Serdica

Bulgariacae mathematicae publicationes

Сердика

Българско математическо списание

ИЗОМОРФИЗМ ПОЛУПРОСТЫХ СКРЕЩЕННЫХ ГРУППОВЫХ АЛГЕБР ЦИКЛИЧЕСКИХ p-ГРУПП НЕЧЕТНОГО ПОРЯДКА

Н. А. НАЧЕВ, Т. Ж. МОЛЛОВ

Пусть $\langle g\rangle$ — циклическая p-группа, где p — нечетное простое число, K — поле, характеристика которого отлична от p, и $K_t\langle g\rangle$ — скрещенная групповая алгебра группы $\langle g\rangle$ над полем K. В настоящей работе находятся необходимые и достаточные условия изоморфизма K-алгебр $K_t\langle g\rangle$ и $K_t\langle g_1\rangle$, где $\langle g_1\rangle$ — циклическая группа порядка p^n, т. е. необходимые и достаточные условия K-изоморфизма фактор-алгебр $K[x]/\langle x^{p^n}-a\rangle$ и $K[x]/\langle x^{p^n}-a_1\rangle$, где $a,\ a_1\in K\setminus\{0\}$ и $\langle x^{p^n}-a_1\rangle$ — главный идеал K-алгебры $K[x]$, порожденный полиномом $x^{p^n}-a$.

Изучение скрещенной групповой алгебры $K_t G$ группы G над коммутативным кольцом K с единицей (и вообще скрещенных произведений групп и колец) происходит в основном в следующих трех направлениях: 1) нахождение полной системы инвариантов алгебры $K_t G$, т. е. найти необходимые и достаточные условия изоморфизма K-алгебр $K_t G$ и $K_t G_1$, где G_1 — группа; 2) описание мультипликативной группы алгебры $K_t G$ и 3) теоретико-кольцевые свойства алгебры $K_t G$. Самое большое количество работ посвящено третьему направлению, но самым важным можно считать первое направление, которое называется еще проблемой изоморфизма скрещенных групповых алгебр. Некоторые авторы называют $K_t G$ групповым кольцом, когда K не является полем, а только кольцом. Если это понятие оправдано, когда речь идет о третьем или о втором из указанных направлений, то его можно считать неправильным, когда исследуется проблема изоморфизма K-алгебр (а не колец) $K_t G$ и $K_t G_1$. Исходя из этой точки зрения, мы будем придерживаться к термину скрещенной груповой алгебры, а не к скрещенному групповому кольцу.

Эта работа посвящена первому из указанных направлений. Формулировки некоторых ее результатов опубликованы в [3]. Настоящая статья — продолжение статьи [4], посвященной третьему направлению, в которой изучались минимальные идемпотенты полупростой скрещенной групповой алгебры $K_t\langle g\rangle$, где $\langle g\rangle$ — циклическая p-группа нечетного порядка. Для получения главного результата этой работы используется разложение биномного полинома $x^{p^n}-a$ над полем K на неприводимые множители [4].

Обозначим через $K[x]$ алгебру полиномов переменной x над полем K и через $\langle x_1,\ x_2,\dots,\ x_n\rangle$ — K-алгебру, порожденную элементами $x_1,\dots,x_n$. Следующая лемма хорошо известна.

Лемма 1. *Если $f(x)=x^n+a_1x^{n-1}+\dots+a_n$ — полином над полем K, то фактор-алгебра $K[x]/\langle f(x)\rangle$ алгебры $K[x]$ по ее главному идеалу $\langle f(x)\rangle$, порожденному полиномом $f(x)$, K-изоморфна K-алгебре*

$$K_f=\langle 1, x,\dots, x^{n-1}\mid x^n=-a_1x^{n-1}-\dots-a_n\rangle$$

с базисом $1,\ x,\dots,\ x^{n-1}$, т. е. $K[x]/\langle f(x)\rangle\cong K_f$.

Доказательство. Определим отображение $\theta: K[x]\to K_f$, сопоставляя каждому полиному $\varphi(x)\in K[x]$ полином $(\varphi(x))\theta=r(x)$, где $r(x)$ — остаток деления по-

СЕРДИКА Българско математическо списание. Том 14, 1988, с. 75—81.

