PLISKA

STUDIA MATHEMATICA BULGARICA

ПЛИСКА

БЪЛГАРСКИ МАТЕМАТИЧЕСКИ СТУДИИ

ИЗОМОРФИЗМ МОДУЛЯРНЫХ ГРУППОВЫХ АЛГЕБР КОНЕЧНЫХ 2-ГРУПП, ДЛЯ КОТОРЫХ ПОРЯДОК ФАКТОР-ГРУППЫ ПО ЦЕНТРУ РАВНЯЕТСЯ ЧЕТЫРЕМ

НАКО А. НАЧЕВ, ТОДОР Ж. МОЛЛОВ

Пусть R — конечное коммутативное кольцо с единицей и характеристики 2 без нильпотентных элементов, G — такая конечная 2-группа с коммутантом порядка 2, что индекс ее центра Z в G равняется 4 и фактор-группа Z по нижнему слою $Z[2]$ группы Z является или цикличной, или элементарной абелевой группой, и H — произвольная группа. Тогда из изоморфизма групповых алгебр RG и RH групп G и H над R следует изоморфизм G и H.

В настоящей работе дается положительный ответ гипотезе 9.4 из [7, с. 61] для определения p-группы G своей модулярной групповой алгеброй RG, а именно в случае, когда R — конечное коммутативное кольцо с единицей и характеристики 2 без нильпотентных элементов и G — такая конечная 2-группа с коммутантом порядка 2, что $|G/Z|=4$ и $Z/Z[2]$ — цикличная или элементарная абелева группа, где $Z[2]$ — нижний слой Z. До сих пор получены следующие частные решения этой гипотезы: в [5], когда R — поле p-элементов и $|G|\leqq p^4$, и в [4], когда R совпадает с кольцом вычетов по модулю p^n при $p\neq 2$, а G — группа класса 2 с експонентой p^n. Результаты работы опубликованы в [3].

Используем следующие обозначения: G — конечная 2-группа, если не оговорено противное; R — коммутативное кольцо с единицей и характеристики 2, если не оговорено противное; G' — коммутант группы G; $\langle\cdots\rangle$ — подгруппа, порожденная...; $C(a)$ — централизатор a в G; $Z=Z(G)$ — центр G; $O(a)$ — порядок элемента $a\in G$; $h_A(a)$ — высота элемента a в подгруппы A; $\sqrt{g}=\{a/a^2=g, a\in G\}$; $\times$ — знак прямого произведения групп; $(G:A)$ — индекс подгруппы A в G; $\circ$ — знак полупрямого произведения групп; $Z(R)$ — центр R; $A[2^i]=\{a/a^{2^i}=1, a\in A\}$, где A — кольцо (группа); RG — групповая алгебра G над R; x_f — коэффициент элемента $x\in RG$ перед элементом f в записи x в некотором базисе алгебры RG; $n(x)=\Sigma_{g\in G}x_g$, если $x=\Sigma_{g\in G}x_g g$; $S(RG)$ — силовская 2-подгруппа группы нормированных единиц RG; $S'(RG)$ — коммутант группы $S(RG)$; $K(RG)$ — коммутант RG; $|A|$ — мощность A; $\varnothing$ — пустое множество; $\cup$ — знак раздельного объединения множеств; $\setminus$ — разность двух множеств.

Если G — конечная 2-группа и $|G/Z|=4$, то в [3] дается следующее описание группы G: имеет место $G=H\times C$, где C — абелева группа, а H определена соотношениями по одному из следующих трех способов:

1) $H=\langle a, b, c\rangle$, $a^{2^n}=b^{2^m}=c^{2^s}=1$, $a^{-1}ba=bc^{2^{s-1}}$, $ac=ca, bc=cb$, $n, m, s\geqq 1$, $n+m+s\geqq 4$, причем $H=\langle a\rangle\circ(\langle b\rangle\times\langle c\rangle)$;

2) $a^{2^n}=b^{2^m}=1$, $a^{-1}ba=b^{1+2^{m-1}}$, $n\geqq 1$ и $m\geqq 2$, причем $H=\langle a\rangle\circ\langle b\rangle$;

3) H совпадает с группой кватернионов порядка 8.

В этом случае будем говорить еще, что G принадлежит классу $\mathscr{K}$, причем, если для H имеют место соотношения 1), 2) или 3), то будем говорить, что G принадлежит подклассам $\mathscr{K}_1$, $\mathscr{K}_2$ и $\mathscr{K}_3$ класса $\mathscr{K}$ и, что для них имеют место соответственно определяющие соотношения вида 1), 2) и 3).

Легко заметить, что если $G \in \mathscr{K}$, то $|G'|=2$. Кроме того, если R — коммутативное кольцо с единицей и характеристики p без нильпотентных элементов, а G — p-группа, то силовская p-подгруппа алгебры RG совпадает с $S(RG)$, так как силовская p-подгруппа группы единиц кольца R тривиальна. Из этого следует, что если $\varphi: RG \to RG_1$ — изоморфизм модулярных алгебр, то он сохраняет нормировку элементов RG. Этот факт будем использовать в дальнейшем в почти всех доказательствах. Везде рассматриваются изоморфизмы R-алгебр (кроме изоморфизмов групп).

(1) Лемма. *Если R — коммутативное кольцо с единицей и характеристики p и G — p-группа, то коммутант $\mathscr{K}(RG)$ совпадает с идеалом $\mathscr{L}(G')$ алгебры RG, порожденным элементами $g'-1$, где $g' \in G'$.*

Доказательство. Предварительно докажем, что $\mathscr{K}(RG)$ совпадает с подмодулем W модуля RG, порожденным, как R-модуль, всевозможными элементами вида $a(bc-cb)$, где $a, b, c \in G$. Очевидно $W \subseteq \mathscr{K}(RG)$. Кроме того, $\mathscr{K}(RG) \subseteq W$, так как для произвольного R-порождающего элемента коммутанта $\mathscr{K}(RG)$ имеет место $a(bc-cb)\,d = ad(d^{-1}bdd^{-1}cd - d^{-1}cd\,d^{-1}bd) \in W$. Следовательно, $\mathscr{K}(RG) = W$.

Очевидно $\mathscr{K}(RG) \subseteq \mathscr{L}(G')$, так как R-порождающие элементы $a(bc-cb)$ коммутанта $\mathscr{K}(RG)$ совпадают с $abc(1-c^{-1}b^{-1}cb) \in \mathscr{L}(G')$. Обратно, пусть $g(1-g')h$ — произвольный порождающий R-модуля $\mathscr{L}(G')$. Тогда $g(1-g')h = gh(1-h^{-1}g'h)$, т. е. порождающие R-модуля $\mathscr{L}(G')$ можно выбирать из элементов $g(1-h')$, где $h' \in G'$. Однако, $h' = h_1 \dots h_n$, где $h_i = a_i^{-1} b_i^{-1} a_i b_i = 1 + a_i^{-1} b_i^{-1}(a_i b_i - b_i a_i)$. Следовательно, $h' = h_1 \dots h_n = 1 + x$, где $x \in \mathscr{K}(RG)$, т. е. $1-h' \in \mathscr{K}(RG)$ и $g(1-h') \in \mathscr{K}(RG)$. Таким образом, $\mathscr{L}(G') \subseteq \mathscr{K}(RG)$ и $\mathscr{K}(RG) = \mathscr{L}(G')$.

Следующее утверждение доказано в [5], когда R — поле p-элементов и G — конечная p-группа.

(2) Предложение. *Если R — коммутативное кольцо с единицей и характеристики p, а G и H — p-группы, то из изоморфизма $RG \cong RH$ как R-алгебрами следует $R(G/G') \cong R(H/H')$.*

Доказательство. Если $\varphi: RG \to RH$ — изоморфизм групповых алгебр, то ввиду леммы (1), φ отображает $\mathscr{L}(G')$ на $\mathscr{L}(H')$. Следовательно, $RG/\mathscr{L}(G') \cong RH/\mathscr{L}(H')$. Докажем, что

$$RG/\mathscr{L}(G') \cong R(G/G'), \tag{3}$$

откуда будет следовать предложение. Для этой цели определим гомоморфизм $\psi: RG \to R(G/G')$, полагая $(\Sigma \alpha_g g)\psi = \Sigma \alpha_g gG'$. Пусть M — полная система представителей G по G'. Тогда, для каждого x из RG имеем

$$x = \sum_{g \in M} \lambda_g g, \quad \lambda_g \in RG'. \tag{4}$$

Если $x \in \mathscr{L}(G')$, то x имеет вид (4) с $n(\lambda_g)=0$. Следовательно,

$$x\psi = \sum_{g \in M} \lambda_g \psi \,.\, g\psi = \sum_{g \in M} n(\lambda_g)\, gG' = 0,$$

т. е. $\mathscr{L}(G') \subseteq \operatorname{Ker}\psi$. Пусть, наоборот, $x \in \operatorname{Ker}\psi$. Представим x в виде (4). Тогда

$$0 = x\psi = \sum_{g \in M} \lambda_g \psi \,.\, gG' = \sum_{g \in M} n(\lambda_g) G' \,.\, gG' = \sum_{g \in M} n(\lambda_g) gG'.$$

Так как полученная запись в последнем равенстве канонична, то $n(\lambda_g)=0$, т. е. $x \in \mathscr{L}(G')$ и $\operatorname{Ker}\psi \subseteq \mathscr{K}(G')$. Формула (3) доказана.

Следующее утверждение доказано в [6], когда R — конечное поле характеристик p, а G и H — конечные p-группы.

(5) Предложение. *Если G и H — p-группы, а R — коммутативное кольцо с единицей и характеристики p, то из изоморфизма $RG \cong RH$ как R-алгебрами следует $RZ \cong RZ_1$, как R-алгебрами, где Z и Z_1 — центры соответственно G и G_1.*

Доказательство аналогично [6]. Оно происходит из замены слова подпространство словом подмодуль.

(6) Лемма. *Если $G \in \mathscr{K}$, то $S'(RG) \subseteq 1+\mathscr{K}(RG)$.*

Доказательство. Если $x, y \in S(RG)$, то $S'(RG)$ порождается коммутаторами вида $x^{-1}y^{-1}xy = 1 - x^{-1}y^{-1}(xy-yx)$. Из доказательства леммы (1) видно, что последний элемент принадлежит $1+\mathscr{K}(RG)$. Следовательно, $S'(RG) \subseteq 1+\mathscr{K}(RG)$.

