Минимальные идемпотенты полупростых скрещенных групповых алгебр циклических p-групп нечетного порядка

Н. А. НАЧЕВ, Т. Ж. МОЛЛОВ (Пловдив)

В настоящей работе дается прямое доказательство критерия полупростоты скрещенной групповой алгебры K^tG конечной группы G над полем K. Если p-нечетное простое число и K — поле с характеристикой отличной от p, то рассматривается разложимость биномного полинома $x^{p^n}-a$ над полем K на неприводимые множители и строятся минимальные идемпотенты скрещенной групповой алгебры $K^t\langle g\rangle$ циклической p-группы $\langle g\rangle$ над полем K.

Формулировки некоторых результатов статьи опубликованы в [6].

§ 1. Некоторые обозначения и результаты о скрещенных групповых алгебрах

Пусть G — группа с операцией «$\cdot$», K — коммутативное кольцо с единицей 1 и K^* — мультипликативная группа кольца K. Чтобы определить понятие скрещенной групповой алгеброй K^tG группы G над кольцом K сначала нужно задать функцию $G\times G\to K^*$, т.е. любым двум элементам g и h группы G сопоставляется такой однозначно определенный елемент $(g,h)\in K^*$, чтобы выполнялось равенство

$$(g\cdot h, f)(g,h)=(g,h\cdot f)(h,f),\quad f\in G. \tag{1.1}$$

Некоторые авторы называют эту функцию системой факторов.

Скрещенная групповая алгебра K^tG группы G над полем K, которая соответствует указанной функции, называется K-алгеброй с базисом G, в которой умножение базисных элементов определено следующим образом:

$$gh=(g,h)(g\cdot h).$$

Отметим, что аналогичным образом можно дать общее определение скрещенного произведения группы G и кольца K (при отображении σ). Первоначальное определение скрещенного произведения группы и кольца дано в [2]. В соответствии с этим определением укажем некоторые обозначения и в связи с ними напомним некоторые факты о скрещенных групповых алгебрах.

Благодаря формуле (1.1) алгебра K^tG ассоциативна. Из определения следует, что каждый элемент $K'G$ единственным образом записывается в виде $\Sigma x_g g$, $x_g\in K$, $g\in G$. Будем обозначать n-ую степень элемента g в труппе G через

$g^{(n)}$, а в скрещенной групповой алгебре K^tG — обычным образом через g^n. Единицу группы будем обозначать через e. Тогда единица 1 алгебры K^tG будет $1=(e,e)^{-1}e$. Эту единицу отождествим с единицей кольца K. Кроме того, из (1.1) следует, что $(g,e)=(e,g)=(e,e)$ для каждого $g\in G$, а из введенного умножения в K^tG — что $g^{-1}=(e,e)^{-1}(g,g^{(-1)})^{-1}g^{(-1)}$. Отметим, что K-алгебра K — подалгебра алгебры K^tG, но группа G не является подгруппой мультипликативной группы алгебры K^tG.

Легко видеть, что если порядок n элемента $g\in G$ больше 1 и $1<k\leqq n$, то имеет место

$$g^k=\varrho(g^k)g^{(k)},\quad \varrho(g^k)=(g,g)(g,g^{(2)})\ldots(g,g^{(k-1)}). \tag{1.2}$$

Специально из формулы (1.2) видно, что элементы $1,g,\ldots,g^{n-1}$ образуют базис скрещенной групповой алгебры $K^t\langle g\rangle$. Высшие степени элемента g в $K^t\langle g\rangle$ определяются равенством $g^n=a$, $a=\varrho(g^n)(e,e)$. Поэтому будем говорить, что это равенство определяет скрещенную групповую алгебру $K^t\langle g\rangle$.

Легко видеть, что скрещенная групповая алгебра K^tG коммутативна тогда и только тогда, когда группа G абелева и имеют места равенства $(g,h)=(h,g)$ для любых элементов g и h группы G. Действительно алгебра K^tG коммутативна тогда и только тогда, когда для любых элементов g и h группы G имеет место $gh=hg$, т .е. когда выполнено $(g,h)(g\cdot h)=(h,g)(h\cdot g)$, откуда следует утверждение.

Хорошо известно, что скрещенная групповая алгебра $K^t\langle g\rangle$ конечной циклической группой $\langle g\rangle$ над коммутативным кольцом K с единицей коммутативна.

Если $\langle g\rangle$ — циклическая группа порядка n и уравнение

$$x^n=a,\quad a=\varrho(g^n)(e,e) \tag{1.3}$$

имеет решение в поле K, то скрещенная групповая алгебра $K^t\langle g\rangle$ изоморфна групповой алгебре $K\langle g\rangle$ группы $\langle g\rangle$ над полем K. Действительно пусть уравнение (1.3) имеет решение α в поле K. Так как $g^n=a$ и $\alpha^n=a$, то $(\alpha^{-1}g)^n=1$, элементы $1,\ \alpha^{-1}g,\ldots,(\alpha^{-1}g)^{n-1}$ образуют групповой базис алгебры $K^t\langle g\rangle$ и $K^t\langle g\rangle=K\langle\alpha^{-1}g\rangle$.