линома $\varphi(x)$ на полином $f(x)$. Если $r_1(x)$ — остаток деления другого полинома $\psi(x) \in K[x]$ на $f(x)$, то остаток произведения полиномов $r(x)$ и $r_1(x)$ в алгебре K_f совпадает с остатком деления произведения $\varphi(x)\psi(x)$ на $f(x)$. Следовательно, отображение θ мультипликативно. Очевидно, θ является K-гомоморфизмом алгебры $K[x]$ на алгебру K_f и $Ker\,\theta = \langle f(x)\rangle$, чем утверждение доказано.

В связи с доказанной леммой условимся говорить, что алгебра

$$K_f = \langle 1, x, \ldots, x^{n-1} \mid x^n = -a_1 x^{n-1} - \ldots - a_n\rangle$$

соответствует полиному $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$ над полем K с определяющим равенством $x^n = -a_1 x^{n-1} - \ldots - a_n$.

Условимся обозначать также умножение в группе G через „$\cdot$“, а умножение базисных элементов $g, h \in G$ в алгебре $K_t G$ — по правилу

$$gh = (g, h)\ (g.h), \quad (g, h) \in K^*$$

[4], где K^* — мультипликативная группа поля K. Обозначим через $g^{(n)}$ n-степень элемента $g \in G$ в группе G и через g^n — n-степень элемента g в алгебре $K_t G$. Единицу 1 алгебры $K_t G$ отождествим с единицей поля K. Пусть $\langle g\rangle$ — циклическая группа порядка p^n. Согласно [4], элементы $1, g, \ldots, g^{p^n-1}$ образуют базис скрещенной групповой алгебры $K_t\langle g\rangle$ и равенство

$$g^{p^n} = a, \ a \in K^* \tag{1}$$

определяет скрещенную групповую алгебру $K_t\langle g\rangle$.

Следствие 2. *Пусть скрещенная групповая алгебра $K_t\langle g\rangle$ циклической группы $\langle g\rangle$ порядка p^n над полем K определена равенством (1). Тогда имеет место K-изоморфизм $K_t\langle g\rangle \cong K[x]/\rangle x^{p^n} - a\rangle$.*

Доказательство. Так как $g^{p^n} = a$, то алгебра $K_t\langle g\rangle$ соответствует полиному $f(x) = x^{p^n} - a$ с определяющим равенством $g^{p^n} = a$, т. е. $K_t\langle g\rangle \cong K_f$. Однако, ввиду леммы 1, имеет место $K_f \cong K[x]/\langle f(x)\rangle$, чем лемма доказана.

В следующем предложении поле $K(u)$ рассматривается как K-алгебра.

Предложение 3. *Если алгебра K_f соответствует полиному $f(x) = f_1(x) \ldots f_\lambda(x)$ над полем K, каждый полином $f_i(x)$, неприводим над K, имеет корень u_i $(i = 1, \ldots, \lambda)$, а полиномы $f_i(x)$ попарно взаимно просты, то алгебра K_f K-изоморфна прямой сумме полей $K(u_1), \ldots, K(u_\lambda)$,* т. е.

$$K_f \cong \sum_{i=1}^{\lambda} K(u_i).$$

Доказательство. Имеет место

$$K_f \cong K[x]/\langle f(x)\rangle = K[x]/\bigcap_{i=1}^{\lambda} \langle f_i(x)\rangle \cong \sum_{i=1}^{\lambda} K[x]/\langle f_i(x)\rangle \cong \sum_{i=1}^{\lambda} K(u_i),$$

где первый изоморфизм следует из леммы 1, второй — из китайской теоремы об остатках, перенесенной для K-алгебр, и последний — из хорошо известного факта $K(x)/\langle f_i(x)\rangle \cong K(u_i)$, где $K(u_i)$ рассматриваются как K-алгебры. Этим предложение доказано.

