МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ.
НОВОСИБИРСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ.
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

А. В. Заварницин, Д. О. Ревин

ТЕОРИЯ ПРЕДСТАВЛЕНИЙ И ХАРАКТЕРОВ

Новосибирск

2011 г.

УДК 512

Заварницин А. В., Ревин Д. О. Теория представлений и характеров / Новосиб. гос. ун-т. Новосибирск, 2011. 124 с.

В основе предлагаемого читателю учебного пособия лежит содержание одноименного спецкурса, в течение нескольких лет читаемого авторами для студентов и аспирантов механико-математического факультета Новосибирского государственного университета. Суть теории представлений можно кратко выразить как изучение конечных групп теоретико-кольцевыми методами. Предлагаемое пособие знакомит читателя с основами этой теории, связью между теорией обыкновенных и модулярных представлений и включает в себя изучение таких понятий, как брауэровы характеры, p-блоки, дефектные группы. Пособие предназначено для студентов и аспирантов математических специальностей университетов.

Рецензент
д-р физ.-мат. наук профессор А. В. Васильев

Подготовлено в рамках реализации программы развития НИУ-НГУ.

Содержание

Предисловие

Суть теории представлений можно кратко выразить как изучение конечных групп теоретико-кольцевыми методами.

Групповые модули и представления над полями конечной характеристики естественно возникают при исследовании подгрупповой структуры данной группы.

Уже в самом начале своего существования теория представлений и характеров продемонстрировала свою мощь, позволив получить ряд исключительно важных результатов теории групп (теорема Бернсайда о разрешимости групп порядка $p^\alpha q^\beta$, теорема о строении групп Фробениуса, теорема Брауэра-Фаулера о конечности числа конечных групп с данным централизатором инволюции и т.д.), причём некоторые из этих результатов до сих пор не имеют чисто теоретико-группового доказательства. В XX веке теория конечных групп сделала огромный рывок. Классификация простых конечных групп и многие другие глубокие результаты были получены с использованием теории представлений и характеров.

Предлагаемое пособие знакомит читателя с основами этой теории, её связью с теорией обыкновенных представлений и предполагает изучение таких понятий, как брауэровы характеры, p-блоки, дефектные группы. В числе прочего, излагается доказательство двух первых основных теорем Брауэра.

Курс предполагает знакомство с алгеброй в объёме стандартной университетской программы для студентов-математиков, основами теории групп и теории полей. Пособие содержит большое число примеров и упражнений, что по мысли авторов должно способствовать лучшему усвоению материала. Упражнения помечены символом ✎. В приложении Б можно найти решения некоторых из них.

1. Используемые обозначения и понятия

Базовые понятия и сведения из теории групп можно найти, например, в [1].

Используемые нами обозначения в основном стандартны.

Конечное поле из q элементов обозначается через $\mathbb{F}_q$.

$\mathbb{Q}$ — поле рациональных чисел.

Через δ_{ij} обозначается *символ Кронекера*, который определяется равенством

$$\delta_{ij} = \begin{cases} 1, & \text{при } i = j; \\ 0, & \text{при } i \neq j. \end{cases}$$

Для матрицы M её транспонированную матрицу будем обозначать через $M^\top$. Если M — квадратная невырожденная матрица, то будем обозначать через M^ι матрицу $(M^{-1})^\top = (M^\top)^{-1}$ и называть её *обратно-транспонированной* к M.

Тривиальной называется группа, состоящая только из нейтрального элемента. При мультипликативной (аддитивной) записи операции нейтральный элемент группы G, а также иногда и тривиальную группу, мы будем обозначать символом 1 (соответственно, символом 0). *Центр* группы G, т. е. множество $\{z \in G \mid zg = gz \text{ для всех } g \in G\}$, обозначается через $Z(G)$. Если $\varphi : G \to H$ — гомоморфизм групп, то $\ker \varphi = \{g \in G \mid g\varphi = 1\}$. Для элементов $g, h \in G$ положим $h^g = g^{-1}hg$. Два элемента $x, y \in G$ называются *сопряжёнными*, если существует $g \in G$ такой, что $y = x^g$. Сопряжённость элементов является отношением эквивалентности в группе G. *Классом сопряжённости x^G, содержащим элемент* $x \in G$ называется класс эквивалентности, которому принадлежит x. Будем обозначать через $\mathscr{K}(G)$ множество всех классов сопряжённости группы G, а через $x_{_K}$ — представитель класса $K \in \mathscr{K}(G)$.

Термин «собственный» в отношении подгруппы (идеала, подкольца, подмножества и т. п.) N группы (кольца, множества и т. п.) M означает, что $N \neq M$.

Под термином *максимальная* (соответственно, *минимальная*) подгруппа подразумевается максимальный (соответственно, минимальный) по включению элемент среди всех собственных (соответственно, нетривиальных) подгрупп данной группы. Аналогичная терминология будет использоваться также и в отношении колец, идеалов, модулей и т. п.

Пусть G — группа, M — множество. Будем говорить, что G *действует* на M, если для любых $m \in M$, $g \in G$ однозначно определён элемент $mg \in M$ так, что выполнены условия $m1 = m$ и $(mg)h = m(gh)$ для произвольных $m \in M$, $g, h \in G$. Если, кроме того, для любых $m_1, m_2 \in M$ существует $g \in G$ такой, что $m_1 g = m_2$, то говорят, что G действует на M *транзитивно*.

2. Кольца и модули

Теперь напомним необходимые определения и введём некоторые обозначения, связанные с кольцами.

✓ Термин «кольцо» всегда будет обозначать ассоциативное кольцо с единицей.

Пусть R — кольцо. Единицу и ноль этого кольца будем обозначать символами 1_R и 0_R, соответственно, или просто 1 и 0, если из контекста ясно, о каком кольце идёт речь.[1)] Аддитивная подгруппа S в R называется *подкольцом* (обозначается $S \leqslant R$), если $1_R \in S$ и для любых $a, b \in S$ выполнено $ab \in S$. В частности, S является кольцом и $1_S = 1_R$. Примером подкольца в произвольном кольце R является его *центр*

$$\mathrm{Z}(R) = \{z \in R \mid zr = rz \text{ для всех } r \in R\}.$$

Аддитивная подгруппа I в R называется *левым* (*правым*) *идеалом* и обозначается $I \trianglelefteq_l R$ ($I \trianglelefteq_r R$), если для любых $a \in I$, $r \in R$ выполнено $ra \in I$ (соответственно $ar \in I$). Подмножество $I \subseteq R$, одновременно являющееся левым и правым идеалом, называется *двусторонним идеалом* или просто *идеалом* и обозначается $I \trianglelefteq R$.

✎ **(2.1)** Когда подкольцо является идеалом кольца? Когда центр является идеалом? Когда идеал является подкольцом? Когда $\{0_R\}$ является подкольцом в R?

(2.2) Примеры колец, подколец и идеалов

1. $\mathbb{Z}$ — кольцо целых чисел. Идеалы кольца $\mathbb{Z}$ исчерпываются множествами $n\mathbb{Z}$ целых чисел, кратных произвольному числу n.

2. $\mathbb{Z}_n$ — кольцо вычетов по модулю n. Идеалы $\mathbb{Z}_n$ исчерпываются множествами вычетов по модулю n элементов из $m\mathbb{Z}$ для произвольного числа m.

---

1) Мы не предполагаем, что $1_R \neq 0_R$.

3. Пусть V — абелева группа. Множество $\mathrm{End}(V)$ её эндоморфизмов является кольцом относительно операций поэлементного сложения и композиции, т. е. $v(\varphi+\psi) = v\varphi+v\psi$ и $v(\varphi\psi) = (v\varphi)\psi$ для произвольных $v \in V$, $\varphi, \psi \in \mathrm{End}(V)$. Если одновременно V является векторным пространством над полем F, то кольцо линейных преобразований $\mathrm{End}_F(V)$ этого пространства будет подкольцом[2)] в $\mathrm{End}(V)$.

4. $R[x_1, \ldots, x_n]$ — кольцо многочленов от n переменных над произвольным коммутативным кольцом R. Многочлены без свободного члена образуют идеал в $R[x_1, \ldots, x_n]$.

5. $M_n(R)$ — кольцо матриц размера $n \times n$ над произвольным кольцом R. Центр $\mathrm{Z}(\mathrm{M}_n(R))$ совпадает с множеством скалярных матриц с элементами из $\mathrm{Z}(R)$. Если R — поле, то единственным ненулевым идеалом кольца $\mathrm{M}_n(R)$ является само это кольцо. Единицу этого кольца будем часто обозначать символом $\mathbf{1}_n$ или просто $\mathbf{1}$, а ноль — символом $\mathbf{0}_n$ или просто $\mathbf{0}$.