(7) Лемма. *Если $G \in \mathscr{K}$, то $(\Sigma_{g \in G} x_g g)^{2^i} = \Sigma_{g \in G} x_g^{2^i} g^{2^i}$ при $i \geqq 2$.*

Доказательство. Введем линейный порядок в G. Очевидно

$$\Big(\sum_{g \in G} x_g, g\Big)^{2^i} = \Sigma_{g \in G} x_g^2 g^2 + \sum_{\substack{g,h \in G\\ g<h}} x_g x_h (gh+hg)^{2^{i-1}} = \sum_{g \in G} x_g^{2^i} g^{2^i}$$

$$+\Big(\sum_{g,h \in G,\, g<h} x_g x_h gh(1+h^{-1}g^{-1}hg)\Big)^{2^{i-1}} = \sum_{g \in G} x_g^{2^i} g^{2^i},$$

так как $(h^{-1}g^{-1}hg)^{2^{i-1}}=1$ и вторая сумма в левой части последнего равенства равна 0.

(8) Следствие. *Если $x \in RG$, где $G \in \mathscr{K}$, и $n(x)=1$, то $x \in S(RG)$.*

(9) Лемма. *Если $G \in \mathscr{K}$, то для $i \geqq 2$ имеет место*

$$|S(RG)[2^i]| = |R|^{|G|-|G|/|G[2^i]|}. \tag{10}$$

Доказательство. Так как $a^{2^i}b^{2^i}=(ab)^{2^i}$ для $i \geqq 2$ и $a, b \in G$, то $G[2^i]$ — подгруппа G. Из леммы (7) и следствия (8) вытекает, что элемент $x = \Sigma_{g \in G} x_g g \in S(RG)[2^i]$ тогда и только тогда, когда

$$\sum_{g \in uG[2^i]} x_g = \begin{cases} 1, & \text{если } u \in G[2^i], \\ 0, & \text{если } u \notin G[2^i]. \end{cases} \tag{11}$$

Число уравнения (11) равняется $(G:G[2^i]) = |G|/|G[2^i]|$, а число параметров в каждом из них — $|G[2^i]|-1$. Следовательно, число параметров системы (11) равно $(|G[2^i]|-1)|G|/|G[2^i]|$. Так как каждый параметр может принимать $|R|$ значений, то число решений (11) равно прямой части (10), т. е. имеет место (10).

(12) Следствие. *Если $G \in \mathscr{K}$, $G_1 \in \mathscr{K}$ и $RG \cong RG_1$ как R-алгебры, то $|G[2^i]| = |G_1[2^i]|$ для $i \geqq 2$.*

Доказательство. Так как $S(RG)[2^i] \cong S(RG_1)[2^i]$, то из (10) получается $|R|^{|G|-|G|/|G[2^i]|} = |R|^{|G_1|-|G_1|/|G_1[2^i]|}$ и так как $|G|=|G_1|$, то получается искомое.

(13) Лемма. *Если $G \in \mathscr{K}$, $G_1 \in \mathscr{K}$, $G' = \langle k \rangle$, $G_1' = \langle k_1 \rangle$, $Z_1 = Z(G_1)$ и $RG \cong RG_1$, то $h_Z(k) = h_{Z_1}(k_1)$.*

Доказательство. Пусть $i=h_Z(k)\geqq 1$ и $k=c^{2^i}$, где $c\in Z$. Если $\varphi: RG \to RG_1$ — изоморфизм, то $c\varphi\in S[Z(LG_1)]$. Следовательно, $c\varphi=u+v$, где $u\in S(RZ_1)$ и v является R-линейной комбинацией классовых сумм группы G_1, содержащих по двум элементам. Тогда

$$k\varphi=(c\varphi)^{2^i}=(u+v)^{2^i}=u^{2^i}+v^{2^i}=u^{2^i}\in S(RZ_1^{2^i}),$$

так как $S(RZ_1)^{2^i}=S(R^{2^i}Z_1^{2^i})$ и $v^2=0$ (см. [3]). С другой стороны, $k\varphi\in S'(RG)\subseteqq 1+\mathscr{K}(RG_1)$, где включение следует из леммы (6). Следовательно, $k\varphi\in S(RZ_1^{2^i})\cap(1+\mathscr{K}(RG_1))\neq\emptyset$, $k\varphi=1+w$, $w\in\mathscr{K}(RG_1)$ и $w=\Sigma_{g\in Z_1^{2^i}}x_g g$ с $\Sigma x_g=0$. Так как $w\neq 0$, то следует, что существует $g\in Z_1^{2^i}$, так что $x_g\neq 0$. Покажем, что $x_g=x_{gR_1}$. Действительно, так как, ввиду леммы (1), $\mathscr{K}(RG_1)$ — идеал алгебры RG_1, порожденный элементом $1+R_1$, то

$$w=(\Sigma\alpha_f f)(1+k_1)=\Sigma\alpha_f f+\Sigma\alpha_f(fk_1)=\Sigma\alpha_f f+\Sigma\alpha_{fk_1}f=\Sigma(\alpha_f+\alpha_{fk_1})f,$$

где суммирование происходит по элементу $f\in G_1$. Следовательно, $x_g=\alpha_g+\alpha_{gk_1}$ и $x_{gk_1}=\alpha_{gk_1}+\alpha_{gk_1^2}=x_g$. Из полученного равенства следует, что $gk_1\in Z_1^{2^i}$, откуда $k_1\in Z_1^{2^i}$, т. е. $h_{Z_1}(k_1)\geqq i=h_Z(k)$. Обратное неравенство доказывается аналогично. Если $h_Z(k)=0$, то из первой части доказательства, используя φ^{-1}, следует, что неравенство $h_{Z_1}(k_1)\geqq 1$ невозможно. Следовательно, $h_{Z_1}(k_1)=0$. Лемма доказана.

(14) Лемма. *Если $x\in RG$, то*

(15) $$(x^2)_g=\sum_{t\in\sqrt{g}}x_t^2+\sum_{t\in G\setminus C(g)}x_t x_{t^{-1}g}.$$

Доказательство. Очевидно $\sqrt{g}\subseteqq C(g)\subseteqq G$. Следовательно,

(16) $$G=\sqrt{g}\cup(C(g)\setminus\sqrt{g})\cup(G\setminus C(g)).$$

Очевидно

(17) $$(x^2)_g=\sum_{t\in G}x_t x_{t^{-1}g}=\sum_{t\in\sqrt{g}}x_t x_{t^{-1}g}+\sum_{t\in(C(g)\setminus\sqrt{g})}x_t x_{t^{-1}g}+\sum_{t\in(G\setminus C(g))}x_t x_{t^{-1}g},$$

где второе равенство следует из (16).

Пусть $t\in\sqrt{g}$. Тогда $t^2=g$ или $t^{-1}g=t$, т. е. общий член первой суммы равенства (17) будет x_t^2.

Пусть $t\in(C(g)\setminus\sqrt{g})$. Тогда $t^{-1}g\neq t$. Кроме того, $t^{-1}g\in(C(g)\setminus\sqrt{g})$, так как в противном случае из $(t^{-1}g)^2=g$ следует $t^2=g$, что невозможно. Тогда

$$\Sigma_{t\in(C(g)\setminus\sqrt{g})}x_t x_{t^{-1}g}=(x_t x_{t^{-1}g}+x_{t^{-1}g}x_{g^{-1}tg})+\cdots=2x_t x_{t^{-1}g}+\cdots=0,$$

т. е. члены указанной суммы группируются по два таким образам, что получаются нули. Следовательно, имеет место (15).

Введем бинарное отношение τ в $G\in\mathscr{K}$ $(G_1\in\mathscr{K}_1)$ следующим образом: для любых двух элементов g и h из G имеет место $g\tau h$ тогда и только тогда, когда $g^2=h^2$. Очевидно τ — отношение эквивалентности. Пусть

(18) $$\tau(t)=\{g/g^2=t^2,\ g\in G\}.$$

Очевидно, что, если $t^2=g$, то $\sqrt{g}=\tau(t)$.

Некоторое время будем рассматривать следующие группы $G \in \mathcal{K}_2$ и $G_1 \in \mathcal{K}_1$:

(19) $$G = H \times C,\ C = \langle a_1 \rangle \times \cdots \times \langle a_r \rangle,\ O(a_i) = 2^{\delta_i}\ (i = 1, \ldots, r),\ H : a^{2^n} = b^4 = 1,\ a^{-1}ba = b^3;$$

(20) $$G_1 = H_1 \times C_1,\ C_1 = \langle b_1 \rangle \times \cdots \times \langle b_r \rangle,\ O(b_i) = 2^{\delta_i}\ (i = 1, \ldots, r),$$
$$H_1 : u^2 = v^{2^n} = w^2 = 1,\ u^{-1}vu = vw,\ uw = wu,\ vw = wv,\ n \geqq 2.$$

Для этих групп будем использовать следующие обозначения:

(21) $$A = \langle a, Z \rangle,\ Z_1 = Z(G_1),\ U_1 = \langle u, Z_1 \rangle,\ V_1 = \langle v, Z_1 \rangle.$$

(22) Лемма. *Если G_1 — группа, заданная формулами* (20), *то для любого элемента $g_1 \in G_1$ имеет место*

(23) $$\tau(g_1) = \begin{cases} g_1 U_1[2], & \text{если } g_1 \in U_1, \\ g_1 t_1[2], & \text{если } g_1 \in G_1 \setminus U_1. \end{cases}$$

Доказательство. Рассмотрим следующие случаи: 1) $g_1 \in U_1$ и 2) $g_1 \in G_1 \setminus U_1$.

1) Пусть $g_1 \in U_1$. Тогда $g_1 = u^\varepsilon z_1$, где $z_1 \in Z_1$ и $\varepsilon = 0$ или $\varepsilon = 1$. Очевидно $g_1 U_1[2] \subseteqq \tau(g_1)$. Пусть $t \in \tau(g_1)$. Предварительно докажем, что $t \in U_1$. Допустим противное. Тогда 1.1) $t \in vZ_1$ или 1.2) $t \in uvZ_1$.

1.1) Пусть $t \in vZ_1$. Тогда $t = vz_2$, $z_2 \in Z_1$ и из $t^2 = v^2 z_2^2 = g_1^2 = (u^\varepsilon z_2)^2$ получается $v^2 = z'^2$, $z' \in Z_1$. Однако, из последнего равенства и из

(24) $$z' = v^{2\mu} w^\nu b_1^{\gamma_1} \ldots b_l^{\gamma_l}$$

следует $4\mu \equiv 2 \pmod{2^n}$, что невозможно, так как $n \geqq 2$.

1.2) Пусть $t \in uvZ_1$. Тогда $t = uvz_2$, где $z_2 \in Z_1$. Из последнего равенства и из $t^2 = g_1^2$ следует $u^2 v^2 w z_2^2 = u^{2\varepsilon} z_1^2$, т. е. $v^2 = wz'^2$, $z' \in Z_1$. Из последнего равенства, представляя z' в виде (24), снова приходим к тому же самому противоречию, как в случае 1.1). Таким образом $t \in u_1$ и из $t^2 = g_1^2$ получится $t \in g_1 U_1[2]$, т. е. $\tau(g_1) \subseteqq g_1 U_1[2]$. Этим установлена первая формула (23).