В дальнейшем рассматривается алгебра $K_t\langle g\rangle$ циклической группы $\langle g\rangle$ порядка p^n, определенная равенством (1), над полем K с характеристикой, отличной от p, где p — нечетное простое число. Через ε_i будем обозначать первообразный корень степени p^i из единицы в некотором расширении поля K, $i \geqq 0$. Пусть $L^{p^k} = \{c^{p^k} \mid c \in L\}$, где L — поле. Полином $f(x) = x^{p^n} - a$ над полем K разлагается в произведение $f_1(x)$

$\dots f_\lambda(x)$ на неприводимые множители $f_i(x)$ над K, каждый из которых имеет корень u_i $(i=1, \dots, \lambda)$ и эти множители попарно взаимно просты. Так как алгебра $K_t\langle g\rangle$ соответствует полиному $f(x)=x^{p^n}-a$, то, применяя последовательно следствие 2, лемму 1 и предложения 3, получим, что алгебра $K_t\langle g\rangle$ изоморфна прямой сумме полей $K(u_i)$, $i=1, \dots, \lambda$, а именно:

$$K_t\langle g\rangle \cong K(u_1)\oplus \dots \oplus K(u_\lambda). \tag{2}$$

Основным результатом настоящей статьи является следующее утверждение, в котором K^* — мультипликативная группа поля K и $\langle aK^{*p^n}\rangle$ — циклическая группа, порожденная смежным классом aK^{*p^n}.

Теорема 4. *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 $g^{p^n}=a$, $a\in K^*$. Алгебры $K_t\langle g\rangle$ и $K_t\langle g_1\rangle$ изоморфны как K-алгебры тогда и только тогда, когда порядок группы $\langle g_1\rangle$ равняется p^n и $\langle aK^{*p^n}\rangle=\langle a_1\ K^{*p^n}\rangle$, где алгебра $K_t\langle g_1\rangle$ определяется равенством $g_1^{p^n}=a_1$, $a_1\in K^*$.*

Доказательство. Необходимость. Из изоморфизма $K_t\langle g\rangle\cong K_t\langle g_1\rangle$ следует, что g_1 — элемент порядка p^n и алгебра $K_t\langle g_1\rangle$ определяется равенством $g_1^{p^n}=a_1$, $a_1\in K^*$. Пусть s и s_1 — максимальные целые числа интервала $[0, n]$, для которых соответственно $a\in K^{p^s}$ и $a_1\in K^{p^{s_1}}$ и $a=b^{p^s}$, $b\in K$. Рассмотрим полиномы $f(x)=x^{p^n}-a$ и $f_1(x)=x^{p^n}-a_1$. Разложениям полиномов $f(x)$ и $f_1(x)$ в произведение неприводимых множителей над полем K соответствует, в силу предложения 3, разложение вида (2) алгебр $K_t\langle g\rangle$ и $K_t\langle g_1\rangle$ в прямые суммы полей. Так как минимальные степени упомянутых неприводимых множителей полиномов $f(x)$ и $f_1(x)$ равняются соответственно p^{n-s} и p^{n-s_1} [4], то поля минимальной степени относительно K, участвующие в разложении алгебр $K_t\langle g\rangle$ и $K_t\langle g_1\rangle$, имеют соответственно степени p^{n-s} и p^{n-s_1} относительно K. Так как $K_t\langle g\rangle\cong K_t\langle g_1\rangle$, то любое поле L минимальной степени относительно K, участвующее в разложении алгебры $K_t\langle g\rangle$, будет изоморфно некоторому полю L_1 минимальной степени относительно K, участвующему в разложении алгебры $K_t\langle g_1\rangle$. Следовательно, степени полей L_1 и L относительно K равны, т. е. $s_1=s$. Таким образом число s определяется инвариантным образом в алгебре $K_t\langle g\rangle$. Из разложения полинома $f(x)$ над полем K [4] видно, что существует элемент $\alpha\in\bar{K}$, являющийся корнем неприводимого множителя $x^{p^{n-s}}-b$ полинома $f(x)$ над K, т. е. для которого $\alpha^{p^{n-s}}=b$ и $(K(\alpha)\colon K)=p^{n-s}$. Так как поле $K(\alpha)$ участвует в разложении (2) алгебры $K_t\langle g\rangle$ в прямую сумму полей, то поле $K(\alpha)$ изоморфно некоторому полю $K(\alpha_1)$ из разложения $K_t\langle g_1\rangle$ в прямую сумму минимальных идеалов и α_1 — корень полинома $f_1(x)=x^{p^n}-a_1$, т. е. $\alpha_1^{p^n}=a_1$. Ввиду того, что степень элемента α_1 над полем K равняется p^{n-s}, то существует такой элемент $b_1\in K$, что $\alpha_1^{p^{n-s}}=b_1$. Следовательно, $b_1^{p^s}=a_1$. Так как $K(\alpha)\cong K(\alpha_1)$, то из необходимости теоремы 1 [2], приложенной для полиномов $x^{p^{n-s}}-b$ и $x^{p^{n-s}}-b_1$, вытекает $\langle bK^{*p^{n-s}}\rangle=\langle b_1\ K^{*p^{n-s}}\rangle$, откуда следует $\langle a_1\ K^{*p^n}\rangle=\langle a_1\ K^{*p^n}\rangle$, чем необходимость теоремы доказана.