6. Множество $\mathscr{P}(X)$ всех подмножеств некоторого множества X является кольцом относительно операций симметрической разности и пересечения. Напомним, что *симметрической разностью* множеств A и B называется множество
$$A \triangle B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$
Пусть $A \subseteq X$. Тогда $\{\varnothing, X, A, X \setminus A\} \leqslant \mathscr{P}(X)$ и $\mathscr{P}(A) \trianglelefteq \mathscr{P}(X)$. Другим примером идеала в $\mathscr{P}(X)$ служит множество всех конечных подмножеств множества A.

✎ Проверить сформулированные в (2.2) утверждения.

(2.3) Предложение. *Любой собственный правый* (*левый, двусторонний*) *идеал кольца R содержится в некотором максимальном правом* (*левом, двустороннем*) *идеале.*

✎ Доказать предложение (2.3). (*Указание.* Использовать лемму Цорна и тот факт, что R содержит единицу 1_R.)

Для любого кольца R можно определить *противоположное кольцо* R^{op}, аддитивная группа которого та же, что и у R, а произведение r на s равно sr для любых $r, s \in R^{op}$. Ясно, что $(R^{op})^{op} = R$ для произвольного кольца R, и $R^{op} = R$ для коммутативного кольца R. Кроме того, левые (правые) идеалы кольца R являются правыми (левыми) идеалами кольца R^{op}.

Легко видеть, что если S — подкольцо, а I — правый (левый, двусторонний) идеал некоторого кольца, то $S \cap I$ — правый (левый, двусторонний) идеал кольца S. Отметим также, что пересечение произвольного семейства подколец (левых, правых, двусторонних идеалов) кольца снова является подкольцом (левым, правым, двусторонним идеалом).

Если S — подкольцо кольца R и $X \subseteq R$, то обозначим через $S[X]$ наименьшее подкольцо в R, содержащее S и X. Будем называть $S[X]$ *подкольцом* кольца R, *порождённым S и X* или *подкольцом, полученным присоединением к S элементов множества X*. В случае, когда множество $X = \{r_1, \ldots, r_n\}$ конечно, будем для краткости писать $S[r_1, \ldots, r_n]$ вместо $S[\{r_1, \ldots, r_n\}]$. Легко показать, что $S[r_1, \ldots, r_n] = S[r_1, \ldots, r_{n-1}][r_n]$.

Аналогично, если $K \leqslant F$ — расширение полей и $X \subseteq F$, то $K(X)$ — наименьшее подполе поля F, содержащее K и X. Будем называть $K(X)$ *подполем* поля F, *порождённым K и X* или *подполем поля F, полученным присоединением к K элементов множества X*. Для $a_1, \ldots, a_n \in F$ обозначим $K(\{a_1, \ldots, a_n\}) = K(a_1, \ldots, a_n)$. Как и в случае колец, легко проверить, что $K(a_1, \ldots, a_n) = K(a_1, \ldots, a_{n-1})(a_n)$.

✎ **(2.4)** Проверить следующие утверждения.

(*i*) Пусть R — коммутативное кольцо, $S \leqslant R$ и $r_1, \ldots, r_n \in R$. Тогда подкольцо $S[r_1, \ldots, r_n]$ состоит из всевозможных значений многочленов $f(r_1, \ldots, r_n)$, где f пробегает $S[x_1, \ldots, x_n]$.

(*ii*) Пусть $K \leqslant F$ — расширение полей и $a_1, \ldots, a_n \in F$. Тогда подполе $K(a_1, \ldots, a_n)$ состоит из значений выражения $f(a_1, \ldots, a_n)/g(a_1, \ldots, a_n)$, где $f, g \in K[x_1, \ldots, x_n]$ и $g(a_1, \ldots, a_n) \neq 0$.

✎ **(2.5)** Описать подкольца поля $\mathbb{Q}$. (*Указание.* Рассмотреть кольца $\mathbb{Z}[\pi^{-1}] = \mathbb{Z}[\,\frac{1}{p} \mid p \in \pi]$, где π — некоторое подмножество множества всех простых целых чисел.)

[2)] Аналогичные примеры подколец в $\mathrm{End}(V)$ можно получить, если рассмотреть все эндоморфизмы, сохраняющие на V какую-либо другую дополнительную структуру (модуля, кольца, и т. п.).

(2.6) Определение. Пусть X — подмножество кольца R. Правым (левым, двусторонним) идеалом из R, *порождённым множеством* X, называется наименьший правый (левый, двусторонний) идеал из R, содержащий X.[3] Легко видеть, что такой идеал совпадает с множеством всевозможных конечных сумм[4] вида $\sum x_i r_i$ в случае правого идеала, вида $\sum r_i x_i$ в случае левого идеала, и вида $\sum r_i x_i s_i$ в случае двустороннего идеала, где $r_i, s_i \in R$, $x_i \in X$.

Если $X = \{x_1, \ldots, x_n\}$ — конечное множество, то правый (левый) идеал, порождённый X, обозначается через $x_1R + \ldots + x_nR$ (соответственно, $Rx_1 + \ldots + Rx_n$), а двусторонний идеал, порождённый X, — через $Rx_1R + \ldots + Rx_nR$. Здесь выражение RxR обозначает множество конечных сумм вида $\sum r_i x s_i$, где $r_i, s_i \in R$.

Пусть $I_1, \ldots, I_n$ – правые (левые, двусторонние) идеалы кольца R. *Суммой идеалов* $I_1, \ldots, I_n$ называется множество

$$I_1 + \ldots + I_n = \{\, r_1 + \ldots + r_n \;\big|\; r_i \in I_i,\ i = 1, \ldots, n\},$$

а *произведением* $I_1 \cdot \ldots \cdot I_n$ называется множество всевозможных конечных сумм произведений $r_1 \cdot \ldots \cdot r_n$, где $r_i \in I_i$, $i = 1, \ldots, n$.

Легко видеть, что сумма, произведение, а также пересечение правых (левых, двусторонних) идеалов снова будет правым (левым, двусторонним) идеалом. В частности, для правого (левого, двустороннего) идеала I из R определены степени I^n для произвольного $n > 0$. Если $n = 0$, то положим по определению $I^0 = R$.

Заметим, что для произвольных двусторонних идеалов $I_1, \ldots, I_n$ из R имеет место включение

$$I_1 \cdot \ldots \cdot I_n \leqslant I_1 \cap \ldots \cap I_n.$$

Правый (левый) идеал $I \trianglelefteqslant_r R$ называется *нильпотентным*, если $I^n = 0$ для некоторого n. Отметим, что $I^n = 0$ тогда и только тогда, когда любое произведение n элементов из I равно нулю.

Элемент $r \in R$ называется *обратимым справа*, если у него есть *правый обратный*, т. е. такой элемент $s \in R$, что $rs = 1_R$. *Обратимый слева* элемент определяется аналогичным образом. Обратимый справа и слева элемент называется просто *обратимым*.

(2.7) Предложение. *Собственный (правый, левый) идеал кольца не содержит обратимых (справа, слева) элементов и, в частности, единицу.*

✎ Доказать предложение (2.7).

✓ Существуют примеры колец, в которых собственный правый идеал содержит обратимый слева элемент.

✎ **(2.8)** Доказать, что у обратимого элемента $r \in R$ любой правый обратный совпадает с любым левым обратным. Этот однозначно определённый элемент называется просто *обратным* к r и обозначается r^{-1}.

Для кольца R положим

$$R^{\times} = \{r \in R \mid r \text{ обратим}\}.$$

(2.9) Предложение. *Пусть R — кольцо. Тогда*

(i) $R^{\times}$ *— группа;*

(ii) $\mathrm{Z}(R)^{\times} = \mathrm{Z}(R) \cap R^{\times}$*;*

(iii) $\mathrm{Z}(R)^{\times} \leqslant \mathrm{Z}(R^{\times})$.

✎ Доказать предложение (2.9).

Множество $R^{\times}$, являющееся группой ввиду (2.9)(i), называется *группой обратимых элементов* кольца R.

В связи с (2.9)(iii) отметим, что для произвольного кольца R включение $\mathrm{Z}(R^{\times}) \leqslant \mathrm{Z}(R)^{\times}$, вообще говоря, не имеет места. См., однако, (2.31).

Кольцо R называется *телом*, если $R^{\times} = R \setminus \{0\}$.

(2.10) Предложение. (i) *Если все ненулевые элементы ненулевого кольца R обратимы справа (слева), то R является телом.*

(ii) *Если $I \trianglelefteqslant R$ и в $R \setminus I$ любой элемент обратим справа, то в $R \setminus I$ любой элемент также обратим и слева.*

---

[3] В частности, из определения вытекает, что правый (левый, двусторонний) идеал, порождённый пустым множеством, нулевой.

[4] Здесь и далее мы естественно предполагаем, что сумма нулевого числа слагаемых равна нулю.

✎ Доказать предложение (2.10).

✎ **(2.11)** Показать, что если идеал кольца является максимальным как правый идеал, то он также является максимальным как левый идеал, и факторкольцо по нему является телом.