2) Пусть $g_1 \in G_1 \setminus U_1$. Очевидно $g_1 Z_1[2] \subseteqq \tau(g_1)$. Пусть, обратно, $t \in \tau(g_1)$. Если допустим, что $t \in U_1$, то по доказанной первой формуле (23) имеет место $\tau(t) = tU_1[2] \subseteqq U_1$, т. е. $g_1 \in U_1$, что невозможно. Следовательно, $t \notin U_1$.

2.1) Пусть $g_1 \in vZ_1$. Тогда $g_1 = vz_1$, $z_1 \in Z_1$. Если допустим, что $t \in uvZ_1$, то $t = uvz_2$, $z_2 \in Z_1$ и $t^2 = u^2 v^2 w t_2^2$. Из последнего равенства и из $t^2 = g_1^2 = v^2 z_1^2$ получается $w = z'^2$, $z' \in Z_1$, что, как в случае 1.1), невозможно, ввиду (24). Таким образом $t \in vZ_1$, т. е. $t = vz_3$. Тогда из $v^2 z_3^2 = t^2 = g_1^2 = v^2 z_1^2$ получится $z_3 \in z_1 Z_1[2]$. Следовательно, $t = vz_3 \in vz_1 Z_1[2] = g_1 Z_1[2]$, т. е. $\tau(g_1) \subseteqq g_1 Z_1[2]$. Ввиду обратного включения, что было установлено предварительно, следует вторая формула (23).

2.2) Пусть $g_1 \in uvZ_1$. Тогда $g_1 = uvz_1$, $z_1 \in Z_1$. Если допустим, что $t \in vZ_1$, то, ввиду случая (2.1), получим, что $\tau(g_1) = tZ_1[2] \subseteqq vZ_1$, т. е. $g_1 \in vZ_1$, что невозможно. Следовательно, $t \in uvZ_1$, т. е. $t = uvz_2$, $z_2 \in Z_1$. Тогда из $t^2 = g_1^2$ следует $z_2 \in z_1 Z_1[2]$, т. е. $t \in uvz_1 Z_1[2] = g_1 Z_1[2]$. Таким образом $\tau(g_1) \subseteqq g_1 Z_1[2]$. Ввиду обратного включения, что было установлено предварительно, следует вторая формула (23).

(24) Лемма. *Если G — группа, заданная формулами* (19), *кольцо R без нильпотентных элементов и $x^2=1$, то*

$$\sum_{t \in Z[2]} x_t = 1. \tag{25}$$

Доказательство. Очевидно $(x^2)_1=1$. Тогда, ввиду (15) и (18), получим

$$1=(x^2)_1=\sum_{t \in \tau(1)} x_t^2=\sum_{t \in Z[2]} x_t^2=\Big(\sum_{t \in Z[2]} x_t\Big)^2,$$

откуда следует (25), так как R не имеет нильпотентных элементов.

(26) Лемма. *Если G и G_1 — группы, заданные формулами* (19) *и* (20), *то существует изоморфизм φ центра Z_1 на центр Z, для которого*

$$v^2\varphi=a^2,\ w\varphi=b^2,\ b_i\varphi=a_i\,(i=1,\ldots,r), \tag{27}$$

который продолжается мультипликативно до изоморфизма группы V_1 на группу A (см. (21)) *посредством сопоставления*

$$v\varphi=a \tag{28}$$

и до взаимно однозначного отображения G_1 на G посредством сопоставления

$$(uv_1)\,\varphi=bv_1\,\varphi, \tag{29}$$

для каждого $v_1 \in V_1$. Кроме того, для любых x и y из G_1 имеют место

$$(xy)\,\varphi=\begin{cases} x\varphi\, y\varphi, & \text{если}\quad x \in V_1 \quad \text{или} \quad y \in V_1,\\ x\varphi\, y\varphi b^2, & \text{если}\quad x \in G_1\setminus V_1,\ y \in G_1\setminus V_1; \end{cases} \tag{30}$$

$$x^{-1}\varphi=\begin{cases} (x\varphi)^{-1}, & \text{если}\quad x \in V_1,\\ (x\varphi)^{-1}b^2, & \text{если}\quad x \in G_1\setminus V_1. \end{cases} \tag{31}$$

Доказательство. Очевидно, что (27) и (28) определяют изоморфизм V_1 на A.

Докажем (30). Если $x, y \in V_1$, то (30) очевидна. Пусть

1) $x \in V_1$, а $y \in uV_1$. Тогда $y=uy_1$, где $y_1 \in V_1$. Если $x \in Z_1$, то, ввиду (29), имеет место $(xy)\,\varphi=(uxy_1)\,\varphi=bx\varphi y_1\varphi$. С другой стороны, опять из (29) получится $x\varphi y\varphi=x\varphi b y\varphi=bx\varphi y_1\varphi$. Следовательно, имеет место первая формула (30). Если же $x \notin Z_1$, то из $y=uy_1\,(y_1 \in V_1)$, ввиду (29) и (27), следует $(xy)\varphi=(uxy_1w)\varphi=bx\varphi y\,\varphi b^2$ и $x\varphi\, y\varphi=x\varphi(uy_1)\varphi=x\varphi b y_1\varphi=bx\varphi y_1\varphi b^2$. Следовательно, имеет место первая формула (30).

2) Пусть $x \in uV_1$, а $y \in V_1$. Тогда (30) доказывается следующим образом: если $y \in Z_1$, то $(xy)\varphi=(yx)\varphi=y\varphi x\varphi=x\varphi y\varphi$, где для получения второго равенства используется результат случая 1), а если $y \notin Z_1$, то $(xy)\varphi=(yxw)\varphi=y\varphi(xw)\varphi=y\varphi x\varphi b^2=x\varphi y\varphi$, где для второго равенства используется результат случая 1), а для третьего равенства — результат случая 1) и (27).

3) Пусть $x \in uV_1$ и $y \in uV_1$. Тогда $x=ux_1$ и $y=uy_1$, где $x_1, y_1 \in V_1$. Имея в виду эти формулы и результаты случая 1), (30) доказывается следующим образом. Если $x_1 \in Z_1$, то $(xy)\varphi=(x_1 y_1)\varphi=x_1\varphi\, y_1\varphi$, а $x\varphi\, y\varphi b^2=(ux_1)\varphi(uy_1)\varphi b^2$ $bx_1\varphi b y_1\varphi b^2=x_1\varphi\, y_1\varphi$, где для второго равенства используется (29), т. е. место (30). Если же $x_1 \in vZ_1$, то $(xy)\varphi=(x_1 y_1 w)\varphi=x_1\varphi y_1\varphi b^2$, где правая часть второго равенства следует из результата случая 2), и $x\varphi y\varphi b^2$ $=bx_1\varphi b y_1\varphi b^2=x_1\varphi y_1\varphi b^2$, где правая часть второго равенства следует из того, что $x_1\varphi \notin Z_1$.

Докажем (31). Достаточно рассмотреть случай, когда $x \in uV_1$, т. е. $x=uv_1$, $v_1 \in V_1$. Тогда, используя (29), получается

$$x^{-1}\varphi=\begin{cases}(uv_1^{-1})\varphi=b(v_1\varphi)^{-1}, & \text{если} \quad v_1 \in Z_1,\\ (uv_1^{-1}w)\varphi=b(v_1\varphi)^{-1}b^2, & \text{если} \quad v_1 \notin Z_1,\end{cases}$$

и

$$(x\varphi)^{-1}=((uv_1)\varphi)^{-1}=b(u_1\varphi)^{-1}=(v_1\varphi)^{-1}b^3=\begin{cases}b(v_1\varphi)^{-1}b^2, & \text{если} \quad v_1 \in Z_1,\\ b(v_1\varphi)^{-1}, & \text{если} \quad v_1 \notin Z_1.\end{cases}$$

Из сопоставления двух серий формул следует (31).

Не трудно видеть, что $1\varphi^{-1}=1$, т. е. полный прообраз 1 является 1. Действительно, пусть $(uv_1)\varphi=bv_1\varphi=1$, где $v_1 \in V_1$. Тогда, $b=(v_1\varphi)^{-1}=v_1^{-1}\varphi$, т. е. $b \in A$, что невозможно.

Докажем, что каждый элемент группы G имеет прообраз при φ. Если baz — любой элемент G, то достаточно доказать, что ba имеет прообраз при φ. Так как $a \in A$, то существует $v_1 \in V_1$, такой, что $v_1\varphi=a$. Следовательно, $ba=bv_1\varphi=(uv_1)\varphi$, т. е. uv_1 — прообраз элемента ba.

Покажем, что, если $x \neq y$, $x, y \in G$, то $x\varphi \neq y\varphi$. Пусть

a) $x \in V_1$, а $y \in G_1 \setminus V_1$. Тогда $x^{-1} \in V_1$ и согласно (30) и (31) получится $(x^{-1}y)\varphi=x^{-1}\varphi y\varphi=(x\varphi)^{-1}y\varphi$. Если допустим, что $x\varphi=y\varphi$, то $1=(x\varphi)^{-1}y\varphi=(x^{-1}y)\varphi$ и согласно сделанному выше замечанию, получается $x^{-1}y=1$, что невозможно.

b) Если $x \in G \setminus V_1$, а $y \in V_1$, то аналогично случаю a) получится $x\varphi \neq y\varphi$.

c) Пусть $x \in G \setminus V_1$ и $y \in G \setminus V_1$ (и $x \neq y$). Тогда $(x^{-1}y)\varphi=x^{-1}\varphi y\varphi b^2=(x\varphi)^{-1}y\varphi$, где первое и второе равенства следуют из второй формулы (31). Если допустим, что $x\varphi=y\varphi$, то получим $(x^{-1}y)\varphi=1$, т. е. согласно замечанию получается $x^{-1}y=1$, что невозможно. Лемма доказана.

Если группа G задана формулами (19), то в дальнейшем будем использовать следующие обозначения (в RG):

$$u=1+a, \quad v=1+b, \quad w_i=1+a_i \quad (i=1, \ldots, r). \tag{32}$$

Очевидно $u^{2^n}=v^4=w_i^{2^{\delta_i}}=0$ и $uw_i=w_iu$, $vw_i=w_iv$. Покажем, что

$$vu=uv+v^2+v^3+uv^2+uv^3. \tag{33}$$

Действительно, из $ba=ab^3$ и (32) следует $(1+v)(1+u)=(1+u)(1+v)^3=(1+u)(1+v+v^2+v^3)$, откуда получается (33). Из (33) следует $(uv)^2=u(vu)v=u(uv+v^2+v^3+uv^2+uv^3)v$, или

$$(uv)^2=u^2v^2+uv^3+u^2v^3. \tag{34}$$

В дальнейшем используется множество $\mathcal{D}$, определенное в следующей лемме, и обозначение $\alpha^0=1$, где $\alpha \in R$.

