Федеральное государственное автономное образовательное учреждение
высшего профессионального образования

КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И МЕХАНИКИ
КАФЕДРА АЛГЕБРЫ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ

Напраление: 010100.62- Математика

Специализация: Математическая логика

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(бакалаврская работа)

КЛАССИЧЕСКИ ПОЛУПРОСТЫЕ ГРУППОВЫЕ АЛГЕБРЫ

Работа завершена:

"____"_____2014 г. _____Карпов Е.В.

Работа проверена:

Научный руководитель
кандидат физико-математических наук,
доцент кафедры алгебры и математической логики
"____"_____2014 г. _____Абызов А.Н.

Заведующий кафедрой алгебры и математической логики,
доктор физико-математичских наук, профессор
"____"_____2014 г. _____Арсланов М.М.

Казань - 2014 г.

Содержание.

Введение.....2

Глава 1. Предварительные сведения.

§1. Группы диэдра и группа кватернионов Q_8.....3

§2. Групповые алгебры.....5

§3. Центр групповой алгебры.....5

§4. Теорема Машке.....7

§5. Идемпотенты и разложение алгебр.....8

Глава 2. Групповые алгебры циклических групп.

§1. Комплексные групповые алгебры циклических групп.....9

§2. Рациональные групповые алгебры.....9

§3 Конечные групповые алгебры циклических групп.....12

Глава 3.Абелевы групповые алгебры.

§1 Циклотомиские классы и их свойства.....14

§2 Разложение Веддерберна конечных полупростых групповых алгебр вида $F_pC_q^n$ 18

Глава 4. Строение групповых алгебр групп диэдра.

§1. Комплексная групповая алгебра группы диэдра.....20

§2 Рациональные групповые алгебры группы диэдра.....23

§3. Конечные групповые алгебры группы диэдра.....26

§4 Групповые алгебры вида $F_pD_{q^n}$.....31

§5 Групповые алгебры вида F_qD_{2p}.....32

Список литературы.....44

Введение.

В последнее время интенсивно изучается строения конечных групповых алгебр над различными группами. Это объясняется тесной связью между теорией конечных групповых алгебр и теорией групповых кодов, поскольку многие хорошо известные групповые коды - это в точности идеалы в конечных групповых алгебрах.

В дипломной работе изучается строения классически полупростых алгебр FG, то есть таких конечномерных групповых алгебр, у которых характеристика поля F не делит порядок группы G. Поскольку классически полупростые алгебры обладают разложением Веддерберна, то есть являются конечным прямым произведением полных матричных алгебр над алгебрами с делением, то изучение строения полупростых групповых алгебр FG сводится к описанию всех примитивных центральных идемпотентов алгебр FG и описанию всех матричных компонент в разложении Веддерберна алгебр FG.

Дипломная работа состоит из 4 глав. В первой главе приводятся вспомогательные сведения из теории групп и полей, которые используются в основном тексте работы. Во второй главе изучается строение циклических групповых алгебр. Описывается строение классически полупростых групповых алгебр циклических групп над полем комплексных чисел, рациональных и над конечными полями. В третьей главе изучается разложение Веддерберна классически полупростых абелевых групповых алгебр.Четвёртая глава посвящена групповым алгебрам групп диэдра над теми же полями, что и в случае групповых алгебр циклических групп. В частности, приводится теорема о разложении Веддерберна конечных групповых алгебр группы диэдра, установленное в работе [7] в 2013 году. Эта же теорема недавно была передоказана в работе [6]. Также найдены все примитивные центральные идемпотенты и разложение Веддерберна групповых алгебр вида $F_pD_{q^n}$, $\quad F_qD_{2p}$, где p, q различные простые числа.

Глава 1. Предварительные сведения.

§1. Группы диэдра и группа квтернионов Q_8.

Определение 1.1.1. Группой диэдра D_n называется группы симметрии правильного n- угольника, включающая вращения и отражения и имеющая вид $D_n = \{e, a, a^2, \ldots, a^{n-1}, b, ba, ba^2, \ldots, ba^{n-1}\}$, где a- поворот на угол $\frac{2\pi}{n}$, $b-$ симметрия относительно одной из осей симметрии правильного $n-$угольника и

$$a^n = e, \quad b^2 = e, \quad bab = a^{-1}$$

Пример.

Рассмотрим группу диэдра для правильного треугольника $n = 3$, и составим для неё таблицу умножения: $D_3 = \{e, a, a^2, b, ba, ba^2\}$. Здесь a есть поворот на угол $120°$, a^2 поворот на $240°$, $a^3 = e$ поворот на $360°$. b- симметрия. Таблица умножения:

	e	a	a^2	b	ba	ba^2
e	e	a	a^2	b	ba	ba^2
a	a	a^2	e	ba^2	b	ba
a^2	a^2	e	a	ba	ba^2	b
b	b	ba	ba^2	e	a	a^2
ba	ba	ba^2	b	a^2	e	a
ba^2	ba^2	b	ba	a	a^2	e

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$. Элементы перемножаются по круговому правилу: $i \to j \to k \to i$ И тоже самое, но со знаком минус и в обратном направлении. Таблица умножения имеет вид:

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	j	$-j$
$-i$	$-i$	i	1	-1	$-k$	k	$-j$	j
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

§2. Групповые алгебры.

Определение 1.2.1. Пусть G - группа относительно операции умножения и K - произвольное ассоциативное кольцо. Групповое кольцо KG группы G над кольцом K состоит из всевозможных формальных сумм вида $\sum \alpha_g g$, в которых лишь конечное число коэффициентов $\alpha_g \in K$ отличных от нуля, причём такие суммы равны тогда и только тогда, когда у них совпадают коэффициенты $\alpha_g \in K$ для всех $g \in G$. Операции в KG определяются так: если

$$x = \textstyle\sum_{g\in G} \alpha_g g, y = \sum_{g\in G} \beta_g g$$

то

$$x + y = \sum_{g\in G} (\beta_g + \alpha_g) g, \quad xy = \sum_{g\in G} (\sum_{g_i\in G} \beta_{g_i}^{-1} \alpha_{g_i}) g.$$

Если кольцо K является полем, то KG называется *групповой алгеброй.*

§3. Центр групповой алгебры.

Определение 1.3.1. Пусть PG- групповая алгебра. Центром групповой алгебры называется множество $C(PG) = \{a \in PG | \forall x \in PG : ax = xa\}$

Пусть G- группа и $G_1, \ldots, G_n$- все его классы сопряжённых элементов. $G_k = \{g_1, \ldots, g_n\} \subset G$ один из этих классов, через $\hat{G}_k$ обозначим сумму всех элементов в этом классе, т.е. $\hat{G}_k = g_1 + \cdots + g_n \in G$.

Лемма 1.3.1.

1)$\hat{C}_1, \ldots, \hat{C}_n$ линейно независимы в PG.

2)$\hat{C}_1, \ldots, \hat{C}_n \in C(PG)$

Доказательство.

1) Пересечение классов сопряжённых элементов пусто. Следовательно, и суммы $\hat{C}_1, \ldots, \hat{C}_n$ будут линейно независимы.

2) Сопряжённый класс $C_i = \{h_1, \ldots, h_k\}, g \in G$,

$gC_ig^{-1} = \{gh_1g^{-1}, \ldots, gh_kg^{-1}\} = C_i$

$\hat{C}_i = h_1 + \cdots + h_k = gh_1g^{-1} + \cdots + gh_kg^{-1} = g\hat{C}_ig^{-1} \Rightarrow g\hat{C}_i = \hat{C}_ig \Rightarrow$

$\Rightarrow \hat{C}_i \in C(PG)$

Теорема 1.3.2 Пусть PG- групповая алгебра, тогда $C(PG) =< \hat{C}_1, \ldots, \hat{C}_n >$.

Доказательство. 1)$C(PG) \supset< \hat{C}_1, \ldots, \hat{C}_n >$ доказано.

2) Пусть $|G| = m$, $G = \{g_1, \ldots, g_m\}$, $\alpha_1g_1 + \cdots + \alpha_mg_m \in C(PG)$, и $g_i \sim g_j, g_i = gg_ig^{-1}$.

$\alpha_1g_1 + \cdots + \alpha_ig_i + \cdots + \alpha_jg_j + \cdots + \alpha_mg_m = g(\alpha_1g_1 + \cdots + \alpha_ig_i + \cdots + \alpha_jg_j + \cdots + \alpha_mg_m)g^{-1} =$

$\alpha_1gg_1g^{-1} + \cdots + \alpha_igg_ig^{-1} + \cdots + \alpha_jg_j + \cdots + \alpha_mgg_mg^{-1}$. Следовательно $\alpha_i = \alpha_j$

§4. Теорема Машке.

Теорема 1.4.1. (Теорема Машке) Пусть G-конечная группа и P-некоторое поле. Если $char P \nmid |G|$, то $GP \cong M_{n_1}(T_1) \times \ldots \times M_{n_k}(T_k)$, где $T_1, \ldots, T_k$ - алгебры с делением над P.

В частности, если G конечная коммутативная группа и $char P \nmid |G|$, то имеет место изоморфизм: $PG \cong T_1 \times \ldots \times T_k$, где $T_1, \ldots, T_k$ - коммутативные алгебры с делением над полем P.

Следствие 1: Пусть $\mathbb{C}G$ групповая алгебра. $|G| < \infty$. Тогда

$\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$.

Следствие 2: Пусть Z_pG групповая алгебра, $|G| < \infty$ $p \nmid |G|$. Тогда

$Z_pG \cong M_{n_1}(P_1) \times \cdots \times M_{n_k}(P_k)$, где $P_1, \ldots, P_k$- конечные поля характеристики p.

Следствие 3: Пусть RG групповая алгебра, $|G| < \infty$, тогда

$RG \cong M_{n_1}(T_1) \times \cdots \times M_{n_k}(T_k)$, где $T_1, \ldots, T_k \cong \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$.

Следствие 4: Пусть QG групповая алгебра, $|G| < \infty$. Тогда

$QG \cong T_1 \times \cdots \times T_k$, где $T_1, \ldots, T_k$- конечномерные алгебры с делением над Q.

Следствие 5: Пусть $\mathbb{C}G \cong M_{n_1}(\mathbb{C}) \times \cdots \times M_{n_k}(\mathbb{C})$, тогда

$dim(\mathbb{C}G) = n_1^2 + \cdots + n_k^2$.

Следствие 6: Пусть F_q - конечное поле, A - конечная абелева группа такая, что $(q, |A|) = 1$. Тогда в групповой алгебре FA существует семейство примитивных центральных ортогональных идемпотентов $\{e_1, e_2, ..., e_r\}$ такое, что

$$FA = \bigoplus_{i=1}^{r} (FA)e_i \simeq \bigoplus_{i=1}^{r} F_i e_i,$$

где для $1 \leq i \leq r : F_i \cong (FA)e_i$ - поля, являющиеся конечными расширениями поля F.

§5. Идемпотенты и разложение алгебр.

Определение 1.5.1 Элемент e из алгебры A называется идемпотентом, если $e^2 = e$.

Определение 1.5.2 Семейство идемпотентов $e_1, \ldots, e_n$ из алгебры A называется ортогональным, если выполняется тождество: $e_i e_j = \delta_{ij} e_i$, где δ_{ij}— символ Кронекера.

Определение 1.5.3 Говорят, что алгебра A является прямой суммой идеалов $I_1, \ldots, I_n$, если выполняется следующее условие: для любого $a \in A$ существует единственное разложение $a_i \in I_1, \ldots, a_n \in I_n$: $a = a_1 + \cdots + a_n$.