Элемент $r \in R$ называется *нильпотентным*, если $r^n = 0$ для некоторого n. Из сказанного выше вытекает, что любой правый (левый) нильпотентный идеал кольца R состоит из нильпотентных элементов. Заметим также, что для нильпотентного элемента r элемент $1 - r$ обратим, поскольку

$$(1-r)(1+r+\ldots+r^{n-1}) = (1+r+\ldots+r^{n-1})(1-r) = 1.$$

✎ **(2.12)** Найти нильпотентные элементы кольца $\mathbb{Z}_n$.

Пусть R, S – кольца. Гомоморфизм $\varphi : R \to S$ аддитивных групп этих колец будем называть *гомоморфизмом колец*, если он сохраняет умножение, т. е. $(xy)\varphi = (x\varphi)(y\varphi)$ для любых $x, y \in R$, а также сохраняет единицу: $(1_R)\varphi = 1_S$.

(2.13) Символы отображений и, в частности, морфизмов мы будем писать как справа, так и слева от аргумента. Так, при левой форме записи гомоморфизм колец удовлетворяет условию $\varphi(xy) = \varphi(x)\varphi(y)$. Для композиции отображений также будут использоваться различные виды записи. Запись $\varphi\psi$ композиции отображений $\varphi : X \to Y$ и $\psi : Y \to Z$ является «правой», т. е. $x(\varphi\psi) = (x\varphi)\psi$, а запись $\psi \circ \varphi$ — «левой», т. е. $(\psi \circ \varphi)(x) = \psi(\varphi(x))$.

Отметим, что для гомоморфизма колец $\varphi : R \to S$ ядро $\operatorname{Ker}\varphi$ является идеалом в R, а образ $\operatorname{Im}\varphi$ — подкольцом в S. Сюръективные гомоморфизмы называются *эпиморфизмами*, инъективные — *мономорфизмами*, а биективные *изоморфизмами*. Легко проверить, что гомоморфизм φ инъективен тогда и только тогда, когда $\operatorname{Ker}\varphi = \{0\}$. Любой изоморфизм $R \to R$ называется *автоморфизмом* кольца R.

(2.14) Предложение. *Пусть R, S, T — кольца.*

(*i*) *Если $\varphi : R \to S$ и $\psi : R \to T$ — гомоморфизмы, причём φ — эпиморфизм и $\operatorname{Ker}\varphi \subseteq \operatorname{Ker}\psi$, то существует единственный гомоморфизм $\tau : S \to T$ такой, что $\psi = \varphi\tau$.*

$$\begin{tikzcd} R \arrow[r, "\psi"] \arrow[d, "\varphi"'] & T \\ S \arrow[ur, dotted, "\tau"'] & \end{tikzcd}$$

(*ii*) *Если $\varphi : S \to R$ и $\psi : T \to R$ — гомоморфизмы, причём φ — мономорфизм и $\operatorname{Im}\varphi \supseteq \operatorname{Im}\psi$, то существует единственный гомоморфизм $\tau : T \to S$ такой, что $\psi = \tau\varphi$.*

$$\begin{tikzcd} R & T \arrow[l, "\psi"'] \arrow[dl, dotted, "\tau"] \\ S \arrow[u, "\varphi"] & \end{tikzcd}$$

✎ Доказать предложение (2.14).

Для колец R, S гомоморфизм (изоморфизм) $\varphi : R \to S$ их аддитивных групп называется *антигомоморфизмом* (*антиизоморфизмом*) *колец*, если $(1_R)\varphi = 1_S$ и $(xy)\varphi = (y\varphi)(x\varphi)$ для любых $x, y \in R$. Антиизоморфизм $R \to R$ называется *антиавтоморфизмом* кольца R.

Например, антиавтоморфизмом матричного кольца $\mathrm{M}_n(R)$ является отображение $A \to A^\top$ для всех $A \in \mathrm{M}_n(R)$.

✎ **(2.15)** Проверить следующие утверждения.

(*i*) Композиция двух антигомоморфизмов колец является гомоморфизмом, а композиция гомоморфизма и антигомоморфизма (в произвольном порядке) является антигомоморфизмом.

(*ii*) Гомоморфизм (антигомоморфизм) $\varphi : R \to S$ осуществляет антигомоморфизмы (гомоморфизмы) $R \to S^{op}$ и $R^{op} \to S$.

(*iii*) Отображение, обратное к антиизоморфизму, является антиизоморфизмом.

(*iv*) Тождественное отображение $R \to R$ является антиавтоморфизмом тогда и только тогда, когда кольцо R коммутативно.

Для двустороннего идеала $I \trianglelefteq R$ на факторгруппе R/I вводится умножение $(x+I)(y+I) = xy + I$. Корректность этого умножения и аксиомы кольца для R/I легко проверяются. Кольцо R/I называется *факторкольцом* кольца R по идеалу I.

Существует конструкция, позволяющая строить новые кольца из уже имеющихся.

(2.16) Определение. Пусть $R_1, \ldots, R_n$ — кольца. Их *прямой суммой* $R_1 \oplus \ldots \oplus R_n$ называется множество

$$\{(r_1, \ldots, r_n) \mid r_i \in R_i, \quad i = 1, \ldots, n\}$$

с покомпонентными операциями сложения и умножения элементов. Ясно, что прямая сумма колец будет кольцом.

Положим $R = R_1 \oplus \ldots \oplus R_n$. Для каждого $i = 1, \ldots, n$ рассмотрим множество I_i элементов из R вида $(0, \ldots, 0, r, 0, \ldots, 0)$, где все компоненты с номерами, отличными от i, нулевые, а r пробегает все элементы кольца R_i. Легко видеть, что $I_i \trianglelefteq R$. Кроме того, каждый идеал I_i является кольцом (но, вообще говоря, не подкольцом в R), изоморфным R_i. Поэтому в дальнейшем мы часто будем отождествлять R_i с I_i. Отметим, что кольцо R совпадает с суммой $I_1 + \ldots + I_n$. Кроме того, для любого $i = 1, \ldots, n$ пересечение I_i с суммой $\sum\limits_{j \neq i} I_j$ тривиально. Последнее свойство позволяет наряду с данным выше определением «внешней» прямой суммы колец ввести понятие «внутренней» прямой суммы идеалов кольца.

Пусть $I_1, \ldots, I_n$ – правые (левые, двусторонние) идеалы кольца R. Сумма $I_1 + \ldots + I_n$ называется *прямой*, если для любого $i = 1, \ldots, n$ пересечение идеала I_i с суммой $\sum\limits_{j \neq i} I_j$ тривиально.

(2.17) Предложение. *Пусть R — кольцо, совпадающее с прямой суммой своих правых (левых, двусторонних) идеалов $I_1, \ldots, I_n$. Тогда справедливы следующие утверждения.*

- (i) *Каждый элемент $r \in R$ однозначно представляется в виде суммы $r = r_1 + \ldots + r_n$, где $r_i \in I_i$. В частности, $1_R = e_1 + \ldots + e_n$ для некоторых $e_i \in I_i$, $i = 1, \ldots, n$.*
- (ii) *Для каждого $i, j = 1, \ldots, n$ имеем $e_i^2 = e_i$ и $e_i e_j = e_j e_i = 0$ при $i \neq j$.*
- (iii) *Каждый идеал I_i, $i = 1, \ldots, n$, совпадает с идеалом $e_i R$ (соответственно, Re_i, Re_iR).*

Если все идеалы $I_1, \ldots, I_n$ двусторонние, то дополнительно справедливы следующие утверждения.

- (iii) $e_1, \ldots, e_n \in \mathrm{Z}(R)$.
- (iv) *Каждый идеал I_i является кольцом, а e_i — его единицей.*
- (v) *Имеет место изоморфизм колец $R \cong I_1 \oplus \ldots \oplus I_n$.*

✎ Доказать предложение (2.17).

Прямую сумму идеалов $I_1, \ldots, I_n$ будем обозначать $I_1 \oplus \ldots \oplus I_n$. Такая запись в случае двусторонних идеалов не вызовет недоразумений, поскольку, в силу предложения (2.17)(v), понятия прямой суммы колец и прямой суммы идеалов по существу эквивалентны. В случае же односторонних идеалов эта запись согласуется с вводимым далее определением прямой суммы R-модулей, см. (2.30).

Элемент e кольца R называется *идемпотентом*, если $e^2 = e$. Идемпотент называется *центральным* , если он лежит в центре $\mathrm{Z}(R)$. Два идемпотента e и f называются *ортогональными*, если $ef = fe = 0$. Легко видеть, что сумма двух ортогональных идемпотентов снова будет идемпотентом. Идемпотент кольца называется *примитивным*, если он не представим в виде суммы двух ненулевых ортогональных идемпотентов.[5)]

Из предложения (2.17) видно, что разложение кольца R в прямую сумму идеалов $I_1 \oplus \ldots \oplus I_n$ однозначно определяет разложение единицы 1_R в сумму ортогональных идемпотентов $e_1 + \ldots + e_n$, которые являются центральными в случае, если идеалы $I_1, \ldots, I_n$ двусторонние. С другой стороны, как показывают следующие два предложения, наличие кольце R (центрального) идемпотента, отличного от нуля и единицы, определяет разложение R в прямую сумму собственных (двусторонних) идеалов.

