УДК 519.44

Э. Р. Моргадо

О группе автоморфизмов конечной абелевой p-группы

1. Известно [1], что для всякой конечной p-группы P группа автоморфизмов $\mathrm{Aut}(P) = A(p)$ индуцирует в фактор-группе $P/\Phi(P)$ ($\Phi(P)$ — группа Фраттини группы P) группу автоморфизмов. Обозначим ее через $L(P)$ и назовем линейной частью группы $A(P)$. $L(P)$ — подгруппа полной линейной группы $GL_r(p)$ над полем $GF(p)$ из p элементов, а r — минимальное число образующих группы P. Тем самым для $A(P)$ имеет место точная последовательность

$$1 \longrightarrow K(P) \longrightarrow A(P) \xrightarrow{\lambda} L(P) \longrightarrow 1, \tag{1}$$

причем ядро $K(P)$ эпиморфизма λ — p-группа. Будем называть ее ядерной подгруппой группы автоморфизмов $A(P)$.

Рассмотрим случай, когда $P = G$ — аддитивно записываемая конечная абелева p-группа типа $[p^{m_1}, p^{m_2}, \dots p^{m_r}]$, $m_1 \geqslant m_2 \geqslant \dots \geqslant m_r$; группа автоморфизмов $A(G)$ записывается мультипликативно.

Ставится вопрос: для каких конечных абелевых p-групп G расширение (1) расщепляется? Сравнительно полный ответ на него содержится в следующей ниже теореме.

Теорема. *Для $p \geqslant 5$ расширение* (1) *расщепляется для групп G типа $[p^m, p, \dots p]$ $\forall (m \in \mathbf{N})$ и только для них. Для $p = 2, 3$ указанные условия достаточны, но не необходимы.*

2. Будем придерживаться терминологии и обозначений монографий [2—4]. Пусть группа G (см. [2, 5]) представлена в виде прямой суммы $G = G_1 \oplus \oplus G_2 \oplus \dots \oplus G_s$. Тогда ее эндоморфизмы представим как совокупность матриц

$$\theta = \begin{pmatrix} \theta_{11} & \theta_{12} \dots \theta_{1s} \\ \theta_{21} & \theta_{22} \dots \theta_{2s} \\ \vdots & \vdots \quad\;\; \vdots \\ \theta_{s1} & \theta_{s2} \dots \theta_{ss} \end{pmatrix}, \tag{2}$$

где $\theta_{ij} \in \mathrm{Hom}(G_i, G_j)$. Они образуют кольцо для обычных операций сложения и умножения матриц. Автоморфизмы представляются обратимыми матрицами.

Пусть G — конечная абелева p-группа типа $[p^{m_1}, p^{m_2}, \dots p^{m_r}]$, причем

$$n_1 = m_1 = m_2 = \dots = m_{t_1} > n_2 = m_{t_1+1} = m_{t_1+2} = \dots = m_{t_2} >$$
$$\vdots$$
$$> n_s = m_{t_{s-1}+1} = m_{t_{s-1}+2} = \dots = m_{t_s},$$

$$t_1 = r_1, \quad t_i = r_1 + r_2 + \dots + r_i, \; t_s = r$$

(здесь $>$ — строгое неравенство), и представлена в виде прямой суммы

$$G = G_1 \oplus G_2 \oplus \dots \oplus G_s, \tag{3}$$

где G_i — группы типа $[p^{n_i}, \overbrace{p^{n_i}, \ldots p^{n_i}}^{r_i}]$ (они гомоциклические в терминологии монографии [4]) с r_i образующими. В этом случае [2] матрица θ обратима тогда и только тогда, когда обратимы все диагональные элементы θ_{ii}, $i = 1, 2, \ldots s$, т. е. когда $\theta_{ii} \in \mathrm{Aut}(G_i)$. Группа автоморфизмов $A(G)$ запишется в виде

$$\begin{pmatrix} \mathrm{Aut}\, G_1 & \mathrm{Hom}\,(G_1, G_2) \ldots & \mathrm{Hom}\,(G_1, G_s) \\ \mathrm{Hom}\,(G_2, G_1) & \mathrm{Aut}\, G_2 \quad \ldots & \mathrm{Hom}\,(G_2, G_s) \\ \vdots & \vdots & \vdots \\ \mathrm{Hom}\,(G_s, G_1) & \mathrm{Hom}\,(G_s, G_2) \ldots & \mathrm{Aut}\, G_s \end{pmatrix}. \tag{4}$$