Теорема 1.5.1

Пусть $I_1, \ldots, I_n$- идеалы алгебры A. Тогда следующие условия равносильны:

1)$A = \oplus_{i=1}^{n} I_i$.

2) Существует такое семейство центральных ортогональных идемпотентов $e_1, \ldots, e_n$ алгебры A, что :

(1)$1 = e_1 + \cdots + e_n$.

(2)$\forall i = \overline{1, n}: \quad e_i A = I_i$.

Глава 2. Групповые алгебры циклических групп.

§1. Комплексные групповые алгебры циклических групп.

Теорема 2.1.1 Пусть $G =< g >$- циклическая группа порядка n над полем $\mathbb{C}$ и ξ- примитивный корень из единицы $n-$той степени. Тогда имеет место следующий изоморфизм:

$$\mathbb{C}G \cong \underbrace{\mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{n}.$$

Доказательство.

Определим $\tau : \mathbb{C}G \to \mathbb{C} \oplus \cdots \oplus \mathbb{C}$, при $\tau(x) = (1, \xi, \ldots, \xi^{n-1})$. Положим, что $\alpha = \sum\limits_{i=0}^{n-1} a_i x^i$ лежит в ядре τ. Получим $0 = \tau(\alpha) = (\sum\limits_{i=0}^{n-1} a_i, \ldots, \sum\limits_{i=0}^{n-1} a_i \xi^{(n-1)i})$ Поскольку матрицей этой системы линейных уравнений относительно неизвестных $a_0, \ldots, a_{n-1}$ будет матрица Вандермондта, то получаем, что $\alpha = 0$- единственное решение.

Пример. Пусть $G =< g >$— циклическсская группа порядка 4. Тогда имеет место изоморфизм:

$$\mathbb{C}G \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C}.$$

§2. Рациональные групповые алгебры.

Теорема2.2.1 Пусть G- циклическая группа порядка n. Тогда имеет место изоморфизм

$$\mathbb{Q}G \cong \oplus_{d|n} \mathbb{Q}(\xi_d).$$

Доказательство. Пусть n- натуральное число, D- все его натуральные делители и $G =< g >$- циклическсская группа порядка n. Для каждого $d \in D$ определим гомоморфизм:

$$\psi_d : \mathbb{Q}G \to \mathbb{Q}(\xi_d),$$

при котором $\psi_d(g) = \xi_d$. Рассмотрим отображение $F : \mathbb{Q}G \to \prod_{d\in D} \mathbb{Q}(\xi_d)$, действующее по правилу $F(a) = (\psi_1(a), \ldots, \psi_d(a), \ldots, \psi_n(a))$. Покажем, что F является изоморфизмом алгебр.

Легко показывается, что F является гомоморфизмом.

Покажем, что $Ker(F) = 0$.

Пусть $u = a_0 + \cdots + a_{n-1}g^{n-1} \in Ker(F)$. Введём многочлен $f(z) = a_0 + \cdots + a_{n-1}z^{n-1}$. Тогда $F(u) = F(a_0 + \cdots + a_{n-1}g^{n-1}) = a_0F(1) + a_1F(g) + \cdots + a_{n-1}F(g^{n-1}) = a_0(1, \ldots, 1)+a_1(1, \ldots, \xi_d, \ldots, \xi_n)+\cdots+a_{n-1}(1, \ldots, \xi_d^{n-1}, \ldots, \xi_n^{n-1}) = (f(1), \ldots, f(\xi_d), \ldots, f(\xi_n)) = 0$. Отсюда следует, что $f(1) = \cdots = f(\xi_n) = 0$. Значит $x^n - 1|f$, но $deg(f) \leq n - 1$. Значит $f(z) \equiv 0$.

Покажем, что размерности алгебр отображения совпадают:

$dim\mathbb{Q}G = n$.

$dim \prod_{d\in D} \mathbb{Q}(\xi_d) = \sum_{d|n} dim_{\mathbb{Q}}\mathbb{Q}(\xi_d) = \sum_{d|n} \psi(d) = n$.

Из всего этого следует, что F является изоморфизмом.

Следствие. Пусть $G =< g >$ порядка p над полем $\mathbb{Q}$ (p- простое число). Пусть ξ- примитивный корень из единицы $p-$той степени. Тогда имеют место изоморфизм:

$$\mathbb{Q}G \cong \mathbb{Q} \oplus \mathbb{Q}(\xi).$$

Пример.

$G =< g >$- циклическесская группа, $|G| = 4$. Делители 4: 1, 2, 4.

Определим гомоморфизмы:

$\psi_1 : \mathbb{Q}G \to \mathbb{Q}$,

$\psi_2 : \mathbb{Q}G \to \mathbb{Q}$,

$\psi_2 : \mathbb{Q}G \to \mathbb{Q}(i)$,

при которых $\psi_1(g^k) = 1$, $\psi_2(g^k) = (-1)^k$, $\psi_4(g^k) = i^k$. Рассмотрим отображение

$F : \mathbb{Q}G \to 2\mathbb{Q} \oplus \mathbb{Q}(i)$, действующее по правилу:

$F(\sum\limits_{j=0}^{3} a_j g^j) = (\sum\limits_{j=0}^{3} a_j \psi_1(g^j), \sum\limits_{j=0}^{3} a_j \psi_2(g^j), \sum\limits_{j=0}^{3} a_j \psi_4(g^j)) = (a_0 + a_1 + a_2 + a_3, a_0 - a_1 + a_2 - a_3, a_0 - a_1 i - a_2 - a_3 i)$. Из доказательства предыдущей теоремы следует, что F изоморфизм и $\mathbb{Q}G \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(i)$.

§3 Конечные групповые алгебры циклических групп.

Теорема 2.3.1 Пусть $G =< g >$ порядка n над полем F_p, где p- простое число и $(n, p) = 1$. Пусть $x^n - 1 = (x-1)f_1(x)\dots f_k(x)$- разложение на неприводимые сомножители $x^n - 1$ над полем F_p . Тогда имеет место изоморфизм:

$$F_pG \cong F_p \times F_{p^{degf_1}} \times \dots \times F_{p^{degf_k}}.$$

Доказательство вышепревидённой теоремы аналогично теореме 2.2.1

Пример 1. Пусть F_2G-групповая алгебра циклической группы G, $|G| = 15$. Над F_2 многочлен $x^{15}-1$ раскладывается на неприводимые сомножители в вид:

$x^{15} - 1 = (x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$.

Введём следующие обозначения:

$f_1 = (x+1)$.

$f_2 = (x^2+x+1)$.

$f_3 = (x^4+x+1)$.

$f_4 = (x^4+x^3+1)$.

$f_5 = (x^4+x^3+x^2+x+1)$.

Из рассуждений, проведённых выше, следует изоморфизм:

$F_2G \cong F_2 \times F_{2^2} \times F_{2^4} \times F_{2^4} \times F_{2^4}$.

Пример 2. Пусть F_3G-групповая алгебра циклической группы G, $|G| = 14$. Над F_3 многочлен $x^{14}-1$ раскладывается на неприводимые сомножители в вид:

$x^{14}-1 = (x+1)(x+2)(x^6+2x^5+x^4+2x^3+x^2+2x+1)(x^6+x^5+x^4+x^3+x^2+x+1)$

Далее, проводя аналогию с предыдущим примером, имеем изоморфизм:

$F_3G \cong F_3 \times F_3 \times F_{3^6} \times F_{3^6}$.

Пример 3. Пусть F_5G-групповая алгебра циклической группы G, $|G| = 42$. Над F_5 многочлен $x^{42}-1$ раскладывается на неприводимые сомножители в вид:

$x^{42} - 1 = (x^6+2x^4+2x^3+2x^2+1)(x^6+4x^5+x^4+4x^3+x^2+4x+1)(x^2+4x+1)(x^6+x^5+x^4+x^3+x^2+x+1)(x+1)(x+4)(x^6+2x^4+3x^3+2x^2+1)(x^6+4x^5+3x^4+x^3+3x^2+4x+1)(x^6+x^5+3x^4+4x^3+3x^2+x+1)(x^2+x+1)$

Получаем изоморфизм:

$F_5G \cong F_5 \times F_5 \times F_{5^2} \times F_{5^2} \times F_{5^6} \times F_{5^6} \times F_{5^6} \times F_{5^6} \times F_{5^6} \times F_{5^6}$.

Глава 3. Абелевы групповые алгебры.

§1 Циклотомиские классы и их свойства.

Определение 3.1.1 Пусть g - элемент конечной абелевой группы A. Тогда $q-$*циклотомическим классом* элемента g будем называть множество вида

$$S_g = \{g^{q^j} | 0 \leq j \leq t_g - 1\},$$

где t_g - наименьшее положительное целое число такое, что $q^{t_g} \equiv 1 (mod\ (o(g))$.

Пусть F - конечное поле из q элементов, A - конечная абелева группа такая, что $(q, |A|) = 1$. Тогда FA - полупроста и, если $\{e_1, ..., e_r\}$ - примитивные идемпотенты FA, то согласно теореме Машке получаем:

$$FA = \bigoplus_{i=1}^{r} (FA)e_i \simeq \bigoplus_{i=1}^{r} Fe_i,$$

где для $1 \leq i \leq r : F_i \simeq (FA)e_i$ - поля, являющиеся конечными расширениями поля F.

В алгебре A рассмотрим подалгебру

$$\mathcal{A} = \bigoplus_{i=1}^{r} Fe_i.$$

Лемма 3.1.1 Если α - элемент FA, то $\alpha \in \mathcal{A} \Leftrightarrow \alpha^q = \alpha$.

Доказательство. Возьмем $\alpha \in FA$ и запишем ее следующим образом:

$$\alpha = \sum_{i=1}^{r} \alpha_i,$$

где $\alpha_i = \alpha e_i \in F_i, 1 \leq i \leq r$. Тогда α будет являтся элементом из $\mathcal{A}$ тогда и только тогда, когда каждый элемет α_i будет из Fe_i. Из того, что $Fe_i \simeq F$, мы получаем, что $\alpha_i^q = \alpha_i \Rightarrow \alpha^q = \alpha$, ч.т.д.

Лемма 3.1.2 (свойства циклотомических классов) 1) Любые два q-циклотомических класса либо совпадают, либо пересекаются по пустому множеству.

2) Если $S_g - q$ - циклотомический класс $\mathcal{A}$, то $(\overline{S_g})^q = \overline{S_g}$

Доказательство. 1) Запишем циклотомический класс $S_g = \{g, ..., g^{q^{t_s-1}}\}$, $g^{q^i} \in S_g$. Покажем, что $S_g = S_{g^{q^i}}$. Ясно, что $g \in S_g$. Поскольку $1, q, ..., q^{t_g-1}$ - все степени q по модулю $o(g)$ и $q^i, q^i \cdot q, ..., q^i \cdot q^{t_g-1}$ - попарно различные степени по модулю $o(g)$, то $\{1, q, ..., q^{t_g-1}\} = \{q^i, q^i \cdot q, ..., q^i \cdot q^{t_g-1}\}$. Тогда имеет место равенство:

$$S_{g^{q^i}} = \{g^{q^i}, ..., g^{q^i q^{t_g-1}}\} = \{g, ..., g^{q^{t_g-1}}\}.$$

Предположим, что $S_{g_1} \neq S_{g_2}$. Если $S_{g_1} \cap S_{g_2} \neq \emptyset$, то существует h такой, что $h = g_1^{q^{i_1}} = g_2^{q^{i_2}} \Rightarrow S_{g_1} = S_h = S_{g_2}$. Получаем противоречие. Следовательно, $S_{g_1} \cap S_{g_2} = \emptyset$.