(2.18) Предложение. *Если R — кольцо и $e_1, \ldots, e_n \in R$ — центральные попарно ортогональные идемпотенты, то справедливы следующие утверждения.*

- (i) $e_i R \trianglelefteq R$, $i = 1, \ldots, n$.
- (ii) $e_1 + \ldots + e_n$ *— центральный идемпотент.*
- (iii) *Если $e_1 + \ldots + e_n = 1_R$, то $R = e_1 R \oplus \ldots \oplus e_n R$.*
- (iv) $\mathrm{Z}(e_i R) = e_i \mathrm{Z}(R)$, $i = 1, \ldots, n$.

✎ Доказать предложение (2.18).

[5)] В частности, нулевой идемпотент примитивен.

(2.19) Предложение. *Если R — кольцо и $e \in R$ — идемпотент, то*

(i) *элемент $1-e$ также является идемпотентом и $e(1-e) = (1-e)e = 0$,*

(ii) $R = eR \oplus (1-e)R$,

(iii) *подмножество $eRe = \{ere \mid r \in R\}$ является кольцом, а идемпотент e — единицей этого кольца.*

✎ Доказать предложение (2.19).

(2.20) Предложение. *Пусть R — кольцо.*

(i) *Если $R = I_1 \oplus \ldots \oplus I_n$, где $I_i \trianglelefteq R$, $i = 1, \ldots, n$, и $I \trianglelefteq_r R$, то $I = (I \cap I_1) \oplus \ldots \oplus (I \cap I_n)$.*

(ii) *Если $R = I_1 \oplus \ldots \oplus I_n$, где $I_i \trianglelefteq_r R$, $i = 1, \ldots, n$, и $I \trianglelefteq R$, то $I = (I \cap I_1) \oplus \ldots \oplus (I \cap I_n)$.*

✎ Доказать предложение (2.20).

(2.21) Предложение. *Пусть $R_1, \ldots, R_n$ — кольца и $R = R_1 \oplus \ldots \oplus R_n$. Тогда*

(i) $\mathrm{Z}(R_i) \trianglelefteq \mathrm{Z}(R)$ *для всех $i = 1, \ldots, n$.*

(ii) $\mathrm{Z}(R) = \mathrm{Z}(R_1) \oplus \ldots \oplus \mathrm{Z}(R_n)$;

✎ Доказать предложение (2.21)

(2.22) Предложение. *Пусть R — кольцо и*

$$R = I_1 \oplus \ldots \oplus I_m = J_1 \oplus \ldots \oplus J_n,$$

где I_i, J_j — ненулевые двусторонние идеалы из R, не представимые в виде прямой суммы меньших ненулевых двусторонних идеалов. Тогда $m = n$ и существует подстановка σ на множестве индексов $\{1, \ldots, m\}$ такая, что $I_i = J_{i\sigma}$ для всех $i = 1, \ldots, m$.

✎ Доказать предложение (2.22).

(2.23) Определение. Пусть R — кольцо. Абелева группа M с аддитивной записью операции называется *левым R-модулем*, если для любых $m \in M$ и $r \in R$ однозначно определён элемент $rm \in M$, и для произвольных $m, n \in M$ и $r, s \in R$ выполнены условия

$$\begin{gathered} r(m+n) = rm + rn, \\ (r+s)m = rm + sm, \\ (rs)m = r(sm), \\ 1_R\, m = m. \end{gathered}$$

Аналогичным образом, путём умножения справа на элементы из R, определяется *правый R-модуль*.

✓ В случае, когда R — поле, определение левого R-модуля становится обычным определением векторного пространства над этим полем.

✓ Часто R-модули, R-подмодули, R-гомоморфизмы, и т. д. мы будем называть просто модулями, подмодулями, гомоморфизмами, и т. д., если из контекста ясно, о чём идёт речь.

Для кольца R, обладающего антиавтоморфизмом φ, левый R-модуль M можно превратить в правый R-модуль, положив $mr = (r\varphi)m$ для всех $r \in R$ и $m \in M$. В частности, если R коммутативно, то можно положить $mr = rm$ для $r \in R$ и $m \in M$.

(2.24) Примеры модулей

1. Левый (правый) идеал произвольного кольца R является левым (правым) R-модулем. В частности, само кольцо R является левым (правым) R-модулем, который обозначается через ${}^\circ R$ (соответственно, через R°) и называется *регулярным левым* (*правым*) *R-модулем.*

2. Произвольная абелева группа A является одновременно левым и правым $\mathbb{Z}$-модулем.

3. Произвольное кольцо является левым и правым модулем над любым своим подкольцом.

4. При правой (левой) записи отображений, см. (2.13), векторное пространство V над полем F является правым (левым) модулем над кольцом $\mathrm{End}_F(V)$ всех своих линейных преобразований.

5. Пространство строк (столбцов) длины n над полем F является правым (левым) $\mathrm{M}_n(F)$-модулем.

6. Для произвольного множества X абелева группа $\mathscr{P}(X)$ с операцией симметрической разности является $\mathbb{Z}_2$-модулем, если для любого $A \in \mathscr{P}(X)$ положить $0A = \varnothing$ и $1A = A$.

✎ Проверить сформулированные в (2.24) утверждения.

✎ **(2.25)** В случае, когда X — n-элементное множество, найти базис и размерность $\mathscr{P}(X)$ как векторного пространства над полем $\mathbb{Z}_2$.

✓ В дальнейшем определения, дающиеся только для левых модулей, аналогично формулируются и для правых модулей.

(2.26) *Подмодулем* левого R-модуля M называется такая подгруппа $N \leqslant M$, что для любых $n \in N$ и $r \in R$ выполнено $rn \in N$. Если N — подмодуль в M, то на факторгруппе M/N можно естественным образом задать структуру левого R-модуля (называемого *фактормодулем* M по N), полагая $r(m+N) = rm+N$ для любых $m \in M$, $r \in R$.

Пусть M, N — левые R-модули. Гомоморфизм $\varphi : M \to N$ абелевых групп такой, что для любых $m \in M$ и $r \in R$ выполнено $(rm)\varphi = r(m\varphi)$ называется *гомоморфизмом R-модулей* (или *R-линейным отображением*). Множество всех R-линейных отображений $\varphi : M \to N$ обозначается через $\mathrm{Hom}_R(M, N)$. Для любых $\varphi, \psi \in \mathrm{Hom}_R(M, N)$ определим $\varphi+\psi$, положив $m(\varphi+\psi) = m\varphi+m\psi$ для любого $m \in M$. Тем самым на $\mathrm{Hom}_R(M, N)$ задана структура[6] абелевой группы.

✎ **(2.27)** Пусть M — левый (правый) R-модуль и $H = \mathrm{Hom}_R({}^\circ R, M)$ (соответственно, $H = \mathrm{Hom}_R(R^\circ, M)$). Зададим на абелевой группе H умножение слева (справа) на элементы из R по правилу $s(r \cdot \varphi) = r(s\varphi)$ (соответственно, $s(\varphi r) = (rs)\varphi$) для любых $\varphi \in H$, $r, s \in R$. Показать, что тем самым на H корректно задана структура левого (правого) R-модуля и имеет место изоморфизм R-модулей $H \cong M$.

✎ **(2.28)** Пусть M — левый (правый) R-модуль и $M^* = \mathrm{Hom}_R(M, {}^\circ R)$ $\big($соответственно, $M^* = \mathrm{Hom}_R(M, R^\circ)\big)$. Зададим на абелевой группе M^* умножение справа (слева) на элементы из R по правилу $m(\varphi r) = (rm)\varphi$ (соответственно, $m(r\varphi) = r(m\varphi)$) для любых $\varphi \in M^*$, $m \in M$, $r \in R$. Показать, что тем самым на M^* корректно задана структура правого (левого) R-модуля, который будем называть *двойственным к R-модулю M*.

Гомоморфизм модуля M в себя называется *эндоморфизмом* R-модуля M. Множество всех эндоморфизмов модуля M, обозначаемое $\mathrm{End}_R(M)$, образует кольцо, умножением в котором является композиция отображений. Легко видеть, что при правой записи отображений M является правым $\mathrm{End}_R(M)$-модулем относительно естественного действия.

✎ **(2.29)** Пусть R — кольцо. Показать, что

(i) кольца $\mathrm{End}_R(R^\circ)$ и R антиизоморфны;

(ii) для любого идемпотента $e \in R$ кольца $\mathrm{End}_R(eR)$ и eRe антиизоморфны.

Если для R-модулей M и N существует взаимно однозначный гомоморфизм, то он называется *изоморфизмом*. В этом случае будем говорить, что модули M и N *изоморфны* и писать $M \cong N$.

