Полупростые скрещенные групповые алгебры циклических p-групп нечетного порядка

Н. А. НАЧЕВ, Т. Ж. МОЛЛОВ (Пловдив)

Пусть $\langle g \rangle$ — циклическая группа порядка p^n, где p — нечетное простое число и K — поле с характеристикой отличной от p. Тогда известно, что скрещенная групповая алгебра $K_t\langle g \rangle$ группы $\langle g \rangle$ над полем K полупроста и разлагается в прямую сумму полей. В настоящей работе строится это разложение с точностью до изоморфизма, учитывая вид полей и число повторений в них. Этим построено и разложение фактор-алгебры $K[x]/\langle x^{p^n}-a \rangle$ в прямую сумму минимальных идеалов, где $a \in K \setminus \{0\}$ и $\langle x^{p^n}-a \rangle$ — главный идеал алгебры полиномов $K[x]$, порожденный полиномом $x^{p^n}-a$. Дается полное описание мультипликативной группы $U(K_t\langle g \rangle)$ алгебры $K_t\langle g \rangle$.

Настоящая работа является продолжением статьи [5] и формулировки некоторых ее результатов опубликованы в [4].

Пусть $\langle g \rangle$ — циклическая p-группа порядка p^n, где p — нечетное простое число и K — поле с характеристикой отличной от p. Обозначим через g^k k-ую степень элемента g в скрещенной групповой алгебре $K_t\langle g \rangle$ [5]. Тогда равенство $g^{p^n}=a$, $a \in K \setminus \{0\}$, определяет алгебру $K_t\langle g \rangle$ [5]. Введем обозначение $L^{p^i}=\{c^{p^i} \mid c \in L\}$, где L поле (группа), а $i \in \mathbf{N}_0$ — множество неотрицательных целых чисел. Пусть s — наибольшее целое число интервала $[0, n]$, для которого $a \in K^{p^s}$. Тогда существует такой элемент $b \in K$, что $b^{p^s}=a$ и такой элемент α алгебраического замыкания $\overline{K}$ поля K, что $\alpha^{p^{n-s}}=b$. Пусть ε_i — первообразный корень степени p^i из единицы в $\overline{K}$, $i \in \mathbf{N}_0$ ($\varepsilon_0=1$). Наибольшее натуральное число m интервала $[1, n]$, для которого $K(\varepsilon_1)=K(\varepsilon_m)$, называется n-константой поля K относительно p. Если $K(\varepsilon_i) \neq K(\varepsilon_1)$ для некоторого $i \in \mathbf{N}$, то K называется полем первого рода относительно p. В противном случае K называется полем второго рода относительно p ([1] или [2, стр. 187]). Если K — поле первого рода относительно p, то максимальное число $m' \in \mathbf{N}$, для которого $K(\varepsilon_1)=K(\varepsilon_{m'})$, называется постоянной поля K относительно p. Очевидно $m=\min(n, m)$]. Пусть $d=\big(K(\varepsilon_1):K\big)$ — степень поля $K(\varepsilon_1)$ над K, L^* — мультипликативная группа поля L и L_p — силовская p-подгруппа группы L^*. Если $c \in K^*$, то обозначим через $H(c)$ [3] p-высоту смежного класса $cK(\varepsilon_1)_p$ во фактор-группе $K(\varepsilon_1)^*/K(\varepsilon_1)_p$. Высота $H(c)$ можно определить и другим образом. Именно, хорошо известно [3], что имеет место прямое разложение $K(\varepsilon_1)^*=K(\varepsilon_1)_p \times V$, где V — подгруппа группы $K(\varepsilon_1)^*$. Тогда, если $c \in K^*$, то $c=uv$ где $u \in K(\varepsilon_1)_p$, а $v \in V$ и высота $H(c)$ совпадает с p-высотой $h(v)$ элемента v в группе V [3]. Введем еще следующие обозначения:

$\oplus$, Σ — знаки для прямых сумм алгебр;
tL — прямая сумма t алгебр, равные алгебре L;
$H_k(b)=\min(k, H(b))$, $k\in \mathbf{N}_0$ (см. [3]);
$\beta_i=\max(0, i-m)$, $0\leqq i\leqq s$;
$d_i=d$, если $i=1, \dots, s$ и $d_0=1$;
$\mu_i=\varphi(p^{i-\beta_i})/d_i$, $0\leqq i\leqq s$, где φ — функция Эйлера;
$\theta=\max(m+s+l-n, 0)$, $l=\min(n-m, l])$, $l'=H_{n-s}(b)$;
$\lambda_i=\min(i, m)-\theta$; $\theta\leqq i\leqq s$;

$$\delta_i=\begin{cases}1, \text{ если } & i=\theta \quad \text{или} \quad \theta=m;\\ \varphi(p^{\lambda_i})/d, & \text{если} \quad i\neq\theta \quad \text{и} \quad \theta\neq m; \quad \theta\leqq i\leqq s.\end{cases}$$