2)$(\overline{S_g})^q = (g+g^q+...+g^{q^{t_g-1}})^q = g^q+g^{q\cdot q}+...+g^{q\cdot q^{t_g-1}} = g+g^q+...+g^{q^{t_g-1}} = \overline{S_g}$, т.к. $1, ..., q^{t_g-1} \bmod o(g) = q^i \cdot 1, ..., q^i \cdot q^{t_q-1} \bmod o(g)$.

Теорема 3.1.3 (Milies C.P.,Ferraz R.A.(2007) Пусть F - конечное поле и $|F| = q$, A - конечная абелева группа такая, что $(q, |A|) = 1$. Тогда количество компонент FA равно количеству q - циклотомических классов A.

Доказательство. Заметим, что количество компонент алгебры FA совпадает с размерностью $\mathcal{A}$. Пусть $S_{g_1}, ..., S_{g_k}$- все попарно различные q-циклотомических класса группы A. Покажем, что множество $\{\overline{S_{g_1}}, ..., \overline{S_{g_k}}\}$ является базисом $\mathcal{A}$. Из леммы 1 следует, что множество $\{\overline{S_{g_1}}, ..., \overline{S_{g_k}}\}$ линейно независимо. Так как $\overline{S_{g_i}^q} = \overline{S_{g_i}}$, то из леммы 1 $\Rightarrow \{S_{g_1}, ..., S_{g_k}\} \subset \mathcal{A}$. Покажем, что любой $\alpha \in \mathcal{A}$ линейно выражается через $\{S_{g_1}, ..., S_{g_k}\}$. Пусть $\alpha = \sum_{g\in A} \alpha_g g$. По лемме 1 получаем:

$$\alpha^q = \alpha,$$

$$(\sum_{g\in A} \alpha_g g)^q = \sum_{g\in A} \alpha_g g,$$

$$\sum_{g\in A} \alpha_g^q g^q = \sum_{g\in A} \alpha_g g,$$

$$\sum_{g\in A} \alpha_g g^q = \sum_{g\in A} \alpha_g g.$$

Тогда для каждого g имеем: $\alpha_g = \alpha_{g^q} = ... = \alpha_{g^{t_q-1}}$ и $\alpha = \sum_{i=1}^{k} \alpha_{g_i} \overline{S_{g_i}}$, что и требовалось.

Следствие. Пусть $\mathbb{Z}_p C_n \cong \mathbb{Z}_p[x]/ < x^n - 1 >$, где $(p, n) = 1$. Тогда количество неразложимых сомножителей $x^n - 1$ совпадает с количеством p - циклотомических классов C_n.

Пусть H - конечная подгруппа группы G. Если $(q, |H|) = 1$, то зададим

$$\widehat{H} = \frac{1}{|H|} \sum_{g \in H} g.$$

Это означает, что $\widehat{H}$ определен и он является идемпотентом FG.

Лемма 3.1.4 Пусть F - поле из q элементов, G - конечная группа, H - ее конечная подгруппа. Если $(q, |H|) = 1$, то

1) $\widehat{H} = \frac{1}{|H|} \sum_{g \in H} g$ - идемпотент.

2) Если $H_1 \supset H_2$, H_1, H_2 - подгруппы G и $(H_2, q) = 1$, то $\widehat{H}_1 \cdot \widehat{H}_2 = \widehat{H}_1$.

Доказательство.

$$1) \widehat{H} \cdot \widehat{H} = \widehat{H}(\frac{1}{|H|} \sum_{g \in H} g) = \frac{\sum_{g \in H} g\widehat{H}}{|H|} = \frac{|H| \cdot \widehat{H}}{|H|} = \widehat{H},$$

что и требовалось доказать.

2)Пусть $H_1 = \{h_1, ..., h_k\}$, $|H_1| = k$, значит $\widehat{H}_1 = \frac{1}{k}(h_1 + ... + h_k)$, и $H_2 = \{p_1, ..., p_m\}$, $|H_2| = m$, $\widehat{H}_2 = \frac{1}{m}(p_1 + ... + p_m)$, причем $k \geq m$. Рассмотрим произведение между $\widehat{H}_1$ и $\widehat{H}_2$:

$$\widehat{H}_1 \cdot \widehat{H}_2 = \frac{1}{k \cdot m}((h_1 + ... + h_k)p_1 + ... + (h_1 + ... + h_k)p_m = \frac{\overline{H} \cdot m}{k \cdot m} = \widehat{H}_1.$$

Лемма 3.1.5 Пусть F - поле из q элементов, p - рациональное число и $A =< a >$ - циклическая группа порядка p^n, $n \geq 1$. Так же пусть

$$A = A_0 \supset A_1 \supset ... \supset A_n = \{1\}$$

убываюшая цепь из подгрупп A. Тогда элементы $e_0 = \widehat{A}$ и $e_i = \widehat{A}_i - \widehat{A}_{i-1}$, $1 \leq i \leq n$ будут ортогональными идемпотентами FA такие, что $e_0 + e_1 + ... + e_n = 1$.

Доказательство. Для начала докажем, что $e_0 + e_1 + ... + e_n = 1$. Зная представление элементов e_i мы имеем:

$$\widehat{A}_0 + (\widehat{A}_1 - \widehat{A}_0) + (\widehat{A}_2 - \widehat{A}_1) + ... + (\widehat{A}_n - \widehat{A}_{n-1}) = \widehat{A}_n = \{1\}.$$

Теперь покажем, что e_i взаимно ортогональны между собой. Для этого рассмотрим произведение e_i на e_j, где $i < j$ (это равносильно системе из двух неравенств $i < j - 1$, $i - 1 < j$):
$e_i e_j = (\widehat{A}_i - \widehat{A}_{i-1})(\widehat{A}_j - \widehat{A}_{j-1}) = \widehat{A}_i\widehat{A}_j - \widehat{A}_i\widehat{A}_{j-1} - \widehat{A}_{i-1}\widehat{A}_j + \widehat{A}_{i-1}\widehat{A}_{j-1} =$
$\widehat{A}_i - \widehat{A}_{i-1} - \widehat{A}_i + \widehat{A}_{i-1} = 0.$

Осталось выяснить, являются ли e_i идемпотентами. Для этого рассмотрим квадрат любого из них.

$$e_i^2 = (\widehat{A}_i - \widehat{A}_{i-1})^2 = \widehat{A}_i^2 - 2\widehat{A}_i\widehat{A}_{i-1} + \widehat{A}_{i-1}^2 = \widehat{A}_i + \widehat{A}_{i-1} - 2\widehat{A}_i = \widehat{A}_i - \widehat{A}_{i-1} = e_i.$$

Лемма 3.1.6 Пусть $< \overline{q} >= \mathbb{Z}_{p^n}$. Тогда количество циклотомических классов C_{p^n} равно $n + 1$.

Лемма 3.1.7 Пусть F - поле из q элементов и $A = C_{p^n} =< g >$ - циклическая группа порядка p^n такая, что $o(q) = \Phi(p^n)$ в $U(\mathbb{Z}_{p^n})$. Пусть

$$A = A_0 \supset A_1 \supset ... \supset A_n = \{1\}$$

убываюшая цепь из подгрупп A. Тогда примитивные идемпотенты FA будут иметь вид : $e_0 = \frac{1}{p^n}\sum_{g\in A} g$ и $e_i = \widehat{A}_i - \widehat{A}_{i-1}$, $1 \leq i \leq n$.

Доказательство. Данное доказательство следует из лемм 3.1.5 и 3.1.6.

Пример 1. Найдём примитивные ортогональные идемпотенты в $F_2C_5 \times C_{11}$.

Так как (5,11)=1, то получаем, что $F_2C_5 \times C_{11} \cong F_2C_{55}$.

$x^{55} - 1$ над F_2 расскладывается следующим образом:

$x^{55} - 1 = (x^{20} + x^{18} + x^{17} + x^{15} + x^{14} + x^{12} + x^9 + x^7 + x^6 + x^5 + x^2 + x + 1)$

$(x^{20} + x^{19} + x^{18} + x^{15} + x^{14} + x^{13} + x^{11} + x^8 + x^6 + x^5 + x^3 + x^2 + 1)$

$(x^4 + x^3 + x^2 + x + 1)(x + 1)(x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$.

Разложение Веддерберна имеет вид:

$F_2C_{55} \cong F_2 \times F_{2^{20}} \times F_{2^{20}} \times F_{2^{10}} \times F_{2^4}$.

Идемпотентами будут $e_0, e_1, e_2, e_2 + e_3, e_2 + e_4$, где $e_i = \widehat{C_{55}} - f_i - (1, 1)$.

§2 Разложение Веддерберна конечных полупростых групповых алгебр вида $F_p \underbrace{C_q \times C_q \times \cdots \times C_q}_{n}$

Теорема 3.2.1[5, p252]

Пусть p, q- различные простые числа и $< \overline{p} >= U(\mathbb{Z}_q)$. Тогда множество всех примитивных идемпотентов алгебры вида $A = F_p \underbrace{C_q \times C_q \times \cdots \times C_q}_{n}$ имеет вид:

$\{e_H = \widehat{H} - \widehat{G} |$ где H подгруппа группы G порядка $q^{n-1}\}$.

Следствие .

Пусть p, q- различные простые числа и $< \overline{p} >= U(\mathbb{Z}_q)$. Тогда имеет место изоморфизм:

$F_pC_q \times C_q \cong F_p \times \underbrace{F_{p^{q-1}} \times \cdots \times F_{p^{q-1}}}_{q+1}$.

Пример 1. Найдём идемпотенты в групповой алгебре $F_3C_5 \times C_5$. Пусть $S_1, \ldots, S_6$ все нетривиальные p-циклотомические классы группы $F_3C_5 \times C_5$ и $f_i = \overline{S_i}$ для $1 \leq i \leq 6$.

$e_i = \frac{f_i + (1,1)}{5} - \frac{\overline{C_5 \times C_5}}{25} = 2(f_i + (1, 1)) - \overline{C_5 \times C_5} = f_i + (1, 1) + 2 \sum\limits_{k \neq i, 0} f_k$. Получаем изоморфизм:

$F_3C_5 \times C_5 \cong F_3 \times F_{3^4} \times F_{3^4} \times F_{3^4} \times F_{3^4} \times F_{3^4} \times F_{3^4}$.

Пример 2. Найдём идемпотенты в групповой алгебре $F_3C_7 \times C_7$. Пусть

$S_1, \ldots, S_8$ все нетривиальные p-циклотомические классы группы $F_3C_7 \times C_7$ и $f_i = \overline{S_i}$ для $1 \leq i \leq 8$

$e_i = \frac{f_i + (1,1)}{7} - \frac{\overline{C_7 \times C_7}}{49} = f_i + (1,1) - \overline{C_7 \times C_7} = f_i + (1,1) - \sum\limits_{k \neq i,0} f_k$. Получаем изоморфизм:

$$F_3C_7 \times C_7 \cong F_3 \times F_{3^6} \times F_{3^6} \times F_{3^6} \times F_{3^6} \times F_{3^6} \times F_{3^6} \times F_{3^6} \times F_{3^6}.$$

Глава 4. Строение групповых алгебр групп диэдра.

§1. Комплексная групповая алгебра группы диэдра.