Пусть $N_1, \ldots, N_s$ — подмодули левого R-модуля M. Их *суммой* $N_1 + \ldots + N_s$ называется подмножество $\{\, n_1 + \ldots + n_s \mid n_i \in N_i,\ i = 1, \ldots, s\}$. Очевидно, что $N_1 + \ldots + N_s$ является наименьшим подмодулем модуля M, содержащим подмодули $N_1, \ldots, N_s$. Сумма подмодулей $N_1, \ldots, N_s$ называется *прямой* , если для любого $i = 1, \ldots, s$ пересечение подмодуля N_i с суммой $\sum_{j\neq i} N_j$ тривиально. Прямая сумма подмодулей обозначается $N_1 \oplus \ldots \oplus N_s$.

(2.30) Как и для колец, для R-модулей $M_1, \ldots, M_s$ можно определить внешним образом *прямую сумму* $M = M_1 \oplus \ldots \oplus M_s$. При этом каждый из модулей $M_1, \ldots, M_s$ можно естественным образом отождествить с подмодулем модуля M так, что M будет совпадать с прямой суммой таких подмодулей.

Если X — подмножество левого R-модуля M, то подмодулем, *порождённым* X, называется наименьший подмодуль из M, содержащий X.

✓ Введённые понятия, в частности, согласуются с данными ранее определениями суммы и прямой суммы левых (правых) идеалов кольца, а также с определением идеала, порождённого множеством.

[6] На группе $\mathrm{Hom}_R(M, N)$ задать структуру левого R-модуля, вообще говоря, нельзя.

(2.31) Предложение. *Если кольцо R порождается множеством $R^\times$ как $\mathrm{Z}(R)$-модуль, то $\mathrm{Z}(R^\times) \leqslant \mathrm{Z}(R)^\times$.*

✎ Доказать предложение (2.31)

Легко видеть, что модуль M порождается множеством X тогда и только тогда, когда всякий элемент из M представим в виде конечной суммы $\sum r_i x_i$, где $r_i \in R$, $x_i \in X$. В случае, когда для любого элемента из M такое представление однозначно, множество X называется *R-базисом* или просто *базисом* модуля M. Если R — поле, то введённое понятие базиса R-модуля совпадает с обычным понятием базиса векторного пространства. В частности, в этом случае базис всегда существует, и все базисы равномощны. Если же R — не поле, то модуль M может не обладать базисом, или же обладать базисами различной мощности.

✎ **(2.32)** Привести пример кольца R и R-модуля M таких, что M не обладает R-базисом. [7)]

Модуль M, обладающий R-базисом X называется *свободным*. В этом случае мы будем говорить, что M *свободно порождается* множеством X.

✎ **(2.33)** Пусть M — свободный R-модуль с конечным R-базисом $m_1, \ldots, m_k$. Показать, что двойственный[8)] модуль M^* свободный, и множество его элементов $m_1^*, \ldots, m_k^*$ таких, что $m_i m_j^* = \delta_{ij}$, где $i, j = 1, \ldots, k$, образует R-базис, который будем называть *базисом модуля M^*, двойственным к базису* $m_1, \ldots, m_k$. В частности, в случае, когда R — поле, имеем $\dim_R M = \dim_R M^*$.

(2.34) Определение. Левый R-модуль M называется *неразложимым*, если для любых подмодулей M_1, $M_2 \leqslant M$ из равенства $M = M_1 \oplus M_2$ следует $M_1 = 0$ или $M_2 = 0$. В противном случае M называется *разложимым*.

(2.35) Предложение. *Пусть R — кольцо и $e \in R$ — идемпотент. Тогда следующие условия эквивалентны.*

(i) e — примитивный идемпотент.

(ii) Левый идеал Re (правый идеал eR) неразложим как левый (правый) R-модуль.

(iii) Единственными идемпотентами кольца eRe являются 0 и e.

✎ Доказать предложение (2.35).

Двусторонний аналог предыдущего предложения также имеет место.

(2.36) Предложение. *Пусть R — кольцо и $e \in R$ — центральный идемпотент. Тогда следующие условия эквивалентны.*

(i) e — примитивный идемпотент кольца $\mathrm{Z}(R)$.

(ii) Идеал Re не представим в виде прямой суммы двух ненулевых двусторонних идеалов из R.

✎ Доказать предложение (2.36).

Следующее предложение обобщает (2.18).

(2.37) Предложение. *Пусть R — кольцо, $e_1, \ldots, e_n \in R$ — центральные попарно ортогональные идемпотенты и M — правый R-модуль. Справедливы следующие утверждения.*

(i) Me_i — R-подмодуль в M для всех $i = 1, \ldots, n$.

(ii) Сумма $Me_1 + \ldots + Me_n$ является прямой.

(iii) Если $e_1 + \ldots + e_n = 1_R$, то $M = Me_1 \oplus \ldots \oplus Me_n$.

✎ Доказать предложение (2.37).

[7)] Пример свободного R-модуля, обладающего базисами различной мощности, приведён в [4, с. 61–62]

[8)] см. (2.28)

3. Алгебры и модули над ними

(3.1) Определение. Пусть R — коммутативное кольцо. Левый R-модуль A называется *R-алгеброй* или *алгеброй над кольцом* R, если он является кольцом и для произвольных $a, b \in A$ и $r \in R$ выполнено

$$r(ab) = (ra)b = a(rb).$$

✓ Далее до конца раздела символом R обозначается некоторое кольцо, а символом A — алгебра над (коммутативным) кольцом R.

(3.2) Примеры R-алгебр

В следующих примерах кольцо R предполагается коммутативным.

1. Кольцо $\mathrm{M}_n(R)$ является R-алгеброй.
2. Для левого R-модуля M кольцо $\mathrm{End}_R(M)$ является R-алгеброй. Умножением в алгебре $\mathrm{End}_R(M)$ является композиция отображений.
3. Для конечной группы G множество RG, состоящее из всевозможных формальных[9] R-линейных комбинаций элементов $g \in G$, т. е. элементов вида
$$\sum_{g\in G} a_g g, \quad a_g \in R$$
является R-алгеброй, которая называется *групповой алгеброй* группы G. Умножение в RG продолжает по линейности умножение в G, т. е.
$$\Big(\sum_{g\in G} a_g\Big)\Big(\sum_{g\in G} b_g\Big) = \sum_{g\in G} c_g g, \quad \text{где} \qquad c_g = \sum_{\substack{(x,y)\in G\times G\\ xy=g}} a_x b_y.$$
4. Произвольное кольцо S является R-алгеброй над любым подкольцом $R \leqslant \mathrm{Z}(S)$ своего центра. В частности, любое поле является алгеброй над любым своим подполем.
5. Произвольное кольцо является $\mathbb{Z}$-алгеброй.
6. Для произвольного множества X множество $\mathscr{P}(X)$ является $\mathbb{Z}_2$-алгеброй, см. (2.2), (2.24).
7. Для произвольного множества X обозначим через $\mathrm{f}_R(X)$ множество всех отображений $X \to R$. Для двух отображений $\varphi, \psi \in \mathrm{f}_R(X)$ естественно определяются сумма, произведение и умножение на элементы кольца R:
$$(\varphi+\psi)(x) = \varphi(x)+\psi(x), \qquad (\varphi\psi)(x) = \varphi(x)\psi(x), \qquad (r\varphi)(x) = r(\varphi(x))$$
для всех $x \in X$, $r \in R$. Относительно определённых операций множество $\mathrm{f}_R(X)$ становится коммутативной R-алгеброй, которую мы будем называть *алгеброй R-значных функций на множестве X*.

✎ Проверить сформулированные в (3.2) утверждения.

(3.3) В случае, когда A — либо R-алгебра над полем R либо групповая алгебра над кольцом, R можно отождествить с подкольцом $R\,1_A = \{r1_A \mid r \in R\}$ центра $\mathrm{Z}(A)$.

✎ **(3.4)** Показать, что для произвольных R-алгебр кольцо $R1_A$ может быть неизоморфно R.

Отметим, что для R-алгебры A противоположное кольцо A^{op} также является R-алгеброй ввиду коммутативности кольца R.

✎ **(3.5)** Показать, что групповая алгебра изоморфна своей противоположной, т. е. обладает антиавтоморфизмом.

Пусть A — R-алгебра. Подкольцо кольца A, являющееся подмодулем R-модуля A называется *подалгеброй* R-алгебры A. *Левым* (*правым, двусторонним*) *идеалом R-алгебры* A называется произвольный левый (правый, двусторонний) идеал кольца A.

[9] Слово «формальных» в данном случае означает, что две такие R-линейные комбинации равны тогда и только тогда, когда равны коэффициенты при соответствующих элементах группы G, т. е. RG свободно порождается множеством G как R-модуль.

✎ **(3.6)** Показать, что левый (правый, двусторонний) идеал R-алгебры A будет R-подмодулем R-модуля A, а подкольцо, вообще говоря, нет.

Заметим, что центр R-алгебры A всегда является подалгеброй. Исследуем более подробно центр $Z(A)$ в важном для нас случае, когда A — групповая алгебра над коммутативным кольцом. Существенную роль при этом будут играть классы сопряжённости группы.