Если $j > i$, то $n_i > n_j$. Выбрав и зафиксировав в G_i и в G_j соответственно базисы $\{a_1^{(i)}, a_2^{(i)}, \ldots a_{r_i}^{(i)}\}$ и $\{a_1^{(j)}, a_2^{(j)}, \ldots a_{r_j}^{(j)}\}$, имеем для всякого $\theta_{ij} \in \mathrm{Hom}\,(G_i, G_j)$

$$a_k^{(i)}\theta_{ij} = \sum_{l=1}^{r_j} \alpha_{kl}^{(ij)} a_l^{(j)}. \tag{5}$$

Таким образом, в выбранных базисах θ_{ij} представляется матрицами

$$(\alpha_{kl}^{(ij)}), \ \alpha_{kl}^{(ij)} \in \mathbf{Z}p^{n_j} \tag{6}$$

типа $r_i \times r_j$ (r_i строк, r_j столбцов) с элементами из $\mathbf{Z}p^{n_j}$, и обратно всякая такая матрица представляет однозначно согласно (5) некоторый элемент из $\mathrm{Hom}\,(G_i, G_j)$.

Если же $j < i$, то $n_j > n_i$; порядок элементов базиса $or\,(a_k^{(i)}) = p^{n_i}$, а $or\,(a_k^{(i)}\theta_{ij})$ делит число p^{n_i} так, что

$$a_k^{(i)}\theta_{ij} = \sum_{l=1}^{r_j} p^{n_j - n_i} \alpha_{kl}^{(ij)} a_l^{(j)} \tag{7}$$

и соответствующая матрица имеет вид $(p^{n_j-n_i}\alpha_{kl}^{(ij)})$. Но, очевидно, коэффициенты $\alpha_{kl}^{(ij)}$ определены гомоморфизмом θ_{ij} в $\mathbf{Z}p^{n_j}$ не однозначно, а лишь по модулю p^{n_i}.

Элементы из $\mathrm{Aut}\, G_i$ однозначно записываются невырожденными квадратными матрицами $(\beta_{kl}^{(i)})$, $\beta_{kl}^{(i)} \in \mathbf{Z}p^{n_i}$, причем невырожденность выражается условием $\det(\beta_{kl}^{(i)}) \not\equiv 0 \pmod p$.

Окончательно автоморфизмы θ группы $A(G)$ записываются в виде клеточных матриц

$$\begin{pmatrix} B_{11} & A_{12} \ldots & A_{1s} \\ A_{21} & B_{22} \ldots & A_{2s} \\ \vdots & \vdots & \vdots \\ A_{s1} & A_{s2} \ldots & B_{ss} \end{pmatrix}, \tag{8}$$

где $A_{ij} \equiv 0 \pmod{p^{n_j - n_i}}$ при $i > j$, $\det B_{ii} \not\equiv 0 \pmod p$.

Линейная часть автоморфизма $\theta \in A(G)$, т. е. автоморфизм θ', индуцированный автоморфизмом θ, будет представляться в базисе, индуцированном в $G/\Phi(G)$ базисами $\{a_1^{(i)}, a_2^{(i)}, \dots a_{r_i}^{(i)}\}$, матрицей вида

$$\begin{pmatrix} B'_{11} & A'_{12} \dots A'_{1s} \\ 0 & B'_{22} \dots A'_{2s} \\ \vdots & \vdots \quad\quad \vdots \\ 0 & 0 \dots B'_{ss} \end{pmatrix}, \tag{9}$$

где B'_{ii} состоит из вычетов по модулю p компонентов матрицы B_{ii}, A'_{ij} — из вычетов по модулю p компонентов матрицы A_{ij}. Причем $B'_{ii} \in GL_{r_i}(p)$. Как нетрудно увидеть, все такие матрицы встречаются в линейной части $L(G)$ группы $A(G)$.