Теорема 4.1.1 Пусть $\mathbb{C}D_n$- групповая алгебра, $|D_n| = 2n$. Тогда имеют место изоморфизмы:

1)$\mathbb{C}D_n \cong \mathbb{C} \times \mathbb{C} \times \underbrace{M_2(\mathbb{C}) \times \cdots \times M_2\mathbb{C})}_{\frac{n-1}{2}}$, если n нечётное;

2)$\mathbb{C}D_n \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \underbrace{M_2(\mathbb{C}) \times \cdots \times M_2\mathbb{C})}_{\frac{n-2}{2}}$, если n чётное.

Доказательство.

Рассмотрим множество всех корней степени n из единицы.

Запишем это множество в виде:

$\sqrt[n]{1} = \{1, \xi_1, \ldots, \xi_{\frac{n-1}{2}}, \overline{\xi_1}, \ldots, \overline{\xi_{\frac{n-1}{2}}}\}$, если n нечётно.

$\sqrt[n]{1} = \{1, \xi_2, \ldots, \xi_{\frac{n-2}{2}}, \overline{\xi_2}, \ldots, \overline{\xi_{\frac{n-2}{2}}}\}$, если n чётно.

Для n нечётного каждому элементу из множества $\{1, \xi_1, \ldots, \xi_{\frac{n-1}{2}}\}$ составим гомоморфизм алгебр:

$\varphi_1 : \mathbb{C}D_n \to \mathbb{C} \times \mathbb{C}$,

$\varphi_{\xi_k} : \mathbb{C}D_n \to M_2(\mathbb{C})$.

Определим отображение на образующих базисных элементах групповой алгебры:

$\varphi_1(e) = (1, 1), \quad \varphi_1(a) = (1, 1), \quad \varphi_1(b) = (1, -1),$

$\varphi_{\xi_k}(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \varphi_{\xi_k}(a) = \begin{pmatrix} \xi_k & 0 \\ 0 & \overline{\xi_k} \end{pmatrix}, \quad \varphi_{\xi_k}(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$

Также для n чётного каждому элементу из множества $\{1, \xi_2, \ldots, \xi_{\frac{n-2}{2}}\}$ сопоставим гомоморфизм алгебр:

$\varphi_1 : \mathbb{C}D_n \to \mathbb{C} \times \mathbb{C}$,

$\varphi_{-1} : \mathbb{C}D_n \to \mathbb{C} \times \mathbb{C}$,

$\varphi_{\xi_k} : \mathbb{C}D_n \to M_2(\mathbb{C})$.

Определим отображение на образующих базисных элементах групповой алгебры:

$\varphi_1(e) = (1,1), \quad \varphi_1(a) = (1,1), \quad \varphi_1(b) = (1,-1),$

$\varphi_{-1}(e) = (1,1), \quad \varphi_{-1}(a) = (-1,-1), \quad \varphi_{-1}(b) = (1,-1),$

$\varphi_{\xi_k}(e) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \varphi_{\xi_k}(a) = \begin{pmatrix} \xi_k & 0 \\ 0 & \overline{\xi_k} \end{pmatrix}, \quad \varphi_{\xi_k}(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$

Легко видеть, что введённые отображения действительно являются гомоморфизмами алгебр: перемножение базисных элементов при отображении должно быть одинаковым.Проверим сохранение следующих условий:

$a^n = e, \quad b^2 = e, \quad bab = a^{-1}.$

$\varphi_1^n(a) = (1,1)^n = (1^n, 1^n) = \varphi_1(e),$

$\varphi_1^2(b) = (1,-1)^2 = (1,1) = \varphi_1(e),$

$\varphi_1(b)\varphi_1(b)\varphi_1(a) = (1,-1)(1,1)(1,-1) = (1,1) = \varphi_1^{-1}(a),$

$\varphi_{-1}^n(a) = (-1,-1)^n = ((-1)^n, (-1)^n) = \varphi_{-1}(e),$

$\varphi_{-1}^2(b) = (-1,-1)^2 = (1,1) = \varphi_{-1}(e),$

$\varphi_{-1}(b)\varphi_{-1}(b)\varphi_{-1}(a) = (1,-1)(-1,-1)(1,-1) = (-1,-1) = \varphi_{-1}^{-1}(a),$

$\varphi_{\xi_k}^n(a) = \begin{pmatrix} \xi_k^n & 0 \\ 0 & \overline{\xi_k}^n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \varphi_{\xi_k}(e),$

$\varphi_{\xi_k}^2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \varphi_{\xi_k}(e),$

$\varphi_{\xi_k}(b)\varphi_{\xi_k}(a)\varphi_{\xi_k}(b) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \xi_k & 0 \\ 0 & \overline{\xi_k} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \overline{\xi_k} & 0 \\ 0 & \xi_k \end{pmatrix} = \varphi_{\xi_k}^{-1}(a).$

Рассмотрим отображение

$F : \mathbb{C}D_n \to \mathbb{C} \times \mathbb{C} \times \underbrace{M_2(\mathbb{C}) \times \cdots \times M_2(\mathbb{C})}_{\frac{n-1}{2}}$, если n нечётное и

$F : \mathbb{C}D_n \to \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \underbrace{M_2(\mathbb{C}) \times \cdots \times M_2(\mathbb{C})}_{\frac{n-2}{2}}$, если n чётное,

действующее по правилу: $F(u) = (\varphi_1(u), \dots, \varphi_{\xi_k}(u), \dots)$.

Так как мы показали, что отображение φ гомоморфизм, то и F есть гомоморфизм.

Покажем, что F- изоморфизм.

Найдём $Ker(F)$. Если $u \in ker(F)$, то $F(u) = (\varphi_1(u), \dots, \varphi_{\xi_k}(u), \dots) = 0$.

Значит и каждая компонента равна нулю: $\varphi_1(u) = 0, \dots, \varphi_{\xi_k}(u) = 0, \dots$

Пусть $u = (\alpha_0 e + \dots + \alpha_{n-1} a^{n-1}) + b(\beta_0 e + \dots + \beta_{n-1} a^{n-1})$ и
$F_1(z) = \alpha_0 + \dots + \alpha_{n-1} z^{n-1}, \quad F_2(z) = \beta_0 + \dots + \beta_{n-1} z^{n-1}$.

Тогда

$\varphi_1(u) = (\alpha_0 + \dots + \alpha_{n-1} + \beta_0 + \dots + \beta_{n-1}, \alpha_0 + \dots + \alpha_{n-1} + \beta_0 - \dots - \beta_{n-1}) = (F_1(1) + F_2(1), (F_1(1) - F_2(1)) = 0$.

$\varphi_{-1}(u) = (\alpha_0 - \alpha_1 + \alpha + 2 - \dots + \beta_0 - \beta_1 + \beta_2 - \dots, \alpha_0 - \alpha_1 + \alpha + 2 - \dots - \beta_0 + \beta_1 - \beta_2 + \dots) = (F_1(-1) + F_2(-1), (F_1(-1) - F_2(-1)) = 0$.

Если $a + b = 0$, $a - b = 0$, то $a = b = 0 \Rightarrow F_1(1) = F_2(1) = F_1(-1) = F_2(-1) = 0$.

$$\varphi_{\xi_k}(u) = \begin{pmatrix} \alpha_0 & 0 \\ 0 & \alpha_0 \end{pmatrix} + \begin{pmatrix} \alpha_1 \xi_k & 0 \\ 0 & \alpha_1 \overline{\xi_k} \end{pmatrix} + \dots + \begin{pmatrix} \alpha_{n-1} \xi_k^{n-1} & 0 \\ 0 & \alpha_{n-1} \overline{\xi_k}^{n-1} \end{pmatrix} + \begin{pmatrix} 0 & \beta_0 \\ \beta_0 & 0 \end{pmatrix} +$$
$$\begin{pmatrix} 0 & \beta_1 \overline{\xi_k} \\ \beta_1 \xi_k & 0 \end{pmatrix} + \begin{pmatrix} 0 & \beta_2 \overline{\xi_k}^2 \\ \beta_2 {\xi_k}^2 & 0 \end{pmatrix} + \dots + \begin{pmatrix} 0 & \beta_{n-1} \overline{\xi_k}^{n-1} \\ \beta_{n-1} {\xi_k}^{n-1} & 0 \end{pmatrix} =$$
$$= \begin{pmatrix} \alpha_0 + \alpha_1 \xi_k + \dots + \alpha_{n-1} \xi_k^{n-1} & \beta_0 + \beta_1 \overline{\xi_k} + \dots + \beta_{n-1} \overline{\xi_k}^{n-1} \\ \beta_0 + \beta_1 \xi_k + \dots + \beta_{n-1} {\xi_k}^{n-1} & \alpha_0 + \alpha_1 \overline{\xi_k} + \dots + \alpha_{n-1} \overline{\xi_k}^{n-1} \end{pmatrix} =$$
$$= \begin{pmatrix} F_1(\xi_k) & F_2(\overline{\xi_k}) \\ F_2(\xi_k) & F_1(\overline{\xi_k}) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Из полученных соотношений следует, что $\forall k \quad F_1(\xi_k) = F_2(\overline{\xi_k}) = F_2(\xi_k) = F_1(\overline{\xi_k}) = 0$

Таким образом, корнями F_1 и F_2 являются все корни n-ной степени из 1. Следовательно, $x^n - 1$ делит F_1 и F_2. Так как $deg(F_1) = deg(F_2) \leq n - 1$ и полином большей степени делит полином меньшей степени, то $F_1 = F_2 = 0$, то есть $u = 0$.

Таким образом F- инъективное отображение.

Найдём размерности области определения и области значения F:

Размерность алгебры $\mathbb{C}D_n$ равна: $dim \mathbb{C}D_n = |D_n| = 2n$.

Если n нечётное, то $dim \mathbb{C} \times \mathbb{C} \times \underbrace{M_2(\mathbb{C}) \times \dots \times M_2(\mathbb{C})}_{\frac{n-1}{2}} = 1 + 1 + 4\frac{n-1}{2} = 2n$.

Если n чётное, то $dim\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\underbrace{M_2(\mathbb{C})\times\cdots\times M_2(\mathbb{C})}_{\frac{n-2}{2}}=1+1+1+1+4\frac{n-2}{2}=2n$.

Так как F-линейное инъективное отображение, у которого размерность области определения и области значения совпадают, то F изоморфизм.

Пример. Исходя из результатов предыдущей теоремы выпишем разложения Веддерберна комплексных групповых алгебр групп диэдра D_n, $\quad n=\overline{3,8}$.

$$\mathbb{C}D_3\cong\mathbb{C}\times\mathbb{C}\times M_2(\mathbb{C}).$$

$$\mathbb{C}D_4\cong\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times M_2(\mathbb{C}).$$

$$\mathbb{C}D_5\cong\mathbb{C}\times\mathbb{C}\times M_2(\mathbb{C})\times M_2(\mathbb{C}).$$

$$\mathbb{C}D_6\cong\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times M_2(\mathbb{C})\times M_2(\mathbb{C}).$$

$$\mathbb{C}D_7\cong\mathbb{C}\times\mathbb{C}\times M_2(\mathbb{C})\times M_2(\mathbb{C})\times M_2(\mathbb{C}).$$

$$\mathbb{C}D_8\cong\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times\mathbb{C}\times M_2(\mathbb{C})\times M_2(\mathbb{C})\times M_2(\mathbb{C}).$$

§2 Рациональные групповые алгебры группы диэдра.

