (3.2_2), (3.3_2), (3.4_1) and (3.4_2) where

factors of inner automorphisms appear, and can be checked similarly. Now we check the relation (3.4_1). For $1 \le u \le p-2$ we see $\delta^u\gamma(a) = a^{u+1}b, \quad \delta^u\gamma(b) = a^u b$. On the other hand, let $t^i \equiv u+1 \pmod p$. Then

$$\begin{aligned}
\alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}}\theta^{-\frac{u}{u+1}}(a) &= \alpha^i\beta^{-i}(ab^{u+1}) = \alpha^i(ab) = a^{u+1}b = \delta^u\gamma(a),\\
\alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}}\theta^{-\frac{u}{u+1}}(b) &= \alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}}(bc^{-\frac{u}{u+1}})\\
&= \alpha^i\beta^{-i}\gamma^{u+1}(a^{\frac{u}{u+1}}bc^{-\frac{u}{u+1}}) = \alpha^i\beta^{-i}((ab^{u+1})^{\frac{u}{u+1}}bc^{-\frac{u}{u+1}})\\
&= \alpha^i\beta^{-i}(a^{\frac{u}{u+1}}b^{u+1}c^{-\frac{u}{u+1}(\frac{u}{u+1}-1)(u+1)/2}c^{-\frac{u}{u+1}})\\
&= \alpha^i(a^{\frac{u}{u+1}}b) = a^u b = \delta^u\gamma(b).
\end{aligned}$$

The relation (3.4_1) follows. The relations (3.5)–(3.6), describing the group of inner automorphism, are easy to show.

By the relations (3.2_2) and (3.3_2) we see that the group of inner automorphisms is contained in the group $\langle \alpha, \beta, \gamma, \delta\rangle$. By Theorem 2.1 the homomorphism $\langle \alpha, \beta, \gamma, \delta\rangle \to \mathrm{GL}(2,p)$ is onto, it maps inner automorphisms to 1, and since $|\operatorname{Aut}(G)| = p^2|\operatorname{GL}(2,p)|$, the group $\langle \alpha, \beta, \gamma, \delta\rangle$ coincides with the whole automorphism group. That is, the factor-group $\operatorname{Aut}(G)/\operatorname{Inn}(G)$ is isomorphic to the linear group $\mathrm{GL}(2,p)$. Again by Theorem 2.1 the relations (3.1)–(3.6) determine the group operation completely. □

Clearly, the group $\operatorname{Aut}(G)$ is not solvable but in case $p = 3$.

4. The automorphism group $\operatorname{Aut}(C_{p^m} \times C_{p^m})$ $(m > 1)$

Theorem 4.1. *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*

$$|\alpha| = \varphi(p^m),\ |\beta| = \varphi(p^m),\ |\gamma| = p^m,\ |\delta| = p^m, \tag{4.1}$$

$$\alpha^{-1}\beta\alpha = \beta, \qquad \alpha^{-1}\gamma\alpha = \gamma^t, \qquad \alpha^{-1}\delta\alpha = \delta^{\frac{1}{t}}, \tag{4.2}$$

$$\beta^{-1}\gamma\beta = \gamma^{\frac{1}{t}}, \qquad \beta^{-1}\delta\beta = \delta^t, \qquad \gamma^{-1}\delta\gamma = \delta^{-1}\gamma^{-1}\delta, \tag{4.3}$$

$$\delta^u\gamma = \alpha^i\beta^{-i}\gamma^{u+1}\delta^{\frac{u}{u+1}}, \qquad \nu^2 = \alpha^{\frac{\varphi(p^m)}{2}}\beta^{\frac{\varphi(p^m)}{2}}, \qquad \nu^{-1}\alpha\nu = \beta, \tag{4.4}$$

$$\delta^{vp-1}\gamma = \alpha^j\beta^{-j}\gamma^{vp-1}\delta^{\frac{vp}{1-vp}}\nu, \tag{4.5}$$

where $\frac{1}{t}$ is the multiplicative inverse of t modulo p^m; $1 \le u \le p^m - 2$, $\gcd(u+1, p) = 1$, $\frac{1}{u+1}$ is the multiplicative inverse of $u+1$ modulo p^m, $t^i \equiv u+1$

$(\mathrm{mod}\ p^m)$; $0 \le v \le p^{m-1}-1$, $t^j \equiv vp-1\ (\mathrm{mod}\ p^m)$, $\frac{1}{1-vp}$ *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.*

PROOF. Let $\langle a' \rangle \times \langle b' \rangle$ be another presentation. As an element $a^i b^j$ is of order p^m if and only if $\gcd(i,p) = 1$ or $\gcd(j,p) = 1$, there are $p^{2m} - p^{2m-2}$ choices for the generator a'. Let b' be any one of the choices for the other generator. To assure that $\langle a' \rangle \cap \langle {a'}^i {b'}^j \rangle$ be trivial and ${a'}^i {b'}^j$ be of order p^m it is necessary that j and p be relatively primes, as otherwise $({a'}^i {b'}^j)^{p^{m-1}} = {a'}^{ip^{m-1}}$, and this property is sufficient also. So there are $p^m \varphi(p^m)$ choices for the second generator. This way altogether there are $(p^{2m}-p^{2m-2})p^m\varphi(p^m) = p^{4m-3}(p^2-1)(p-1)$ choices, which is the order of the automorphism group in view of Theorem 1.1.