3. Доказательство теоремы. Достаточность. Покажем, что для групп G типа $[p^m, p, \dots p]$ расширение (1) расщепляется. Для $m=1$ утверждение тривиально. Пусть $m \geqslant 2$. Как видно из п. 2, группа G — прямая сумма $G = \mathbf{Z}^+_{p^m} \oplus Q$ циклической группы $\mathbf{Z}^+_{p^m}$ и элементарной абелевой группы Q типа $[\overbrace{p, p, \dots, p}^{r-1}]$, а ее автоморфизмы при подходящем выборе базиса можно представить в виде матриц

$$\theta = \begin{pmatrix} \alpha_{11} & \alpha_{12} \dots \alpha_{1r} \\ p^{m-1}\alpha_{21} & \alpha_{22} \dots \alpha_{2r} \\ \vdots & \vdots \quad\quad \vdots \\ p^{m-1}\alpha_{r1} & \alpha_{r2} \dots \alpha_{rr} \end{pmatrix}, \alpha_{ij} \in \mathbf{Z_p} \tag{10}$$

для всех $j \geqslant 2$, $\alpha_{11} \in \mathbf{Z}^*_{p^m}$, $\alpha_{i1} \in \mathbf{Z}_{p^m}$ (здесь через $\mathbf{Z}^*_{p^m}$ обозначена мультипликативная группа кольца $\mathbf{Z}_{p^m}$), а линейная часть этого автоморфизма запишется в соответствующем базисе матрицей

$$\theta' = \begin{pmatrix} \alpha'_{11} & \alpha'_{12} \dots \alpha'_{1r} \\ 0 & \alpha'_{22} \dots \alpha'_{2r} \\ \vdots & \\ 0 & \alpha'_{r2} \dots \alpha'_{rr} \end{pmatrix}. \tag{11}$$

Здесь $\alpha'_{ij} \in \mathbf{Z}_p$, причем $\alpha'_{11} \neq 0$, $\alpha'_{11} \equiv \alpha_{11} \pmod p$ и $\alpha'_{ij} = \alpha_{ij}$ при $j \geqslant 2$. Как известно (см. например, [6]), группа $\mathbf{Z}^*_{p^m}$ изоморфна прямому произведению $K \times \mathbf{Z}^*_p$, где K — силовская p-подгруппа группы $\mathbf{Z}^*_{p^m}$. (Если $p \neq 2$, K — циклическая, порожденная элементом $p+1$; если $p=2$, K — не циклическая, а $\mathbf{Z}^*_p = \{1\}$). Пусть ι — мономорфизм $\mathbf{Z}^*_p$ в группу $\mathbf{Z}^*_{p^m}$ при таком прямом разложении. Положим

$$\psi : \theta' \longrightarrow \begin{pmatrix} (\alpha'_{11})\iota & \alpha_{12} \dots \alpha_{1r} \\ 0 & \alpha_{22} \dots \alpha_{2r} \\ \vdots & \vdots \quad\quad \vdots \\ 0 & \alpha_{r2} \dots \alpha_{rr} \end{pmatrix}.$$

Тогда $\psi\lambda = I_d$ и расширение (1) расщепляется.

Необходимость. Для доказательства необходимости условия при $p \geqslant 5$ воспользуемся одной леммой («редукционная лемма), представляющей и самостоятельный интерес. Она позволяет свести рассмотрение произвольной абелевой p-группы к случаю абелевых p-групп типа $[p^{m_1}, p^2, \dots p^{m_r}]$, $m_i \leqslant 2$, $i > 2$.

Редукционная лемма. *Пусть*

$$1 \longrightarrow K(pG) \longrightarrow A(pG) \xrightarrow{\lambda'} L(pG) \longrightarrow 1 \tag{12}$$

— точная последовательность вида (1) *для группы* pG. *Расщепляемость расширения* (1) *имплицирует расщепляемость последовательности* (12).

Доказательство. Обозначим через (p) эндоморфизм $g \longrightarrow pg$ группы G. Его образ pG есть группа Фраттини $\Phi(G)$ группы G, а ее ядро — цоколь $G_{[p]}$ группы G (см. [3]). Эндоморфизм (p) индуцирует гомоморфизм группы $A(G)$ в группу $A(pG)$. Обозначив его через π, получим коммутативную диаграмму

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K(G) & \longrightarrow & A(G) & \xrightarrow{\lambda} & L(G) & \longrightarrow & 1 \\ & & \downarrow k & & \downarrow \pi & & \downarrow \pi' & & \\ 1 & \longrightarrow & K(pG) & \longrightarrow & A(pG) & \xrightarrow{\lambda'} & L(pG) & \rightarrow & 1 \end{array} \tag{13}$$

где k — ограничение π на $K(G)$, а π' — образ π при λ и λ'.