Отметим следующие тривиальные свойства введенных чисел:
а) $i-\beta_i\geqq 0$; имеет место $i-\beta_i=0$ тогда и только тогда, когда $i=0$;
б) $\partial_i\geqq 0$; $\partial_i=0$ тогда и только тогда, когда $i=\theta$ или $\theta=m$;
в) имеет место $\delta_i=\varphi(p^{\lambda_i})/d_{\lambda_i}$, $\theta\leqq i\leqq s$;
г) если K — поле второго рода относительно p, то $m=n$, $l=0$ и $\theta=s$.
Справедливы следующие неравенства:

$$m-i+\beta_i\geqq 0,\quad s-i+\beta_i\geqq 0,\quad n-s-l'\geqq 0, \tag{1}$$
$$n-s-l\geqq 0,\quad \theta\leqq m,\quad \theta\leqq s.$$

Докажем, например, предпоследнее из этих неравенств. Если допустим, что $\theta>m$, то получится $m<\theta=m+s+l-n$, откуда вытекает противоречие $l>n-s$.
Имеет место формула

$$i-\beta_i-\lambda_i=\theta,\quad \theta\leqq i\leqq s. \tag{2}$$

Действительно,

$$i-\beta_i-\lambda_i=i-\max(0, i-m)-\min(i, m)+\theta=\min(i, m)-\min(i, m)+\theta=\theta.$$

Если (c, d) — наибольший обший делитель чисел c, $d\in\mathbf{Z}$, то

$$(\varphi(p^{\lambda_i}), \mu_i)=\delta_i,\quad \theta\leqq i\leqq s. \tag{3}$$

Для доказательства этого равенства обозначим через v_i левую часть формулы (3) . Рассмотрим два случая.
1) Пусть $i=\theta$ или $\theta=m$. Тогда $\delta_i=1$ и $\partial_i=0$. Следовательно, $v_i=1$, т. е. $v_i=\delta_i$.
2) Пусть $i\neq\theta$ и $\theta<m$, т. е. $\theta<i$. Тогда $\lambda_i\geqq 1$, $i-\beta_i\geqq 1$ и

$$v_i=\frac{p-1}{d}(p^{\lambda_i-1}d, p^{i-\beta_i-1})=\frac{p-1}{d}p^{\lambda_i-1}=\frac{\varphi(p^{\lambda_i})}{d}=\delta_i,$$

где второе равенство выполняется в силу (2).
Если $\theta>0$, то

$$n-s-l\leqq m-i,\quad i=1, \dots, \theta. \tag{4}$$

Действительно, из $1 \leqq i \leqq \theta = \max(m+s+l-n, 0)$ вытекает

$$\max(m+s+l-n-i, -i) \geqq 0,$$

т. е. $m+s+l-n-i \geqq 0$, откуда получается $n-s-l \leqq m-i$.

Перейдем теперь к формулировке основного результата о разложении алгебры $K_t\langle g\rangle$.

Теорема 1. *Пусть $\langle g\rangle$ — циклическая группа порядка p^n, где p — нечетное простое число, K — поле с характеристикой отличной от p, скрещенная групповая алгебра $K_t\langle g\rangle$ определена равенством $g^{p^n}=a$, $a \in K^*$, и u — первообразный корень по модулью p^m. Тогда алгебра $K_t\langle g\rangle$ разлагается с точностью до K изоморфизма, в прямую сумму полей следующим образом:*

1) *если $K=K(\varepsilon_1)$ и 1.1) $\theta \neq m$ или $\theta=m=s$, то*

$$K_t\langle g\rangle \cong p^\theta \sum_{i=\theta}^{s} \sum_{j=0}^{\delta_i-1} K(\alpha\varepsilon_{n-s+i}^{u^j}); \tag{5}$$

1.2) *если $\theta=m<s$, то*

$$K_t\langle g\rangle \cong p^m K(\alpha) \oplus p^{m-1}(p-1) \sum_{i=m+1}^{s} K(\alpha\varepsilon_{n-s+i}); \tag{6}$$

2) *если $K \neq K(\varepsilon_1)$ и 2.1) $\theta=s$, то*

$$K_t\langle g\rangle \cong K(\alpha) \oplus \frac{p^s-1}{d} K(\alpha\varepsilon_n); \tag{7}$$

2.2) *если $s>\theta$ и $m>\theta$, то*

$$K_t\langle g\rangle \cong K(\alpha) \oplus \frac{p^\theta-1}{d} K(\alpha\varepsilon_{n-s+\theta}) \oplus p^\theta \sum_{i=\theta+1}^{s} \sum_{j=0}^{\delta_i-1} K(\alpha\varepsilon_{n-s+i}^{u^j}); \tag{8}$$

2.3) *если $s>\theta=m$, то*

$$K_t\langle q\rangle \cong K(\alpha) \oplus \frac{p^m-1}{d} K(\alpha\varepsilon_{n-s+m}) \oplus \frac{p^{m-1}(p-1)}{d} \sum_{i=m+1}^{s} K(\alpha\varepsilon_{n-s+i}). \tag{9}$$

Отдельные слагаемые любого из этих разложений неизоморфны.