Достаточность. Если $a\in K^{*p^n}$, то $a_1\in K^{*p^n}$ и уравнения $x^{p^n}=a$ и $x^{p^n}=a_1$, обладают решениями в поле K. Тогда $K_t\langle g\rangle\cong K\langle g\rangle$ [4] и $K_t\langle g_1\rangle\cong K\langle g_1\rangle$. Следовательно, $K_t\langle g\rangle\cong K_t\langle g_1\rangle$. Предположим, что $a\notin K^{*p^n}$, т. е. что $a_1\notin K^{*p^n}$. Из $\langle a\ K^{*p^n}\rangle=\langle a_1\ K^{*p^n}\rangle$ вытекает, что $a_1\ K^{*p^n}$ — образующий элемент циклической группы $\langle a\ K^{*p^n}\rangle$. Следовательно, существует такое натуральное l, что $(l, p)=1$ и $a=a_1^l\, c^{p^n}$, $c \in K^*$. Определим отображение $\varphi: K_t\langle g\rangle \to K_t\langle g_1\rangle$. Для этой цели положим

(3) $$(g^i)\,\varphi = c^i\, g_1^{il}, \quad i=0,\ 1, \dots, p^n-1$$

и продолжим φ по линейности. Докажем, что φ — инъективное отображение. Действительно, пусть

$$x=\sum_{i=0}^{p^n-1} \lambda_i\, g^i \in Ker\, \varphi.$$

Тогда, ввиду (3),

$$x\varphi = \sum_{i=0}^{p^n-1} \lambda_i\, c^i\, g_1^{il}=0.$$

Пусть $il=p^n q_i+r_i$, где $0 \leqq r_i < p^n$, r_i и q_i — целые числа. Тогда

(4) $$x\varphi = \sum_{i=0}^{p^n-1} \lambda_i\, c^i\, a_1^{q_i}\, g_1^{r_i}=0.$$

Однако элементы $g_1^{r_i}\,(i=0,\ 1, \dots, p^n-1)$ образуют базис алгебры $K_t\langle g_1\rangle$. Действительно, так как $0 \leqq r_i < p^n$, то достаточно доказать что если $j \neq i$ и $0 \leqq j \leqq p^n-1$, то $r_j \neq r_i$. Допустим противное, что $r_j=r_i$ при $j \neq i$. Тогда $il-p^n q_i=r_i=r_j=jl-p^n q_j$. Следовательно, $(i-j)\, l \equiv 0 \pmod{p^n}$ и из $(l, p)=1$ вытекает $i \equiv j \pmod{p^n}$, что противоречит тому, что i и j принимают значения в множестве $\{0,\ 1, \dots, p^n-1\}$. Ввиду того, что элементы $g_1^{r_i}$ образуют базис алгебры $K_t\langle g_1\rangle$, то из справедливости формулы (4) получается, что $\lambda_i\, c^i\, a_1^{q_i}=0$ и $\lambda_i=0$ для $i=0,\ 1, \dots, p^n-1$, так как c, $a_1 \in K^*$. Следовательно, $Ker\, \varphi=0$, т. е. φ — инъективное отображение.