Теорема 4.2.1 Пусть D_n- группа диэдра порядка $2n$. Тогда

$\mathbb{Q}D_n\cong\oplus_{d|n}A_d$,

где $A_d\cong\mathbb{Q}\oplus\mathbb{Q}$ если $d=1,2$ и $A_d=M_2([\xi_d+\xi_d^{-1}])$ если $d>2$, где ξ_d- примитивный корень из единицы.

Доказательство. Для d-натурального делителя n введём отображение

$\psi_d:\mathbb{Q}D_n\to\mathbb{Q}\oplus\mathbb{Q}$.

При $d=1,2$ положим $\psi_1(x)=(1,1)$, $\quad\psi_1(y)=(1,-1)$, $\quad\psi_2(x)=(-1,-1)$, $\psi_2(y)=(1,-1)$. Если $d>2$, то $\psi_d:\mathbb{Q}D_n\to M_2(\mathbb{Q}[\xi_d])$,

действующее по правилу: $\psi_d(x)=\begin{bmatrix}\xi_d & 0\\ 0 & \xi_d^{-1}\end{bmatrix}$, $\psi_d(y)=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

Покажем, что имеют место следующие соотношения:

$(\psi_d(x))^n=(\psi_d(y))^2=1$,

$\psi_d(y)\psi_d(x)\psi_d(y) = \psi_d(x)^{-1}$,

$(\psi_d(y))^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,

$\psi_d(x)^n = \begin{bmatrix} \xi_d & 0 \\ 0 & \xi_d^{-1} \end{bmatrix}^n = \begin{bmatrix} \xi_d^n & 0 \\ 0 & \xi_d^{-n} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, так как d является натуральным делителем n.

$\psi_d(y)\psi_d(x)\psi_d(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{bmatrix} \xi_d & 0 \\ 0 & \xi_d^{-1} \end{bmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{bmatrix} \xi_d^{-1} & 0 \\ 0 & \xi_d \end{bmatrix} = (\xi_d(x))^{-1}$.

Так как базисные элементы алгебры $\mathbb{Q}D_n$ и алгебры A_d перемножаются одинаково, то ψ_d является не только линейным отображением, но и гоморфизмом алгебр.

Если $d = 1, 2$, то $E_d \cong \mathbb{Q} \oplus \mathbb{Q}$, если $d > 2$, то $E_d = M_2(\mathbb{Q}[\xi_d])$.

Определим следующее отображение, $\psi : \mathbb{Q}D_n \to \oplus_{d|n} E_d$, действующее по следующему правилу:

$\psi(u) = (\psi_1(u), \ldots, \psi_d(u), \ldots, \psi_n(u))$.

Легко проверяется, что ψ является гомоморфизмом алгебр.

Покажем, что ψ является инъективным гомоморфизмом, то есть $Ker(\psi) = 0$.

Пусть $u \in Ker(\psi)$. Запишем u в виде $u = (a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}) + (b_0 + +b_1 x + \cdots + b_{n-1}x^{n-1})y$.

Введём следующие многочлены:

$F_1(z) = a_0 + \cdots + a_{n-1}z^{n-1}$,

$F_2(z) = b_0 + \cdots + b_{n-1}z^{n-1}$.

Если $d = 1$ имеем $\psi_1(u) = 0$:

$\psi_1(u) = \psi_1(F_1(x)) + \psi_1(F_2(x)y) = F_1(1)(1,1) + F_2(1)(1,1)(1,-1) =$
$= (F_1(1) + F_2(1), F_1(1) - F_2(1)) = 0 \Rightarrow$

$$\begin{cases} F_1(1) + F_2(1) = 0 \\ F_1(1) - F_2(1) = 0 \end{cases} \Rightarrow F_1(1) = F_2(1) = 0.$$

Если $d = 2$ имеем $\psi_2(u) = 0$:

$\psi_1(u) = \psi_2(F_1(x)) + \psi_2(F_2(x)y) = F_1(1)(-1,-1) + F_2(1)(-1,-1)(1,-1) =$

$= (F_1(-1) + F_2(-1), F_1(-1) - F_2(-1)) = 0 \Rightarrow$

$$\begin{cases} F_1(-1) + F_2(-1) = 0 \\ F_1(-1) - F_2(-1) = 0 \end{cases} \Rightarrow F_1(-1) = F_2(-1) = 0.$$

При $d > 2$ имеем $\psi_d(u) = \psi_d(F_1(x)) + \psi_d(F_2(x)y) = \begin{bmatrix} F_1(\xi_d) & F_2(\xi_d) \\ F_2(\xi_d^{-1} & F_1(\xi_d^{-1}) \end{bmatrix} =$

$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$

Корнями многочленов F_1 и F_2 являются все корни n-ной степени из 1, то есть

$x^n - 1 | F_1, \quad x^n - 1 | F_2$, но степени многочленов не превосходит $n - 1$. Таким образом мы получаем, что $F_1 = F_2 = 0$ и, следовательно, $u = 0$, что показывает тривиальность ядра.

Для каждого $d, \quad (d|n)$ введём отображение μ_d. Если $d = 1, 2 \quad \mu_d = \psi_d$, если $d > 2$, то μ_d отображение, действующее из $\mathbb{Q}D_n$ в $M_2(\mathbb{Q}[\xi_d])$ по следующему правилу:

$u \to Z_d^{-1}\psi_d(u)Z_d$

Для каждого $d > 2$ рассмотрим матрицу

$Z_d = \begin{bmatrix} 1 & -\xi_d \\ 1 & -\xi_d^{-1} \end{bmatrix}.$

Рассмотрим отображение $\mu : \mathbb{Q}D_n \to \oplus_{d|n} M_d$, где $M_2 \cong \mathbb{Q} \oplus \mathbb{Q}$ при $d = 1, 2$ и

$M_d \cong M_2(\mathbb{Q}[\xi_d])$ действующее по правилу:

$u \to (\mu_1(u), \ldots, \mu_d(u), \ldots, \mu_n(u))$.

Легко проверяется, что:

$\mu_d(x) = Z_d^{-1}\psi_d(x)Z_d = \begin{bmatrix} 0 & 1 \\ -1 & \xi_d + \xi_d^{-1} \end{bmatrix}.$

$\mu_d(y) = Z_d^{-1}\psi_d(y)Z_d = \begin{bmatrix} 1 & -(\xi_d + \xi_d^{-1}) \\ 0 & -1 \end{bmatrix}.$

$Z_d^{-1} = \frac{1}{\xi_d - \xi d^{-1}} \begin{bmatrix} -\xi_d^{-1} & \xi_d \\ -1 & 1 \end{bmatrix}$.

Следовательно, для каждого $d > 2$ $\mu_d(\mathbb{Q}D_n) \subset M_2(\mathbb{Q}[\xi_d + \xi_d^{-1}])$

Таким образом считаем, что отображение μ действует из $\mathbb{Q}D_n$ в $\oplus_{d|n} A_d$. Найдём размерность $\oplus_{d|n} A_d$.

Если $d = 1, 2$, то $dim A_d = 2$. Так как $dim \mathbb{Q}[\xi_d + \xi_d^{-1}]) = \frac{\varphi(d)}{2}$, то

$dim M_2(\mathbb{Q}[\xi_d + \xi_d^{-1}]) = 4\frac{\varphi(d)}{2} = 2\varphi(d)$.

Следовательно, $dim(\oplus_{d|n} A_d) = 2\varphi(1) + 2\varphi(2) + \sum\limits_{d|n, d\neq 1,2} 2\varphi(d) = 2\sum\limits_{d|n} \varphi(d) = 2n$.

Поскольку $\mu : \mathbb{Q}D_n \to \oplus_{d|n} A_d$ является инъективным и $dim \mathbb{Q}D_n = dim \oplus_{d|n} A_d = 2n$, то μ- изоморфизм.

Пример. Имеют место следующие разложения Веддерберна рациональных групповых алгебр групп диэдра D_n, $\quad n = \overline{8, 14}$.

$$\mathbb{Q}D_8 \cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\sqrt{2})).$$

$$\mathbb{Q}D_9 \cong 2\mathbb{Q} \oplus M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\cos\frac{2\pi}{9})).$$

$$\mathbb{Q}D_{10} \cong 4\mathbb{Q} \oplus 2M_2(\mathbb{Q}(\sqrt{5}).$$

$$\mathbb{Q}D_{11} \cong 2\mathbb{Q} \oplus M_2(\mathbb{Q}(\cos\frac{2\pi}{11})).$$

$$\mathbb{Q}D_{12} \cong 4\mathbb{Q} \oplus 3M_2(\mathbb{Q}) \oplus M_2(\mathbb{Q}(\sqrt{3})).$$

$$\mathbb{Q}D_{13} \cong 2\mathbb{Q} \oplus M_2(\mathbb{Q}(\cos\frac{2\pi}{13})).$$

$$\mathbb{Q}D_{14} \cong 4\mathbb{Q} \oplus M_2(\mathbb{Q}(\cos\frac{2\pi}{7}))) \oplus M_2(\mathbb{Q}(\cos\frac{\pi}{11})).$$

§3. Конечные групповые алгебры группы диэдра.

Теорема 4.3.1 Пусть p- простое число, n- натуральное число, $(n, p) = 1$. $f_1, \ldots, f_s$- все самовозвратные неразложимые нелинейные множители из разложения $x^n - 1$ над F_p. Тогда имеет место следующее утверждение:

a) Если n- нечётное и $x^n - 1 = (x-1)f_1 \dots f_s g_1 g_1' \dots g_t g_t'$- разложение многочлена $x^n - 1$ на неразложимые над F_p многочлены, то

$F_p D_n \cong F_p \times F_p \times M_2(F_{p^{deg f_1/2}}) \times \dots \times M_2(F_{p^{deg f_s/2}}) \times \dots \times M_2(F_{p^{deg g_1}}) \times \dots \times M_2(F_{p^{deg g_t}})$.

b) Если n- чётное и $x^n - 1 = (x-1)f_1 \dots f_s g_1 g_1' \dots g_t g_t'$- разложение многочлена $x^n - 1$ на неразложимые над F_p многочлены, то

$F_p D_n \cong F_p \times F_p \times F_p \times F_p \times M_2(F_{p^{deg f_1/2}}) \times \dots \times M_2(F_{p^{deg f_s/2}}) \times \dots \times M_2(F_{p^{deg g_1}}) \times \dots \times M_2(F_{p^{deg g_t}})$.

Доказательство. Введём отображения α, β, ψ, μ. Отображение

$$\alpha : F_p D_n \to F_p \times F_p,$$

действует по правилам: $\alpha(x) = (1,1), \alpha(y) = (1,-1)$.

Если n- чётное, то рассмотрим отображение:

$$\beta : F_p D_n \to F_p \times F_p,$$

которое действует по правилам: $\beta(x) = (-1,-1), \beta(y) = (1,-1)$.

Для любых $1 \le i \le s$ рассмотрим отображение

$$\psi_i : F_p D_n \to M_2(F_{p^{deg f_i/2}}),$$

действующее по правилам: $\psi_i(x) = Z_{\xi_i}^{-1} \begin{bmatrix} \xi_i & 0 \\ 0 & \xi_i^{-1} \end{bmatrix} Z_{\xi_i}, \psi_i(y) = Z_{\xi_i}^{-1} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} Z_{\xi_i}$,

где ξ_i- корень многочлена f_i,

$Z_{\xi_i} = \begin{bmatrix} 1 & -\xi_i \\ 1 & -\xi_i^{-1} \end{bmatrix}$.