В следующем замечании поле $K(\alpha)$ рассматривается как K-алгебра.

Если $\langle g\rangle$ — циклическая группа порядка n и уравнение (1.3) неразложимо над полем K, то скрещенная групповая алгебра $K^t\langle g\rangle$ изоморфна K-алгебре $K(\alpha)$, где α — корень этого уравнения в его поле разложения над K.

В самом деле, отображение $g\mapsto\alpha$ единственным образом продолжается до изоморфизма K-алгебр $K^t\langle g\rangle\to K(\alpha)$, поскольку g и α удовлетворяют один и тот же неразложимый полином над K.

Пассман [7] доказывает, что если G — конечная группа и K — алгебраически замкнутое поле характеристики $p\neq 0$, причем p не делит порядка группы G, то скрещенная групповая алгебра K^tG полупроста. В [8] доказан этот результат, если G — разрешимая группа и или а) K — поле характеристики 0 или в) K поле характеристики p и G не содержит элемента порядка p. Первый и достаточно сильный результат в этом направлении (в более общей ситуации для скрещенного произведения группы и кольца) дает Бовди [2] при предполо-

жении, что G — локально конечная группа и K — регулярное кольцо, в котором можно однозначно делить на порядок любого элемента группы. Очевидно, что упомянутый результат в [7] следует непосредственно из [2], но в [7] дано, при сделанных предположениях, прямое доказательство полупростоты скрещенной алгебры K^tG. Следующее утверждение дает прямое доказательство критерия полупростоты скрещенной алгебры K^tG, используя идею «правого регулярного представления конечной группы G».

Предложение 1.1. *Елси G — конечная группа и K — поле, характеристика которого не делит порядка группы G, то скрещенная групповая алгебра K^tG полупроста.*

Доказательство. Пусть группа G имеет порядок n. Воспользуемся аналогом правого регулярного представления группы G в общую линейную группу $GL(n, K)$ степени n над полем K. Метрицы из $GL(n, K)$ будем рассматривать как функции $G\times G\to K$ и если M — любая такая матрица, то $M(g, h)$, где $g, h\in G$, обозначает элемент из K, которой лежит в g-ой строке и h-ом столбце этой матрицы. Далее, определим отображение φ: $G\to GL(n, K)$ при помощи формулы

$$(g\varphi)(h, f) = \begin{cases}(h, g), & \text{если } f = h\cdot g;\\ 0, & \text{если } f \neq h\cdot g,\end{cases}$$

для всех $g, h, f\in G$. Легко видеть, что $g\varphi\in GL(n, K)$ и что φ—корректно определенное отображение. Заметим, что φ-инъекция. В самом деле, если $g_1\neq g_2$, то

$$(g_1\varphi)(e, g_1) = (e, g_1) \neq 0 = (g_2\varphi)(e, g_1),$$

откуда $g_1\varphi\neq g_2\varphi$. Очевидно φ продолжается по линейности до гомоморфизма K-алгебры K^tG в общей матричной алгебре $ML(n, K)$, причем инъективность сохраняется. Докажем, что радикал J Джекобсона алгебры K^tG равен нулю. С этой целью допустим, что существует такое $x\in J$, что $x\neq 0$. Тогда $x=\sum\limits_{g\in G} x_g g$ и существует элемент $h\in G$, такой что $x_h\neq 0$. Отсюда вытекает, что коэффициент перед единицей элемента $xh^{(-1)}=y\in J$ равняется $y_e=$ $=x_h(h, h^{(-1)})(e, e)$ и отличен от нуля. Пусть $y=\sum\limits_{g\in G} y_g g$. Рассмотрим матрицу

$$z = y\varphi = y_e E + \sum_{g\in G\setminus\{e\}} y_g g,$$

где E — единичная матрица порядка n. Вычисляя след $\operatorname{tr} z$ матрица z, получим

$$\operatorname{tr} z = ny_e + \sum_{g\in G\setminus\{e\}} y_g \operatorname{tr}(g\varphi).$$

Так как элемены главного диагоналя матрицы $g\varphi$ при $g\neq e$ равняются нулю, то $\operatorname{tr}(g\varphi)=0$. Отсюда следует

$$\operatorname{tr} z = ny_e \neq 0, \tag{1.4}$$

где неравенство имеет место ввиду того, что характеристика поля K не делит n и $y_e\neq 0$. Теперь учтем, что алгебра K^tG артинова, так что J — нильпотентный

идеал. Поэтому y — нильпотентный элемент, откуда матрица z также нильпотентна. Но все характеристические корни любой нильпотентной матрицы равны нулю. Таким образом, $\operatorname{tr} z=0$, что противоречит формуле (1.4). Следовательно, $J=0$, что и требовалось доказать.

§ 2. Разложение специальных биномных полиномов над полем на неприводимые множители

Пусть p — простое число. Следующая лемма дает одно достаточное условие для неприводимости полинома $\varphi(x^{p^l})$ над полем K, когда полином $\varphi(x)$ неприводим над K.