Поскольку

$$\Big(\sum_{i=0}^{p^n-1} \lambda_i\, g^i \sum_{j=0}^{p^n-1} \mu_j\, g^j\Big)\,\varphi = \sum_{i=0}^{p^n-1} \sum_{j=0}^{p^n-1} \lambda_i\, \mu_j\, (g^{i+j})\,\varphi,$$

то для мультипликативности φ достаточно доказать, что

(5) $$(g^{i+j})\,\varphi = g^i\,\varphi\, g^j\,\varphi.$$

Если $i+j<p^n$, то ввиду (3), имеет место формула (5). Пусть $i+j \geqq p^n$. Тогда, используя формулу (3), получается

$$(g^{i+j})\,\varphi=(g^{i+j-p^n}\, g^{p^n})\,\varphi = c^{i+j-p^n}\, g_1^{l\,(i+j-p^n)}\, a$$

и

$$g^i\varphi g^j\,\varphi = c^i\, g_1^{il}\, c^j\, g_1^{jl} = c^{i+j-p^n}\, a\, a_1^{-l}\, g_1^{l(i+j-p^n)}\, a_1^l.$$

Из сравнения полученных двух результатов вытекает формула (5). Следовательно, φ является K-гомоморфизмом K-алгебр $K_t\langle g\rangle$ и $K_t\langle g_1\rangle$. Поскольку φ — инъекция K-алгебр $K_t\langle g\rangle$ и $K_t\langle g_1\rangle$ одинаковой размерности p^n и φ является K-гомоморфизмом, то φ является K-изоморфизмом алгебр $K_t\langle g\rangle$ и $K_t\langle g_1\rangle$, чем теорема доказана.

В следующем утверждении кольцо $K[x]$ рассматривается как K-алгебра.

Следствие 5. Имеют место K-изоморфизмы

а) $K[x]/\langle x^{p^n}-a\rangle \cong K[x]/\langle x^{p^n}-a_1\rangle$, a, $a_1 \in K^*$,

б) $K[x]/\langle x^{p^n}-a\rangle \cong K[x]/\langle x^{p^n}-1\rangle$, $a \in K^*$, *где K — поле с характеристикой, отличной от p, а p — нечетное простое число тогда и только тогда, когда выполняются соответственно*: а) $\langle aK^{*p^n}\rangle = \langle a_1 K^{*p^n}\rangle$ и б) *уравнение* $x^{p^n}=a$ *имеет решение в* K^*.

Следствие 6. *Если p — нечетное простое число, K — поле с характеристикой, отличной от p и алгебра $K_t\langle g\rangle$ определена равенством $g^{p^n}=a, a\in K^*$, то $K_t\langle g\rangle$ K-изоморфна групповой алгебре $K\langle g\rangle$ тогда и только тогда, когда уравнение $x^{p^n}=a$ имеет решение в* K.

Доказательства этих следствий непосредственно вытекают из теоремы 4 и из следствия 2.

Следствие 7. *Существует взаимнооднозначное отображение между множеством классов изоморфных скрещенных групповых алгебр циклической группы $\langle g\rangle$ нечетного порядка p^n над фиксированным полем K, характеристика которого отлична от p, и множеством всех циклических подгрупп фактор-группы K^*/K^{*p^n}. При этом отображении единичная подгруппа фактор-группы K^*/K^{*p^n} соответствует классу изоморфных скрещенных групповых алгебр, который содержит групповую алгебру $K\langle g\rangle$ группы $\langle g\rangle$ над полем K.*

Доказательство. Определим отображение φ множества скрещенных групповых алгебр циклической группы $\langle g\rangle$ над K на множество циклических подгрупп фактор-группы K^*/K^{*p^n} следующим образом: для любой такой алгебры $K_t\langle g\rangle$ положим $(K_t\langle g\rangle)\varphi=\langle aK^{*p^n}\rangle$, где $g^{p^n}=a$. Ввиду теоремы 4, имеет место $K_t\langle g\rangle\cong K_t\langle g_1\rangle$ тогда и только тогда, когда $\langle aK^{*p^n}\rangle=\langle a_1K^{*p^n}\rangle$, где $g_1^{p^n}=a_1$. Следовательно, существует инъективное отображение множества классов изоморфных скрещенных групповых алгебр в множество всех циклических подгрупп группы K^*/K^{*p^n}.