Напомним, что через $\mathscr{K}(G)$ обозначается множество всех классов сопряжённости группы G, а через $x_{_K}$ — представитель класса $K \in \mathscr{K}(G)$.

Пусть R — коммутативное кольцо. Для $K \in \mathscr{K}(G)$ положим

$$\widehat{K} = \sum_{x \in K} x \in RG.$$

Будем называть $\widehat{K}$ *суммой класса* K или *классовой суммой*.

(3.7) Предложение. *Пусть R — коммутативное кольцо и G — конечная группа. Имеют место следующие утверждения.*

(*i*) *Если $K \in \mathscr{K}(G)$, то $\widehat{K} \in \mathrm{Z}(RG)$.*

(*ii*) *Любой элемент из $\mathrm{Z}(RG)$ однозначно представим в виде R-линейной комбинации элементов $\widehat{K}$, $K \in \mathscr{K}(G)$.*

(*iii*) *Пусть $K, L, M \in \mathscr{K}(G)$ и $z \in M$. Тогда число $a_{_{KLM}}$ всевозможных пар $(x, y) \in K \times L$ таких, что $xy = z$ не зависит от выбора z.*

(*iv*) *Если $K, L \in \mathscr{K}(G)$, то*

$$\widehat{K}\widehat{L} = \sum_{M \in \mathscr{K}(G)} a_{_{KLM}} \widehat{M}.$$

✎ Доказать предложение (3.7)

Как видно из (3.7)(*ii*), (*iv*) классовые суммы $\widehat{K}$, $K \in \mathscr{K}(G)$, являются базисом R-модуля $\mathrm{Z}(RG)$, а числа $a_{_{KLM}}$ оказываются *структурными константами* алгебры $\mathrm{Z}(RG)$ относительно этого базиса, т. е. однозначно определяют произведение произвольных элементов из $\mathrm{Z}(RG)$.

(3.8) Следствие. *Пусть R — коммутативное кольцо, S — его подкольцо и G — конечная группа. Тогда*

$$\mathrm{Z}(SG) = \mathrm{Z}(RG) \cap SG.$$

✎ **(3.9)** Доказать следствие (3.8).

(3.10) Пусть G — конечная группа. Тогда любой гомоморфизм (эпиморфизм) $\varphi : R \to S$ коммутативных колец естественным образом поднимается до кольцевого гомоморфизма (эпиморфизма) $\tilde{\varphi} : RG \to SG$ соответствующих групповых алгебр и, как следует из (3.7)(*ii*), до гомоморфизма (эпиморфизма) $\tilde{\varphi} : \mathrm{Z}(RG) \to \mathrm{Z}(SG)$ их центров.

(3.11) Предложение. *Пусть отображение $\tilde{\varphi} : RG \to SG$ (соответственно, $\tilde{\varphi} : \mathrm{Z}(RG) \to \mathrm{Z}(SG)$) определено как выше. Тогда $\operatorname{Ker}\tilde{\varphi}$ состоит из $\operatorname{Ker}\varphi$-линейных комбинаций элементов (соответственно, классовых сумм) группы G.*

✎ Доказать предложение (3.11).

(3.12) Определение. Пусть A и B — R-алгебры. Произвольное R-линейное отображение из A в B, являющееся гомоморфизмом колец, называется *гомоморфизмом R-алгебр* (или *R-гомоморфизмом*).

✓ Теория представлений группы G изучает гомоморфизмы R-алгебры RG в алгебру $\mathrm{M}_n(R)$.

Пусть I — (двусторонний) идеал R-алгебры A. Легко проверить, что структуры факторкольца и фактормодуля A/I согласованы и определяют R-алгебру, называемую *факторалгеброй* A по I. Отметим, что ядро $\operatorname{Ker}\varphi$ любого R-гомоморфизма $\varphi : A \to B$ является двусторонним идеалом в A, и имеет место R-изоморфизм $A/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$.

✓ Отметим классический изоморфизм F-алгебр $\mathrm{End}_F(V)$ и $\mathrm{M}_n(F)$, где V — n-мерное векторное пространство над полем F.

✎ **(3.13)** Показать, что для произвольного множества X имеет место изоморфизм $\mathbb{Z}_2$-алгебр $\mathscr{P}(X) \cong \mathrm{f}_{\mathbb{Z}_2}(X)$, см. (3.2), примеры 6 и 7.

✎ **(3.14)** Пусть Y — подмножество множества X и R — коммутативное кольцо. Показать, что отображение $\mathrm{f}_R(X) \to \mathrm{f}_R(Y)$, сопоставляющее каждой функции из $\mathrm{f}_R(X)$ её ограничение на Y, является сюръективным гомоморфизмом R-алгебр. Найти его ядро.

✎ **(3.15)** Пусть G — группа, $H \trianglelefteqslant G$ и $\varphi : G \to G/H$ — естественный эпиморфизм групп. Показать, что φ продолжается по линейности до эпиморфизма групповых алгебр $RG \to R(G/H)$. В случае, когда R — поле, найти размерность и базис ядра этого эпиморфизма.

✎ **(3.16)** Пусть $I \trianglelefteqslant RG$ и $\varphi : (RG)^\times \to (RG/I)^\times$ — гомоморфизм групп, являющийся ограничением на $(RG)^\times$ естественного эпиморфизма R-алгебр $RG \to RG/I$. Показать, что

(i) $\ker\varphi = \{a \in (RG)^\times \mid 1 - a \in I\}$;

(ii) $\{a \in G \mid 1 - a \in I\} \trianglelefteqslant G$.

(3.17) Определение. Пусть A — R-алгебра и V — правый A-модуль (где A рассматривается как кольцо). Наделим V структурой левого R-модуля, положив $rv = v(r1_A)$ для произвольных $v \in V$ и $r \in R$ (это можно сделать в силу коммутативности кольца R). Такой A-модуль V с дополнительной структурой левого R-модуля будем называть *модулем над алгеброй A* или просто *A-модулем*.

✎ **(3.18)** Пусть A — R-алгебра и V — A-модуль. Показать, что для любых $v \in V$, $r \in R$, $a \in A$ выполнено

$$r(va) = (rv)a = v(ra).$$

✓ В случае, когда R — поле, произвольный A-модуль V является векторным пространством над R и, в частности, для него определены такие понятия как базис над R, размерность над R, и т. д.

(3.19) Примеры A-модулей

1. *Регулярный A-модуль A°* — сама алгебра A, действующая на себе умножением справа.

2. Пусть R — коммутативное кольцо и V — левый R-модуль. Тогда V является правым модулем над R-алгеброй $\mathrm{End}_R(V)$ относительно естественного действия.

3. Пусть S — кольцо. Тогда любой правый S-модуль можно рассматривать как модуль над $\mathbb{Z}$-алгеброй S или как модуль над R-алгеброй S, где $R \leqslant \mathrm{Z}(S)$.

4. Пусть R — коммутативное кольцо и H — некоторая подгруппа группы G. Поскольку алгебра RH является подалгеброй алгебры RG, то каждый RG-модуль V будет также и RH-модулем, который мы будем обозначать символом V_H.

5. Пусть G — группа, F — поле и V — векторное пространство конечной размерности n над F. Пусть действие групповой алгебры FG на V задаётся по правилу $vg = v$ для всех $g \in G$, $v \in V$ и продолжается по линейности на всю алгебру FG. Таким образом на V определяется структура FG-модуля. Этот модуль мы будем называть *тривиальным n-мерным* модулем алгебры FG. Одномерный тривиальный FG-модуль называется *главным*.

6. Пусть G — группа, F — поле и V — FG-модуль. На двойственном [10] векторном пространстве V^* можно задать структуру FG-модуля, если положить $v(\varphi g) = (vg^{-1})\varphi$ для всех $v \in V$, $g \in G$ и продолжить это действие по линейности на всю алгебру FG. Такой FG-модуль V^* называется *контрагредиентным*[11] к модулю V.

---

[10] Т.е. на пространстве всех F-линейных отображений $\varphi : V \to F$, см. (2.28).

[11] Мы намеренно избегаем употребления для V^* термина «двойственный FG-модуль», зарезервированного нами для левого GF-модуля $\mathrm{Hom}(V, FG^\circ)$. Однако обозначение V^* будет в дальнейшем использоваться именно для контрагредиентного FG-модуля.

7. Пусть группа G действует на непустом конечном множестве M. Пусть F — поле, V — векторное пространство размерности $|M|$ над F с базисом $\{e_m \mid m \in M\}$. Действие групповой алгебры FG на V задаётся действием групповых элементов на базисных векторах по правилу $e_m g = e_{mg}$ для всех $g \in G$, $m \in M$, которое затем продолжается по линейности на всё пространство V и всю алгебру FG. Таким образом на V определяется структура FG-модуля, называемого *подстановочным модулем* групповой алгебры FG, соответствующим данному действию группы на множестве. В частном случае, когда G — подгруппа симметрической группы S_n, действующая на множестве $M = \{1, \ldots, n\}$, определённый таким образом FG-модуль будем называть *естественным подстановочным модулем.*

✎ Проверить сформулированные в (3.19) утверждения.