Лемма 2.1. *Пусть $\varphi(x)$ — неприводимый полином над полем K и x_1 — корень этого полинома в алгебраическом замыкании $\overline{K}$ поля K. Если $x^{p^l}-x_1$ — неприводнимый полином над полем $K(x_1)$, то $\varphi(x^{p^l})$ — неприводимый полином над полем K.*

Доказательство. Пусть m — степень полинома $\varphi(x)$ и y_1 — корень полинома $x^{p^l}-x_1$ в $\overline{K}$. Из $y_1^{p^l}=x_1$ вытекает $K(y_1)=K(x_1, y_1)$. Так как полином $x^{p^l}-x_1$ неприводим над полем $K(x_1)$, то $(K(x_1, y_1)\colon K(x_1))=p^l$. Следовательно, $(K(x_1, y_1)\colon K)=mp^l$, т. е. $(K(y_1)\colon K)=mp^l$. Однако полином $\varphi(x^{p^l})$ степени mp^l над полем K имеет корень y_1 и степень алгебраичности элемента y_1 над K равна также mp^l. Следовательно, $\varphi(x^{p^l})$ — неприводимый полином над K.

Введем обозначение $(j, p)=1$, если j и p — взаимно простые целые числа и $L^{p^k}=\{x^{p^k}|x\in L\}$, где L — поле.

Замечание 2.2. *Если L — поле, $a\in L$ и $a^j\in L^p$ для $(j, p)=1$, то $a\in L^p$.*

Доказательство. Существуют такие целые числа u и v, что $ju+pv=1$. Следовательно, $a=(a^j)^u(a^p)^v\in L^p$.

Следующее определение хорошо известно (см. например [3, стр. 173]).

Определение 2.3. Пусть α принадлежит конечному расширению L поля K и $\varphi(x)=x^t+a_1x^{t-1}+\ldots+a_t$ является минимальным полиномом элемента α над полем K. След $\operatorname{tr}\alpha$ элемента α (из L в K) называется элементом

$$\operatorname{tr}\alpha=-a_1\frac{(L:K)}{t}$$

а норма $N(\alpha)$ элемента α (из L в K) — элементом

$$N(\alpha)=((-1)^ta_t)^{((L:K)/t)}.$$

Заметим, что $\operatorname{tr}(\alpha+\beta)=\operatorname{tr}\alpha+\operatorname{tr}\beta$ и $N(\alpha\beta)=N(\alpha)N(\beta)$. Кроме того, если $a\in K$, то $\operatorname{tr} a=a(L:K)$ и $N(a)=a^{(L:K)}$.

В дальнейшем будем предполагать, что p — нечетное простое число и K — поле, характеристика которого отлична от p. Рассмотрим разложение фиксированного биномного полинома вида

$$f(x)=x^{p^n}-a,\quad a\in K,$$

в произведение неприводимых множителей над K, где $n\in\mathbf{N}$. Пусть s — наибольшее целое число интервала $[0, n]$, для которого $a\in K^{p^s}$. Тогда существует такой элемент $b\in K$, что

$$b^{p^s} = a,$$

причем $b\in K\setminus K^p$, если $s<n$ 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 $\overline{K}$, $i\in\mathbf{N}$, и $\varepsilon_0=1$.

Определение 2.4. Наибольшее натуральное число m интервала $[1, n]$, для которого $K(\varepsilon_1)=K(\varepsilon_m)$, называется n-константой поля K относительно p.

Определение 2.5. Поле K называется полем первого рода относительно (нечетного простого числа) p, если $K(\varepsilon_i)\neq K(\varepsilon_1)$ для некоторого $i\in\mathbf{N}$, а в противном случае — полем второго рода относительно p ([1] или [4, стр. 187]). Если K — поле первого рода относительно p, то максимальное натуральное m', для которого $K(\varepsilon_1)=K(\varepsilon_{m'})$. называется константой поля κ относительно p.

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, $t\in\mathbf{N}$ и $d=(K(\varepsilon_1)\colon K)$ ($(K(\varepsilon_1)\colon K)$ — степень поля $K(\varepsilon_1)$ над K). Следующая лемма хорошо известна, но для полноты приводим ее доказательство.

Лемма 2.6. *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, определено следующим образом: для каждого $\tau\in G$ положим $\varphi_t(\tau)=\lambda+\langle p^t\rangle$, где λ — такое целое число, что $\tau(\varepsilon_{m'})=\varepsilon^{\lambda}_{m'}$. Образ $\varphi_t(G)$ состоит из всех смежных классов $\lambda+\langle p^t\rangle$, для которых $\lambda^d\equiv 1 \pmod{p^t}$.*

Доказательство. Так как τ — автоморфизм поля $K(\varepsilon_1)$ над K и $\tau(\varepsilon_t)=\varepsilon_t^{\lambda}$, то $(\lambda, p)=1$, т. е. $\lambda+\langle p^t\rangle\in\mathbf{Z}^*_{p^t}$. Очевидно φ_t — гомоморфизм. Кроме того $\tau\in\operatorname{Ker}\varphi_t$ тогда и только тогда, когда $1+\langle p^t\rangle=\lambda+\langle p^t\rangle$, т. е. тогда и только тогда, когда $\lambda\equiv 1 \pmod{p^t}$, что эквивалентно условию $\tau(\varepsilon_t)=\varepsilon_t^{\lambda}=\varepsilon_t$ или $\tau=1_G$, где 1_G — единица группы G. Поскольку порядок группы G равняется d и $\mathbf{Z}^*_{p^t}$ содержит единственную подгруппу порядка d, то $\varphi_t(G)$ обладает указанным свойством. Этим лемма доказана.