Нетрудно убедиться, что $(K(G))\pi \subseteq K(pG)$.

1) Если $m_r \geqslant 2$, то цоколь $G_{[p]}$ содержится в группе Фраттини pG. Из этого следует, что ядро $K(G) = (K(pG))\pi^{-1}$. Действительно, если $(A)\pi \in K(pG)$, то $\forall g \in G \;\; pg \equiv (pg)A \pmod{p^2G}$. Тогда $\forall g \in G$ существует такой $g' \in G$, что $p(g - pg') = p(gA)$, т. е. $g - pg' \equiv gA \pmod{G_{[p]}}$. Следовательно, $g \equiv gA \pmod{pG}$. Из этого вытекает, что $A \in K(G)$.

Выполняются условия предложения V из [7, гл. 1, § 4], так как гомоморфизм π сюръективен (см. [3, предложение 113.3]). Следовательно, в этом случае π' — изоморфизм и легко проверить, что если мономорфизм $\psi : L(G) \rightarrow A(G)$ расщепляет последовательность (1), то $\psi' = \pi'^{-1}\psi\pi$ расщепляет (12).

2) Пусть $m_r = n_s = 1$. Тогда естественно отщепить прямое слагаемое G_s в представлении (3) и положить $G = G' \oplus G_s$, где $G' = G_1 \oplus G_2 \oplus \dots \oplus G_{s-1}$, а G_s — элементарная абелева p-подгруппа с r_s образующими. Матрица, представляющая элемент из $L(G)$, может быть приведена в подходящем базисе к виду

$$\theta' = \begin{pmatrix} \theta'_{11} & \theta'_{12} \\ 0 & \theta'_{22} \end{pmatrix} \; \theta'_{11} \in L(G'), \;\; \theta'_{22} \in L(G_s).$$

В этом случае pG — группа типа $[p^{m_1-1}, p^{m_2-1}, \dots p^{m_{t_{s-1}}-1}]$, где $t_{s-1} = r_1 + r_2 + \dots + r_{s-1}$ и, очевидно, $L(G') \simeq L(pG)$, тогда $\theta' \rightarrow \theta'_{11}$ и есть гомоморфизм π' в (13). Нетрудно убедиться, что последовательность

$$1 \longrightarrow K \longrightarrow L(G) \xrightarrow{\pi'} L(pG) \longrightarrow 1, \tag{14}$$

где K — ядро гомоморфизма π', расщепляется. Пусть ψ — расщепляющий мономорфизм для (1), а φ — мономорфизм, расщепляющий (14), тогда $\psi' = \varphi\psi\pi$ расщепляет (12). ■

Предполагаем, что $p \geqslant 5$. Доказательство необходимости ведется от противного. Предположим, что условия теоремы не выполнены (тогда $m_2 \geqslant 2$), и тем не менее расширение (1) расщепляется. Переходя последовательно к группам pG, $p^2G \dots$, $p^{m_2-2}G$, согласно редукционной лемме можем сразу считать, что $m_2 = 2$. Пусть $\psi : L(G) \rightarrow A(G)$ мономорфизм, который расщепляет расширение (1), и

$$A' = (A)\lambda = \begin{pmatrix} 1 & 1 \dots 0 \\ 0 & 1 \dots 0 \\ 0 & 0 \dots 1 \end{pmatrix}$$

— матрица, представляющая элемент из группы $L(G)$ и являющаяся образом элемента

$$A = \begin{pmatrix} 1 & 1 \dots 0 \\ 0 & 1 \dots 0 \\ \vdots & \vdots \quad \vdots \\ 0 & 0 \dots 1 \end{pmatrix}$$

группы $A(G)$ при гомоморфизме λ. Имеем $(A')\,\psi \equiv A\,(\mathrm{mod}\,K(G))$. Представим

$$(A')\,\psi = A + pB,$$

где $B = (\beta_{ij})$, а $\beta_{ij} \in \mathbf{Z}_{p^{m_j}}$. Матрица A' имеет в $L(G)$ порядок p и тот же порядок должна была бы иметь матрица $A + pB$. Но тогда

$$E = (A + pB)^p = A^p + p \sum_{i=0}^{p-1} A^{p-1-i} B A^i + p^2(\dots). \tag{15}$$