(35) Лемма. *Если группа G определена соотношениями* (19), *то множество*

$$\mathcal{D}=\{u^\alpha v^\beta w_1^{\gamma_1} \ldots w_r^{\gamma_r} / 0 \leq \alpha \leq 2^n-1,\ 0 \leq \beta \leq 3,\ 0 \leq \gamma_i \leq 2^{\delta_i}-1,\ i=1, 2, \ldots, r\} \tag{36}$$

является R-базисом групповой алгебры RG.

Доказательство. Так как $|\mathcal{D}|=|G|$, то достаточно доказать, что элементы множества $\mathcal{D}$ линейно независимы. Допустим, что

$$\Sigma_{\alpha,\beta,\gamma_1,\dots,\gamma_r}\lambda_{\alpha\beta\gamma_1\dots\gamma_r}u^\alpha v^\beta w_1^{\gamma_1}\dots w_r^{\gamma_r}=0.$$

Если $(\alpha,\beta,\gamma_1,\dots,\gamma_r)=(2^n-1,3,2^{\gamma_1-1},\dots,2^{\gamma_r-1})$, то используя (32), очевидно получается $\lambda_{2^n-1,3,2^{\gamma_1-1},\dots,2^{\gamma_r-1}}=0$. В дальнейшем доказательство, что все коэффициенты равны нулю, проводится по индукции относительно системы $\{(\alpha,\beta,\gamma_1,\dots,\gamma_r)\}$ индексов, которая становится линейно упорядоченным множеством относительно следующей лексикографической упорядоченности: для любых двух ее элементов положим $(\alpha,\beta,\gamma_1,\dots,\gamma_r)\leqq(\alpha',\beta',\gamma_1',\dots,\gamma_r')$, если для их первых соответствующих компонент, считаемых в обратном порядке, которые различны, выполнено обратное строгое неравенство „$>$".
(37) Определение. *Будем говорить, что 2-группа G удовлетворяет* $(*)$, *если $Z/Z[2]$ — цикличная или элементарная абелева группа.*
(38) Лемма. *Если G — группа, определенная соотношениями* (19), *G удовлетворяет условие* $(*)$, *кольцо R без нильпотентных элементов и $x^2=0$ для $x\in RG$, то*

$$(39)\qquad x_{u^\alpha v^\beta w_1^{\gamma_1}\dots w_r^{\gamma_r}}=0,\ \alpha=0,1,\dots,2^{n-1}-1,\ \beta=0,1;\ \gamma_i=0,1,\dots,2^{\delta_i-1}-1$$

$$(i=1,\dots,r).$$

Доказательство. Очевидно, что x можно представить в виде $x=A_1+A_uu+A_vv+A_{uv}uv$, где $A_1, A_u, A_v, A_{uv}\in RZ$. Тогда, используя (33) и (34), получается

$$x^2=A_1^2+A_u^2u^2+A_v^2v^2+A_{uv}^2u^2v^2+A_uA_vv^2+A_uA_{uv}u^2v^2+(A_uA_vv^2+A_uA_{uv}v^2)u$$
$$+(A_{uv}^2u^2v^2+A_uA_vv^2+A_uA_{uv}u^2v^2+A_vA_{uv}v^2)v$$
$$+(A_{uv}^2v^2+A_uA_vv^2+A_uA_{uv}v^2+A_vA_{uv}v^2)uv=0.$$

Из формул $Z=b^2\times Z'$ и $RZ=(RZ')\langle b^2\rangle$ следуют представления

$$(40)\qquad A_{u^\alpha v^\beta}=B_{u^\alpha v^\beta}+B_{u^\alpha v^{\beta+2}}v^2,\ B_{u^\alpha v^\beta}\in RZ',\ \alpha=0,1,\quad \beta=0,1.$$

Так как $x^2=0$, то коэффициенты перед 1, u, v и uv в вышеуказанном представлении элемента x^2 должны быть равны нулю, т. е. используя (40), получится

$$B_1^2+B_u^2u^2+B_v^2v^2+B_{uv}^2u^2v^2+B_uB_vv^2+B_uB_vu^2v^2=0,$$
$$B_uB_vv^2+B_uB_{uv}v^2=0,\ B_{uv}^2u^2v^2+B_uB_vv^2+B_uB_{uv}u^2v^2+B_vB_{uv}v^2=0,$$
$$B_{uv}^2v^2+B_vB_{uv}v^2=0.$$

Прибавляя третье равенство полученной системы к первому и определяя $B_uB_vv^2$ и $B_{uv}^2v^2$ соответственно из второго и четвертого равенства и подставляя их в третье равенство, получится

$$(41)\qquad \begin{aligned} &B_1^2=B_u^2u^2+B_v^2v^2+B_vB_{uv}v^2=0,\\ &B_uB_vv^2+B_uB_{uv}v^2=0,\\ &B_vB_{uv}u^2v^2+B_uB_{uv}v^2+B_uB_{uv}u^2v^2+B_vB_{uv}v^2=0,\\ &B_{uv}^2v^2+B_vB_{uv}v^2=0.\end{aligned}$$

Очевидно третье равенство системы (41) можно записать в виде $(B_vB_{uv}+B_uB_{uv})(1+v^2)=0$ и второй множитель сократить. Так как $\{1, b^2\}$ — базис групповой алгебры RZ над кольцом RZ', то $\{1, v^2\}$ — также базис алгебры RZ над RZ'. Тогда (41) можно записать в виде

$$(42)\qquad B_1^2+B_u^2u^2=0,\ B_v^2+B_vB_{uv}=0,\ B_uB_v+B_uB_{uv}=0,\ B_vB_{uv}+B_uB_{uv}=0,$$
$$B_{uv}^2+B_vB_{uv}=0.$$

Пусть

$$(43)\qquad B_{u^iv^t}=\sum_{\alpha=0,\ \gamma_j=0}^{2^{n-1}-1,\ 2^{\delta_j}-1} x_{u^{2\alpha+i}v^tw_1^{\gamma_1}\dots w_r^{\gamma_r}}u^{2\alpha}w_1^{\gamma_1}\dots w_r^{\gamma_r},\quad i=0,1,\quad t=0,1.$$

Подставляя B_1 и B_u, определенные из (43), в первом уравнении системы (42) и учитывая, что $u^{4\alpha}\neq u^{4\beta+2}$, получится $B_1^2=0$ и $B_u^2u^2=0$. Если представим B_u в виде $B_u=\Sigma_\alpha C_{u^{2\alpha+1}}u^{2\alpha}$, то из $B_u^2u^2=0$ получится $C^2_{u^{2\alpha+1}}=0$, $\alpha\leqq 2^{n-2}-1$, т. е. $B_u^2=0$. Прибавляя и второе уравнение (42) к пятому, из (42) окончательно получится

$$(44)\qquad B_1^2=0,\ B_u^2=0,\ B_v^2=B_{uv}^2=B_vB_{uv}=B_uB_{uv}=B_uB_v.$$

Из (44) следует

$$(45)\qquad B_v^3=0.$$

Так как множество $\mathcal{D}$, определенное через (36), образует базис алгебры RG, то из первых двух уравнений (44) вытекает

$$x^2_{u^{2\alpha}w_1^{\gamma_1}\dots w_r^{\gamma_r}}=0,\quad x^2_{u^{2\alpha+1}w_1^{\gamma_1}\dots w_r^{\gamma_r}}=0,\quad \alpha=0,1,\dots,2^{n-2}-1,$$
$$\gamma_i=0,1,\dots,2^{\delta_i-1}-1.$$

Так как R — кольцо без нильпотентных элементов, то последние два равенства для коэффициентов объединяются в

$$(46)\qquad x_{u^\alpha w_1^{\gamma_1}\dots w_r^{\gamma_r}}=0,\ \alpha=0,1,\dots,2^{n-1}-1,\ \gamma_i=0,1,\dots,2^{\delta_i-1}-1\ (i=1,\dots,r).$$

Докажем, что

$$(47)\qquad x_{u^{2\alpha}vw_1^{\gamma_1}\dots w_r^{\gamma_r}}=0,\ \alpha=0,1,\dots,2^{n-2}-1,\ \gamma_i=0,1,\dots,2^{n_i-1}\ (i=1,\dots,r).$$

Действительно, так как G удовлетворяет условие (*), то для нее имеет место одно из следующих определяющих соотношений:

$$(\mathrm{I})\qquad a^{2^n}=b^4=a_1^2=\dots=a_r^2=1,$$

$$(\mathrm{II})\qquad a^4=b^4=a_1^{2^{\delta_1}}=a_2^2=\dots=a_r^2=1,$$

$$(\mathrm{III})\qquad a^4=b^4=a_1^4=\dots=a_i^4=a_{i+1}^2=\dots=a_r^2=1,\quad i\geqq 2,$$

$$(\mathrm{VI})\qquad a^8=b^4=a_1^4=\dots=a_i^4=a_{i+1}^2=\dots=a_r^2=1,\quad i\geqq 1.$$

Докажем сначала (47) в случае, когда для G имеют место соотношения (I) и (II). Тогда формула $B_v^2=B_uB_v$ из (44), имея ввиду (43), принимает вид

(48) $$x^2_{u^{2\alpha}vw_1^{\gamma_1}\dots w_r^{\gamma_r}} = \sum_{\lambda,\nu_1,\dots,\nu_r} x_{u^{2\lambda+1}w_1^{\nu_1}\dots w_r^{\nu_r}} x_{u^{4\alpha-2\lambda}vw_1^{2\gamma_1-\nu_1}\dots w_r^{2\gamma_r-\nu_r}}.$$

Если для G имеет место (I), то формулы (47), которые мы должны доказать, принимают вид

(47′) $$x_{u^{2\alpha}v}=0, \quad \alpha=0, 1, \dots, 2^{n-2}-1,$$

а полученная формула (48) — вид

(48′) $$x^2_{u^{2\alpha}v} = \sum_{\lambda=0}^{2\alpha} x_{u^{2\lambda+1}} x_{u^{4\alpha-2\lambda}v}.$$

(47′) доказывается индукцией относительно α. При $\alpha=0$ (48′) получает вид $x_v^2=x_u x_v=0$, где второе равенство следует из (46). Следовательно, $x_v=0$, т. е. (47′) имеет место при $\alpha=0$. Допустим, что (47′) имеет место для $0, 1, \dots, \alpha-1$. Докажем, что (47′) имеет место (для α). Действительно, ввиду (46), при $\lambda \leqq 2^{n-2}-1$ каждый первый множитель слагаемых в (48′) равен нулю. Пусть $\lambda > 2^{n-2}-1$. Так как $2^{n-2}-1 \geqq \alpha$, то $\alpha \leqq \lambda-1$, откуда последовательно получаются неравенства $2\alpha \leqq 2\lambda-2$, $4\alpha \leqq 2\alpha+2\lambda-2$ и $4\alpha-2\lambda \leqq 2(\alpha-1)$. Тогда, согласно индуктивному предположению, имеет место $x_{u^{4\alpha-2\lambda}v}=0$, т. е. в (48′) каждое слагаемое (при $\lambda > 2^{n-2}-1$) равно нулю. Таким образом, (47′) доказана.