Введем еще следующие обозначения:

$$\beta_i = \max(0, i-m), \quad i = 0, 1, \ldots, s;$$

$$d_i = \begin{cases} 1, & \text{если } i = 0; \\ d, & \text{если } 1 \leqq i \leqq s; \end{cases}$$

$$\mu_i = \frac{\varphi(p^{i-\beta_i})}{d_i}, \quad i = 0, 1, \ldots, s,$$

где φ — функция Эйлера. Отметим только, что $i-\beta_i=0$ тогда и только тогда, когда $i=0$. Исползуя эти обозначения, докажем следующую теорему.

Теорема 2.7. *Пусть p — нечетное простое число, K — поле с характеристикой отличной от p, $f(x)=x^{p^n}-a$ — полином над K, $a\neq 0$ и u — первообразный корень по модулю p^m. Тогда*

$$f(x)=\prod_{i=0}^{s}\prod_{j=0}^{\mu_i-1}\Big[\prod_{k=0}^{d_i-1}\big(x^{p^{n-s+\beta_i}}-b^{p^{\beta_i}}\varepsilon_{i-\beta_i}^{u^{j+k\mu_i}}\big)\Big] \tag{2.1}$$

является разложением полинома $f(x)$ на неприводимые множители над K и эти неприводимые множители — указанные полиномы в средных скобках.

Доказательство. Обозначим правую часть разложения (2.1) через $g(x)$, т. е.

$$g(x)=\prod_{i=0}^{s}\prod_{j=0}^{\mu_i-1}f_{ij}(x),\quad f_{ij}(x)=\prod_{k=0}^{d_i-1}\big(x^{p^{n-s+\beta_i}}-b^{p^{\beta_i}}\varepsilon_{i-\beta_i}^{u^{j+k\mu_i}}\big). \tag{2.2}$$

Так как полином $f(x)$ степени p^n не имеет многократных корней, то формула (2.1) будет справедливой, если установим следующие утверждения: (*a*) степень полинома $g(x)$ равна p^n; (*b*) каждый корень полинома $g(x)$ — корень полинома $f(x)$; (*c*) корни полинома $g(x)$ однократны и (*d*) старший коэффициент полинома $g(x)$ равен единице.

Доказательство утверждения (*a*). Степень r полинома $g(x)$ равняется числу

$$\sum_{i=0}^{s}d_i\mu_i p^{n-s+\beta_i}=p^{n-s}\sum_{i=0}^{s}\varphi(p^{i-\beta_i})p^{\beta_i}.$$

Если $m<s$, то

$$r=p^{n-s}\Big[\sum_{i=0}^{m}\varphi(p^i)+\sum_{i=m+1}^{s}\varphi(p^m)p^{i-m}\Big]=p^n,$$

а если $s\leqq m$, то

$$r=p^{n-s}\sum_{i=0}^{s}\varphi(p^i)=p^n.$$

Доказательство утверждения (*b*). Любой корень полинома $g(x)$ имеет вид

$$\alpha\varepsilon_{n-s+i}^{u^{j+k\mu_i}}\cdot\varepsilon_{n-s+\beta_i}^{t},\quad t=0,1,\ldots,p^{n-s+\beta_i}-1;\quad k=0,1,\ldots,d_i-1; \tag{2.3}$$

$$i=0,1,\ldots,s;\quad j=0,1,\ldots,\mu_i-1$$

и так как $\beta_i\leqq i\leqq s$, то, ввиду равенства $\alpha^{p^n}=b$, получается, что элементы (2.3) — корни полинома $f(x)$.

Доказательство утверждения (*c*). Допустим, что два элемента вида (2.3) равны, т. е. что имеет место

$$\varepsilon_{n-s+i}^{u^{j+k\mu_i}}+tp^{i-\beta_i}=\varepsilon_{n-s+i'}^{u^{j'+k'\mu_{i'}}}+tp^{i'-\beta_{i'}}, \tag{2.4}$$

где для i', j', k' и t' справедливы ограничения вида (2.3), аналогичны соответствующим ограничениям для i, j, k и t. Докажем, что $(i,j,k,t)=(i',j',k',t')$. Рассмотрим два подслучая: (с.1) $i=0$ и (с.2) $i\neq 0$.

(с.1) Пусть $i=0$. Тогда $\beta_i=0$, $\mu_i=1$, $j=0$ и $k=0$. Допустим, что $i'\neq 0$. Тогда $i'\neq\beta_i$, и так как степенный показатель элемента $\varepsilon_{n-s+i'}$, в (2.4) взаимно прост с p, то правая часть равентсва (2.4) является первообразным корнем единицы степени $p^{n-s+i'}$, а левая часть (2.4) — первообразным корнем единицы степени $p^{n-s}<p^{n-s+i'}$, что есть противоречие. Следовательно, $i'=0$, откуда $j'=0$, $k'=0$ и (2.4) принимает вид $\varepsilon_{n-s}^{1+t}=\varepsilon_{n-s}^{1+t'}$. Из этого равенства вытекает

$$t \equiv t' \pmod{p^{n-s}}$$

и, ввиду ограничения (2.3) для t и t', получится $t=t'$. Следовательно, $(i, j, k, t)=(i', j', k', t')$.