Для доказателства теоремы нам понадобятся несколько лемм. Специально в первой из них используется следующий тривиальный факт: *если G — такая абелева группа, что $G_p=1$, то $h(gp^k)=h(g)+k$ для любого $g \in G$ и $k \in \mathbf{N}_0$.*

Лемма 1. *Для любых $k, r \in \mathbf{N}_0$ и $c \in K^*$ имеет место $H_{k+r}(c^{p^r}) = H_k(c)+r$.*

Доказательство. Пуст $K(\varepsilon_1)^* = K(\varepsilon_1)_p \times V$, $c=uv$, где $u \in K(\varepsilon_1)_p$ и $v \in V$, $q'=H(c)$ и $H_k(c)=q$. Тогда $H(c)=h(v)$, $q=\min(k, q')$ и $v=v_1 p^q$, $v_1 \in V$, $h(v_1) \geqq 0$. Из $c=uv_1^{p^q}$ следует $c^{p^r}=u^{p^r} v_1^{p^{q+r}}$ и

$$H(C^{p^r}) = h(v_1^{p^{q+r}}) = h(v_1)+q+r.$$

Следовательно,

$$H_{k+r}(c^{p^r}) = \min(k+r, h(v_1)+q+r) = \min(k-q, h(v_1))+q+r = q+r = H_k(c)+r,$$

поскольку $\min(k=q, h(v_1))=0$.

Лемма 2. *Имеет место*

$$\langle \varepsilon_t \rangle \cap K(\varepsilon_1)_p^{p^{n-s-l'}} = \langle \varepsilon_\theta \rangle,$$

где $t=\min(m, s)$.

Доказательство. Действительно

$$\varepsilon_\theta = \varepsilon_m^{p^{n-s-l}} \in K(\varepsilon_1)_p^{p^{n-s-l}} \subseteqq K(\varepsilon_1)_p^{p^{n-s-l'}}.$$

Кроме того $\langle \varepsilon_\theta \rangle \subseteqq \langle \varepsilon_t \rangle$, так как $\theta \leqq \min(m, s)=t$. Следовательно,

$$\langle \varepsilon_\theta \rangle \subseteqq \langle \varepsilon_t \rangle \cap K(\varepsilon_1)_p^{p^{n-s-l'}}.$$

Докажем обратное включение. Рассмотрим два случая.

1) Пусть $l' \geqq n-m$. Тогда $l=n-m$, откуда вытекает $\theta=s$. Кроме того $n-m \leqq l' \leqq n-s$. Отсюда получается $s \leqq m$. Следовательно, $t=s=\theta$. Таким образом, имеет место

$$\langle \varepsilon_t \rangle \cap K(\varepsilon_1)_p^{p^{n-s-l'}} \subseteqq \langle \varepsilon_t \rangle = \langle \varepsilon_\theta \rangle.$$

2) Пусть $l' < n-m$. Тогда $m<n$ и $l'=l$. Следовательно,

$$\langle \varepsilon_t \rangle \cap K(\varepsilon_1)_p^{p^{n-s-l'}} \subseteqq K(\varepsilon_1)_p^{p^{n-s-l'}} = \langle \varepsilon_m \rangle^{p^{n-s-l}} = \langle \varepsilon_\theta \rangle.$$

Лемма доказана.

Пусть $\mathbf{Z}^{p^t}$ — мультипликативная группа фактор-кольца $\mathbf{Z}/\langle p^t \rangle$, где $\langle p^t \rangle$-главный идеал кольца $\mathbf{Z}$, порожденный элементом p^t, $t \in \mathbf{N}$. Следующая лемма хорошо известна (см. [5]).

Лемма 3. *Пусть* $t \in \mathbf{N}$ *и если* K *— поле первого рода относительно* p, *то* $t \leqq m'$. *Существует вложение* $\varphi_t\colon G \to \mathbf{Z}_{p^t}{}^*$ *группы* G *Галуа поля* $K(\varepsilon_1)$ *над* K, *определенное следующим образом: для каждого* $\tau \in G$ *положим* $\varphi_t(\tau) = \lambda + \langle p^t \rangle$, *где* λ *— такое целое число, что* $\tau(\varepsilon_{m'}) = \varepsilon_{m'}^{\lambda}$. *Образ* $\varphi_t(G)$ *состоит из всех смежных классов* $\lambda + \langle p^t \rangle$, *для которых* $\lambda^d \equiv 1 \pmod{p^t}$.