Докажем, что φ — сюръективное отображение. Пусть $\langle a K^{*p^n}\rangle$ — любая циклическая подгруппа группы K^*/K^{*p^n}. Построим скрещенную алгебру $K_t\langle g\rangle$, для которой $(K_t\langle g\rangle)\varphi=\langle a K^{*p^n}\rangle$. Именно определим функцию $\langle g\rangle\times\langle g\rangle\to K^*$ декартового произведения $\langle g\rangle\times\langle g\rangle$ в K^*, значения которой обозначаем через $(g^{(i)}, g^{(j)})$ следующим образом:

$$(g^{(i)}, g^{(j)})=\begin{cases}1, & \text{если } 0\leqq i,\ j,\ i+j<p^n;\\ a, & \text{если } 0<i,\ j<p^n\leqq i+j.\end{cases}$$

Нетрудно увидеть, что $(g^{(i+j)}, g^{(k)})\,(g^{(i)}, g^{(j)})=(g^{(i)}, g^{(j+k)})\,(g^{(j)}, g^{(k)})$ для всех целых чисел i, j и k интервала $[0, p^n)$. Тогда K-алгебра с базисом $\langle g\rangle$, в которой умножение базисных элементов определяется следующим образом: $ab=(a, b)\,(a.b)$, где „ · “ — умножение в $\langle g\rangle$ и a, $b\in\langle g\rangle$, является скрещенной алгеброй $K_t\langle g\rangle$. Так как $g^{p^n}=a$, то $(K_t\langle g\rangle)\varphi=\langle aK^{*p^n}\rangle$, т. е. φ — сюръекция.

Докажем вторую часть следствия. Пусть единичная подгруппа $\langle K^{*p^n}\rangle$ фактор-группы K^*/K^{*p^n} соответствует при отображении φ классу $\mathscr{A}$ скрещенных групповых алгебр. Если $K_t\langle g\rangle\in\mathscr{A}$, то $(K_t\langle g\rangle)\varphi=\langle aK^{*p^n}\rangle=\langle K^{*p^n}\rangle$, где значение a определено выше. Так как уравнение $x^{p^n}-a=0$ имеет решение в K, то $K_t\langle g\rangle\cong K\langle g\rangle$ (см., например [4]). Следовательно, $K\langle g\rangle\in\mathscr{A}$, чем следствие доказано.

Вещественно замкнутое поле K называется полем, которое может быть линейно упорядочено, но никакое собственное алгебраическое расширение которого не допускает линейного упорядочивания [5, с. 369]. Оно имеет характеристику 0.

Следствие 8. *Если p — нечетное простое число, то любая скрещенная алгебра $K_t\langle g\rangle$ циклической p-группы $\langle g\rangle$ над вещественным замкнутым полем K изоморфна групповой алгебре $K\langle g\rangle$.*

Доказательство. Ввиду [5, с. 370, теорема 127.4], K^*/K^{*p^n} — единичная группа. Тогда из второй части следствия 7 вытекает $K_t\langle g\rangle \cong K\langle g\rangle$.

Следствие 9. *Если p — нечетное простое число, $\langle g\rangle$ — циклическая группа порядка p^n, K — поле, характеристика q которого отлична от p, $|K|=q^l$, и k — наибольшее целое число интервала $[0, n]$, для которого $q^l \equiv 1 \pmod{p^k}$, то существуют ровно $k+1$ классов, каждый из которых состоится из изоморфных скрещенных групповых алгебр группы $\langle g\rangle$ над полем K и каждый такой класс определяется элементом c^{p^i}, $0 \leqq i \leqq k$, где c — фиксированный образующий элемент мультипликативной группы K^*.*

Доказательство. Имеет место прямое разложение $K^*=K_p \times A$, где K_p — силовская p-подгруппа группы K^*. Тогда $K^*/K^{*p^n} \cong K_p/K_p^{p^n} \cong \langle cK_p^{p^n}\rangle$ и $\langle cK_p^{p^n}\rangle$ — циклическая группа порядка p^k. Все подгруппы $\langle cK_p^{p^n}\rangle$ являются $\langle c^{p^i} K_p^{p^n}\rangle$, $0 \leqq i \leqq k$ и, ввиду следствия 7, они определяют все классы изоморфных скрещенных групповых алгебр группы $\langle g\rangle$ над K. Следствие доказано.