The relations (4.1)–(4.4$_1$) are immediate and may be checked just as in Theorem 2.1. We prove now that these four automorphisms generate the whole automorphism group. The subgroup $A = \langle \alpha, \beta \rangle$ is of order $\varphi(p^m)^2$, and elements of this subgroup map a to an a-power and b to a b-power, while nonidentity automorphisms in the subgroup $\langle \gamma \rangle$ do not. Hence $A \cap \langle \gamma \rangle = \{1\}$, and by the relations (4.2$_2$) and (4.3$_1$), the subgroup $B = \langle A, \gamma \rangle$ is the semidirect product $A \ltimes \langle \gamma \rangle$ of order $\varphi(p^m)^2 p^m$, of index $(p+1)p^{m-1}$. Since

$$\alpha^i \beta^j \gamma^k(a) = a^{t^i} b^{t^j k}$$

$(0 \le i \le \varphi(p^m)-1,\ 0 \le j \le \varphi(p^m)-1,\ 0 \le k \le p^m-1)$ equals a only if $i = 0$, $k = 0$, we see that nonidentity automorphisms in the subgroup $\langle \delta \rangle$ are not in the subgroup B, and the subgroup $\langle B, \delta \rangle$ is of order $p^{4m-2}(p-1)^2$ at least. But the greatest proper divisor of $p^{4m-3}(p^2-1)(p-1)$ is $\frac{p+1}{2}p^{4m-3}(p-1)^2$, which is less than $p^{4m-2}(p-1)^2$, and these four automorphisms generate the whole automorphism group $\mathrm{Aut}(C_{p^m} \times C_{p^m})$.

The automorphism $\nu = \delta\gamma^{-1}\delta$ maps a to b^{-1} and b to a. We see that elements of the set $\cup_{i=0}^{p^m-1} B\delta^i$ map a to an element $a^j b^k$ with j relatively prime to p while elements of the set $\cup_{i=0}^{p^{m-1}-1} B\delta^{ip}\nu$ map a to an element of form $a^j b^k$ with j divisible by the prime p. So the cosets $B\delta^i$ $(0 \le i \le p^m-1)$ and $B\delta^{jp}\nu$ $(0 \le j \le p^{m-1}-1)$ are all distinct. There remained to show that these are all the cosets, using relations only. For this aim we shall need the remaining three relations. The relations (4.4$_2$) and (4.4$_3$) are immediate as in Theorem 2.1, and imply that, in fact, the automorphisms α, γ and δ generate the whole automorphism group. Furthermore, for $0 \le v \le p^{m-1}-1$

$$\delta^{vp-1}\gamma(a) = a^{vp}b, \quad \delta^{vp-1}\gamma(b) = a^{vp-1}b.$$

On the other hand, if $t^j \equiv vp-1 \pmod{p^m}$, we have

$$\begin{aligned}\alpha^j\beta^{-j}\gamma^{vp-1}\delta^{\frac{vp}{1-vp}}\nu(a) &= \alpha^j\beta^{-j}\gamma^{vp-1}\delta^{\frac{vp}{1-vp}}(b^{-1}) = \alpha^j\beta^{-j}\gamma^{vp-1}(a^{\frac{vp}{vp-1}}b^{-1})\\ &= \alpha^j\beta^{-j}(a^{\frac{vp}{vp-1}}b^{vp-1}) = a^{vp}b = \delta^{vp-1}\gamma(a),\\ \alpha^j\beta^{-j}\gamma^{vp-1}\delta^{\frac{vp}{1-vp}}\nu(b) &= \alpha^j\beta^{-j}\gamma^{vp-1}\delta^{\frac{vp}{1-vp}}(a)\\ &= \alpha^j\beta^{-j}(ab^{vp-1}) = a^{vp-1}b = \delta^{vp-1}\gamma(b).\end{aligned}$$

The relation (4.5) follows.

By the relation (4.2_3) $B\delta^u\alpha = B\delta^{\frac{u}{t}}$, and by the relations (4.4_2)–(4.4_3)

$$B\delta^{up}\nu\alpha = B\delta^{up}\beta\nu = B\delta^{up^\beta}\nu = B\delta^{upt}\nu.$$

(clearly, by the relations (4.2_1)-(4.3_2) the automorphism $\alpha\beta$ is central). By the relations (4.4_1) $B\delta^u\gamma = B\delta^{\frac{u}{u+1}}$ $(u \not\equiv -1 \pmod{p})$, by the relation (4.5) $B\delta^{vp-1}\gamma = B\delta^{\frac{vp}{1-vp}}\nu$ and, since by the relation (4.3_3) $\nu\gamma = \gamma^{-1}\delta$,

$$B\delta^{vp}\nu\gamma = B\delta^{vp}\gamma^{-1}\delta = B\delta^{\frac{vp}{1-vp}}\delta = B\delta^{\frac{1}{1-vp}}.$$

Finally,

$$B\delta^{vp}\nu\delta = B\delta^{vp}\nu^{-1}\delta = B\delta^{vp}\delta^{-1}\gamma\delta^{-1}\delta = B\delta^{vp-1}\gamma = B\delta^{\frac{vp}{1-vp}}\nu.$$

Hence there are no more cosets, the elements δ^i $(i = 0, \dots, p^m-1)$, $\delta^{pj}\nu$ $(j = 0, \dots, p^{m-1}-1)$ form a right transversal to the subgroup B, and the relations (4.1)–(4.5) determine the group operation completely.

Let $\mho$ be the characteristic subgroup generated by a^p and b^p, then the factor-group $\langle a, b\rangle/\mho$ is elementary abelian of order p^2. The automorphisms α, γ and δ act on this factor-group, the induced automorphisms may be viewed as elements of the linear group $\mathrm{GL}(2,p)$ of order $(p^2-1)(p^2-p)$. Hence the group $\mathrm{Aut}(C_{p^m} \times C_{p^m})$ maps homomorphically into the group $\mathrm{GL}(2,p)$, and by Theorem 2.1 this homomorphism is onto, and its kernel is of order p^{4m-4}. □

In the course of the proof a permutation representation has been given on the right cosets of the subgroup B. Clearly, the group $\mathrm{Aut}(C_{p^m} \times C_{p^m})$ is solvable if and only if the linear group $\mathrm{GL}(2,p)$ is solvable (that is, if $p = 3$).