Для доказательства теоремы используем, что полином $x^{p^n}-a$ разлагается в произведение

$$f(x) = \prod_{i=0}^{s} \prod_{j=0}^{\mu_i - 1} f_{ij}(x), \quad f_{ij}(x) = \prod_{k=0}^{d_i - 1} \left(x^{p^{n-s+\beta_i}} - b^{p^{\beta_i}} \varepsilon_{i-\beta_i}^{u^{j+k\mu_i}}\right), \tag{10}$$

неприводимых множителей над K (см. [5]) и что полином $f_{ij}(x)$ имеет корень $\alpha \varepsilon_{n-s+i}^{u^j}$. Так как различные множители $f_{ij}(x)$, $0 \leqq i \leqq s$, $0 \leqq j \leqq \mu_i - 1$, взаимно просты и алгебра $K_t\langle g \rangle$ соответствует полиному $f(x)$, то имеет место

$$K_t\langle g \rangle \cong \sum_{i=0}^{s} \sum_{j=0}^{\mu_i - 1} K_{ij} \tag{11}$$

(см. [6]), где

$$K_{ij} = K(\alpha\varepsilon_{n-s+i}^{u^j}), \quad 0 \leqq i \leqq s, \quad 0 \leqq j \leqq \mu_i - 1, \tag{12}$$

Далее докажем следующие утверждения.

Лемма 4. *Если* $K \neq K(\varepsilon_1)$, *то для полей* (12) *имеет место* K-*изоморфизм* $K_{ij} \cong K(\alpha)$ *тогда и только тогда, когда* $i=0$ *и* $j=0$.

Доказательство. Пусть $K_{ij} \cong K(\alpha)$. Тогда

$$d_i p^{n-s+\beta_i} = (K_{ij}:K) = \big(K(\alpha):K\big) = p^{n-s}.$$

Отсюда следует $d_i=1$. Поскольку $K \neq K(\varepsilon_1)$, то получается $i=0$. Так как $\mu_0=1$, то из ограничений (12) для i и j вытекает $j=0$.

Наоборот, если $i=j=0$, то $K_{ij}=K(\alpha\varepsilon_{n-s})$. Поскольку минимальные полиномы для $\alpha\varepsilon_{n-s}$ и α совпадают, то $K(\alpha\varepsilon_{n-s}) \cong K(\alpha)$. Следовательно, $K_{ij} \cong K(\alpha)$.

Лемма 5. *Для полей* (12), *где* $i \neq 0$ *и* $i' \neq 0$ *при* $K \neq K(\varepsilon_1)$ *имеет место* K-*изоморфизм* $K_{i'j'} \cong K_{ij}$, *тогда и только тогда, когда* $\beta_{i'}=\beta_i$ *и существует такое целое число* $k \in [0, d_i-1]$, *что*

$$\varepsilon_{i-\beta_i}^{u^{j+k\mu_i}}\, \varepsilon_{i'-\beta_i}^{-u^{j'}} \in \langle \varepsilon_\theta \rangle.$$

Доказательство. Ввиду [3, следствие 1 и теорема 3] имеет место K-изоморфизм $K_{i'j'} \cong K_{ij}$ тогда и только тогда, когда выполняются следующие две условия:

(a) $\deg f_{i'j'}(x) = \deg f_{ij}(x)$, где $\deg f_{ij}(x)$-степень полинома $f_{ij}(x)$;

(в) существует такой элемент $\sigma \in G\big(K(\varepsilon_1): K\big)$, что

$$\sigma(\varepsilon_{i-\beta_i}^{u^j})\varepsilon_{i'-\beta_i}^{-u^{j'}} \in K(\varepsilon_1)_p^{p^{n-s+\beta_i-l_{\beta_i}}}, \tag{13}$$

где $l_{\beta_i} = H_{n-s+\beta_i}(b^{p^{\beta_i}})$. Условие (а) эквивалентно равенству $\beta_{i'}=\beta_i$, так как $d_i=d_{i'}=d$ и $\deg f_{i'j'}(x)=d_{i'}\,p^{n-s+\beta_{i'}}$, а $\deg f_{ij}(x)=d_i\,p^{n-s+\beta_i}$. Чтобы условие (в) будем использовать лемму 1, из которой получается $l_{\beta i}=l'+\beta_i$ и лемму 3, из которой следует существование такого $\lambda \in \mathbf{Z}$, что

$$\sigma(\varepsilon_{i-\beta_i}^{u^j}) = \varepsilon_{i-\beta_i}^{\lambda u^j} \quad \text{и} \quad \lambda^{d_i} \equiv 1 \,(\mathrm{mod}\ p^{i-\beta_i}). \tag{14}$$