Для любых $1 \le i \le t$ рассмотрим отображение

$$\mu_i : F_p D_n \to M_2(F_{p^{deg g_i'}}),$$

действующее по правилам: $\mu_i(x) = \begin{bmatrix} \xi_i & 0 \\ 0 & \xi_i^{-1} \end{bmatrix}, \mu_i(y) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$,

где ξ_i- корень многочлена g_i'.

Данные отображения являются гомоморфизмами. Для отображений α, β это легко показывается. Покажем, что ψ также является гомоморфизмом.

Непосредственным умножением найдём явный вид $\psi_i(y) = \begin{bmatrix} 1 & -(\xi_i + \xi_i^{-1}) \\ 0 & -1 \end{bmatrix}$.

$\psi_i(y)^2 = \begin{bmatrix} 1 & -(\xi_i + \xi_i^{-1}) \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & -(\xi_i + \xi_i^{-1}) \\ 0 & -1 \end{bmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,

$\psi_i(x)^n = Z_{\xi_i}^{-1} \begin{bmatrix} \xi_i^n & 0 \\ 0 & \xi_i^{-n} \end{bmatrix} Z_{\xi_i} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,

$\psi_i(y)^{-1}\psi_i(x)\psi_i(y) = \begin{bmatrix} \xi_i + \xi_i^{-1} & -1 \\ 1 & 0 \end{bmatrix} = \psi_i(x)^{-1}$.

Покажем, что имеет место включеие

$$\psi_i(F_pD_n) \subset M_2(F_p[\xi_i + \xi_i^{-1}])$$

для каждого i. Для этого достаточно показать, что

$\psi_i(x), \psi_i(y) \in M_2(F_p[\xi_i + \xi_i^{-1}])$.Явный вид этих отображений:

$\psi_i(x) = \begin{bmatrix} 0 & 1 \\ -1 & \xi_i + \xi_i^{-1} \end{bmatrix}$,

$\psi_i(y) = \begin{bmatrix} 1 & -(\xi_i + \xi_i^{-1}) \\ 0 & -1 \end{bmatrix}$.

Определим отображения

$F : F_pD_n \to F_p \times F_p \times M_2(F_{p^{degf_{1/2}}}) \times \cdots \times M_2(F_{p^{degg_1}}) \times \dots$ действующее по правилу:

$F(u) = (\alpha(u), \psi_1(u), \dots, \mu_1(u), \dots)$ для нечётных n и

$F' : F_pD_n \to F_p \times F_p \times F_p \times F_p \times M_2(F_{p^{degf_{1/2}}}) \times \cdots \times M_2(F_{p^{degg_1}}) \times \dots$ действующее по правилу:

$F'(u) = (\alpha(u), \beta(u), \psi_1(u), \dots, \mu_1(u), \dots)$ для чётных n .

Так же легко показывается, что F и F' являются гомоморфизмами алгебр.

Покажем, что $Ker(F) = 0$.

Пусть $u \in Ker(F)$. Запишем u в виде: $u = (a_0 + \cdots + a_{n-1}x^{n-1}) + (b_0 + \cdots + b_{n-1}x^{n-1})y$.

Введём следующие многочлены:

$F_1(z) = a_0 + \cdots + a_{n-1}z^{n-1}$,

$F_2(z) = b_0 + \cdots + b_{n-1}z^{n-1}$.

Применяя выкладки, аналогичные выкладкам предыдущих параграфов, легко получить, что $F_1(1) = F_2(1) = F_1(\xi_i) = F_2(\xi_i) = F_1(\xi_i^{-1}) = F_2(\xi_i^{-1}) = 0$.

Таким образом, все корни многочлена $x^n - 1$ являются корнями многочленов F_1, F_2. Следовательно эти многочлены делятся на $x^n - 1$, но так как степени многочленов F_i не превосходят $n-1$ получаем, что $F_1 = F_2 = 0$. Следовательно, $Ker(F) = 0$. Для чётных n доказательство тривиальности ядра F' аналогичное.

Если n- нечётно, то

$dim(F_p \times F_p \times M_2(F_{p^{degf_{1/2}}}) \times \cdots \times M_2(F_{p^{degg_1}}) \times \ldots M_2(F_{p^{degg_t}}) = 2n$.

С другой стороны $dimF_pD_n = 2n$.

$dim(F_p \times F_p \times F_p \times F_p \times M_2(F_{p^{degf_{1/2}}}) \times \cdots \times M_2(F_{p^{degg_1}}) \times \ldots M_2(F_{p^{degg_t}})) = 2n$.

Из вышеизложенного непосредственно следует, что F и F' являются изоморфизмами.

Пример 1.

Пусть $n = 3, \quad p = 7$. Тогда имеют место следущее разложение $x^3 - 1$ и изоморфизм:

$x^3 - 1 = (x + 6)(x + 5)(x + 3)$.

В данном случае $f_1 = x + 5$ и $f_2 = x + 3$ являются самовозвратными.

$F_7D_3 \cong F_7 \times F_7 \times M_2(F_7)$.

Пример 2.

Пусть $n = 3, \quad p = 5$. Тогда имеют место следущее разложение $x^3 - 1$ и изоморфизм:

$x^3 - 1 = (x + 4)(x^2 + x + 1)$.

$F_5D_3 \cong F_5 \times F_5 \times M_2(F_5)$.

Пример 3.

Пусть $n = 6, \quad p = 7$. Тогда имеют место следущее разложение $x^3 - 1$ и изоморфизм:

$x^6 - 1 = (x+6)(x+5)(x+3)(x+2)(x+4)(x+1)$.

$F_7D_6 \cong F_6 \times F_6 \times F_6 \times F_6 \times M_2(F_6) \times M_2(F_6) \times M_2(F_6)$.

§4 Групповые алгебры вида $F_pD_{q^n}$.

Лемма 4.4.1 Если $< \overline{p} >= U(\mathbb{Z}_{q^n})$, то разложение многочлена $x^{q^n} - 1$ над F_p имеет вид: $x^{q^n} - 1 = (x-1)f_1 \dots f_k$, где f_i являются симметрическими многочленами.

Теорема 4.4.2 Пусть $F_pD_{q^n}$- конечноменрная групповая алгебра, p, q различные нечётные простые числа и $< \overline{p} >= U(\mathbb{Z}_{q^n})$. Тогда имеет место изоморфизм:

$$F_pD_{q^n} \cong F_p \times F_p \times \underbrace{M_2(F_{p^{(q-1)/2}}) \times M_2(F_{p^{q(q-1)/2}}) \times \dots \times M_2(F_{p^{q^{n-1}(q-1)/2}})}_{n}.$$

Доказательство. Разложим многочлен $x^{q^n} - 1$ на неприводимые сомножители над полем F_p: $x^{q^n} - 1 = (x-1)f_1 \dots f_k$. Количество неприводимых сомножителей у многочлена $x^{q^n} - 1$ совпадает с количеством простых компонент в разложении Веддерберна групповой алгебры $F_pC_{q^n}$, которая, в свою очередь, согласно теореме 2.3.1, равно $n+1$. Таким образом $k = n$. Согласно [3, 390 p] $degf_i = dim(e_iA) = dim_{F_p}G/G_i - dim_{F_p}G/G_{i-1} = q^{i-1}(q-1)$. Так как, согласно лемме 4.4.1, многочлены f_i являются симметрическими, то из доказательства теоремы о разложении Веддерберна конечных групповых алгебр группы диэдра следует изоморфизм:

$$F_pD_{q^n} \cong F_p \times F_p \times \underbrace{M_2(F_{p^{(q-1)/2}}) \times M_2(F_{p^{q(q-1)/2}}) \times \dots \times M_2(F_{p^{q^{n-1}(q-1)/2}})}_{n}.$$

Сравним размерности левой и правой части последнего изоморфизма:

$2q^n = 2 + 4\frac{q-1}{2}(1 + q + \dots + q^{n-1})$.

Пример 1. Пусть $p = 3, n = 2, q = 5$. Тогда имеют место следущее разложение $x^{25} - 1$ и изоморфизм:

$x^{25} - 1 = (x^4 + x^3 + x^2 + x + 1)(x+2)(x^{20} + x^{15} + x^{10} + x^5 + 1)$.

$F_3D_{25} \cong F_3 \times F_3 \times M_2(F_{3^2}) \times M_2(F_{3^{10}})$..

Пример 2. Пусть $p = 3, n = 2, q = 7$. Тогда имеют место следущее разложение $x^{49} - 1$ и изоморфизм:

$x^{49} - 1 = (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)(x+2)(x^{42} + x^{35} + x^{28} + x^{21} + x^{14} + x^7 + 1)$.

$F_3D_{49} \cong F_3 \times F_3 \times M_2(F_{3^3}) \times M_2(F_{3^{21}})$.

Пример 3. Пусть $p = 5, n = 2, q = 3$. Тогда имеют место следущее разложение $x^9 - 1$ и изоморфизм:

$x^9 - 1 = (x^2 + x + 1)(x + 4)(x^6 + x^3 + 1)$.

$F_5D_9 \cong F_5 \times F_5 \times M_2(F_5) \times M_2(F_{5^3})$.

§5 Групповые алгебры вида F_qD_{2p}.

Теорема 4.5.1 Пусть F_qD_n- групповая алгебра группы диэдра, причём $n = 2p$, (p, q)=1 и q - степень нечетного простого числа . Тогда

$e_1 = \frac{1}{2n}(1 + x + x^2 + x^3 + \cdots + x^{n-1} + y + yx + \cdots + yx^{n-1})$,

$e_2 = \frac{1}{2n}(1 + x + x^2 + x^3 + \cdots + x^{n-1} - y - yx - \cdots - yx^{n-1})$,

$e_3 = \frac{1}{2n}(1 - x + x^2 - x^3 + \cdots - x^{n-1} + y - yx + \cdots - yx^{n-1})$,

$e_4 = \frac{1}{2n}(1 - x + x^2 - x^3 + \cdots - x^{n-1} - y + yx - yx^2 + \cdots + yx^{n-1})$

-центральные примитивные идемпотенты и

$$e_1F_qD_n \cong F_q,$$

$$e_2F_qD_n \cong F_q,$$

$$e_3F_qD_n \cong F_q,$$

$$e_4F_qD_n \cong F_q.$$

Доказательство.

Имеем следующие равенства:

$e_1x^i = \frac{1}{2n}(1 + x + x^2 + x^3 + \cdots + x^{n-1} + y + yx + \cdots + yx^{n-1})x^i = e_1 = e_1x^iy$.

Отсюда получаем, что $e_1e_1 = e_1$.

$e_1F_qD_{2p} = e_1F_q$.

Также выведем равенства и для e_2:

$e_2x^i = \frac{1}{2n}(1 + x + x^2 + x^3 + \cdots + x^{n-1} - y - yx - \cdots - yx^{n-1})x^i = e_2$,

$e_2x^iy = \frac{1}{2n}(1 + x + x^2 + x^3 + \cdots + x^{n-1} - y - yx - \cdots - yx^{n-1})x^iy = \frac{1}{2n}(y + yx + \cdots + yx^{n-1} - x - x^2 - \cdots - x^{n-1}) = -e_2$.

Возводя e_2 в квадрат получим, что $e_2e_2 = e_2$.

$e_2F_qD_{2p} = e_2F_q$.