5. The case of the group $G = \langle a, b \,|\, a^{p^m} = b^{p^m} = c^p = 1,\ [a,b] = c,\ [a,c] = 1,\ [b,c] = 1\rangle$ with $m > 1$, $|G| = p^{2m+1}$

Theorem 5.1. *Consider the automorphism group Aut(G) (with G as in the title). 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 $a \mapsto a$, $b \mapsto ab$, the automorphism η by the substitution $a \mapsto ac$, $b \mapsto b$; and the automorphism θ*

by the substitution $a \mapsto a$, $b \mapsto bc$. Then the automorphism group Aut(G) is generated by the automorphisms α, β, γ, δ. Furthermore, the group of inner automorphisms is Inn$(G) = \langle \eta, \theta \rangle$ and the factor-group Aut$(G)/$ Inn(G) of outer automorphisms is isomorphic to the group Aut$(C_{p^m} \times C_{p^m})$.

PROOF. Let $G = \langle a', b' \,|\, a'^{p^m} = b'^{p^m} = c'^p = 1, [a', b'] = c', [a', c'] = 1, [b', c'] = 1 \rangle$ be another presentation. As an element $a^i b^j c^k$ is of order p^m if and only if $\gcd(i, p) = 1$ or $\gcd(j, p) = 1$, there are $p^{2m+1} - p^{2m-1}$ choices for the generator a'. Let b' be any of the possible choices for the second generator. Then the element $a'^i b'^j c'^k$ can be chosen to be another second generator if only if its order is p^m, it does not commute with a' and $\langle a' \rangle \cap \langle a'^i b'^j c'^k \rangle = \{1\}$. These three requirements are fulfilled if and only if $\gcd(j, p) = 1$, so there are $\varphi(p^m)p^{m+1}$ choices for the generator b'. So altogether there are $(p^{2m+1} - p^{2m-1})\varphi(p^m)p^{m+1} = p^{4m-1}(p^2-1)(p-1)$ choices, which is the order of the automorphism group. Notice that this is just $p^2 |\operatorname{Aut}(C_{p^m} \times C_{p^m})|$.

Put $C = \langle c \rangle$, then the factor-group G/C is of type $C_{p^m} \times C_{p^m}$. The automorphisms α, β, γ and δ act on the factor-group G/C, the induced automorphisms may be viewed as elements of the automorphism group $\operatorname{Aut}(C_{p^m} \times C_{p^m})$ of order $p^{4m-3}(p^2-1)(p-1)$. Hence the group $\langle \alpha, \beta, \gamma, \delta \rangle$ maps homomorphically into the group $\operatorname{Aut}(C_{p^m} \times C_{p^m})$. The generating relations for the group $\operatorname{Aut}(G)$ are analogous to the relations (4.1)–(4.5) of the previous paragraph but not identical, because factors of inner automorphisms may appear as, for instance, in $\alpha^{-1}\gamma\alpha = \eta^{-\frac{t-1}{2}}\gamma^t$ and $\beta^{-1}\delta\beta = \theta^{-\frac{t-1}{2}}\delta^t$. Clearly, the group of inner automorphisms is $\operatorname{Inn}(G) = \langle \eta \rangle \times \langle \theta \rangle$ of type $C_p \times C_p$. We see that the group of inner automorphism is contained in the group $\langle \alpha, \beta, \gamma, \delta \rangle$. By Theorem 4.1 of the previous paragraph the homomorphism $\langle \alpha, \beta, \gamma, \delta \rangle \to \operatorname{Aut}(C_{p^m} \times C_{p^m})$ is onto, it maps inner automorphisms to 1, and since $|\operatorname{Aut}(G)| = p^2 |\operatorname{Aut}(C_{p^m} \times C_{p^m})|$, the group $\langle \alpha, \beta, \gamma, \delta \rangle$ coincides with the whole automorphism group. That is, the factor-group $\operatorname{Aut}(G)/\operatorname{Inn}(G)$ is isomorphic to the automorphism group $\operatorname{Aut}(C_{p^m} \times C_{p^m})$. □

One can determine the generating relations as well on the basis of Theorem 4.1 easily as the only difference is a factor of an inner automorphism at certain places, and actions of the automorphisms α, β, γ, δ on the group of inner automorphisms Inn(G) are the same as in Theorem 3.1. Clearly, the group Aut(G) is not solvable but in case $p = 3$.

6. The automorphism group Aut$(C_{p^m} \times C_{p^n})$ where $m > n > 0$

THEOREM 6.1. *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

$$|\alpha| = \varphi(p^m),\ |\beta| = \varphi(p^n),\ |\gamma| = p^n,\ |\delta| = p^n, \tag{6.1}$$

$$\alpha^{-1}\beta\alpha = \beta, \qquad \alpha^{-1}\gamma\alpha = \gamma^t, \qquad \alpha^{-1}\delta\alpha = \delta^{\frac{1}{t}}, \tag{6.2}$$

$$\beta^{-1}\gamma\beta = \gamma^{\frac{1}{t}}, \qquad \beta^{-1}\delta\beta = \delta^t, \tag{6.3}$$

$$\delta^u\gamma = \alpha^i\beta^{-i}\gamma^{up^{m-n}+1}\delta^{\frac{u}{up^{m-n}+1}}, \tag{6.4}$$

where $\frac{1}{t}$ is the multiplicative inverse of t modulo p^n, an integer between 1 and p^n, $1 \le u \le p^n - 1$, $\frac{1}{up^{m-n}+1}$ 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.

PROOF. Let $\langle a' \rangle \times \langle b' \rangle$ be another presentation. As an element a^ib^j is of order p^m if and only if $\gcd(i,p) = 1$, there are $\varphi(p^m)p^n$ choices for the generator a' (it is understood that the cyclic subgroup $\langle a' \rangle$ of maximal order always has a direct complement). Let b' be any one of the choices for the other generator. To assure that $\langle a' \rangle \cap \langle a'^i b'^j \rangle$ be trivial and $a'^i b'^j$ be of order p^n it is necessary that j and p be relatively primes, as otherwise $(a'^i b'^j)^{p^{n-1}} = a'^{ip^{n-1}}$, and this property together with $i = p^{m-n}i_1$ is sufficient also. So there are $p^n\varphi(p^n)$ choices for the second generator. This way altogether there are $\varphi(p^m)p^np^n\varphi(p^n) = p^{m+3n-2}(p-1)^2$ choices, which is the order of the automorphism group by virtue of Theorem 1.1.