Так как $i-\beta_i \leqq m$, ти u — первообразный корень по модулю $p^{i-\beta_i}$, откуда, ввиду известных фактов теории чисел, вытекает, что указанное сравнение в (14) эквивалентно условию $\lambda \equiv u^{k\mu_i}(\mathrm{mod}\ p^{i-\beta_i})$, $k \in \mathbf{Z}$. Поскольку $\varphi(p^{i-\beta_i})=\mu_i d_i$, то решения последнего сравения относительно k берутся по модулю d_i, т. е. k можно выбрать в интервале $[0,\ d_i-1]$. Тогда условие (13) принимает вид

$$\varepsilon_{i-\beta_i}^{u^{j+k\mu_i}}\varepsilon_{i'-\beta_i}^{-u^{j'}} \in K(\varepsilon_1)_p^{p^{n-s-l'}}. \tag{15}$$

Так как $i-\beta_i \leqq \min(m, s)=t$, и $i^i\beta_i \leqq t$, то (15) эквивалентно условию

$$\varepsilon_{i-\beta_i}^{u^{j+k\mu_i}}\varepsilon_{i'-\beta_i}^{-u^{j'}} \in \langle \varepsilon_t \rangle \cap K(\varepsilon_1)_p^{p^{n-s-l'}}.$$

Остается применить лемму 2, чем утверждение доказано.

Лемма 6. *Если* $i>\theta$, *то для полей* (12) *имеет место* K-*изоморфизм* $K_{i'j'}\cong\cong K_{ij}$ *тогда и только тогда, когда* $i'=i$ *и* $j'\equiv j\ (\mathrm{mod}\ \delta_i)$.

Доказательство. Сначбла докажем, что K-изоморфизм $K_{i'j'}\cong K_{ij}$ имеет место тогда и только тогда, когда выполнены следующие две условия:

$$\text{(A)}\quad i'=i;$$

$$\text{(B)}\quad \varepsilon_{i-\beta_i}^{u^j+k\mu_i-u^{j'}}\in\langle\varepsilon_\theta\rangle.$$

Действительно, из (A) и (B), ввиду леммы 5, очевидно следует $K_{i'j'}\cong K_{ij}$. Для доказательства обратного утверждения сначала допустим, что $\theta=m$. Тогда, виду леммы 5, имеет место

$$0<i-m=\beta_i=\beta_{i'}=\max(0,\ i'-m)=i'-m.$$

Следовательно, (A) выполнено, а отсюда, ввиду леммы 5, вытекает и (B).

Пусть теперь $\theta<m$. Тогда $\lambda_i>0$ и из формулы (2) получается $i-\beta_i==\theta+\lambda_i>\theta$. Отсюда, ввиду $(u,p)=1$, следует, что $\varepsilon_{i-\beta_i}^{u^j+k\mu_i}\notin\langle\varepsilon_\theta\rangle$. Тогда из леммы 5 вытекает $i'-\beta_i=i-\beta_i$. Таким образом выполнено условие (A), откуда, ввиду леммы 5, следует и (B).

Далее, преобразуем условие (B). Оно, ввиду формулы (2), принимает вид

$$\varepsilon_{\theta+\lambda_i}^{u^j+k\mu_i-u^{j'}}\in\langle\varepsilon_\theta\rangle=\langle\varepsilon_{\theta+\lambda_i}^{p^{\lambda_i}}\rangle.$$

Последнее условие эквивалентно разрешимости сравнения

$$u^{j+k\mu_i}\equiv u^{j'}\ (\mathrm{mod}\ p^{\lambda_i})$$

относительно k. Так как $\lambda_i\leqq m$, то u — первообразный корень по модулю p^{λ_i}. Следовательно, последнее сравнение эквивалентно сравнению

$$j+k\mu_i\equiv j'\ (\mathrm{mod}\ \varphi(p^{\lambda_i})).$$

Из формулы (3) следует, что это сравнение разрешимо относительно k тогда и только тогда, когда $j'\equiv j\ (\mathrm{mod}\ \delta_i)$ Лемма доказана.

Лемма 7. *Если* $K=K(\varepsilon_1)$ *и* $i\leqq\theta$, *то для полей* (12) *имеет место* K-*изоморфизм* $K_{i'j'}\cong K_{ij}$ *тогда и толко тогда ‚лоса‚* $i'\leqq\theta$,

Доказательство. Необходимость. Если допустим что $i'>\theta$, то из леммы 6 вытекает $i=i'>\theta$, что ведет и противоречию.

Достаточность. Из $i\leqq\theta$, $i'\leqq\theta$ и $\theta\leqq m$ вытекает $\beta_i=\beta_{i'}=0$. Опять из $i\leqq\theta$, $i'\leqq\theta$ следует $\varepsilon_i^{u^j}\varepsilon_{i'}^{-u^{j'}}\in\langle\varepsilon_\theta\rangle$. Применяя достаточность леммы 5, получаем K-изоморфизм $K_{i'j'}\cong K_{ij}$.