Для e_3 запишем тождества:

$e_3x^i = \frac{1}{2n}(1-x+x^2-x^3+\cdots-x^{n-1}+y-yx+\cdots-yx^{n-1})x^i = \begin{cases} e_3, i = 2j \\ -e_3, i = 2j+1 \end{cases}$,

$e_3yx^i = \frac{1}{2n}(1-x+x^2-x^3+\cdots-x^{n-1}+y-yx+\cdots-yx^{n-1})yx^i =$

$= \begin{cases} e_3, i = 2j \\ -e_3, i = 2j+1 \end{cases}$.

Тогда имеем:

$e_3e_3 = \frac{1}{2n}e_3(1-x+x^2-x^3+\cdots-x^{n-1}+y-yx+\cdots-yx^{n-1}) = \frac{1}{2n}(e_3 - e_3x+\cdots-e_3x^{n-1}+e_3y-e_3yx+\cdots+e_3yx^{n-1}) = \frac{1}{2n}2ne_3 = e_3$.

$e_3F_qD_{2p} = e_3F_q$.

Аналогично показываются равенства и для e_4:

$e_4x^i = \frac{1}{2n}(1-x+x^2-x^3+\cdots-x^{n-1}-y+yx-\cdots+yx^{n-1})x^i = \begin{cases} e_4, i = 2j \\ -e_4, i = 2j+1 \end{cases}$,

$e_4yx^i = \frac{1}{2n}(1-x+x^2-x^3+\cdots-x^{n-1}-y+yx-\cdots+yx^{n-1})yx^i =$

$= \begin{cases} e_4, i = 2j+1 \\ -e_4, i = 2j \end{cases}$.

Тогда:

$e_4e_4 = \frac{1}{2n}e_4(1-x+x^2-x^3+\cdots-x^{n-1}-y+yx-\cdots+yx^{n-1}) = \frac{1}{2n}2ne_4 = e_4$.

$e_4F_qD_{2p} = e_4F_q$.

Легко показывается, что $e_ie_j = e_i\delta_{ij}$, где δ_{ij}- символ Кронекера.

Лемма 4.5.2 Если p, q нечётные простые числа и $< \overline{q} >= U(\mathbb{Z}_p)$, то разложение многочлена $x^{2p} - 1$ над F_q имеет вид $x^{2p} - 1 = (x^2 - 1)f_1f_2$, причём $deg(f_1) = deg(f_2) = q - 1$ и эти многочлены являются симметрическими.

Теорема 4.5.3 Пусть F_qD_{2p}- групповая алгебра, причём p, q нечётные простые числа и $< \overline{q} >= U(\mathbb{Z}_p)$. Тогда имеет место изоморфизм:

$F_qD_{2p} \cong F_q \times F_q \times F_q \times F_q \times M_2(F_{q^{(p-1)/2}}) \times M_2(F_{q^{(p-1)/2}})$.

$e_5 = \frac{1}{2}(1 + x^{n/2}) - \frac{1}{n}\overline{C}_n$,

$e_6 = \frac{1}{2}(1 - \frac{2}{n})(1 - x^{n/2}) + \frac{1}{n}(x - x^2 + \widehat{\ldots}^{n/2} - x^{n-2} + x^{n-1})$

-примитивные центральные идемпотенты, отвечающие за матричные компоненты.

Доказательство.

Согласно теореме 4.3.2 и лемме 4.5.2 имеем изоморфизм

$F_qD_{2p} \cong F_q \times F_q \times F_q \times F_q \times M_2(F_{q^{(p-1)/2}}) \times M_2(F_{q^{(p-1)/2}})$.

Проверим размерности:

$4p = 4 + 4(p-1) = 4p$.

Покажем, что e_5 и e_6 являются идемпотентами. Имеем:

$e_5^2 = (\frac{1}{2}(1+x^{n/2}) - \frac{1}{n}\overline{C}_n)^2 = \frac{1}{2^2}(1+2x^{n/2}+1) - \frac{2}{n}\overline{C}_n + \frac{1}{n^2}\overline{C}_n^2 = e_5$.

Проверим ортогональность e_i:

$e_1e_5 = \frac{1}{2}e_1(1+x^{n/2}) - \frac{1}{n}e_1\overline{C}_n = e_1 - e_1 = 0$,

$e_2e_5 = \frac{1}{2}e_2(1+x^{n/2}) - \frac{1}{n}e_2\overline{C}_n = e_2 - e_2 = 0$,

$e_3e_5 = \frac{1}{2}e_3(1+x^{n/2}) - \frac{1}{n}e_3\overline{C}_n = \frac{1}{2}(e_3 - e_3) = 0$,

$e_4e_5 = \frac{1}{2}e_4(1+x^{n/2}) - \frac{1}{n}e_4\overline{C}_n = \frac{1}{2}(e_4 - e_4) = 0$.

Таким образом получаем, что $e_6^2 = (1 - e_1 - e_2 - e_3 - e_4 - e_5)^2 = e_6$.

Пример 1. Пусть $q = 5, p = 3$. Тогда многочлен $x^6 - 1$ имеет разложение:

$x^6 - 1 = (x^2-1)(x^2+x+1)(x^2+4x+1)$.

Значит:

$F_5D_6 \cong F_5 \times F_5 \times F_5 \times F_5 \times M_2(F_5) \times M_2(F_5)$.

Отображение действует следующим образом:

$$a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5+b_0y+b_1xy+b_2x^2y+b_3x^3y+b_4x^4y+b_5x^5y \to$$

$$(\sum_{i=0}^{5}(a_i+b_i), \sum_{i=0}^{5}(a_i-b_i), \sum_{i=0}^{5}(-1)^i(a_i+b_i), \sum_{i=0}^{5}(-1)^i(a_i-b_i), \begin{pmatrix} \sum\limits_{i=0}^{5} a_i\xi^i & \sum\limits_{i=0}^{5} b_i\xi^i \\ \sum\limits_{i=0}^{5} b_i\xi^{-i} & \sum\limits_{i=0}^{5} a_i\xi^{-i} \end{pmatrix}$$

Найдём куда переходят идемпотенты под действием этого отображения. Для этого запишем систему уравнений и разберём случаи:

1.(1,0,0,0,0,0).

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=1 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=0 \\ a_0-a_2+a_3-a_5=0 \\ a_1-a_2+a_4-a_5=0 \\ a_0-a_2-a_3+a_5=0 \\ a_1+a_2-a_4-a_5=0 \\ b_0-b_2+b_4-b_5=0 \\ b_1-b_2+b_4-b_5=0 \\ b_0-b_2-b_3+b_5=0 \\ b_1+b_2-b_4-b_5=0 \end{cases}.$$

Решая данную систему находим, что идемпотент имеет вид:

$3+3x+3x^2+3x^3+3x^4+3x^5+3y+3xy+3x^2y+3x^3y+3x^4y+3x^5y.$

2.(0,1,0,0,0,0).

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=0 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=1 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=0 \\ a_0-a_2+a_3-a_5=0 \\ a_1-a_2+a_4-a_5=0 \\ a_0-a_2-a_3+a_5=0 \\ a_1+a_2-a_4-a_5=0 \\ b_0-b_2+b_4-b_5=0 \\ b_1-b_2+b_4-b_5=0 \\ b_0-b_2-b_3+b_5=0 \\ b_1+b_2-b_4-b_5=0 \end{cases}.$$

Решая данную систему находим, что идемпотент имеет вид:

$3+3x+3x^2+3x^3+3x^4+3x^5+2y+2xy+2x^2y+2x^3y+2x^4y+2x^5y.$

3.(0,0,1,0,0,0).

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=0 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=1 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=0 \\ a_0-a_2+a_3-a_5=0 \\ a_1-a_2+a_4-a_5=0 \\ a_0-a_2-a_3+a_5=0 \\ a_1+a_2-a_4-a_5=0 \\ b_0-b_2+b_4-b_5=0 \\ b_1-b_2+b_4-b_5=0 \\ b_0-b_2-b_3+b_5=0 \\ b_1+b_2-b_4-b_5=0 \end{cases}.$$

Решая данную систему находим, что идемпотент имеет вид:

$3+2x+3x^2+2x^3+3x^4+2x^5+3y+2xy+3x^2y+2x^3y+3x^4y+2x^5y.$

4.(0,0,0,1,0,0).

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=0 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=1 \\ a_0-a_2+a_3-a_5=0 \\ a_1-a_2+a_4-a_5=0 \\ a_0-a_2-a_3+a_5=0 \\ a_1+a_2-a_4-a_5=0 \\ b_0-b_2+b_4-b_5=0 \\ b_1-b_2+b_4-b_5=0 \\ b_0-b_2-b_3+b_5=0 \\ b_1+b_2-b_4-b_5=0 \end{cases}.$$

Решая данную систему находим, что идемпотент имеет вид:

$3 + 2x + 3x^2 + 2x^3 + 3x^4 + 2x^5 + 2y + 3xy + 2x^2y + 3x^3y + 2x^4y + 3x^5y.$

5.$(0, 0, 0, 0, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, 0).$

$$\begin{cases} a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + b_0 + b_1 + b_2 + b_3 + b_4 + b_5 = 0 \\ a_0 + a_1 + a_2 + a_3 + a_4 + a_5 - b_0 - b_1 - b_2 - b_3 - b_4 - b_5 = 0 \\ a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + b_0 - b_1 + b_2 - b_3 + b_4 - b_5 = 0 \\ a_0 - a_1 + a_2 - a_3 + a_4 - a_5 - b_0 + b_1 - b_2 + b_3 - b_4 + b_5 = 0 \\ a_0 - a_2 + a_3 - a_5 = 1 \\ a_1 - a_2 + a_4 - a_5 = 0 \\ a_0 - a_2 - a_3 + a_5 = 0 \\ a_1 + a_2 - a_4 - a_5 = 0 \\ b_0 - b_2 + b_4 - b_5 = 0 \\ b_1 - b_2 + b_4 - b_5 = 0 \\ b_0 - b_2 - b_3 + b_5 = 0 \\ b_1 + b_2 - b_4 - b_5 = 0 \end{cases}.$$

Решая данную систему находим, что идемпотент имеет вид:

$2 + 4x + 4x^2 + 2x^3 + 4x^4 + 4x^5.$

6.$(0, 0, 0, 0, 0, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}).$

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=0 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=0 \\ a_0-a_2+a_3-a_5=0 \\ a_1-a_2+a_4-a_5=0 \\ a_0-a_2-a_3+a_5=1 \\ a_1+a_2-a_4-a_5=0 \\ b_0-b_2+b_4-b_5=0 \\ b_1-b_2+b_4-b_5=0 \\ b_0-b_2-b_3+b_5=0 \\ b_1+b_2-b_4-b_5=0 \end{cases}.$$

Решая данную систему находим, что идемпотент имеет вид:

$2+x+4x^2+3x^3+4x^4+x^5$.

Легко проверяется, что $e_1+\cdots+e_6=1$.

1)Проверим квадраты 3-го и 5-го компонент:

$e_3^2=(3+2x+3x^2+2x^3+3x^4+2x^5+3y+2xy+3x^2y+2x^3y+3x^4y+2x^5y)^2=$

$12(4+x+4x^2+x^3+4x^4+x^5+4y+xy+4x^2y+x^3y+4x^4y+x^5y)=$

$2(4+x+4x^2+x^3+4x^4+x^5+4y+xy+4x^2y+x^3y+4x^4y+x^5y)=e_3$.

$e_5^2=(2+4x+4x^2+2x^3+4x^4+4x^5)^2=4+x+2*x^2+3*x^4+4*x^5+3*x^6+3*x^7+2*x^8+2*x^9+x^10=e_5$.