Для любого натурального числа a и любого простого числа q существуют такие однозначно определенные числа $k \in \mathrm{N}$ и $l \in \mathrm{N} \cup \{0\}$, что $a=kq^l$ и $(k, q)=1$. Число l, определенное этим образом, называется порядком элемента a в q [1, с. 91] и обозначается через $l=\mathrm{ord}_q\, a$. Очевидно, $\mathrm{ord}_q(ab)=\mathrm{ord}_q a+\mathrm{ord}_q b$. Пусту Π — множество всех простых чисел. Если $a \in \mathrm{N}$, то пусть

$$\Pi(a)=\{q \in \Pi \mid \mathrm{ord}_q a \neq 0\},$$

$$\Pi_p(a)=\{q \in \Pi(a) \mid \mathrm{ord}_p \mid \mathrm{ord}_q(a)) \leqq \mathrm{ord}_p(\mathrm{ord}_r a),\ \forall r \in \Pi(a)\}$$

и $q(a)$ — наименьший элемент множества $\Pi_p(a)$. Пусть n — фиксированное натуральное число, p — простое число и T — множество, содержащее число 1 и все неединичные натуральные числа a, для которых выполняются следующие два условия:

1) $0<\mathrm{ord}_q a \leqq p^n-1$ для любого $q \in \Pi(a)$ и

2) $\mathrm{ord}_{q(a)}(a)=p^{l_a}$.

Пусть Q — поле рациональных чисел. Тогда имеет место следующее утверждение.

Лемма 10. *Если $\mathscr{A}$ — множество всех циклических подгрупп фактор-группы $\mathrm{Q}^*/\mathrm{Q}^{*p^n}$, то отображение $\varphi: T \to \mathscr{A}$, для которого $\varphi(a)=\langle a\mathrm{Q}^{*p^n}\rangle$, биективно.*

Доказательство. Докажем, что отображение φ инъективно. Очевидно, что если $a \in T$ и $a \neq 1$, то $\langle a\mathrm{Q}^{*p^n}\rangle \neq \langle \mathrm{Q}^{*p^n}\rangle$. Пусть a и b — неединичные элементы множества T и $\varphi(a)=\varphi(b)$, т. е. $\langle a\mathrm{Q}^{*p^n}\rangle=\langle b\mathrm{Q}^{*p^n}\rangle$. Следовательно, $b=a^t x^{p^n}$, где $(t, p)=1$. Отсюда вытекает, что для любого $q \in \Pi$ имеет место

$$\mathrm{ord}_q b \equiv t\, \mathrm{ord}_q a \pmod{p^n}. \tag{6}$$

Так как $(t, p)=1$, то из этого сравнения получается, что максимальная степень числа p, которая делит $\mathrm{ord}_q a$, равняется максимальной степени числа p, которая делит $\mathrm{ord}_q b$, т. е. для каждого $q \in \Pi$ имеет место

$$\mathrm{ord}_p(\mathrm{ord}_q b)=\mathrm{ord}_p(\mathrm{ord}_q a).$$

Отсюда в частности вытекает, что $\Pi(a)=\Pi(b)$, $q(a)=q(b)$ и $l_a=l_b=l$. Если в (6) заменим q на $q(a)$, получим $p^l \equiv tp^l \pmod{p^n}$. Следовательно, $t \equiv 1 \pmod{p^{n-l}}$ и $t=1+rp^{n-l}$. Подставляя t в (6), получим

$$\mathrm{ord}_q b \equiv \mathrm{ord}_q a+rp^{n-l}\, \mathrm{ord}_q a \pmod{p^n}.$$

Так как $p/\mathrm{ord}_q a$, то $\mathrm{ord}_q b \equiv \mathrm{ord}_q a \pmod{p^n}$. Следовательно, для любого $q \in \Pi$ имеет место $\mathrm{ord}_q a=\mathrm{ord}_q b$, т. е. $b=a$. Таким образом отображение φ инъэктивно.