Пусть имеют место соотношения (II) для G. Тогда (47), которую мы должны доказать, принимает вид

(47″) $$x_{vw_1^{\gamma_1}}=0, \quad \gamma_1=0, 1, \dots, 2^{\delta_1-1}-1,$$

а полученная формула (48) — вид

(48″) $$x^2_{vw_1^{\gamma_1}} = \sum_{\nu_1=0}^{2\gamma_1} x_{uw_1^{\nu_1}} x_{vw_1^{2\gamma_1-\nu_1}}.$$

(47″) доказывается индукцией относительно γ_1. При $\gamma_1=0$ (48″) принимает вид $x_v^2=x_u x_v=0$, где второе равенство следует из (46) т. е. (47″) имеет место для $\gamma_1=0$. Допустим, что (47″) имеет место для $0, 1, \dots, \gamma_1-1$. Докажем, что (47″) имеет место (для γ_1). Действительно, ввиду (46), при $\nu_1 \leqq 2^{\delta_1-1}-1$, каждый первый множитель слагаемых в (48″) равен нулю. Если же $\nu_1 > 2^{\delta_1-1}-1$, то, ввиду $\gamma_1 \leqq 2^{\delta_1-1}-1 < \nu_1$ следует $\gamma_1 \leqq \nu_1-1$ и $2\gamma_1-\nu_1 \leqq \gamma_1-1$. Тогда, согласно индуктивному предположению, имеет место $x_{vw_1^{2\gamma_1-\nu_1}}=0$, т. е. каждый второй множитель слагаемых в (48″) (при $\nu_1 > 2^{\delta_1-1}$) равен нулю. Таким образом (47″) доказана.

Пусть имеют место соотношения (III) для G. Тогда (47), которое мы должны доказать, принимает вид

(47‴) $$x_{vw_1^{\gamma_1}\dots w_l^{\gamma_l}}=0, \ \gamma_s=0, 1 \ (s=1, \dots, l).$$

Для ее доказательства используем (45) и выражение для B_v^2, вычисленное из (43), которое теперь принимает вид

$$B_v^2 = \sum_{\gamma_1,\dots,\gamma_l} x^2_{vw_1^{2\gamma_1}\dots w_l^{2\gamma_l}} w_1^{2\gamma_1}\dots w_l^{2\gamma_l}.$$

Можем предполагать (эвентуальной перенумерацией), что в (47''') имеет место $\gamma_1=\cdots=\gamma_s=1$, а $\gamma_{s+1}=\cdots=\gamma_i=0$. Если переобозначим показатели B_v^2, полагая $\gamma_t=\lambda_t$, то базисный элемент $w_1^3\ldots w_s^3$ в левой части равенства $B_v^3=B_vB_v^2$ получится как произведение тех элементов из B_v и B_v^2, соответствующие показатели которых должны удовлетворять условиям $\gamma_t+2\lambda_t=3\,(t=1,\ldots,s)$. Следовательно, $\gamma_t=1$ и $\lambda_t=1$, т. е. $w_1^3\ldots w_s^3$ получится как произведение двух единственных членов из B_v и B_v^2 и коэффициент $x^3_{vw_1\ldots w_s}$ перед ним должен быть равен нулю, т. е. выполнена (47''').

Случай, когда имеют место соотношения (IV) для G, сводится к предыдущему, полагая $a^2=c_0$.

Так как $x^2=0$, то из (47), имея в виду формулы $B_v^2=B_{uv}^2$, из (44) и из выражения для B_u и B_{uv} в (43) получается

(49) $x_{u^{2\alpha+1}vw_1^{\gamma_1}\ldots w_r^{\gamma_r}}=0,\ \alpha=0,1,\ldots,2^{n-2}-1,\ \gamma_i=0,1,\ldots,2^{\delta_i-1}-1\ (i=1,\ldots,r).$

Тогда (47) и (49) объединяются в $x_{u^\alpha vw_1^{\gamma_1}\ldots w_r^{\gamma_r}}=0$, где $\alpha=0,1,\ldots,2^{n-1}-1$ и $\gamma_i=0,1,\ldots,2^{\delta_i-1}-1\ (i=1,\ldots,r)$, а из полученной формулы и (46) следует (39).

(50) Лемма. *Если G — группа, определенная формулами* (19), *то базис $\mathfrak{D}$ групповой алгебры RG, определенный через* (36), *является булевой алгеброй (относительно некоторого порядка).*

Доказательство. В $\mathfrak{D}$ вводим частичную упорядоченность $\leqq$ следующим образом. Очевидно, что показатели α, β, γ_i любого элемента $d=u^\alpha v^\beta u_1^{\gamma_1}\ldots u_r^{\gamma_r}$ множества $\mathfrak{D}$ можно записать в двоичной системе однозначно в виде

$$(51)\quad \begin{gathered}\alpha=\alpha_0+\alpha_1 2+\cdots+\alpha_{n-1}\,.\,2^{n-1},\quad \alpha_s=0,1,\quad \beta=\beta_0+\beta_1\,.\,2,\quad \beta_s=0,1,\\ \gamma_i=\gamma_{i0}+\gamma_{i1}\,.\,2+\cdots+\gamma_{i,\delta_i-1}\,.\,2^{\delta_i-1},\quad \gamma_{is}=0,1.\end{gathered}$$

Если $d'=u^{\alpha'}v^{\beta'}w_1^{\gamma_1}\ldots w_r^{\gamma_r}$ — другой элемент $\mathfrak{D}$, то показатели α', β', γ_i' представим в виде (51), в котором коэффициенты обозначены через α_s', β_s', γ_{is}' и положим $d\leqq d'$ тогда и только тогда, когда $\alpha_i\leqq\alpha_i'$, $\beta_j\leqq\beta_j'$ и $\gamma_{st}\leqq\gamma_{st}'$ для каждого i, j, s, t. Очевидно, что F — частично упорядоченное множество. Если d и d' — любые элементы $\mathfrak{D}$, d и d', имеют вышеуказанный вид и $\alpha_i''=\max(\alpha_i,\alpha_i')$, $\beta_j''=\max(\beta_j,\beta_j')$, $\gamma_{st}''=\max(\gamma_{st},\gamma_{st}')$, то элемент d'' с показателями α'', β'' и γ_i'', которыми в их представлении (51) имеют коэффициенты α_i'', β_j'', γ_{st}'', является точной верхней гранью элементов f и f'. Таким образом $\mathfrak{D}$ — структура. Очевидно самый большой элемент в $\mathfrak{D}$ является $h^*=u^{2^n-1}v^3w_1^{2^{\delta_1}-1}\ldots w_r^{2^{\delta_r}-1}$, а самый меньший — $\bar{1}=u^0v^0w_1^0\ldots w_r^0$. Структура $\mathfrak{D}$ дистрибутивна, так как выполнен дистрибутивный закон $(d\vee d')\wedge d''=(d\wedge d'')\vee(d'\wedge d'')$ для любых $d,d',d''\in\mathfrak{D}$. Действительно, если показатели записаны в двоичной системе в вышеуказанном виде, то проверка указанного равенства сводится до проверки равенства $\min(\max(\alpha_i,\alpha_i'),\alpha_i'')=\max(\min(\alpha_i,\alpha_i''),\min(\alpha_i,\alpha_i''))$ и аналогично до проверки еще двух серий равенств относительно β_j, γ_{st}. Если $d=u^\alpha v^\beta w_1^{\gamma_1}\ldots w^\gamma_r$ — любой элемент $\mathfrak{D}$, то непосредственно видно, что его дополнение — $f^* = u^{\alpha^*}v^{\beta^*}w_1^{\gamma_1^*} \ldots w_r^{\gamma_r^*}$, где α^*, β^*, γ_i^* получаются из соответствующих записей (51) элементов α, β, γ_i через замену их коэффициентов α_i, β_i, γ_{st} с их „противоположными", т. е. $0 \to 1$ и $1 \to 0$. Следовательно, $\mathcal{D}$ — булева алгебра.

(52) Лемма. *Если G—группа, заданная формулами* (19), $d \in \{u, v, w_1, \ldots, w_r\}$, α — *целое число интервала* $[0, 2^n-1]$, *то в RG имеет место*

$$(1+d)^\alpha = 1 + \sum_{f \in (\overline{1},\, d^\alpha]} f.$$

Доказательство. Если α представим в виде (51) и $A = \{i/\alpha_i = 1\}$, то

$$(1+d)^\alpha = \prod_{i=0}^{n-1}(1+d^{2^i})^{\alpha_i} = \prod_{i \in A}(1+d^{2^i}) = 1 + \sum_{i \in A} d^{2^i} + \sum_{i,j \in A} d^{2^i+2^j} + \cdots = 1 + \sum_{f \in (\overline{1},\, d^\alpha]} f.$$

Последнее равенство доказывается следующим образом. Очевидно каждое слагаемое левой части этого равенства содержится в правой. Наоборот, пусть $d^{\alpha'} \in (\overline{1}, d^\alpha]$ и $\alpha' = \alpha_0' + \alpha_1' . 2 + \cdots + \alpha_{n-1}' 2^{n-1}$ $(\alpha_i' = 0, 1)$ — представление α' в двоичной системе. Так как $d^{\alpha'} \leqq d^\alpha$, то $\alpha_i' \leqq \alpha_i$. Кроме того, очевидно, $d^{\alpha'} = d^{\alpha_0'}(d^2)^{\alpha_1'} \ldots (d^{2^i})^{\alpha_i'} \ldots (d^{2^{n-1}})^{\alpha_{n-1}'}$. Так как из $\alpha_i' = 1$ следует $\alpha_i = 1$ и $i \in A$, то получается, что $d^{\alpha'}$ принадлежит к указанной левой части. Лемма доказана.

(53) Лемма. *Если G — группа, заданная формулами* (19) *и* λ — *взаимно однозначное отображение* $\mathcal{D}$ *на G, определенное через* $(u^\alpha v^\beta w_1^{\gamma_1} \ldots w_r^{\gamma_r})\lambda = a^\alpha b^\beta a_1^{\gamma_1} \ldots a_r^{\gamma_r}$, *то G — булева алгебра, и для каждого d из* $\mathcal{D}$ *имеет место*

(54) $$x_d = \sum_{g \in [d\lambda,\, h]} x_g,$$

где $h = a^{2^n-1} b^3 a_1^{2^{\delta_1}-1} \ldots a_r^{2^{\delta_r}-1}$.