(с.2) Пусть $i\neq 0$. Ввиду подслучая (с.1) получится $i'\neq 0$. Следовательно, $i-\beta'>0$ и $i'-\beta_{i'}>0$. Тогда степенные показатели элементов ε_{n-s+i} и $\varepsilon_{n-s+i'}$ в (2.4) являются первообразными корнями единицы соответственно степеней p^{n-s+i} и $p^{n-s+i'}$. Следовательно, $i=i'$. Тогда из (2.4) получается

$$u^{j+k\mu_i}+tp^{i-\beta_i} \equiv u^{j'+k'\mu_i}+t'p^{i-\beta_i} \pmod{p^{n-s+i}} \tag{2.5}$$

и так как $i-\beta_i\leqq i\leqq n-s+i$, то

$$u^{j+k\mu_i} \equiv u^{j'+k'\mu_i} \pmod{p^{i-\beta_i}}.$$

Так как u — первообразный корень по модулю $p^{i-\beta_i}$, то из последнего сравнения следует

$$j+k\mu_i \equiv j'+k'\mu_i \pmod{\mu_i d_i}, \tag{2.6}$$

откуда вытекает $j\equiv j' \pmod{\mu_i}$. Отсюда, ввиду ограничений (2.3) для j и j', получается $j=j'$. Тогда из (2.6) следует $k\equiv k' \pmod{d_i}$ и, ввиду (2.3), что $k=k'$. Теперь (2.5) принимает вид

$$tp^{i-\beta_i} \equiv t'p^{i-\beta_i} \pmod{p^{n-s+i}},$$

откуда получится

$$t \equiv t' \pmod{p^{n-s+\beta_i}},$$

т. е., ввиду ограничений (2.3) для t и t', что $t=t'$. Следовательно, $(i, j, k, t)=(i', j', k', t')$. Этим утверждение (c) доказано. Утверждение (d) очевидно. Таким образом имеет место формула (2.1).

Докажем, что множители $f_{ij}(x)$ неприводимы над полем K. С этой целью рассмотрим два подслучая: 1) $s=0$ и 2) $s\neq 0$.

1) Пусть $s=0$. Тогда $i=0$, $\beta_i=0$, $\mu_i=1$, $j=0$, $d_i=1$, разложение (2.1) содержит только множитель $x^{p^n}-a$ и, ввиду $a=b\notin K^p$, следует [5, стр. 254, следствие 1], что этот множитель неприводим.

2) Пусть $s\neq 0$. Сначала докажем, что $f_{ij}(x)$ — полином над K. Так как $i-\beta_i$ имеет значение i, если $0\leqq i\leqq m$ и — значение m, если $m+1\leqq i\leqq s$, то (2.1) — разложение над $K(\varepsilon_1)$. Докажем, что элементы

$$\varepsilon_{i-\beta_i}^{u^{j+k\mu_i}}, \quad k=0, 1, \ldots, d_i-1, \quad i\neq 0, \tag{2.7}$$

в разложении (2.2) полинома $f_{ij}(x)$ образуют полную систему сопреженных элементов над K. Дейсвительно, пусть τ — отображение поля $K(\varepsilon_1)$ в $K(\varepsilon_1)$,

определено через

$$\tau(\varepsilon_{i-\beta_i}) = \varepsilon_{i-\beta_i}^{u^{k\mu_i}}$$

и продолжено по мультипликативности и линейности над K. Поскольку, в силу определния d_i и μ_i, справедливо

$$(u^{k\mu_i})^d = u^{k\varphi(p^{i-\beta_i})} \equiv 1 (\mathrm{mod}\, p^{i-\beta_i}),$$

то, ввиду леммы 2.6, имеет место $\tau \in G = G(K(\varepsilon_1); K)$. Так как

$$\tau(\varepsilon_{i-\beta_i}^{u^j}) = \varepsilon_{i-\beta_i}^{u^{j+k\mu_i}},$$

то любой элемент формулы (2.7) сопрежен элементу $\varepsilon_{i-\beta_i}^{n^j}$. Следовательно, $f_{ij}(x)$ — полином над K.

Теперь докажем, что $f_{ij}(x)$ — неприводимый полином над K. Рассмотрим два подслучая: 2.1) $i=0$ и 2.2) $i \neq 0$.

2.1) Nусть $i=0$. Тогда $\beta_i=0$, $\mu_i=1$, $j=0$ и $f_{ij}(x)=f_{00}(x)=x^{p^{n-s}}-b$. Если $s=n$, то очевидно $f_{ij}(x)$ неприводим. Пусть $s<n$. Тогда $b \in K \setminus K^p$ и полином $f_{ij}(x)$, ввиду [5, стр. 254, следствие 1], неприводим над K.