The relations (6.1)–(6.3) can be checked just as in the foregoing. For $1 \le u \le p^n - 1$, if $t^i \equiv 1 + up^{m-n} \pmod{p^m}$ where i is an integer between 1 and p^m,

$$\delta^u\gamma(a) = a^{up^{m-n}+1}b, \quad \delta^u\gamma(b) = a^{up^{m-n}}b,$$

and on the other hand, with $\frac{1}{1+u^{p^{m-n}}}$ the multiplicative inverse of $1 + u^{p^{m-n}}$ modulo p^n, an integer between 1 and p^n,

$$\begin{aligned}
&\alpha^i\beta^{-i}\gamma^{up^{m-n}+1}\delta^{\frac{u}{up^{m-n}+1}}(a) = \alpha^i\beta^{-i}(ab^{up^{m-n}+1}) \\
&\quad = \alpha^i(ab) = a^{up^{m-n}+1}b = \delta^u\gamma(a), \\
&\alpha^i\beta^{-i}\gamma^{up^{m-n}+1}\delta^{\frac{u}{up^{m-n}+1}}(b) = \alpha^i\beta^{-i}\gamma^{up^{m-n}+1}(a^{\frac{up^{m-n}}{up^{m-n}+1}}b) \\
&\quad = \alpha^i\beta^{-i}(a^{\frac{up^{m-n}}{up^{m-n}+1}}b^{up^{m-n}+1}) = \alpha^i(a^{\frac{up^{m-n}}{up^{m-n}+1}}b) = a^{up^{m-n}}b = \delta^u\gamma(b).
\end{aligned}$$

The relation (6.4) follows.

We prove now that these four automorphisms generate the whole automorphism group. The subgroup $A = \langle \alpha, \beta \rangle$ is of order $\varphi(p^m)\varphi(p^n)$, and elements of this subgroup map a to an a-power and b to a b-power, while nonidentity automorphisms in the subgroup $\langle \gamma \rangle$ do not. Hence $A \cap \langle \gamma \rangle = \{1\}$, and by the relations (6.2_2) and (6.3_1), the subgroup $B = \langle A, \gamma \rangle$ is the semidirect product $A \ltimes \langle \gamma \rangle$ of order $\varphi(p^m)\varphi(p^n)^2 p^n$, of index p^n. Since

$$\alpha^i \beta^j \gamma^k(a) = a^{t^i} b^{t^j k}$$

$(0 \le i \le \varphi(p^m) - 1,\ 0 \le j \le \varphi(p^n) - 1,\ 0 \le k \le p^n - 1)$ equals a only if $i = 0$, $k = 0$, we see that nonidentity automorphisms in the subgroup $\langle \delta \rangle$ are not in the subgroup B, and the subgroup $\langle B, \delta \rangle$ is of order $\varphi(p^m)\varphi(p^n)^2 p^{2n}$ at least. But this is the order of the whole automorphism group $\mathrm{Aut}(C_{p^m} \times C_{p^n})$, which is thus generated by these four automorphisms.

By the relation (6.2_3) $B\delta^u\alpha = B\delta^{\frac{u}{t}}$, and by the relation (6.3_2) $B\delta^u\beta = B\delta^{ut}$. By the relations (6.4) $B\delta^u\gamma = B\delta^{\frac{u}{up^{m-n}+1}}$. Hence there are no more cosets, the elements δ^i $(i = 0, \dots, p^n - 1)$ form a right transversal to the subgroup B, and the relations (6.1)–(6.4) determine the group operation completely.

Let $\mho$ be the characteristic subgroup generated by a^p and b^p, then the factor-group $\langle a, b \rangle / \mho$ is elementary abelian of order p^2. Hence the group $\mathrm{Aut}(C_{p^m} \times C_{p^n})$ maps homomorphically into the group $\mathrm{GL}(2, p)$. Its kernel consists of automorphisms fixing cosets of the subgroup $\mho$. One finds that such an automorphism may substitute the element a with any element in the coset $a\mho$, and the element b with any element of form $a^{ip^{m-n}} b^{1+pj}$, so the order of the kernel is p^{m+3n-3}, and the image is of order $p(p-1)^2$. As the automorphism δ is in the kernel, the image is metabelian by Theorem 2.1. □

In the course of the proof a permutation representation has been given on the right cosets of the subgroup B.

7. The case of the group $G = \langle a, b \mid a^{p^m} = b^{p^n} = c^p = 1,\ [a,b] = c,\ [a,c] = 1,\ [b,c] = 1 \rangle$ with $m > n > 0$, $|G| = p^{m+n+1}$

Theorem 7.1. *Consider the automorphism group Aut(G) (with G as in the title). 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 $a \mapsto a$, $b \mapsto b^t$ (note that t is a primitive root modulo p^m and hence modulo p^n); the automorphism γ by the substitution $a \mapsto ab$, $b \mapsto b$; the automorphism δ by the substitution $a \mapsto a$, $b \mapsto a^{p^{m-n}} b$, the automorphism η by the substitution $a \mapsto ac$, $b \mapsto b$; and the automorphism θ by the substitution $a \mapsto a$, $b \mapsto bc$. Then the automorphism group Aut(G) is generated by the automorphisms α, β, γ, δ and θ. Furthermore, the group of*

inner automorphisms is $Inn(G) = \langle \eta, \theta \rangle$ *and the factor-group* $Aut(G)/\, Inn(G)$ *of outer automorphisms is isomorphic to the group* $Aut(C_{p^m} \times C_{p^n})$. *In particular, the group* $Aut(G)$ *is solvable.*