Доказательство. Очевидно G — булева алгебра и h — самый большой ее элемент. Тогда для любого $g \in G$ имет место

$$g = a^\alpha b^\beta a_1^{\gamma_1} \ldots a_r^{\gamma_r} = (1+u)^\alpha (1+v)^\beta (1+w_1)^{\gamma_1} \ldots (1+w_r)^{\gamma_r}$$

$$= (1 + \sum_{f \in (\overline{1},\, u^\alpha]} f)(1 + \sum_{f \in (\overline{1},\, v^\beta]} f)(1 + \sum_{f \in (\overline{1},\, w_1^{\gamma_1}]} f) \ldots (1 + \sum_{f \in (\overline{1},\, w_r^{\gamma_r}]} f)$$

$$= \prod_{l \in M} \sum_{f \in [\overline{1},\, l]} f = \sum_{f \in [\overline{1},\, \xi]} f = \sum_{f \in [\overline{1},\, g\lambda^{-1}]} f,$$

где для получения третьего равенства использована лемма (52), $\xi = u^\alpha v^\beta w_1^{\gamma_1} \ldots w_r^{\gamma_r}$ и $M = \{u^\alpha, v^\beta, w_1^{\gamma_1}, \ldots, w_r^{\gamma_r}\}$. Так как $\overline{1} \leqq f \leqq g\lambda^{-1}$, то $f\lambda \leqq g \leqq h_1$. Из $x = \Sigma_{g \in G} x_g g$ и из последнего равенства полученной серии равенств получится

$$x = \sum_{f \in \mathcal{D}} \Big(\sum_{g \in [f\lambda,\, h]} x_g \Big) f,$$

откуда вытекает (54).

Из теории булевых алгебр легко можно получить следующее

(55) Замечание. Пусть $t \leqq g \leqq h$ в булевой алгебре $\mathcal{D}$. Тогда $t = g \wedge h_1$ и

$h_1 \leq h$ тогда и только тогда, когда $g \in [t, h_1']$, где h_1' — дополнение элемента h_1 в интервале $[t, h]$.

(56) Лемма. *Если G — группа, заданная формулами* (19), *G удовлетворяет условие* (*), *кольцо R без нильпотентных элементов и $x^2=0$, где $x \in RG$, то для любого t из G имеет место*

$$z_t = \sum_{g \in Z[2]} x_{tg} = 0. \tag{57}$$

Доказательство. Пусть

$$\mathscr{D} = \{u^\alpha v^\beta w_1^{\gamma_1} \ldots w_r^{\gamma_r} / \alpha = 0, 1, \ldots, 2^{n-1}-1\,;\ \beta = 0, 1\,;$$
$$\gamma_i = 0, 1, \ldots, 2^{\delta_i - 1} - 1 \quad (i = 1, \ldots, r)\}$$

и $h_1 = a^{2n-1-1} b a_1^{2^{\delta_1 - 1}-1} \ldots a_r^{2^{\delta_r - 1}-1}$. Очевидно, $h_1\lambda^{-1} = u^{2^{n-1}-1} v w_1^{2^{\delta_1-1}-1} \ldots w_r^{2^{\delta_r-1}-1}$ (см. (53)) — самый большой элемент в $\mathscr{D}_1$. Достаточно доказать лемму для каждого $t \in [1, h_1]$. Действительно, не трудно увидеть, что если $t^1 \notin [1, h_1]$, то имея в виду представление $t' = u^\alpha v^\beta w_1^{\gamma_1} \ldots w_r^{\gamma_r}$ и, разделив α, β, γ_i соответственно на 2^{n-1}, 4, $2^{\delta_i - 1}$, то получается $t' = td$, где $t \in [1, h_1]$ и $d \in Z[2]$, откуда следует, что $z_{t'} = z_t$. Согласно (39) и (54), получим

$$0 = \sum_{f \in [t\lambda^{-1}, h_1\lambda^{-1}]} x_f = \sum_{f \in [t\lambda^{-1}, h_1\lambda^{-1}]} \ \sum_{g \in [f\lambda, h]} x_g$$
$$= \sum_{g \in [t,h]} \ \sum_{f \in [t\lambda^{-1}, \eta]} x_g = \sum_{g \in [t,h]} |[t, g \wedge h_1]| x_g,$$

где $\eta = g\lambda^{-1} \wedge h_1\lambda^{-1}$ и для последнего равенства мы использовали, что $|[x\lambda^{-1}, y\lambda^{-1}]| = |[x, y]|$. Имея в виду, что любой интервал в булевой алгебре содержит 2^t элемента, то ненулевые слагаемые в правой части последнего равенства являются только тривиальными интервалами $[t, g_1 h_1]$, т. е. для которых $t = g \wedge h_1$. Из (55) следует, что $g \in [t, h_1']$, где h_1' — дополнение элемента h_1 в интервале $[t, h]$, т. е.

$$0 = \sum_{g \in [t,\, h]} |[t, g \wedge h_1]| x_g = \sum_{g \in [t, h_1']} x_g. \tag{58}$$

Докажем, что

$$[t, h_1'] = tZ[2]. \tag{59}$$

Тогда из (58) и (59) будет следовать (57). Для доказательства (59) обозначим $t = a^\alpha b^\beta a_1^{\gamma_1} \ldots a_r^{\gamma_r}$. Так как $t \leq h_1$ то для $\alpha, \beta, \gamma_i (i = 1, \ldots, r)$ имеют место формулы (51) с $\alpha_{n-1} = 0$, $\beta_1 = 0$ и $\gamma_{i, \delta_i - 1} = 0$. Нетрудно проверить, что $h_1' = ta^{2^{n-1}} b^2 a_1^{2^{\delta_1 - 1}} \ldots a_r^{2^{\delta_r - 1}}$, т. е. $h_1' = a^{\alpha + 2^{n-1}} b^{\beta+2} a_1^{\gamma_1 + 2^{\delta_1 - 1}} \ldots a_r^{\gamma_r + 2^{\delta_r - 1}}$. Пусть $s \in [t, h_1']$, $s = a^{\alpha'} b^{\beta'} a_1^{\gamma_1'} \ldots a_r^{\gamma_r'}$ и в представлении (51) $\alpha', \beta', \gamma_i' (i = 1, \ldots, r)$ имеют коэффициенты $\alpha_i', \beta_j', \gamma_{ir}'$. Тогда из $t \leq s \leq h_1'$ получится $\alpha_0' = \alpha_0, \ldots, \alpha_{n-2}' = \alpha_{n-2}$ и $\alpha_{n-1}' = 0$ или $\alpha_{n-1}' = 1$; $\beta_0' = \beta_0$ и $\beta_1' = 0$ или $\beta_1' = 1$; $\gamma_{i0}' = \gamma_{i0}, \ldots, \gamma_{i, \delta_i - 2}' = \gamma_{i, \delta_i - 2}$ и $\gamma_{i, \delta_i - 1}' = 0$ или $\gamma_{i, \delta_{i-1}}' = 1$. Тогда

(60) $$s=a^{\alpha+\alpha'_{n-1}\cdot 2^{n-1}}b^{\beta+\beta'_1\cdot 2}a_1^{\gamma_1+\gamma'_{1,\delta_1-1}\cdot 2^{\delta_1-1}}\dots a_r^{\gamma_r+\gamma'_{r,\delta_r-1}\cdot 2^{\delta_r-1}}\in tZ[2].$$

Обратно, взяв представления (51) показателей α, β, γ_i, обратным путем видно, что любой элемент множества $tZ[2]$, а именно элемент (60), принадлежит интервалу $[t, h'_1]$. Лемма доказана.

Если группы G и G_1 определены формулами (19) и (20), то в следующих утверждениях используем отображение $\varphi^*: RG\to RG_1$, определенное следующим образом: если $x\in RG$, то

(61) $$(x\varphi^*)_{g_1}=x_{g_1\varphi}$$

для каждого $g_1\in G_1$, где φ — отображение, определенное леммой (26).

(62) Лемма. *Отображение φ^* взаимно однозначно отображает алгебру RG на RG_1.*

Доказательство. Пусть $y=\Sigma_{g_1\in G_1} y_{g_1}g_1$ — любой элемент RG_1. Тогда для $x=\Sigma_{g_1\in G_1} y_{g_1}g_1\varphi$ имеет место $x\varphi^*=y$, так как ввиду (61), $(x\varphi^*)_{g_1}=x_{g_1\varphi}=v_{g_1}$, т. е. каждый элемент алгебры RG_1 имеет прообраз. Пусть $x\neq x'$ и $x, x'\in RG$. Следовательно, по крайней мере для одного $g\in G$ имеет место $x_g\neq x'_g$. Тогда $x\varphi^*\neq x'\varphi^*$, так как $(x\varphi^*)_{g\varphi^{-1}}=x_{(g\varphi^{-1})\varphi}=x_g$ и $(x'\varphi^*)_{g\varphi^{-1}}=x'_{(g\varphi^{-1})\varphi}=x'_g$.

(63) Лемма. *Если группа G определена формулами* (19), *G удовлетворяет условие* (*), *кольцо R без нильпотентных элементов, $x\in RG$ и $x^2=1$, то $(x\varphi^*)^2=1$, т. е. инволюция алгебры RG отображается в инволюции.*

Доказательство. Обозначим $x\varphi^*=y$. Мы должны доказать, что для каждого $g_1\in G_1$ имеет место

(64) $$(y^2)_{g_1}=\begin{cases}1, & \text{если } g_1=1,\\ 0, & \text{если } g_1=0.\end{cases}$$

Рассмотрим следующие случаи:

1) $g_1\notin V_1$. Без ограничения общности можем считать, что $g_1\in uZ_1$. Имея в виду, что $\sqrt{g_1}=\emptyset$, то из (15) и (61) следует

$$(y^2)_{g_1}=\sum_{t\in G_1\setminus C(g_1)} y_t y_{t^{-1}g_1}=\sum_{t\in(vZ_1\cup uvZ_1)} x_{t\varphi}x_{(t^{-1}g_1)\varphi}=\sum_{t\in vZ_1} x_{t\varphi}x_{(t\varphi)^{-1}g_1\varphi}$$

$$+\sum_{t\in uvZ_1} x_{t\varphi}x_{(t\varphi)^{-1}g_1\varphi}=\sum_{s\in aZ} x_s x_{s^{-1}g}+\sum_{s\in abZ} x_s x_{s^{-1}g}=\sum_{s\in G\setminus C(g)} x_s x_{s^{-1}g}=(x^2)_g=0,$$

где для получения третьего равенства использовано (30) и (31) и, кроме того, положено $g_1\varphi=g\in bZ$, учитывая, что $g\neq 1$ и $\sqrt{g}=\emptyset$.