2.2) Пусть $i \neq 0$. Применим лемму 2.1 для полинома

$$\varphi_{ij}(x) = \prod_{k=0}^{d_i-1} (x - b^{p^{\beta_i}} \varepsilon_{i-\beta_i}^{u^{j+k\mu_i}}),$$

который неприводим над K, так как $\varphi_{ij}(x)$ — произведение сопреженных полиномов первой степени над полем K. Пусть x_1 — один из корней полинома $\varphi_{ij}(x)$, скажем $x_1 = b^{p^{\beta_i}} \varepsilon_{i-\beta_i}^{u^j}$, получающийся при $k=0$. Надо доказать, что полином

$$\psi_{ij}(x) = x^{p^{n-s+\beta_i}} - b^{p^{\beta_i}} \varepsilon_{i-\beta_i}^{u^j} \tag{2.8}$$

неприводим над $K(x_1)=K(\varepsilon_1)$. Рассмотрим два подслучая случая 2.2), а именно 2.2.1) $s=n$ и 2.2.2) $s<n$. 2.2.1. Пусть $s=n$. Тогда

$$\psi_{ij}(x) = x^{p^{\beta_i}} - b^{p^{\beta_i}} \varepsilon_{i-\beta_i}^{u^j}.$$

Если $1 \leqq i \leqq m$, то $\beta_i=0$ и $\psi_{ij}(x)$ неприводим над $K(\varepsilon_1)$. Пусть $m+1 \leqq i \leqq s$. Следовательно, $m<s$, K — поле первого рода относительно p и $m'=m$. Тогда $\beta_i = i-m > 0$ и

$$\psi_{ij}(x) = x^{p^{i-m}} - b^{p^{i-m}} \varepsilon_m^{u^j}.$$

Докажем, что $b^{p^{i-m}} \varepsilon_m^{u^j} \notin K(\varepsilon_1)^p$. В противном случае из $b^{p^{i-m}} \varepsilon_m^{u^j} \in K(\varepsilon_1)^p$ вытекает $\varepsilon_m^{u^j} \in K(\varepsilon_1)^p$ и так как $(u^j, p)=1$, то, в силу замечания 2.2, получится $\varepsilon_m \in K(\varepsilon_1)^p$. Следовательно, $\varepsilon_m = v^p$, $v \in K(\varepsilon_1)$ и порядок элемента v равняется p^{m+1}. Это является противоречием, так как для силовской p-подгруппы $K(\varepsilon_1)_p$ мултипликативной группы $K(\varepsilon_1)^*$ поля $K(\varepsilon_1)$ имеет место $K(\varepsilon_1)_p = K(\varepsilon_m)_p = \langle \varepsilon_m \rangle$, где $\langle \varepsilon_m \rangle$ — циклическая группа (с образующим элементом ε_m), порядок которой равняется p^m. Следовательно, ввиду [5, стр. 254, следствие 1], $\psi_{ij}(x)$ — неприводим полином над $K(\varepsilon_1)$.

2.2.2) Пусть $s<n$. Предположим, что $1\leqq i\leqq m$. Тогда $\beta_i=0$ и

$$\psi_{ij}(x) = x^{p^{n-s}} - b\varepsilon_i^{uj}.$$

Допустим, что $b\varepsilon_m^{uj}\in K(\varepsilon_1)^p$. Тогда имеет место $b\varepsilon_i^{uj}=\delta^p$, где $\delta\in K(\varepsilon_1)$. Так как норма N обладает мультипликативным свойством, то $N(b)N^{uj}(\varepsilon_i)=N^p(\delta)$. Следовательно, существует такой элемент $c\in K$, что

$$b^d = c^p\in K^p.$$

Поскольку $d/(p-1)$, то $(d,p)=1$. Следовательно, ввиду замечания 2.2, $b\in K^p$, что ведет к противоречию. Таким образом $b\varepsilon_i^{uj}\notin K(\varepsilon_1)^p$ и, ввиду [5, стр. 254, следствие 1], $\psi_{ij}(x)$ — неприводимый полином над $K(\varepsilon_1)$.

Пусть $m+1\leqq i\leqq s$. Тогда $m<s$, K — поле первого рода относительно p, $m=m'$, $\beta_i=i-m\geqq 1$ и

$$\psi_{ij}(x) = x^{p^{n-s+i-m}} - b^{p^{i-m}}\varepsilon_m^{uj}.$$

Как в случае 2.2.1) видно, что $b^{p^{i-m}}\varepsilon_m^{uj}\notin K(\varepsilon_1^p)$, т. е. $\psi_{ij}(x)$ — неприводимый полином над $K(\varepsilon_1)$.

Чтобы закончить подслучай 2.2) нужно применить лемму 2.1 для полинома $\varphi_{ij}(x)$ и для полинома (2.8). Именно, из леммы 2.1 следует, что $\varphi_{ij}(x^{p^{n-s+\beta_i}})=f_{ij}(x)$ — неприводимый полином над полем K. Теорема доказана.

Следствие 2.8. *Если* $K=K(\varepsilon_1)$, *то разложение полинома* $f(x)=x^{p^n}-a$, $a\in K^*$, *на неприводимые множители над* K *дается формулой*

$$f(x) = \prod_{i=0}^{s}\prod_{j=0}^{\varphi(p^{i-\beta_i})-1}(x^{p^{n-s+\beta_i}} - b^{p^{\beta_i}}\varepsilon_{i-\beta_i}^{uj}).$$

Действительно, тогда $d_i=1$, $k=0$ и из формулы (2.1) получается следствие.