(3.20) Пусть A — R-алгебра и V — A-модуль. Тогда A-подмодуль W правого A-модуля V (здесь A рассматривается как кольцо) автоматически будет левым R-подмодулем, поскольку $rw = w(r1_A) \in W$ для всех $r \in R$ и $w \in W$. Поэтому такие подмодули будут A-модулями над алгеброй A. Это замечание устраняет двусмысленность термина *«A-подмодуль»* для A-модуля V. В частности, для регулярного A-модуля A-подмодули — это, в точности, правые идеалы алгебры A. Аналогично для A-подмодуля $W \leqslant V$ фактормодуль V/W будет A-модулем.

Пусть $\varphi : V \to W$ — гомоморфизм A-модулей (рассматриваемых как правые модули над кольцом A). Тогда φ будет также гомоморфизмом левых R-модулей (то есть R-линейным), поскольку

$$(rv)\varphi = (v(r1_A))\varphi = (v\varphi)(r1_A) = r(v\varphi)$$

для любых $r \in R$ и $v \in V$. Гомоморфизмы (эндоморфизмы, изоморфизмы) A-модулей мы будем называть также *A-гомоморфизмами* (*A-эндоморфизмами, A-изоморфизм*). Таким образом группа $\mathrm{Hom}_A(V, W)$ совпадает с множеством всех A-гомоморфизмов из V в W, а $\mathrm{End}_A(V)$ — с множеством всех A-эндоморфизмов модуля V. Если рассматривать A-модули V и W как левые R-модули, то $\mathrm{Hom}_A(V, W)$ состоит из тех элементов $\varphi \in \mathrm{Hom}_R(V, W)$, которые перестановочны с действием алгебры A, т. е. таких, что для любых $v \in V$ и $a \in A$ выполнено $(va)\varphi = (v\varphi)a$. В связи с этим отметим, что эндоморфизм регулярного A-модуля A° может не быть эндоморфизмом алгебры A и наоборот.

Группу $\mathrm{Hom}_A(V, W)$ легко превратить в левый R-модуль, положив $v(r\varphi) = r(v\varphi)$ для любых $r \in R$ и $\varphi \in \mathrm{Hom}_A(V, W)$. Композиция отображений задаёт на $\mathrm{End}_A(V)$ операцию умножения.

✎ **(3.21)** Пусть A — R-алгебра и V — A-модуль. Показать, что $\mathrm{End}_A(V)$ является подалгеброй R-алгебры $\mathrm{End}_R(V)$. В частности, V можно рассматривать как правый $\mathrm{End}_A(V)$-модуль.

✎ **(3.22)** Пусть R — коммутативное кольцо и V — левый R-модуль. Положим $A = \mathrm{End}_R(V)$. Показать, что $\mathrm{End}_A(V) = \mathrm{Z}(A)$.

✎ **(3.23)** Пусть F — поле и G — конечная группа. Показать, что для любого FG-модуля V имеет место изоморфизм $V^{**} \cong V$.

В следующей теореме собраны некоторые факты об A-модулях, аналогичные теоремам о гомоморфизмах для групп.

(3.24) Теорема (о гомоморфизмах A-модулей).

(*i*) *Пусть $\varphi : V \to W$ — гомоморфизм A-модулей V и W. Тогда $\mathrm{Ker}\,\varphi \leqslant V$, $\mathrm{Im}\,\varphi \leqslant W$ и отображение $v + \mathrm{Ker}\,\varphi \mapsto v\varphi$ для $v \in V$ определяет изоморфизм A-модулей $V/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\,\varphi$.*

(*ii*) *Если имеются включения A-модулей $U \leqslant W \leqslant V$ и $M \leqslant V$, то*

$$(W + M)/(U + M) \cong W/(U + W \cap M).$$

В частности,

$$(W + M)/M \cong W/(W \cap M).$$

(*iii*) *Пусть U — A-подмодуль A-модуля V. Тогда отображение $M \mapsto M/U$ задаёт биекцию между A-подмодулями из V, содержащими U, и A-подмодулями A-модуля V/U. Эта биекция сохраняет отношение включения. При этом, если $U \leqslant M \leqslant V$, то*

$$(V/U)/(M/U) \cong V/M.$$

✎ **(3.25)** Доказать теорему (3.24).

(3.26) Определение. Ненулевой A-модуль V называется *неприводимым* или *простым*, если он не содержит подмодулей, отличных от 0 и V. В противном случае V называется *приводимым*.

Очевидно, что минимальные подмодули A-модуля V — это, в точности, неприводимые подмодули, а максимальные — это, те подмодули, фактор по которым неприводим.

✎ **(3.27)** Показать, что регулярный A-модуль A° неприводим тогда и только тогда, когда A является телом.

✎ **(3.28)** Пусть R-коммутативное кольцо. Показать, что следующие условия эквивалентны.

(i) Любой ненулевой левый R-модуль V неприводим как правый $\mathrm{End}_R(V)$-модуль.

(ii) R является полем.

(*Указание.* Рассмотреть в качестве V регулярный модуль ${}^\circ R$.)

(3.29) Предложение. *Показать, что для любого FG-модуля V контрагредиентный модуль V^* неприводим тогда и только тогда, когда V неприводим.*

✎ Доказать предложение (3.29). (*Указание.* Для FG-подмодулей W из V и W^* из V^* рассмотреть множества

$$\{\varphi \in V^* \mid v\varphi = 0 \text{ для всех } v \in W\} \quad \text{и} \quad \{v \in V \mid v\varphi = 0 \text{ для всех } \varphi \in W^*\},$$

соответственно.)

Понятие неприводимого A-модуля является усилением понятия неразложимого A-модуля. Всякий неприводимый A-модуль, очевидно, неразложим, но обратное неверно, как показывает следующее упражнение.

✎ **(3.30)** Показать, что регулярный модуль групповой алгебры $\mathbb{F}_2\mathbb{Z}_2$ неразложим, но приводим.

Конечный ряд A-модулей

(3.31)
$$V = V_0 \geqslant V_1 \geqslant \ldots \geqslant V_n = 0$$

называется *композиционным рядом A-модуля V*, если все факторы V_{i-1}/V_i, $i = 1, \ldots, n$, называемые *факторами ряда* (3.31), неприводимы.

В случае, когда R — поле, примером A-модуля, обладающего композиционным рядом, служит любой A-модуль R-алгебры A, имеющий как векторное пространство конечную размерность над R. В общем же случае A-модуль может не иметь композиционного ряда.

✎ **(3.32)** Привести пример A-модуля, не обладающего композиционным рядом.

Два композиционных ряда некоторого A-модуля называются *эквивалентными*, если они имеют одинаковое число факторов, и между этими факторами можно установить взаимно однозначное соответствие, при котором соответствующие факторы будут изоморфны.

Следующая теорема, утверждающая единственность с точностью до эквивалентности композиционного ряда A-модуля по существу вытекает из теоремы о гомоморфизмах (3.24).

(3.33) Теорема (Жордана–Гёльдера). *Любые два композиционных ряда A-модуля V эквивалентны.*

✎ **(3.34)** Доказать теорему (3.33).

Теорема Жордана–Гёльдера позволяет ввести важное понятие композиционных факторов для A-модулей, обладающих композиционным рядом.

(3.35) Определение. *Композиционными факторами* A-модуля V называются факторы его композиционного ряда.

Как вытекает из теоремы (3.24), наборы композиционных факторов изоморфных A-модулей по существу совпадают. Следующее упражнение показывает, что есть примеры неизоморфных A-модулей с одинаковыми наборами композиционных факторов.

✎ **(3.36)** Показать, что регулярный и тривиальный двумерный модули групповой алгебры $\mathbb{F}_2S_2$ неизоморфны, но имеют один и тот же набор композиционных факторов.

✎ **(3.37)** Найти размерности композиционных факторов естественных подстановочных модулей для алгебр $\mathbb{F}_2S_4$ и $\mathbb{F}_3S_4$.

Теорема Жордана-Гёльдера показывает важность изучения неприводимых модулей. Одним из ключевых фактов о неприводимых модулях является следующее утверждение.

(3.38) Теорема (лемма Шура). *Пусть V, W — неприводимые A-модули. Тогда любой ненулевой A-гомоморфизм $\mathrm{Hom}_A(V, W)$ является изоморфизмом.*

✎ **(3.39)** Доказать теорему (3.38).

Очевидным следствием из леммы Шура является следующее утверждение.

(3.40) Следствие. *Если V — неприводимый A-модуль, то алгебра $\mathrm{End}_A(V)$ является телом.*

Отметим важный частный случай.