2) Пусть $g_1\in vZ_1$. Аналогичным образом, полагая $g_1\varphi=g$, получим

$$(y^2)_{g_1}=\sum_{t\in uZ_1} x_{t\varphi}x_{(t\varphi)^{-1}gb^2}+\sum_{t\in uvZ_1} x_{t\varphi}x_{(t\varphi)^{-1}gb^2}$$

$$=\sum_{s\in(bZ\cup abZ)} x_s x_{s^{-1}gb^2}=\sum_{s\in G\setminus C(gb^2)} x_s x_{s^{-1}gb^2}=(x^2)_{gb^2}=0.$$

3) Пусть $g_1\in Z_1\setminus G_1^2$. Тогда (15) очевидно дает $(y^2)_{g_1}=0$.

4) Пусть $g_1\in G_1^2$. Если $t_1\in G_1$ или $t_1^2=g_1$, то

$$(65) \qquad (y^2)_{g_1} = \sum_{s \in \sqrt{g_1}} y_s^2.$$

Рассмотрим следующие подслучаи.

4.1) Пусть $t_1 \in G_1 \setminus U_1$. Можем предполагать, что $t_1 \in vZ_1$, т. е. $t = vz_1$, $z_1 \in Z_1$ (случай $t \in uvZ_1$ аналогичен). Так как $\sqrt{g_1} = \tau(t_1)$, то из (65), применяя лемму (22), (28) и (30), получится

$$(y^2)_{g_1} = \sum_{s \in vz_1Z_1[2]} y_s^2 = \sum_{s \in vz_1Z_1[2]} x_{s\varphi}^2 = \sum_{t \in adZ[2]} ((x+1)_t)^2 = z_{ad}^2 = 0,$$

где $d = z_1\varphi$ и использовано, ввиду леммы (56), $z_{ad} = 0$.

4.2) Пусть $t \in U_1$. Если $t_1 \in uZ_1$, то $t_1 = uz_1$, $z_1 \in Z_1$, и $g_1 = z_1^2$. Следовательно, можем предполагать, что $t_1 \in Z_1$. Пусть

4.2.1) $t_1 \in Z_1 \setminus Z_1[2]$. Тогда $1 \neq t_1^2 = g_1$. Из (65), применяя леммы (22) и 56) и полагая $d = t_1\varphi$, получится

$$(y^2)_{g_1} = \sum_{t \in t_1U_1[2]} (x_{s\varphi})^2 = \sum_{t \in dZ[2]} ((x+1)_t)^2 + \sum_{t \in bdZ[2]} ((x+1)_t)^2 = 0 + 0 = 0.$$

4.2.2) Пусть $t_1 \in Z_1[2]$. Тогда $g_1 = t_1^2 = 1$. Из (65), используя леммы (22), (24) и (56), получится

$$(y^2)_1 = \sum_{s \in t_1, U_1[2]} y_s^2 = \sum_{t \in Z[2]} x_t^2 + \sum_{t \in bZ[2]} ((x+1)_t)^2 = 1.$$

(66) Лемма. *Если группы G и G_1 определены соотношениями* (19) *и* (20), *G и G_1 удовлетворяют условие* (*) *и кольцо R без нильпотентных элементов, то имеет место* $|(RG)[2]| < |(RG_1)[2]|$.

Доказательство. Так как, ввиду леммы (62), отображение $\varphi^* : RG \to RG_1$ взаимно однозначно и, ввиду леммы (63), инволюция отображается через φ^* в инволюции, то $|(RG)[2]| \leq |(RG_1)[2]|$. Докажем, что это неравенство строго. Очевидно u — инволюция алгебры RG. Ввиду (29), $(b\varphi^*)_{g_1} = b_{g_1\varphi} = 1$, если $g_1\varphi = b$, т. е. если $g_1 = u$, и, кроме того, $(b\varphi^*)_{g_1} = b_{g_1\varphi} = 0$, если $g_1\varphi \neq b$, т. е. если $g_1 \neq u$. Следовательно, $b\varphi^* = u$, т. е. прообраз u является b. Однако b не является инволюцией в RG. Лемма доказана.

(67) Предложение. *Если $G \in \mathscr{K}$, $G_1 \in \mathscr{K}$, G и G_1 удовлетворяют условие* (*), $G' = \langle k \rangle$, $G_1' = \langle k_1 \rangle$, *кольцо R без нильпотентных элементов и $RG \cong RG_1$, то $h_G(k) = h_{G_1}(k_1)$.*

Доказательство. Пусть $h_G(k) = i$. Сначала докажем утверждение, когда $i \geq 2$. В G существует элемент g, такой, что $k = g^{2^i}$. Пусть φ — изоморфизм алгебры RG на RG_1. Так как k принадлежит коммутанту $S'(RG)$ группы $S(RG)$, то $k\varphi \in S'(RG_1)$ или, ввиду леммы (6), $k\varphi \in 1 + \mathscr{K}(RG_1)$. С другой стороны,

$$k\varphi = (g\varphi)^{2^i} = \Big(\sum_{h \in G_1} \alpha_h h\Big)^{2^i} = \sum_{h \in G_1} \alpha_h^{2^i} h^{2^i},$$

где последнее равенство следует из леммы (7), т. е. $k\varphi \in S(RG_1^{2^i}) \cap (1 + \mathscr{K}(RG_1)) \neq \emptyset$. Тогда $k\varphi = 1 + w$, где $w \in \mathscr{K}(RG_1)$ и $w \neq 0$, так как $k\varphi \neq 1$. Аналогично рассуждениям в лемме (13) заключаем, что если $w = \Sigma x_g g$, где g пробегает $G_1^{2^i}$, то $x_g = x_{gk_1}$. Следовательно, $gk_1 \in G_1^{2^i}$ или $k_1 \in G_1^{2^i}$, т. е. $h_{G_1}(k_1) \geq h_G(k)$. Обратное неравенство доказывается аналогично. Таким образом, если $h_G(k)\geqq 2$, то $h_G(k)=h_{G_1}(k_1)$.

Пусть $h_G(k)=1$. Из уже рассмотренного случая следует, что $h_{G_1}(k_1)=1$ или $h_{G_1}(k_1)=0$.

Допустим, что $h_{G_1}(k_1)=0$. Тогда очевидно $G_1\in\mathscr{K}_1$. Если допустим, что $G\in\mathscr{K}_1$ и G_1 имеет определяющие соотношения типа 1), то из $k=c^{2^{s-1}}$ получается $s=2$, т. е. $k=c^2$, и, ввиду леммы (13), следует, что $1\leqq h_Z(k)\leqq h_{Z_1}(k_1)\leqq h_{G_1}(k_1)$, а это невозможно. Следовательно, $G\in\mathscr{K}_2$ или $G\in\mathscr{K}_3$. Пусть в разложении $G=H\times C$ имеет место $C=\langle a_1\rangle\times\cdots\times\langle a_r\rangle$, $O(a_i)=2^{\delta_i}$, $i=1,\ldots,r$ (H определяется соотношениями 2) или 3)).

Пусть $G\in\mathscr{K}_3$(а $G_1\in\mathscr{K}_1$). Тогда для G и G_1 имеют место, соответственно, определяющие соотношения 3) и 1), причем будем предполагать, что если $G=H_1\times C_1$, то число прямых множителей в разложении группы C_1 в прямом произведении циклических групп равняется r_1 (и r в разложении группы C). Обозначим $Z(G_1)=Z_1$. Тогда ввиду предложения (2) вытекает $R(G/G')\cong R(G_1/G_1')$. В силу предложения 5 следует $RZ\cong RZ_1$ и, ввиду [1], получится что $G/G'\cong G_1/G_1'$ и $Z\cong T_1$. Так как G/G^1 содержит $r+2$ циклических множителя в своем разложении в прямое произведение циклических групп, а $G_1/G_1'-r_1+2$ циклических множителя, то из $G/G'\cong G_1/G_1^*$ следует, что $r_1=r$. Однако нетрудно видеть что Z содержит $r+1$ циклических множителя в своем разложении в прямое произведение циклических групп, а Z_1 (при $r_1=r$) — $r+2$ (при $n_1=1$) или $r+3$ (при $n_1\geqq 2$) циклические множители, что невозможно.

Пусть $G\in\mathscr{K}_2$ (а $G_1\in\mathscr{K}_1$). Тогда в определяющих соотношениях 2) группы G имеем $m=2$, т. е. для G имеют место определяющие соотношения (19). Пусть $G_1=H_1\times C_1$, где $C_1=\langle x_1\rangle\times\cdots\times\langle x_{r_1}\rangle$, $O(x_i)=2^{\varepsilon_i}$, а $H_1=\langle a_1\rangle\circ(\langle b_1\rangle\times\langle c_1\rangle)$ с определяющими соотношениями

$$a_1^{2^{n_1}}=b_1^{2^{m_1}}=c_1^{2^{s_1}}=1,\ a_1^{-1}b_1a_1=b_1c_1^{2^{s_1-1}},\ a_1c_1=c_1a_1,\ b_1c_1=c_1b_1,\ n_1+m_1+s_1\geqq 4,$$

где $n_1, m_1, s_1\geqq 1$. Можем предполагать, что

$$n_1\leqq m_1. \tag{68}$$

Так как $h_{G_1}(k_1)=0$, то $s_1=1$. Легко видеть, что циклические множители групп G/G' и G_1/G_1' в их разложении в прямое произведение циклических групп имеют соответственно порядки

$$2^n,\ 2,\ 2^{\delta_1},\ldots,2^{\delta_r} \tag{69}$$

и

$$2^{n_1},\ 2^{m_1},\ 2^{\varepsilon_1},\ldots,2^{\varepsilon_{r_1}}. \tag{70}$$

Следовательно, $r_1=r$. Циклические множители в разложение Z и Z_1 в прямые произведения циклических групп имеют соответственно порядки

$$2^{n-1},\ 2,\ 2^{\delta_1},\ldots,2^{\delta_r} \tag{71}$$

и

$$2^{n_1-1},\ 2^{m_1-1},\ 2,\ 2^{\varepsilon_1},\ldots,2^{\varepsilon_r}. \tag{72}$$

Кроме того, $n \neq 1$, так как, если $n=1$, то следует $n_1=1$ и $m_1=1$, что противоречит условию $n_1+m_1+s_1 \geq 4$. Так как $n_1 \leq m_1$, то из $Z \cong Z_1$ и $n \neq 1$ следует, учитывая (67), (71) и (72), что $n_1=1$, $m_1>1$ и или 1) $n-1=\varepsilon_1$, или 2) $n-1=m_1-1$, т. е. $m_1=n$. Докажем, что случай 1) ведет к случаю 2). Именно, из $n-1=\varepsilon_1$ и из (71) и (72) следует, что $m_1-1=\delta_1$ (с эвентуальной перенумерации элементов a_i) и $\delta_2=\varepsilon_2, \ldots, \delta_r=\varepsilon_r$. Тогда из (69) и (70), ввиду $n-1=\varepsilon_1$, следует $n=m_1$. Таким образом G_1 определяется соотношениями (20). Тогда, согласно лемме (66), имеет место $|(RG)[2]|<|(RG_1)[2]|$, что противоречит изоморфизму $RG \cong RG_1$. Этим доказано, что $h_{G_1}(k_1)=1$.