PROOF. Let $G = \langle a', b' \,|\, a'^{p^m} = b'^{p^n} = c'^p = 1, [a', b'] = c', [a', c'] = 1, [b', c'] = 1 \rangle$ be another presentation. As an element $a^i b^j c^k$ is of order p^m if and only if $\gcd(i, p) = 1$, there are $\varphi(p^m)p^{n+1}$ choices for the generator a' (since it is of maximal order, is not in G^p and every such choice is possible). Let b' be any of the possible choices for the second generator. To assure that $\langle a' \rangle \cap \langle a'^i b'^j c'^k \rangle$ be trivial and $a'^i b'^j c'^k$ be a noncentral element of order p^n it is necessary that j and p be relatively primes, as otherwise for $n = 1$ the elements a' and $a'^i b'^j c'^k = a'^i c'^k$ commute, and for $n > 1$ $(a'^i b'^j c'^k)^{p^{n-1}} = a'^{ip^{n-1}}$, and this property together with $i = p^{m-n} i_1$ is sufficient also. So there are $p^{n+1}\varphi(p^n)$ choices for the second generator. This way altogether there are $\varphi(p^m)p^{n+1}p^{n+1}\varphi(p^n) = p^{m+3n}(p-1)^2$ choices, which is the order of the automorphism group. Notice that this is just $p^2 |\operatorname{Aut}(C_{p^m} \times C_{p^n})|$.

Put $C = \langle c \rangle$, then the factor-group G/C is of type $C_{p^m} \times C_{p^n}$. The automorphisms α, β, γ, δ and θ act on the factor-group G/C, the induced automorphisms may be viewed as elements of the automorphism group $\operatorname{Aut}(C_{p^m} \times C_{p^n})$ of order $p^{m+3n-2}(p-1)^2$. Hence the group $\langle \alpha, \beta, \gamma, \delta, \theta \rangle$ maps homomorphically into the group $\operatorname{Aut}(C_{p^m} \times C_{p^n})$. Generating relations for the group $\operatorname{Aut}(G)$ are analogous to the relations (6.1)–(6.4) of Theorem 6.1 of the previous paragraph but not identical, because factors of inner automorphisms may appear as, for instance, in $\alpha^{-1}\gamma\alpha = \eta^{-\frac{t-1}{2}}\gamma^t$. Clearly, the group of inner automorphisms is $\operatorname{Inn}(G) = \langle \eta \rangle \times \langle \theta \rangle$ of type $C_p \times C_p$. By Theorem 6.1 the homomorphism $\langle \alpha, \beta, \gamma, \delta, \theta \rangle \to \operatorname{Aut}(C_{p^m} \times C_{p^n})$ is onto, and its kernel contains the subgroup $\operatorname{Inn}(G)$. Since $|\operatorname{Aut}(G)| = p^2 |\operatorname{Aut}(C_{p^m} \times C_{p^n})|$, the group $\langle \alpha, \beta, \gamma, \delta, \theta \rangle$ coincides with the whole automorphism group. That is, the factor-group $\operatorname{Aut}(G)/\operatorname{Inn}(G)$ is isomorphic to the automorphism group $\operatorname{Aut}(C_{p^m} \times C_{p^n})$. Clearly, the group $\operatorname{Aut}(G)$ is solvable by Theorem 6.1. □

One can determine the generating relations as well on the basis of Theorem 6.1 easily as the only difference is a factor of an inner automorphism at certain places, and actions of the automorphisms α, β, γ, δ on the group of inner automorphisms $\operatorname{Inn}(G)$ are identical as in Theorem 3.1 with few exceptions, such as $\delta^{-1}\eta\delta = \eta$.

We have completed the description of automorphism groups of minimal nonabelian p-groups for odd primes p in case (B). Case (A) for odd primes and the 2-group case will be subjects of forthcoming papers.

8. Solvable automorphism groups of finite abelian groups

As a byproduct of the foregoing investigations, we are able to characterize finite abelian groups with solvable automorphism groups. From now on we relax the assumption that the prime p is odd.

Theorem 8.1. *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 $k_1 > k_2 > \cdots > k_r > 0$ $(r > 1)$.*

Proof. For, we see at once that, as primary components are characteristic, the automorphism group $\mathrm{Aut}(A)$ is the direct product of the automorphism groups of the primary components, hence the automorphism group $\mathrm{Aut}(A)$ is solvable if and only if the automorphism group of every primary component is solvable.

Sufficiency. We have to show that in each of the cases (i), (ii) and (iii) the automorphism groups of the primary components P are solvable. This is evident if the primary component P is cyclic, of type $C_2 \times C_2$ or $C_3 \times C_3$ and has just been proved above for the type $C_{3^k} \times C_{3^k}$.

Let $p = 2$, and let $P = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_r \rangle$ be of type $C_{2^{k_1}} \times C_{2^{k_2}} \times \cdots \times C_{2^{k_r}}$ with $k_1 \geq k_2 \geq \cdots \geq k_r > 0$ $(r > 1)$ with at most two consecutive exponents coinciding. We shall prove by induction that the automorphism group $\mathrm{Aut}(P)$ is of order of form $2^i 3^j$, which at once implies that it is solvable by Burnside's Theorem. Let $\langle a'_1 \rangle \times \langle a'_2 \rangle \times \cdots \times \langle a'_r \rangle$ be another presentation.

If the exponent k_1 is alone, since a cyclic subgroup of maximal order always has a direct complement, for a'_1 we may choose any element of order 2^{k_1}, number of which is $\varphi(2^{k_1}) \frac{|P|}{2^{k_1}}$, a 2-power.