Лемма 8. *Если* $K\neq K(\varepsilon_1)$ *и* $0<i\leqq\theta$, *то для полей* (12) *имеет место* K-*изморфизм* $K_{i'j'}\cong K_{ij}$, *тогда и только тогда, когда* $0<i'\leqq\theta$.

Доказательство Необходимость. Если допустим, что $i'>\theta$, то из леммы 6 вытекает $i=i'>\theta$, что является противоречием. Следовательно, $i'\leqq\theta$.

Если $i'=0$, то из $\mu_0=1$ и из ограничений (12) для j' получается $j'=0$. Тогда, ввиду леммы 4, $i=0$, что противоречит условию. Таким образом $0<i'\leqq\theta$.

Достаточность. доказывается аналогично доказательству достаточности леммы 7.

Далее, обозначим через A_{ij} класс изоморфных полей в разложении (11), содержащий фиксированное поле K_{ij}, а через v_{ij} — число элементов этого класса.

Лемма 9. *Множество $\mathscr{A}$ всех полей K_{ij} формулы* (11) *разбивается на различные между собой классы изоморфных полей следующим образом:*

1) *если $K=K(\varepsilon_1)$, то эти классы — A_{ij}, где $\theta\leqq i\leqq s$ и $0\leqq j\leqq\delta_i-1$;*

2) *если $K\neq K(\varepsilon_1)$ и* 2.1) *$\theta=0$, то A_{ij}, $0\leqq i\leqq s$, $0\leqq j\leqq\delta_i-1$ — классы множества $\mathscr{A}$.*

2.2) *если $\theta=s>0$, то эти классы — A_{00} и $A_{\theta 0}$;*

2.3) *если $0<\theta<s$, то классы множества $\mathscr{A}$ являются A_{00}, $A_{\theta 0}$ и A_{ij}, где $\theta+1\leqq i\leqq s$ и $0\leqq j\leqq\delta_i-1$.*

Доказательство леммы вытекает из лемм 4, 6, 7, и 8.

Лемма 10. *Пусть $K=K(\varepsilon_1)$, $\theta\leqq i\leqq s$ и $0\leqq j\leqq\delta_i-1$. Тогда*

а) *если $\theta<m$ или $i=\theta$, то $v_{ij}=p^{\theta}$;*

в) *если $\theta=m<i$, то $v_{ij}=p^{m-1}(p-1)$.*

Доказательство. Так как $K=K(\varepsilon_1)$, то $d_i=1$. Рассмотрим два случая.

1) Пусть $i>\theta$. Из леммы 6 и из разложения (11) следует, что $v_{ij}=\mu_i/\delta_i$.

1 1) Пусть $\theta<m$. Тогда, ввиду свойства б), $\lambda_i\neq 0$. Так как, в силу а), $i-\beta_i>0$, то

$$v_{ij}=\frac{\mu_i}{\delta_i}=\frac{p^{i-\beta_i-1}(p-1)}{p^{\lambda_i-1}(p-1)}=p^{i-\beta_i-\lambda_i}=p^{\theta},$$

где последнее равенство следует из (2).

1.2) Пусть $\theta=m$. Тогда $\lambda_i=0$, откуда следует $\delta_i=1$. Так как $m=\theta<i$, то $i-\beta_i=m$. Тогда

$$v_{ij}=p^{i-\beta_i-1}(p-1)=p^{m-1}(p-1).$$

2) Пусть $i=\theta$. Так как $\theta\leqq m$, то для каждого $t, 0\leqq t\leqq\theta$, имеет место $\beta_t=0$. Из леммы 7, имея ввиду (11), получается

$$v_{\theta 0}=\sum_{t=0}^{\theta}\mu_t=\sum_{t=0}^{\theta}\varphi(p^t)=p^{\theta}.$$

Лемма 11. *Пусть $K\neq K(\varepsilon_1)$. Тогда* 1) *если $\theta>0$, то $v_{\theta 0}=\dfrac{p^{\theta}-1}{d}$;*

2) *если $\theta<i\leqq s$ и* 2.1) *$\theta<m$, ро $v_{ij}=p^{\theta}$;*

2.2) *если $\theta=m$, то $v_{ij}=p^{m-1}(p-1)/d$.*

Доказательство. Так как $\theta \leqq m$, то для каждого t, $1 \leqq t \leqq \theta$, имеет место, $\beta_t = 0$. Из леммы 8 и из (11) следует, что

$$\nu_{\theta 0} = \sum_{t=1}^{\theta} \mu_t = \sum_{t=1}^{\theta} \frac{\varphi(p^t)}{d} = \frac{p^\theta - 1}{d}.$$