§ 3. Минимальные идемпотенты полупростых скрещенных групповых алгебр циклических p-групп над полем

Пусть $\langle g\rangle$ — циклическая группа порядка p^n, где p — нечетное простое число и K — поле, характеристика которого отлична от p. Скрещенная групповая алгебра $K^t\langle g\rangle$ определяется равенством $g^{p^n}=a$, где $a\in K^*$. Сначала найдем идемпотенты скрещенной групповой алгебры $\overline{K}^t\langle g\rangle$, где $\overline{K}$ — алгебраическое замыкание поля K, а потом — скрещенной алгебры $K^t\langle g\rangle$, складывая K — сопряженные идемпотенты алгебры $\overline{K}^t\langle g\rangle$.

Пусть s — наибольшее целое число интервала $[0,n]$, для которого $a\in K^{p^s}$, b — такой элемент поля K, что $a=b^{p^s}$ и α — такой элемент поля $\overline{K}$, что $\alpha^{p^{n-s}}=b$. Так как $a=\alpha^{p^n}$, то алгебра $\overline{K}^t\langle g\rangle$ совпадает с групповой алгеброй $\overline{K}\langle\alpha^{-1}g\rangle$. Пусть χ — характер группы $\langle g\rangle$ (в поле $\overline{K}$). Хорошо известно, что если $\chi(g)=\varepsilon_n^j$, $0\leqq j\leqq p^n-1$, то характеру χ соответствует идемпотент $\bar{e}_j$ групповой алгебры $\overline{K}\langle g\rangle$, а именно

$$\bar{e}_j = \frac{1}{p^n}\sum_{i=0}^{p^n-1}\chi(g)^{-i}g^i.$$

Идемпотенты в $\overline{K^t\langle g\rangle}$ получатся из указанных идемпотентов $\bar{e}_j$ заменяя g с $\alpha^{-1}g$ и имея ввиду, что $\chi(\alpha^{-1}g)=\varepsilon_n^j$, $j=0, 1, \ldots, p^n-1$. Следовательно, эти идемпотенты будут иметь вид

$$\bar{e}_j = \frac{1}{p^n}\sum_{i=0}^{p^n-1}(\alpha\varepsilon_n^j)^{-i}g^j, \quad j = 0, 1, \ldots, p^n-1. \tag{3.1}$$

Элементы $\alpha\varepsilon_n^j$, $j=0, 1, \ldots, p^n-1$, участвующие в (3.1), исчерпывают корни полинома $f(x)=x^{p^n}-a$. Все K-сопряженные идемпотенты фиксированного идемпотента получатся, заменяя элемент $\alpha\varepsilon_n^j$ в формуле (3.1) на его сопряженные элементы над K. Следовательно, нужно отделить неприводимые множители $f_q(x)$ полинома $f(x)$ над K и все корни полинома $f_q(x)$, поставленные на место элемента $\alpha\varepsilon_n^j$ в (3.1), дадут сопряженные идемпотенты, соответствующие множителю $f_q(x)$ (и идемпотенту $\bar{e}_j$). Складывая эти сопряженные идемпонтенты получим минимальный идемпотент e_q алгебры $K^t\langle g\rangle$, соответствующий множителю $f_q(x)$. Таким образом докажем следующую теорему.

Теорема 3.1. *Пусть скрещенная групповая алгебра $K^t\langle g\rangle$ циклической группы $\langle g\rangle$ порядка p^n, где p — нечетное простое число, над полем K с характеристикой отличной от p определена равенством $g^{p^n}=a$, $a\in K^*$ и u — первообразный корень по модулю p^m. Тогда минимальные идемпотенты алгебры $K^t\langle g\rangle$ являются следующими*

$$e_{ij} = \frac{1}{p^{s-\beta_i}}\sum_{t=0}^{p^{s-\beta_i}-1}\Big[\sum_{k=0}^{d_i-1}(b^{p^{\beta_i}}\varepsilon_{i-\beta_i}^{u^j+k\mu_i})^{-t}\Big]g^{tp^{n-s+\beta_i}}, \tag{3.2}$$

$$i = 0, 1, \ldots, s; \quad j = 0, 1, \ldots, \mu_i-1.$$

Идемпотент e_{ij} порождает идеал алгебры $K^t\langle g\rangle$, который изоморфен полю $K(\alpha\varepsilon_{n-s+i}^{u^j})$.