If the exponents k_1 and k_2 coincide then for a'_1 we may choose any element of order 2^{k_1} from the subgroup $\langle a_1 \rangle \times \langle a_2 \rangle$, number of which is $2^{2k_1} - 2^{2k_1-2} = 2^{2k_1-2} \cdot 3$, multiplied by any element of the subgroup $\langle a_3 \rangle \times \cdots \times \langle a_r \rangle$, 2-power in number. If a' is any of the possible choices for the second new basis element and $P = \langle a'_1 \rangle \times \langle a' \rangle \times P'_3$, then for a'_2 we may choose any element of order

2^{k_1}, with $\langle a'_1\rangle \cap \langle a'_2\rangle = \{1\}$, $\varphi(2^{k_1})\frac{|P|}{2^{k_1}}$ in number, which is a 2-power. If the group P is of type $C_{2^k} \times C_{2^k}$ then the proof of solvability stops here.

Assume that the new basis elements $a'_1, \ldots, a'_{s-1}$ have been already chosen, if the exponent k_{s-1} has a pair then $k_{s-2} = k_{s-1}$, and the number of possible choices up to this point is a 2-power times a 3-power. Put $P'_{s-1} = \langle a'_1\rangle \times \langle a'_2\rangle \times \cdots \times \langle a'_{s-1}\rangle$. If the exponent k_s is alone then, since in the factor-group P/P'_{s-1} every cyclic subgroup of maximal order is a direct factor, any element a'_s of order 2^{k_s} with $\langle a'_s\rangle \cap P'_{s-1} = \{1\}$ can be chosen to be the new generator. Let a' be any of the possible choices, P'_{s+1} a direct complement to $P'_{s-1} \times \langle a'\rangle$. The new generators a'_s are of form $ua'^i v$, where $\gcd(i, 2) = 1$, $u \in P'_{s-1}$ is of order dividing 2^{k_s}, $v \in P'_{s+1}$. The number of the i's is $\varphi(2^{k_s})$, a 2-power, the u's form a subgroup in P'_{s-1}, so the number of the u's is a 2-power, and, clearly, the number of the v's is also a 2-power.

If $k_s = k_{s+1}$ and a' and b' are any of the possible choices for the two new basis elements and $P = P'_{s-1} \times \langle a'\rangle \times \langle b'\rangle \times P'_{s+2}$, then for a'_s we may choose any element of order 2^{k_s} with $\langle a'_s\rangle \cap P'_{s-1} = \{1\}$, these are of form $ua'^i b'^j v$ with $u \in P'_{s-1}$ of order dividing 2^{k_s}, the element $a'^i b'^j$ is of order 2^{k_s}, and $v \in P'_{s+2}$. Such elements u form a subgroup, so their number is a 2-power, the number of the elements $a'^i b'^j$ is $2^{2k_s} - 2^{2k_s-2} = 2^{2k_s-2} \cdot 3$, and, clearly, the number of the v's is a 2-power. For a'_{s+1} we may choose any element satisfying $\langle a'_{s+1}\rangle \cap P'_{s-1} \times \langle a'_s\rangle = \{1\}$ of order 2^{k_s}. Let b'' be any of the possible choices, P''_{s+2} a direct complement to $P'_{s-1} \times \langle a'_s\rangle \times \langle b''\rangle$. The new generators a'_{s+1} are of form $ub''^i v$, where $\gcd(i, 2) = 1$, $u \in P'_{s-1} \times \langle a'_s\rangle$ of order dividing 2^{k_s}, $v \in P''_{s+2}$. The number of the i's is $\varphi(2^{k_s})$, a 2-power, the u's form a subgroup in $P'_{s-1} \times \langle a'_s\rangle$, so the number of the u's is a 2-power, and, clearly, the number of the v's is also a 2-power.

By virtue of induction applying Theorem 1.1 we conclude that the order of the automorphism group $\mathrm{Aut}(P)$ is of form $2^i 3^j$.

Let $p = 3$, and let $P = \langle a_1\rangle \times \langle a_2\rangle \times \cdots \times \langle a_r\rangle$ be of type $C_{3^{k_1}} \times C_{3^{k_2}} \times \cdots \times C_{3^{k_r}}$ with $k_1 \geq k_2 \geq \cdots \geq k_r > 0$ $(r > 1)$ with at most two consecutive exponents coinciding. We shall prove by induction that the automorphism group $\mathrm{Aut}(P)$ is of order of form $2^i 3^j$, which at once implies that it is solvable by Burnside's Theorem. Let $\langle a'_1\rangle \times \langle a'_2\rangle \times \cdots \times \langle a'_r\rangle$ be another presentation.

If the exponent k_1 is alone, since a cyclic subgroup of maximal order always has a direct complement, for a'_1 we may choose any element of order 3^{k_1}, number of which is $\varphi(3^{k_1})\frac{|P|}{3^{k_1}}$, a 2-power times a 3-power.

If the exponents k_1 and k_2 coincide, then for a'_1 we may choose any element of order 3^{k_1} from the subgroup $\langle a_1\rangle \times \langle a_2\rangle$, number of which is $3^{2k_1} - 3^{2k_1-2} = 3^{2k_1-2} \cdot 8$, multiplied by any element of the subgroup $\langle a_3\rangle \times \cdots \times \langle a_r\rangle$, 3-power in number. For a'_2 we may choose any element of order 3^{k_1} with $\langle a'_1\rangle \cap \langle a'_2\rangle = \{1\}$, $\varphi(3^{k_1})\frac{|P|}{3^{k_1}}$ in number, which is a 2-power times a 3-power.

Assume that the new basis elements $a'_1, \ldots, a'_{s-1}$ have been already chosen, if the exponent k_{s-1} has a pair then $k_{s-2} = k_{s-1}$, and the number of possible choices up to this point is a 2-power times a 3-power. Put $P'_{s-1} = \langle a'_1 \rangle \times \langle a'_2 \rangle \times \cdots \times \langle a'_{s-1} \rangle$. If the exponent k_s is alone then, since in the factor-group P/P'_{s-1} every cyclic subgroup of maximal order is a direct factor, any element a'_s of order 3^{k_s} with $\langle a'_s \rangle \cap P'_{s-1} = \{1\}$ can be chosen to be the new generator. Let a' be any of the possible choices, P'_{s+1} a direct complement to $P'_{s-1} \times \langle a' \rangle$. The new generators a'_s are of form $ua'^i v$, where $\gcd(i, 3) = 1$, $u \in P'_{s-1}$ of order dividing 3^{k_s}, $v \in P'_{s+1}$. The number of the i's is $\varphi(3^{k_s})$, a 2-power times a 3-power, the u's form a subgroup in P'_{s-1}, so the number of the u's is a 3-power, and, clearly, the number of the v's is also a 3-power.