2)Проверим ортогональность:

$e_3e_5=(3+2x+3x^2+2x^3+3x^4+2x^5+3y+2xy+3x^2y+2x^3y+3x^4y+2x^5y)(2+4x+4x^2+2x^3+4x^4+4x^5)=2e_3-2e_3-4*2e_3+4*2e_3=0$.

Квадраты и ортогональность остальных компонент и пар проверяется аналогично.

Пример 1. Пусть $q=7, p=3$. Тогда многочлен x^6-1 имеет разложение:

$x^6-1=(x^2-1)(x+5)(x+3)(x+4)(x+2)$.

Мрогочлены $x+5$, $x+3$ и $x+4$, $x+2$ являются самовозвратыми. Значит:

$F_7D_6 \cong F_7 \times F_7 \times F_7 \times F_7 \times M_2(F_7) \times M_2(F_7)$.

Отображение действует следующим образом:

$a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5+b_0y+b_1xy+b_2x^2y+b_3x^3y+b_4x^4y+b_5x^5y \to$
$(\sum\limits_{i=0}^{5}(a_i+b_i), \sum\limits_{i=0}^{5}(a_i-b_i), \sum\limits_{i=0}^{5}(-1)^i(a_i+b_i), \sum\limits_{i=0}^{5}(-1)^i(a_i-b_i),$
$\begin{pmatrix} a_0+2a_1+4a_2+a_3+2a_4+4a_5 & b_0+2b_1+4b_2+b_3+2b_4+4b_5 \\ b_0+4b_1+2b_2+b_3+4b_4+2b_5 & a_0+4a_1+2a_2+a_3+4a_4+2a_5 \end{pmatrix},$
$\begin{pmatrix} a_0+3a_1+2a_2+6a_3+4a_4+5a_5 & b_0+3b_1+2b_2+6b_3+4b_4+5b_5 \\ b_0+5b_1+4b_2+6b_3+2b_4+3b_5 & a_0+5a_1+4a_2+6a_3+2a_4+3a_5 \end{pmatrix}).$

Найдём куда переходят идемпотенты под действием этого отображения. Для этого запишем систему уравнений и разберём случаи:

1.(1,0,0,0,0,0).

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=1 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=0 \\ a_0+2a_1+4a_2+a_3+2a_4+4a_5=0 \\ b_0+2b_1+4b_2+b_3+2b_4+4b_5=0 \\ b_0+4b_1+2b_2+b_3+4b_4+2b_5=0 \\ a_0+4a_1+2a_2+a_3+4a_4+2a_5=0 \\ a_0+3a_1+2a_2+6a_3+4a_4+5a_5=0 \\ b_0+3b_1+2b_2+6b_3+4b_4+5b_5=0 \\ b_0+5b_1+4b_2+6b_3+2b_4+3b_5=0 \\ a_0+5a_1+4a_2+6a_3+2a_4+3a_5=0 \end{cases}.$$

Решая данную систему находим, что идемпотент имеет вид:

$3+3x+3x^2+3x^3+3x^4+3x^5+3y+3xy+3x^2y+3x^3y+3x^4y+3x^5y$.

2.(0,1,0,0,0,0).

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=0 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=1 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=0 \\ a_0+2a_1+4a_2+a_3+2a_4+4a_5=0 \\ b_0+2b_1+4b_2+b_3+2b_4+4b_5=0 \\ b_0+4b_1+2b_2+b_3+4b_4+2b_5=0 \\ a_0+4a_1+2a_2+a_3+4a_4+2a_5=0 \\ a_0+3a_1+2a_2+6a_3+4a_4+5a_5=0 \\ b_0+3b_1+2b_2+6b_3+4b_4+5b_5=0 \\ b_0+5b_1+4b_2+6b_3+2b_4+3b_5=0 \\ a_0+5a_1+4a_2+6a_3+2a_4+3a_5=0 \end{cases}.$$

Решая данную систему находим, что идемпотент имеет вид:

$3+3x+3x^2+3x^3+3x^4+3x^5+4y+4xy+4x^2y+4x^3y+4x^4y+4x^5y.$

3.(0,0,1,0,0,0).

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=0 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=1 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=0 \\ a_0+2a_1+4a_2+a_3+2a_4+4a_5=0 \\ b_0+2b_1+4b_2+b_3+2b_4+4b_5=0 \\ b_0+4b_1+2b_2+b_3+4b_4+2b_5=0 \\ a_0+4a_1+2a_2+a_3+4a_4+2a_5=0 \\ a_0+3a_1+2a_2+6a_3+4a_4+5a_5=0 \\ b_0+3b_1+2b_2+6b_3+4b_4+5b_5=0 \\ b_0+5b_1+4b_2+6b_3+2b_4+3b_5=0 \\ a_0+5a_1+4a_2+6a_3+2a_4+3a_5=0 \end{cases}$$

Решая данную систему находим, что идемпотент имеет вид:

$3+4x+3x^2+4x^3+3x^4+4x^5+3y+4xy+3x^2y+4x^3y+3x^4y+4x^5y.$

4.(0,0,0,1,0,0).

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=0 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=1 \\ a_0+2a_1+4a_2+a_3+2a_4+4a_5=0 \\ b_0+2b_1+4b_2+b_3+2b_4+4b_5=0 \\ b_0+4b_1+2b_2+b_3+4b_4+2b_5=0 \\ a_0+4a_1+2a_2+a_3+4a_4+2a_5=0 \\ a_0+3a_1+2a_2+6a_3+4a_4+5a_5=0 \\ b_0+3b_1+2b_2+6b_3+4b_4+5b_5=0 \\ b_0+5b_1+4b_2+6b_3+2b_4+3b_5=0 \\ a_0+5a_1+4a_2+6a_3+2a_4+3a_5=0 \end{cases}$$

Решая данную систему находим, что идемпотент имеет вид:

$3+4x+3x^2+4x^3+3x^4+4x^5+4y+3xy+4x^2y+3x^3y+4x^4y+3x^5y.$

5.$(0,0,0,0,\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},0)$.

$$\begin{cases} a_0+a_1+a_2+a_3+a_4+a_5+b_0+b_1+b_2+b_3+b_4+b_5=0 \\ a_0+a_1+a_2+a_3+a_4+a_5-b_0-b_1-b_2-b_3-b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5+b_0-b_1+b_2-b_3+b_4-b_5=0 \\ a_0-a_1+a_2-a_3+a_4-a_5-b_0+b_1-b_2+b_3-b_4+b_5=0 \\ a_0+2a_1+4a_2+a_3+2a_4+4a_5=1 \\ b_0+2b_1+4b_2+b_3+2b_4+4b_5=0 \\ b_0+4b_1+2b_2+b_3+4b_4+2b_5=0 \\ a_0+4a_1+2a_2+a_3+4a_4+2a_5=1 \\ a_0+3a_1+2a_2+6a_3+4a_4+5a_5=0 \\ b_0+3b_1+2b_2+6b_3+4b_4+5b_5=0 \\ b_0+5b_1+4b_2+6b_3+2b_4+3b_5=0 \\ a_0+5a_1+4a_2+6a_3+2a_4+3a_5=0 \end{cases}$$

Решая данную систему находим, что идемпотент имеет вид:

$5 + x + x^2 + 5x^3 + x^4 + x^5$.

6.$(0, 0, 0, 0, 0, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})$.

$$\begin{cases} a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + b_0 + b_1 + b_2 + b_3 + b_4 + b_5 = 0 \\ a_0 + a_1 + a_2 + a_3 + a_4 + a_5 - b_0 - b_1 - b_2 - b_3 - b_4 - b_5 = 0 \\ a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + b_0 - b_1 + b_2 - b_3 + b_4 - b_5 = 0 \\ a_0 - a_1 + a_2 - a_3 + a_4 - a_5 - b_0 + b_1 - b_2 + b_3 - b_4 + b_5 = 0 \\ a_0 + 2a_1 + 4a_2 + a_3 + 2a_4 + 4a_5 = 0 \\ b_0 + 2b_1 + 4b_2 + b_3 + 2b_4 + 4b_5 = 0 \\ b_0 + 4b_1 + 2b_2 + b_3 + 4b_4 + 2b_5 = 0 \\ a_0 + 4a_1 + 2a_2 + a_3 + 4a_4 + 2a_5 = 0 \\ a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 = 1 \\ b_0 + 3b_1 + 2b_2 + 6b_3 + 4b_4 + 5b_5 = 0 \\ b_0 + 5b_1 + 4b_2 + 6b_3 + 2b_4 + 3b_5 = 0 \\ a_0 + 5a_1 + 4a_2 + 6a_3 + 2a_4 + 3a_5 = 1 \end{cases}$$

Решая данную систему находим, что идемпотент имеет вид:

$5 + 6x + x^2 + 2x^3 + x^4 + 6x^5$.

Согласно теореме 4.5.1 первые 4 идемпотента ортогональны между собой и являются идемпотентами. Покажем, что 3-й идемпотент ортогонален последним двум:

$e_3e_5 = (3 + 4x + 3x^2 + 4x^3 + 3x^4 + 4x^5 + 3y + 4xy + 3x^2y + 4x^3y + 3x^4y + 4x^5y)$

$(5 + x + x^2 + 5x^3 + x^4 + x^5) = 5e_3 - e_3 + e_3 - 5e_3 + e_3 - e_3 = 0$,

$e_3e_6 = (3 + 4x + 3x^2 + 4x^3 + 3x^4 + 4x^5 + 3y + 4xy + 3x^2y + 4x^3y + 3x^4y + 4x^5y)$

$(5 + 6x + x^2 + 2x^3 + x^4 + 6x^5) = 5e_3 - 6e_3 + e_3 - 2e_3 + e_3 - 6e_3 = -7e_3 = 0$.

Проверим квадраты e_5 и e_6 :

$e_5^2 = (5 + x + x^2 + 5x^3 + x^4 + x^5)^2 = 4 + 3x + 4x^2 + 3x^3 + x^5 + 1 + 5x + 4x^2 + 2x^3 + x^4 + 0x^4 = e_5$,

$e_6^2 = (5 + 6x + x^2 + 2x^3 + x^4 + 6x^5)^2 = 4 + 4x + 4x^2 + 4x^3 + 6x^5 + 1 + 2x +$

$4x^2 + 5x^3 + x^4 + 0x^5 = e_6,$

Также, очевидно, что $e_1 + e_2 + e_3 + e_4 + e_5 + e_6 = 1$.

Список литературы:

1. Кострикин А.Н. Введение в алгебру. Часть III. Основные структуры. 2-е изд. -М.:Физико-математическая литература, 2001.-272 с

2. Лидл, Р. Конечные поля - М.: Мир, 1988. - 821 с.

3. R.A. Ferraz, C. Polcino Milies, Idempotents in group algebras and minimal abelian codes, Finite Fields and their Applications, 2007, V. 13, P. 382-393.

4. C.R.G. Vergara F.E.B.Martinez, Paper Wedderburn decomposition of some special rational group algebras // Lectures on Matematics, 2002, 99–106 p.

5. R. A. Ferraz, M. Guerreiro, C. P. Milies: G -Equivalence in Group Algebras and Minimal Abelian Codes. IEEE Transactions on Information Theory 60(1), 2014 252-260

6. F.E. Brochero Martínez, Structure of Finite dihedral group algebra, arXiv:1405.3716 ,2014, 8 p.

7. Мишурин В.Г. Конечные групповые алгебры, дипломная работа, КФУ, 2013, 36 с

8. Смирнова Д.Ю. Абелевы коды, дипломная работа, КФУ, 2013, 34 с