Докажем, что отображение φ сюръективно. Пусть $\langle c\mathrm{Q}^{*p^n}\rangle$ — любая циклическая подгруппа группы $\mathrm{Q}^*/\mathrm{Q}^{*p^n}$. Если $c\in \mathrm{Q}^{*p^n}$, то $\varphi(1)=\langle c\mathrm{Q}^{*p^n}\rangle$. Пусть $c\notin \mathrm{Q}^{*p^n}$. Положим

$$\mathrm{ord}_{q(c)}\, c=\delta p^{l_c}\,,\ (\delta, p)=1 \tag{7}$$

и $l_c=l$. Так как $c\notin \mathrm{Q}^{*p^n}$, то $l<n$. Из $(\delta, p^{n-l})=1$ вытекает равенство

$$\delta u+p^{n-l}\, v=1, \tag{8}$$

где $u, v\in \mathrm{Z}$. Так как $(u, p)=1$, то $\langle c\mathrm{Q}^{*p^n}\rangle=\langle c^u\ \mathrm{Q}^{*p^n}\rangle=\langle a\mathrm{Q}^{*p^n}\rangle$, где

$$a=c^u\, x^{p^n} \tag{9}$$

и x можно подобрать так, что $0<\mathrm{ord}_q\, a\leqq p^n-1$, т. е. для числа a выполняется условие 1) определения множества T (для каждого $q\in\Pi$). Как выше, из равенства (9) следует $q(a)=q(c)$ и $l=l_c=l_a$. Покажем, что $\mathrm{ord}_q\, a$ является степенью числа p, т. е., что a удовлетворяет условию 2) определения множества T. Из (9) вытекает $\mathrm{ord}_{q(a)}a=u\ \mathrm{ord}_{q(a)}\, c+p^n\ \mathrm{ord}_{q(a)}\, x$.
Из этого равенства, используя, что $q(a)=q(c)$, $l_c=l$ и (7), получается $\mathrm{ord}_{q(a)}\, a=u\delta p^l+p^n\ \mathrm{ord}_{q(a)}\, x$, откуда, ввиду (8), следует $\mathrm{ord}_{q(a)}\, a=p^l-p^n v+p^n\ \mathrm{ord}_{q(a)}\, x$, т. е. $\mathrm{ord}_{q(a)}\, a\equiv p^l \pmod{p^n}$. Так как $l<n$ и $0<\mathrm{ord}_{q(a)}\, a<p^n$, то $\mathrm{ord}_{q(a)}\, a=p^l=p^{l_a}$ (поскольку $l=l_a$). Этим условие 2) для числа a доказано. Следовательно, $a\in T$ и $\varphi(a)=\langle cQ^{*p^n}\rangle$, т. е. отображение φ сюръективно. Лема доказана.

Следствие 11. Если $\langle g\rangle$ — циклическая группа порядка p^n, где p — нечетное простое число, то множество всех классов изоморфных скрещенных групповых алгебр $\mathrm{Q}_t\langle g\rangle$ группы $\langle g\rangle$ над полем Q рациональных чисел счетно. Класс, содержащий групповую алгебру $\mathrm{Q}\langle g\rangle$ определяется числом 1, а любой другой класс — произвольным натуральным числом a, для которого выполнены следующие два условия

1) $0<\mathrm{ord}_q\, a\leqq p^n-1$ для любого $q\in\Pi(a)$ и

2) $\mathrm{ord}_{q(a)}\, a$ — степень числа p.

Доказательство вытекает непосредственно из следствия 7 и из леммы 10.

ЛИТЕРАТУРА

1. С. Ленг. Алгебра. М., 1968.
2. Н. А. Начев. Инварианты биномных сепарабельных расширений. *Доклады БАН*, 39, 1986, № 11, 9—10.
3. Н. А. Начев, Т. Ж. Моллов. О полупростых скрещенных групповых алгебр циклических p-групп. *Доклады БАН*, 40, 1987, № 7, 13—15
4. Н. А. Начев, Т. Ж. Моллов. Минимальные идемпотенты полупростых скрещенных групповых алгебр циклических p-групп нечетного порядка. *Publ. Math.* (в печати).
5. Л. Фукс. Бесконечные абелевы группы. М., 2, 1977.

Пловдивский университет „П. Хилендарски"
4000 Пловдив

Поступила 26. 9. 1986