If $k_s = k_{s+1}$ and a' and b' are any of the possible choices for the two new basis elements and $P = P'_{s-1} \times \langle a' \rangle \times \langle b' \rangle \times P'_{s+2}$, then for a'_s we may choose any element of order 3^{k_s} with $P'_{s-1} \cap \langle a'_s \rangle = \{1\}$, these are of form $ua'^i b'^j v$ with $u \in P'_{s-1}$ of order dividing 3^{k_s}, the element $a'^i b'^j$ is of order 3^{k_s}, and $v \in P'_{s+2}$. Such elements u form a subgroup, so their number is a 3-power, the number of the elements $a'^i b'^j$ is $3^{2k_s} - 3^{2k_s-2} = 3^{2k_s-2} \cdot 8$, and, clearly, the number of the v's is a 3-power. For a'_{s+1} we may choose any element of order 3^{k_s} with $P'_{s-1} \times \langle a'_s \rangle \cap \langle a'_{s+1} \rangle = \{1\}$. Let b'' be any of the possible choices, P''_{s+2} a direct complement to $P'_{s-1} \times \langle a'_s \rangle \times \langle b'' \rangle$. The new generators a'_{s+1} are of form $ub''^i v$, where $\gcd(i, 3) = 1$, $u \in P'_{s-1} \times \langle a'_s \rangle$ of order dividing 3^{k_s}, $v \in P''_{s+2}$. The number of the i's is $\varphi(3^{k_s})$, a 2-power times a 3-power, the u's form a subgroup in $P'_{s-1} \times \langle a'_s \rangle$, so the number of the u's is a 3-power, and, clearly, the number of the v's is also a 3-power.

By virtue of induction we conclude that the order of the automorphism group $\mathrm{Aut}(P)$ is of form $2^i 3^j$.

Consider the case $p \geq 5$. Let $P = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_r \rangle$ of type $C_{p^{k_1}} \times C_{p^{k_2}} \times \cdots \times C_{p^{k_r}}$ with $k_1 > k_2 > \cdots > k_r > 0$ ($r > 1$). We shall prove by induction that the automorphism group $\mathrm{Aut}(P)$ is of order of form $p^i(p-1)^r$. Let $\langle a'_1 \rangle \times \langle a'_2 \rangle \times \cdots \times \langle a'_r \rangle$ be another presentation. Since a cyclic subgroup of maximal order always has a direct complement, for a'_1 we may choose any element of order p^{k_1}, number of which is $\varphi(p^{k_1}) \frac{|P|}{p^{k_1}}$, which is of form $p^i(p-1)$. Assume that the new basis elements $a'_1, \ldots, a'_{s-1}$ have been already chosen, and the number of possible choices up to this point is of form $p^i(p-1)^{s-1}$. Put $P'_{s-1} = \langle a'_1 \rangle \times \langle a'_2 \rangle \times \cdots \times \langle a'_{s-1} \rangle$. Since in the factor-group P/P'_{s-1} every cyclic subgroup of maximal order is a direct factor, any element a'_s of order p^{k_s} with $\langle a'_s \rangle \cap P'_{s-1} = \{1\}$ can be chosen to be the new generator. Let a' be any of the possible choices, P'_{s+1} a direct complement to $P'_{s-1} \times \langle a' \rangle$. The new generators a'_s are of form $ua'^j v$, where $\gcd(j, p) = 1$, $u \in P'_{s-1}$ of order dividing p^{k_s}, $v \in P'_{s+1}$. The number of the j's is $\varphi(p^{k_s}) = p^{k_s-1}(p-1)$, the u's form a subgroup in P'_{s-1}, so the number of the u's is a p-power, and, clearly, the number of the v's is also a p-power. By virtue of induction

we conclude that the order of the automorphism group $\mathrm{Aut}(P)$ is of form $p^i(p-1)^r$.

Finally, we shall show that the automorphism group $\mathrm{Aut}(P)$ factors into the product of a p-Sylow subgroup and an abelian subgroup E. Indeed, let α_i be the automorphism determined by the substitution $a_i \mapsto a_i^t$, $a_j \mapsto a_j$ $(j \neq i)$, where t is a primitive root modulo p^{k_1} (and hence modulo $p^{k_2}, \ldots, p^{k_r}$ also, $i = 1, \ldots, r$). Obviously, the α_i are of order $\varphi(p^{k_i})$ and generate an abelian subgroup of type $C_{\varphi(p^{k_1})} \times C_{\varphi(p^{k_2})} \times \cdots \times C_{\varphi(p^{k_r})}$. The subgroup $E = \langle \alpha_1^{p^{k_1-1}} \rangle \times \langle \alpha_2^{p^{k_2-1}} \rangle \times \cdots \times \langle \alpha_r^{p^{k_r-1}} \rangle$ is abelian of type C_{p-1}^r, its order is relatively prime to p, hence it has the trivial intersection with the p-Sylow subgroup. The product of their orders is the order of the whole automorphism group, thus the required factorization has been obtained. By the theorem of Kegel and Wielandt the automorphism group $\mathrm{Aut}(P)$ is solvable as a product of two nilpotent groups. The proof of sufficiency is complete.