Доказательство. Все корни неприводимого множителя $f_{ij}(x)$ формулы (2.2) полинома $f(x)=x^{p^n}-a$ $(0\leqq i\leqq s,\ 0\leqq j\leqq\mu_i-1)$ являются

$$\alpha\varepsilon_{n-s+i}^{u^j+k\mu_i}\cdot\varepsilon_{n-s+\beta_i}^{r}, \quad r = 0, 1, \ldots, p^{n-s+\beta_i}-1,$$

$$k = 0, 1, \ldots, d_i-1.$$

Следовательно, минимальный идемпотент e_{ij}, соответствуюший множителю $f_{ij}(x)$, будет

$$e_{ij} = \frac{1}{p^n}\sum_{t=0}^{p^n-1}\Big[\sum_{k=0}^{d_i-1}(\alpha\varepsilon_{n-s+i}^{u^j+k\mu_i})^{-t}\sum_{r=0}^{p^{n-s+\beta_i-1}}\varepsilon_{n-s+\beta_i}^{-rt}\Big]g^t.$$

Для фиксированного t, для которого $p^{n-S+\beta_i}\nmid t$, последняя сумма равна нулью. Следовательно, в указанной формуле остаются только те t, для которых $p^{n-S+\beta_i}/t$, т. е. t можно заменить на $tp^{n-s+\beta_i}(t=0, 1, \ldots, p^{S-\beta_i}-1)$ и для e_{ij} получится

$$e_{ij} = \frac{1}{p^n}\sum_{t=0}^{p^{s-\beta_i}-1}\Big[\sum_{k=0}^{d_i-1}(\alpha\varepsilon_{n-s+i}^{u^j+k\mu_i})^{-tp^{n-s+\beta_i}}p^{n-s+\beta_i}\Big]g^{tp^{n-s+\beta_i}}.$$

Отсюда вытекает формула (3.2).

Следствие 3.2. *Если* $K=K(\varepsilon_1)$, *то минимальные идемпотенты алгебры* $K^t\langle g\rangle$ *являются*

$$e_{ij}=\frac{1}{p^{s-\beta_i}}\sum_{t=0}^{p^{s-\beta_i}-1}(b^{p^{\beta_i}}\varepsilon_{i-\beta_i}^{u^j})^{-t}g^{tp^{n-s+\beta_i}}, \tag{3.3}$$

$$i=0,1,\ldots,s;\quad j=0,1,\ldots,\mu_i-1.$$

Доказательство. Действительно, в этом случае $d_i=1$, $k=0$ и формула (3.2) принимает вид (3.3).

Следствие 3.3. Минимальные идемпотенты групповой алгебры $K\langle g\rangle$ являются

$$e_{ij}=\frac{1}{p^{n-\beta_i}}\sum_{t=0}^{p^{n-\beta_i}-1}\Big[\sum_{k=0}^{d_i-1}(\varepsilon_{i-\beta_i}^{u^{j+k\mu_i}})^{-t}\Big]g^{tp^{\beta_i}}.$$

Доказательство. Групповая алгебра $K\langle g\rangle$ можно рассматривать как скрещенной групповой алгеброй $K^t\langle g\rangle$, которая определена равенством $g^{p^n}=1$, т. е. для которой $a=1$. Следовательно, можно выбрать $b=1$, откуда вытекает $s=n$. Подставляя в формуле (3.2) $b=1$ и $s=n$ получится формула следствия.

Следствие 3.4. *Минимальные идемпотенты фактор-алгебры* $K[x]/I$, *где* I — *идеал алгебры* $K[x]$, *порожденный полиномом* $x^{p^n}-a$, $a\in K^*$ *являются*

$$e_{ij}=\frac{1}{p^{s-\beta_i}}\sum_{t=0}^{p^{s-\beta_i}-1}\Big[\sum_{k=0}^{d_i-1}(b^{p^{\beta_i}}\varepsilon_{i-\beta_i}^{u^{j+k\mu_i}})^{-t}(x^{tp^{n-s+\beta_i}}+I)\Big], \tag{3.4}$$

$$i=0,1,\ldots,s;\quad j=0,1,\ldots,\mu_i-1.$$

Доказательство. Определим отображение $\varphi\colon K^t\langle g\rangle\to K[x]/I$, полагая $\varphi(g)=x+I$ и продолжая φ по линейности над K и по мультипликативности. Нетрудно увидеть, что φ — изморфизм алгебр $K^t\langle g\rangle$ и $K[x]/I$. Тогда формула (3.2) переходит в (3.4).

Замечание. В формулах (3.2) и (3.3) для идемпотентов алгебры $K^t\langle g\rangle$ участвуют степени g^k элемента g в $K^t\langle g\rangle$. Эти формулы можно записать в другом виде посредством степени $g^{(k)}$ элемента g в группе G, используя формулу (1.2) для связи между g и $g^{(k)}$.

Литература

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

[2] А. А. Бовди, Скрещенные произведения полугруппы и кольца. Сиб. мат. журнал, IV (1963), 481—500.

[3] Ван дер Варден, Алгебра. «Наука», Москва, 1976, 648 стр.

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

[5] С. Ленг, Алгебра. «*Наука, Москва*», 1968, 564 стр.

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

[7] D. S. Passman, Radicals of twisted group rings. *Proc. London Math. Soc.*, (3) **20** (1970), 409—437.

[8] D. S. Passman, On the semisimplicity of twisted group algebras. *Proc. Amer. Math. Soc.* **25** (1970), 161—166.

ПЛОВДИВСКИЙ УНИВЕРСИТЕТ
«П. ХИЛЕНДАРСКИ», Кафедра алгебры
4000 ПЛОВДИВ

(Поступила: 28. II. 1986)