2) Пусть $\theta < i$. Тогда, ввиду а), $i - \beta_i \neq 0$. Так как для фиксированного i существуют μ_i полей K_{ij}, то из леммы 6 вытекает, что $\nu_{ij} = \mu_i/\delta_i$, т. е. ввиду свойство в), что

$$\nu_{ij} = \frac{p^{i-\beta_i-1}(p-1)d_{\lambda_i}}{d\varphi(p^{\lambda_i})}. \tag{16}$$

2.1) Пусть $\theta < m$. Тогда $\lambda_i = \min(i-\theta, m-\theta) > 0$ и (16) принимает вид

$$\nu_{ij} = \frac{p^{i-\beta_i-1}(p-1)}{p^{\lambda_i-1}(p-1)} = p^{i-\beta_i-\lambda_i} = p^\theta,$$

где последнее равенство следует из (2).

2.2) Пусть $\theta = m$. Тогда $\lambda_i = 0$, $i - \beta_i = m$ и (16) принимает вид $\nu_{ij} = p^{m-1}(p-1)/d$. Лемма доказана.

Доказательство теоремы 1. 1) Пусть $K = K(\varepsilon_1)$. Разложение (11), на основании леммы 9, можно занисать в виде

$$K_t\langle g\rangle \cong \sum_{i=\theta}^{s} \sum_{j=0}^{\delta_i - 1} \nu_{ij} K_{ij}. \tag{17}$$

1.1) Пусть $\theta \neq m$ или $\theta = m = s$. Если $\theta = m = s$, то ввиду случая а) леммы 10, (17) принимает вид (5), так как при $i = \theta = s$ имеет место $\delta_i = 1$ и $j = 0$. Поэтому рассмотрим случай, когда $\theta \neq m$. Так как ввиду случая а) леммы 10, числа ν_{ij} в формуле (17) равняются p^θ, то разложение (17) принимает вид (5), т. е. формула (5) справедлив.а

1.2) Пусть $\theta = m < s$. Из случаев а) и в) леммы 10 вытекает соответственно, что в (17) имеет место $\nu_{\theta 0} = p^\theta$ и $\nu_{ij} = p^{m-1}(p-1)$ при $i < \theta$. Так как $K_{\theta 0} \cong K_{00} \cong K(\alpha)$, где первый изоморфизм следует из леммы 7, а второй — из леммы 4, то (17) принимает вид (6).

2) Пусть $K \neq K(\varepsilon_1)$ и 2.1) $\theta = s$. Рассмотрим два подслучая: а) $s = 0$ и в) $s \neq 0$.

а) Пусть $s = 0$. Тогда из случая 2.1 леммы 9 вытекает, что (17) принимает вид $K_t\langle g\rangle \cong \nu_{00} K_{00}$, а из леммы 4, что $\nu_{00} = 1$ и $K_{00} \cong K(\alpha)$. Следовательно, имеет место формула (7).

в) Пусть $s \neq 0$. Тогда из случая 2.2) леммы 9 вытекает, что (17) принимает вид

$$K_t\langle g\rangle \cong \nu_{00} K_{00} \oplus \nu_{\theta 0} K_{\theta 0}. \tag{18}$$

Так как $\nu_{00} = 1$, $K_{00} \cong K(\alpha)$ и, ввиду леммы 11, $\nu_{\theta 0} = (p^s - 1)/d$, а $K_{\theta 0} = K(\alpha\varepsilon_n)$, то (18) принимает вид (7).

2.2) Пусть $s > \theta$ и $m > \theta$. Рассмотрим два подслучая.

а) Пусть $\theta=0$. Формулу (11), на основании случая 2.1) леммы 9, можно записать в виде

$$K_t\langle g\rangle \cong v_{00}K_{00}\oplus \sum_{i=1}^{s}\sum_{j=0}^{\delta_i-1} v_{ij}K_{ij}. \tag{19}$$

Так как в этой формуле, ввиду леммы 11, $v_{ij}=p^{\theta}$, то (19) принимает вид (8), чем случай 2.2.а) закончен.

Далее на основании леммы 9, формула (11) при $\theta\neq 0$ записывается в виде

$$K_t\langle g\rangle \cong v_{00}K_{00}\oplus v_{\theta 0}K_{\theta 0}\oplus \sum_{i=\theta+1}^{s}\sum_{j=0}^{\delta_i-1} K_{ij}. \tag{20}$$

2.2.в) Пусть $\theta\neq 0$. Так как, ввиду случаев 1) и 2.1) леммы 11, в формуле (20) имеет место соответственно $v_{\theta 0}=(p^{\theta}-1)/d$ и $v_{ij}=p^{\theta}$, то формула (20) принимает вид (8).

2.3) Пусть $s>\theta=m$. Так как, ввиду леммы 11, $v_{\theta 0}=(p^m-1)/d$, $v_{ij}=$ $=p^{m-1}(p-1)/d$ и $\delta_i=1$, то (20) принимает вид (9). Теорема доказана.