Necessity. Notice that if a group has a direct factor then the automorphism group of the whole group has a subgroup isomorphic to the automorphism group of this direct factor. Considering the facts that the automorphism groups of groups of type $C_2 \times C_2 \times C_2$, $C_3 \times C_3 \times C_3$ and $C_{p^m} \times C_{p^m}$ $(p \geq 5$ and $m \geq 1)$ are nonsolvable (these facts are well-known or has just been proved above), there remained to prove that the automorphism group of a group of type $C_{2^m} \times C_{2^m} \times C_{2^m}$ or $C_{3^m} \times C_{3^m} \times C_{3^m}$ $(m > 1)$ is nonsolvable, because these properties together imply that in all the left-out cases in (i), (ii) and (iii) for the primary component P the automorphism group is nonsolvable.

Let the group $T = \langle a \rangle \times \langle b \rangle \times \langle c \rangle$ be of type $C_{2^m} \times C_{2^m} \times C_{2^m}$ $(m \geq 2)$ and let $\langle a' \rangle \times \langle b' \rangle \times \langle c' \rangle$ be another presentation. By applying analogous arguments as in the foregoing, for the new generator a' there are $2^{3m} - 2^{3(m-1)} = 2^{3m-3} \cdot 7$ choices, for b' there are $(2^{2m} - 2^{2(m-1)})2^m = 3 \cdot 2^{3m-2}$ choices, and for c' there are $\varphi(2^m)2^{2m} = 2^{3m-1}$ choices. Therefore altogether there are $2^{9m-6} \cdot 3 \cdot 7$ choices, which is the order of the automorphism group $\mathrm{Aut}(T)$. Let $\mathfrak{U}$ be the characteristic subgroup generated by a^2, b^2 and c^2, then the factor-group $T/\mathfrak{U}$ is elementary abelian of order 8. Automorphisms of $\mathrm{Aut}(T)$ act on the factor-group $G/\mathfrak{U}$, the induced automorphisms may be viewed as elements of the linear group $\mathrm{GL}(3,2)$ of order $2^3 \cdot 3 \cdot 7$. The kernel of the homomorphism consists of those automorphisms that map a to an element of the coset $a\mathfrak{U}$, b to an element of the coset $b\mathfrak{U}$ and c to an element of the coset $c\mathfrak{U}$. So in case of elements of the kernel for the substitutions $a \mapsto a'$ there are $2^{3(m-1)}$ choices as any $a' \in a\mathfrak{U}$ will do. In case of the substitutions $b \mapsto b'$, b' also may be any element of the coset $b\mathfrak{U}$ since these elements are of order 2^m and the property $\langle a' \rangle \cap \langle b' \rangle = \{1\}$ will also be satisfied, hence there are $2^{3(m-1)}$ choices. Similarly for c' there are $2^{3(m-1)}$ choices. We conclude that the kernel is of order 2^{9m-9}, the homomorphism is onto and $\mathrm{Aut}(T)$ has a nonsolvable homomorphic image and is nonsolvable.

Let the group $T = \langle a\rangle \times \langle b\rangle \times \langle c\rangle$ be of type $C_{3^m} \times C_{3^m} \times C_{3^m}$ $(m \geq 2)$ and let $\langle a'\rangle \times \langle b'\rangle \times \langle c'\rangle$ be another presentation. By applying analogous arguments as in the foregoing, for the new generator a' there are $3^{3m} - 3^{3(m-1)} = 2 \cdot 3^{3m-3} \cdot 13$ choices, for b' there are $(3^{2m} - 3^{2(m-1)})3^m = 2^3 \cdot 3^{3m-2}$ choices, and for c' there are $\varphi(3^m)3^{2m} = 2 \cdot 3^{3m-1}$ choices. Therefore altogether there are $2^5 \cdot 3^{9m-6} \cdot 13$ choices, which is the order of the automorphism group $\mathrm{Aut}(T)$. Let $\mho$ be the characteristic subgroup generated by a^3, b^3 and c^3, then the factor-group $T/\mho$ is elementary abelian of order 27. Automorphisms of $\mathrm{Aut}(T)$ act on the factor-group $G/\mho$, the induced automorphisms may be viewed as elements of the linear group $\mathrm{GL}(3,3)$ of order $2^5 \cdot 3^3 \cdot 13$. The kernel of the homomorphism consists of those automorphisms that map a to an element of the coset $a\mho$, b to an element of the coset $b\mho$ and c to an element of the coset $c\mho$. So in case of elements of the kernel for the substitutions $a \mapsto a'$ there are $3^{3(m-1)}$ choices as any $a' \in a\mho$ will do. In case of the substitutions $b \mapsto b'$, b' also may be any element of the coset $b\mho$ since these elements are of order 3^m and the property $\langle a'\rangle \cap \langle b'\rangle = \{1\}$ will also be satisfied, hence there are $3^{3(m-1)}$ choices. Similarly for c' there are $3^{3(m-1)}$ choices. We conclude that the kernel is of order 3^{9m-9}, the homomorphism is onto and $\mathrm{Aut}(T)$ has a nonsolvable homomorphic image and is nonsolvable. □

References

[1] Y. Berkovich and Z. Janko, *On subgroups of finite p-groups*, Israel J. Math. **171** (2009), 29–49.

[2] G. Birkhoff, *Subgroups of abelian groups*, Proc. London Math. Soc. **38** (1934), 385–401.

[3] D. Gorenstein, Finite groups, Harper and Row, New York, 1968.

[4] B. Huppert, Endliche gruppen. I, Springer, Berlin–New York, 1967.

[5] L. Rédei, *Das "schiefe Produkt" in der Gruppentheorie mit Anwendung auf die endlichen nichtkommutativen Gruppen mit lauter kommutativen echten Untergruppen und die Ordnungszahlen, zu denen nur kommutative Gruppen gehören* Comment. Math. Helv. **20** (1947), 225–264.

J. Kurdics
Institute of Mathematics and Informatics
Nyíregyháza College
31/b Sóstói u. Nyíregyháza 4400
Hungary
E-mail: kurdics@nyf.hu

Received: 18.6.2010.
Revised: 12.7.2010.