Из вышерассмотренных двух случаев следует, что если $h_G(k)=0$, то и $h_{G_1}(k_1)=0$. Предложение доказано.

(73) Теорема. *Если G — конечная 2-группа, Z — ее центр с нижним слоем $Z[2]$, $|G/Z|=4$ и фактор-группа $Z/Z[2]$ циклична или элементарная абелева, R — конечное коммутативное кольцо с единицей, характеристики 2 без нильпотентных элементов и G_1 — произвольная группа, то из изоморфизма R-алгебр RG и RG_1 следует $G \cong G_1$.*

Доказательство. Так как $|G|=|G_1|$, то G_1 — конечная 2-группа. Ввиду предложения (2) имеет место $R(G/G') \cong R(G_1/G_1')$ и, по [1], что $G/G' \cong G_1/G_1'$. Тогда из $|G|=|G_1|$ следует $|G_1'|=2$, т. е. G_1 имеет коммутант порядка 2. Из предложения (5) и [1] видно, что $Z \cong Z_1$, где Z_1 — центр группы G_1. Следовательно, $|G_1/Z_1|=4$ и $Z_1/Z_1[2] \cong Z/Z[2]$, т. е. $Z_1/Z_1[2]$ — цикличная или элементарная абелева группа. Таким образом $G_1 \in \mathcal{K}$ и G_1 удовлетворяет условие (*). Ввиду предложения (67), леммы (13) и следствия (12) имеет место

$$(74) \qquad h_G(k)=h_{G_1}(k_1),\ h_Z(k)=h_{Z_1}(k_1),\ |G[2^i]|=|G_1[2^i]|,\ i \geq 2,$$

где $G'=\langle k\rangle$ и $G_1'=\langle k_1\rangle$. Из (74) следует, что если $G \in \mathcal{K}_1$, то и $G_1 \in \mathcal{K}_1$. Пусть $G \in \mathcal{K}_3$. Докажем, что $G_1 \in \mathcal{K}_3$. Если $G_1 \in \mathcal{K}_2$, то $G_1=H_1 \times C_1$, где H_1 — группа диедра порядка 8, т. е. $H_1=\langle u, v\rangle$, $u^2=v^4=1$, $u^{-1}vu=v^3$. Тогда $h_{G_1}(k_1)=1$ и, имея ввиду (74), следует $h_G(k)=1$. Это возможно только тогда, когда в $G=H \times C$ подгруппа H является группой кватернионов порядка 8, т. е. $H=\langle a, b\rangle$, $a^2=b^2$, $a^4=1$, $b^{-1}ab=a^3$. Так как $G/G' \cong G_1/G_1'$, то $|C[2]|=|C_1[2]|$ и из последней формулы (74) получается, что $C \cong C_1$. Существует изоморфизм φ центра Z_1 на центр Z, для которого $v^2\varphi=a^2$, который продолжается мультипликативно до изоморфизма группы $V_1=\langle v, Z_1\rangle$ на группу $A=\langle a, Z\rangle$ посредством сопоставления $v\varphi=a$ и до взаимно однозначного отображения группы G_1 на G посредством сопоставления (29). Для групп G и G_1 и отображения φ аналогично доказываются леммы (26), (35), (38), (50), (52), (53) и (56), определяется отображение φ^* посредством сопоставления (61) и доказываются леммы (62), (63) и (66). Однако лемма (66) противоречит изоморфизму $RG \cong RG_1$. Следовательно, $G \in \mathcal{K}_3$. Таким образом G и G_1 принадлежат одному и тому же подклассу $\mathcal{K}_i$ класса $\mathcal{K}$.

Докажем, что

$$(75) \qquad |G[2]|=|G_1[2]|.$$

Пусть $G_1=H_1 \times C_1$ $(G=H \times C)$, (2^t) — циклическая группа порядка 2^t, $C \cong (2^{\delta_1}) \times \cdots \times (2^{\delta_r})$ и $C_1 \cong (2^{\varepsilon_1}) \times \cdots \times (2^{\varepsilon_{r_1}})$. Рассмотрим следующие случаи.

Пусть $G \in \mathcal{K}_1$ и $G_1 \in \mathcal{K}_1$. Предположим, что G_1 определяется соотношениями типа 1), в которых показатели элементов индексированы элементом 1. Так как $s-1=h_G(k)=h_{G_1}(k_1)=s_1-1$, то $s_1=s$. Тогда

$$G/G'\cong(2^n)\times(2^m)\times(2^{s-1})\times(2^{\delta_1})\times\cdots\times(2^{\delta_r}),$$

$$G_1/G_1'\cong(2^{n_1})\times(2^{m_1})\times(2^{s-1})\times(2^{\varepsilon_1})\times\cdots\times(2^{\varepsilon_r}),$$

и из $G/G'\cong G_1/_1'$ вытекает $r_1=r$. Следовательно, $|G[2]|=|G_1[2]|$.

Пусть $G\in\mathscr{K}_2$ и $G_1\in\mathscr{K}_2$. Так как $G/G'\cong(2^n)\times(2^{m-1})\times(2^{\delta_1})\times\cdots\times(2^{\delta_r})$, $G_1/G_1'\cong(2^{n_1})\times(2^{m_1-1})\times(2^{\varepsilon_1})\times\cdots\times(2^{\varepsilon_{r_1}})$, $G/G'\cong G_1/G_1'$, $m\geqq2$ и $m_1\geqq2$, то $|G[2]|=|G_1[2]|$.

Пусть $G\in\mathscr{K}_3$ и $G_1\in\mathscr{K}_3$. Очевидно $G[2]=Z[2]$ и $G_1[2]=Z_1[2]$. Так как $Z\cong Z_1$, то $|G[2]|=|G_1[2]|$. Этим (75) доказана.

Так как имеют место (74) и (75), то из [2] следует, что $G\cong G_1$.

ЛИТЕРАТУРА

1. С. Д. Берман, Т. Ж. Моллов. О групповых кольцах абелевых p-групп любой мощности. *Мат. заметки*, **6**, 1969, № 4, 381—392.
2. Н. А. Начев, Крайни 2-групи с фактор-група по центъра от ред четири. *Научни трудове на ПУ „П. Хилендарски“*, **19**, 1981, 27—48.
3. Н. А. Начев, Т. Ж. Моллов. Об изоморфизме модулярных групповых алгебр конечных 2-групп с коммутантами порядка 2, фактор-группы по которому имеют порядок четыре. *Доклады БАН*, **34**, 1981, 1633—1636.
4. B. S. Passi, S. K. Sehgal. Isomorfism of modular group algebras. *Math. Zeitschr*, **129**, 1972, № 1, 65—73.
5. D. S. Passman. The group algebras of groups of order p^4 over a modular field. *Mich. Math. J.*, **12**, 1965, 405—415.
6. S. K. Sehgal. On the isomorfism of group algebras. *Math. Zeitschr.*, **95**, 1967, 71—75.
7. А. Е. Залесский, А. В. Михалев. Групповые кольца. *Итоги науки и техники, Современные проблемы математики*, **2**, 1973, 5—118.

Пловдивский университет
Пловдив 4000 Болгария

Поступила 7. 7. 1981

ИНВАРИАНТЫ УЛЬМА-КАПЛАНСКОГО ГРУППЫ НОРМИРОВАННЫХ ЕДИНИЦ ГРУППОВЫХ АЛГЕБР АБЕЛЕВЫХ p-ГРУПП НАД КОММУТАТИВНЫМ КОЛЬЦОМ, В КОТОРОМ p ОБРАТИМЫЙ ЭЛЕМЕНТ

НАКО А. НАЧЕВ

Пусть G — абелева p-группа, L — коммутативное кольцо с единицей, в котором простое число p обратимо, q — любое простое число (не требуется $p \neq q$) и $S_q(LG)=S_q$ — силовская q-подгруппа группы нормированных единиц группового кольца LG. Для любого натурального числа n обозначим через $Z(\xi_n)$ фактор-кольцо кольца многочленов $Z[x]$ по циклотомичному многочлену $\Phi_{p^n}(x)=x^{p^{n-1}(p-1)}+\ldots+x^{p^{n-1}}+1$. Иными словами, кольцо $Z(\xi_n)$ получается из кольца целых чисел, присоединяя элемент ξ_n, для которого $\Phi_{p^n}(\varepsilon_n)=0$. Естественным образом получается кольцевой гомоморфизм $Z(\xi_n)\to Z(\xi_{n+1})$, если подобрать ξ_{n+1} так, что $\xi^p_{n+1}=\xi_n$ $(n=1, 2, \ldots)$. Таким образом, возникает возрастающая цепочка

$$Z\to Z(\xi_1)\to Z(\xi_2)\to\ldots\to Z(\xi_n)\to\ldots,$$

объединение которой обозначим через $\overline{Z}$.

Предположим, что, если G имеет показатель p^n (бесконечный показатель), то существует кольцевой гомоморфизм $Z(\xi_n)\to L(\overline{Z}\to L)$. В такой ситуации мы будем исследовать группу $S_q(LG)$. Основной результат этой работы выглядит так.

Пусть $f_\alpha(G)$ — α-й инвариант Ульма — Капланского группы G [5, с. 182], где α — любое порядковое число, L_q — силовская q-подгруппа мультипликативной группы кольца L, S^*_q — максимальная делимая подгруппа группы S_q, и максимальная делимая подгруппа L^*_q группы L_q разлагается в прямое произведение квазициклических групп $Z(q^\infty)$ типа q^∞, мощность множества которого равняется ν, т. е.

$$L^*_q\cong\prod_\nu Z(q^\infty).$$

Тогда, если $|G|$ — мощность группы G, то

$$f_\alpha(S_q)=(|G|-1)f_\alpha(L_q)$$

и

$$S^*_q\cong\prod_{(|G|-1)\nu}Z(q^\infty).$$

Пусть LG — групповое кольцо абелевой p-группы G над коммутативным кольцом L с единицей, в котором простое число p обратимо, и $S_q(LG)$ — силовская q-подгруппа группы нормированных единиц кольца LG (q — простое число). Описание группы $S_p(LG)$, когда L и G счетны, дано в [1]. В настоящей работе вычисляются инварианты Ульма—Капланского группы $S_q(LG)$, когда L и G имеют любые мощности при условии, что существует кольцевой гомоморфизм $Z(\xi_n)\to L$ (соответственно, $\overline{Z}\to L$), где p^n— показатель группы G (соответственно, бесконечный показатель).

ПЛИСКА Български математически студии. Том 8, 1986, с. 21—33.