Теорема 2. *Если p — нечетное простое число и K — поле с характеристикой отличной от p, то фактор-алгебра $K[x]/\langle x^{p^n}-a\rangle$, где $a\in K^*$, обладает разложениями (5)—(9), соответственно когда* 1) $K=K(\varepsilon_1)$ *и* а) $\theta\neq m$ *или* в) $\theta=m=s$; 2) $K=K(\varepsilon_1)$ *и* $\theta=m<s$; 3) $K\neq K(\varepsilon_1)$ *и* $\theta=s$; 4) $K\neq K(\varepsilon_1)$, $s>\theta$ *и* $m>\theta$ *и* 5) $K\neq K(\varepsilon_1)$ *и* $s>\theta=m$.

Доказателсьтво следует непосредственно из теоремы 1 и из K-изоморфизма $K[x]/\langle x^{p^n}-a\rangle\cong K_t\langle g\rangle$ (см. [6]), где алгебра $K_t\langle g\rangle$ определена равенством $g^{p^n}=a$.

Пусть $U(L)$ — мултипликативная группа алгебры L и Π — знак прямого произведения групп.

Теорема 3. *Пуст p — нечетное простое число, K — поле с характеристикой отличной от p, алгебра $K_t\langle g\rangle$ определена равенством $g^{p^n}=a$ и u — первообразный корень по модулю p^m. Тогда*

1) *если* $K=K(\varepsilon_1)$ *и* а) $\theta\neq m$. *или* в) $\theta=m=s$, *то*

$$U(K_t\langle q\rangle)\cong \prod_{i=\theta}^{s}\prod_{j=0}^{\delta_i-1} U^{p^{\theta}}\big(K(\alpha\varepsilon_{n-s+i}^{u^j})\big);$$

2) *если* $K=K(\varepsilon_1)$ *и* $\theta=m<s$, *то*

$$U(K_t\langle g\rangle)\cong U^{p^m}\big(K(\alpha)\times \prod_{i=m+1}^{s} U^{p^{m-1}(p-1)}\big(K(\alpha\varepsilon_{n-s+i})\big);$$

3) *если* $K\neq K(\varepsilon_1)$ *и* $\theta=s$, *то*

$$U(K_t\langle g\rangle\cong U\big(K(\alpha)\big)\times U^{\frac{p^s-1}{d}}\big(K(\alpha\varepsilon_n)\big);$$

4) *если* $K \neq K(\varepsilon_1)$, $s > \theta$ *и* $m > \theta$, *то*

$$U(K_t\langle g\rangle) \cong U\big(K(\alpha)\big)\times U^{\frac{p^\theta-1}{d}}\big(K(\alpha\varepsilon_{n-s+\theta})\big)\times \prod_{i=\theta+1}^{s}\prod_{j=0}^{\delta_i-1} U^{p^\theta}\big(K(\alpha\varepsilon_{n-s+i}^{u^j})\big)$$

и

5) *если* $K \neq K(\varepsilon_1)$ *и* $s > \theta = m$, то

$$U(K_t\langle g\rangle) \cong U\big(K(\alpha)\big)\times U^{\frac{p^m-1}{d}}\big(K(\alpha\varepsilon_{n-s+m})\big)\times \prod_{i=m+1}^{s} U^{\frac{p^{m-1}(p-1)}{d}}\big(K(\alpha\varepsilon_{n-s+i})\big).$$

Доказательство непосредственно следует из теоремы 1.

Литература

[1] С. Д. Берман. Групповые алгебры счетных абелевых p-групп. *Publ. Math. (Debrecen)* **14**, (1967), 365—405.

[2] Gr. Karpilovsky. Commutative Group Algebras, Marcel Dekker, Inc., *New York* and *Bassel*, 1983.

[3] Н. А. Начев. Инварианты биномных сепарабельных расширений. *Доклады БАН* **39**, (1986), 9—10.

[4] Н. А. Начев, Т. Ж. Моллов. О полупростых скрещенных групповых алгебрах циклических p-групп. *Доклады БАН* **40**, (1987), 13—15.

[5] Н. А. Начев, Т. Ж. Моллов, Минимальные идемпотенты полупростых скрещенных групповых алгебр циклических p-групп нечетного порядка. *Publ. Math. (Debrecen)* **35**, (1988), 309—319.

[6] Н. А. Начев, Т. Ж. Моллов. Изоморфизм полупростых скрещенных групповых алгебр циклических p-групп нечетного порядка. *Сердика* **14**, (1988), 75—81.

ПЛОВИДИВСКИЙ УНИВЕРСИТЕТ «П. ХИЛЕНДАРСКИ»
КАФЕДРА АЛГЕБРЫ, 4000 ПЛОВДИВ

(Поступило 16. августа 1986 г.)