Положим $\sum\limits_{i=0}^{p-1} A^{p-1-i} B A^i = (\gamma_{ij})$,

$$A^p = \begin{pmatrix} 1 & p \dots 0 \\ 0 & 1 \dots 0 \\ 0 & 0 \dots 1 \end{pmatrix}, \tag{16}$$

тогда имело бы место сравнение

$$p + p\gamma_{12} \equiv 0\,(\mathrm{mod}\,p^2). \tag{17}$$

Но согласно (16) имеем

$$\gamma_{12} = \binom{p}{2}(\beta_{11} + \beta_{22}) + p\beta_{12} + \binom{p}{3}\beta_{21}. \tag{18}$$

Так как $p \geqslant 5$, то p делит γ_{12}. Из (17) получаем, что $p \equiv 0\ (\mathrm{mod}\,p^2)$. Это и есть искомое противоречие. Теорема полностью доказана.

4. Для $p = 2$ и $p = 3$ условия теоремы не необходимы.

1) При $p = 2$ нетрудно убедиться, что для группы типа [4, 4] расширение (1) расщепляемо.

Действительно, в этом случае линейная часть — полная линейная группа $GL_2(2)$ (2) над полем из двух элементов. Это, как известно, группа 6-го порядка, изоморфная S_3. Укажем расщепляющий мономорфизм ψ группы $L(G)$ в $A(G)$.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \leftrightarrow \begin{pmatrix} 2 & 3 \\ 3 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \leftrightarrow \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix}$$

где матрицы слева принадлежат группе $L(G)$ и справа — группе $A(G)$.

Непосредственным счетом убеждаемся, что указанное отображение ψ — мономорфизм $L(G)$ в $A(G)$, обратный к λ.

2) Для $p = 3$ рассмотрим в качестве контрпримера группу G типа [9, 9]. Линейная часть — полная линейная группа $GL_2(3)$. Для построения расщепляющего мономорфизма $\psi : L(G)$ в $A(G)$ введем в рассмотрение об-

разующие группы $L(G)$:

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \tag{19}$$

Они удовлетворяют, как нетрудно увидеть, следующим определяющим отношениям:

$$a^8 = b^2 = c^3 = 1,\ bab = a^3,\ bcb = c^2,\ ac = c^2ba^2,\ ac^2 = ca^7. \tag{20}$$

Пусть $(a)\psi$, $(b)\psi$, $(c)\psi$ —элементы из $A(G)$, записываемые в виде следующих матриц:

$$(a)\psi = \begin{pmatrix} 3 & 4 \\ 1 & 1 \end{pmatrix}, \quad (b)\psi = \begin{pmatrix} 2 & 2 \\ 3 & 7 \end{pmatrix}, \quad (c)\psi = \begin{pmatrix} 7 & 4 \\ 6 & 1 \end{pmatrix}. \tag{21}$$

Нетрудными выкладками можно убедиться, что эти матрицы удовлетворяют тем же отношениям(20), как и соответствующие им элементы из $L(G)$, и что для отображения ψ имеет место $\psi\lambda = I_d$. Тем самым отображение ψ распространенное на всю группу $L(G)$ и будет расщепляющим мономорфизмом для расширения (1).

Примерами 1) и 2) не исчерпываются случаи расщепления последовательностей (1) для 2- и 3-групп, не удовлетворяющих условиям теоремы.

ЛИТЕРАТУРА

1. Холл М. Теория групп.— М.: Изд-во иностр. лит., 1972.— 468 с.
2. Курош А. Г. Теория групп.— 2-е изд.— М.: Гостехиздат, 1953.— 467 с.
3. Фукс Л. Бесконечные абелевы группы. В 2-х т.— М.: Мир, 1974—1977. Т. 1. 1974. 335 с.; т. 2. 1977. 416 с.
4. Gorenstein D. Finite Groups. N. Y.: Harper & Row, 1968.— 527 p.
5. Кишкина З. М. Эндоморфизмы p-примитивных абелевых групп без кручения.— Изв. АН СССР. Сер. мат., 1945, 9, с. 201—232.
6. Хассе Х. Лекции по теории чисел.— М.: Изд-во иностр. лит., 1953.— 527 с.
7. Ленг С. Алгебра.— М.: Мир, 1968.— 564 с.

Санта Клара, Куба
Центральный университет

Поступила в редакцию
30.I 1979 г.