(3.41) Следствие. *Пусть F — алгебраически замкнутое поле, A — F-алгебра, V — неприводимый A-модуль и размерность $\dim_F(V)$ конечна. Тогда имеет место изоморфизм F-алгебр $\mathrm{End}_A(V) \cong F$.*

Доказательство. Очевидно, что $F1 \leqslant \mathrm{End}_A(V)$. Рассмотрим произвольный элемент $\theta \in \mathrm{End}_A(V)$. Тогда θ является линейным преобразованием конечномерного векторного пространства V над алгебраически замкнутым полем F и, значит, имеет собственное значение λ. Следовательно эндоморфизм $\theta - \lambda 1 \in \mathrm{End}_A(V)$ необратим. По лемме (3.38) получаем $\theta - \lambda 1 = 0$, т. е. $\theta = \lambda 1 \in F1$. Таким образом, $\mathrm{End}_A(F) = F1$, а так как F — поле, имеем $F1 \cong F$. □

Покажем, что по существу источником всех неприводимых A-модулей является сама алгебра A. Для этого, введём следующие понятия.

Пусть V — A-модуль. *Аннулятором элемента* $v \in V$ называется множество

$$\mathrm{Ann}(v) = \{a \in A \mid va = 0\}.$$

Аннулятором A-модуля V называется

$$\mathrm{Ann}(V) = \bigcap_{v \in V} \mathrm{Ann}(v) = \{a \in A \mid va = 0 \ \text{ для всех } \ v \in V\}.$$

Отметим некоторые элементарные свойства аннуляторов.

(3.42) Предложение. *Пусть V — A-модуль и $v \in V$. Имеют место следующие утверждения.*

(*i*) $\mathrm{Ann}(v) \trianglelefteq_r A$.

(*ii*) $\mathrm{Ann}(V) \trianglelefteq A$.

(*iii*) *Из изоморфизма A-модулей $V \cong W$ следует равенство* $\mathrm{Ann}(V) = \mathrm{Ann}(W)$.

(*iv*) *Для любого идеала $I \trianglelefteq A$ такого, что $I \leqslant \mathrm{Ann}(V)$, модуль V можно рассматривать как A/I-модуль, если для $v \in V$ и $a \in A$ положить $v(a + I) = va$. При этом модуль V неприводим тогда и только тогда, когда он неприводим как A/I-модуль.*

✎ Доказать предложение (3.42).

Выше мы отмечали, что подмодуль максимален тогда и только тогда, когда фактор по нему неприводим. Сейчас покажем, что любой неприводимый A-модуль может быть получен как фактормодуль регулярного модуля A° по некоторому его максимальному подмодулю.

(3.43) Предложение. *Пусть V — неприводимый A-модуль R-алгебры A и v — ненулевой элемент из V. Тогда*

(*i*) $\mathrm{Ann}(v)$ *— максимальный правый идеал в A;*

(*ii*) $V \cong A^\circ / \mathrm{Ann}(v)$.

✎ Доказать предложение (3.43).

4. Радикал

В дальнейшем мы зафиксируем некоторую систему представителей всех классов изоморфных неприводимых A-модулей и будем обозначать её через $\mathscr{M}(A)$.

Теперь мы можем ввести следующее важное понятие.

(4.1) Определение. *Радикалом* R-алгебры A, обозначаемом через $\mathrm{J}(A)$, называется[12)] пересечение аннуляторов всех неприводимых A-модулей.

Ввиду предложения (3.42)(*iii*) можно записать

$$\mathrm{J}(A) = \bigcap_{V \in \mathscr{M}(A)} \mathrm{Ann}(V).$$

Из (3.42)(*ii*) следует также, что $\mathrm{J}(A) \trianglelefteq A$.

✓ Строго говоря, определённый таким образом радикал было бы правильнее назвать *правым радикалом*, поскольку речь идёт о правых A-модулях. Однако, можно проверить, что если ввести аналогичное понятие левого радикал, то правый и левый радикалы алгебры совпадут, см. (4.8).

(4.2) Предложение. *Радикал* $\mathrm{J}(A)$ *совпадает с пересечением всех максимальных правых идеалов алгебры* A.

Доказательство. Пусть J — пересечение множества всех максимальных правых идеалов алгебры A. По предложению (3.43) множество J содержится в аннуляторах $\mathrm{Ann}(v)$ всех ненулевых элементов всех неприводимых A-модулей V. Поэтому

$$J \subseteq \bigcap_{V \in \mathscr{M}(A)} \bigcap_{0 \neq v \in V} \mathrm{Ann}(v) = \bigcap_{V \in \mathscr{M}(A)} \mathrm{Ann}(V) = \mathrm{J}(A).$$

Для обратного включения достаточно показать, что любой максимальный правый идеал $I \trianglelefteq_r A$ содержит аннулятор некоторого неприводимого A-модуля. В качестве такого модуля можно взять фактормодуль A°/I. В самом деле, если $x \in \mathrm{Ann}(A^\circ/I)$, то, в частности, x аннулирует элемент $1_A + I \in A^\circ/I$ и мы получаем $I = (1_A + I)x = x + I$, т. е. $x \in I$. □

Доказанное предложение даёт «внутреннюю» и с практической точки зрения более удобную, чем исходное определение, характеризацию радикала $\mathrm{J}(A)$ в терминах правых идеалов алгебры A.

(4.3) Предложение. *Пусть* A_1, A_2 — R-*алгебры и* $A = A_1 \oplus A_2$. *Тогда* $\mathrm{J}(A) = \mathrm{J}(A_1) \oplus \mathrm{J}(A_2)$.

✎ Доказать предложение (4.3).

(4.4) Зафиксируем кольцо S. Как мы видели ранее (см. (3.2), пп. 4,5), это кольцо можно различными способами превратить в алгебру над подходящим коммутативным кольцом R. Естественно возникает вопрос, как соотносятся радикалы алгебр, возникающих из S. На самом деле эти радикалы совпадают. Это видно, например, из предложения (4.2), поскольку совпадают множества максимальных правых идеалов таких алгебр (ведь по определению правые идеалы R-алгебры S — это, в точности, правые идеалы кольца S). Таким образом, если определить *радикал* $\mathrm{J}(S)$ *кольца* S как пересечение всех максимальных правых идеалов из S, то это определение будет согласовано с определением радикала R-алгебры.

(4.5) Предложение. *Если* $I \trianglelefteq_r A$ *и для любого* $a \in I$ *элемент* $1 - a$ *обратим справа, то для любого* $a \in I$ *элемент* $1 - a$ *также обратим и слева.*

✎ Доказать предложение (4.5).

(4.6) Предложение. *Если* $I \trianglelefteq_r A$ *и для любого* $a \in I$ *элемент* $1 - a$ *обратим справа, то* $I \subseteq \mathrm{J}(A)$.

✎ Доказать предложение (4.6).

(4.7) Предложение. *Если* A — R-*алгебра и* $a \in \mathrm{J}(A)$, *то элемент* $1 - a$ *обратим.*

[12)] В литературе радикал алгебры также часто называется *радикалом Джекобсона*.

Доказательство. Рассмотрим правый идеал $(1-a)A$ алгебры A. Если он собственный, то по предложению (2.3) содержится в некотором максимальном правом идеале M, и поэтому $1-a \in (1-a)A \leqslant M$. Но с другой стороны $a \in \mathrm{J}(A) \leqslant M$ и, значит, $1 \in M$. Противоречие. Поэтому $(1-a)A = A$ откуда, очевидно, следует правая обратимость элемента $1-a$. По предложению (4.5) элемент $1-a$ также обратим слева. □

✎ **(4.8)** Показать, что «левый радикал» алгебры A (т. е. пересечение аннуляторов всех неприводимых левых A-модулей) совпадает с $\mathrm{J}(A)$.

✎ **(4.9)** Доказать, что $\mathrm{J}(A)$ не содержит ненулевых идемпотентов.

Если e — идемпотент R-алгебры A, то eAe — R-алгебра с единицей e в силу (2.19)(ii). Следующее утверждение описывает радикал алгебры eAe.

(4.10) Предложение. *Пусть A — R-алгебра и $e \in A$ — идемпотент. Тогда*

$$\mathrm{J}(eAe) = e\mathrm{J}(A)e = \mathrm{J}(A) \cap eAe.$$

✎ Доказать предложение (4.10).

(4.11) Предложение. (i) *Любой правый идеал R-алгебры A, состоящий из нильпотентных элементов, лежит в радикале* $\mathrm{J}(A)$.

(ii) *Любой нильпотентный правый идеал R-алгебры A лежит в радикале* $\mathrm{J}(A)$.

✎ Доказать предложение (4.11).

(4.12) Предложение. *В коммутативной R-алгебре множество всех нильпотентных элементов образует идеал. В частности, любой нильпотентный элемент лежит в радикале.*

✎ Доказать предложение (4.12).

A-модуль V называется *конечно порождённым*, если он имеет конечное число *порождающих*, т. е. таких элементов $v_1, \ldots, v_n \in V$, что

$$V = v_1A + \ldots + v_nA.$$

(4.13) Предложение. *Любой ненулевой конечно порождённый A-модуль содержит максимальный подмодуль.*

✎ Доказать предложение (4.13). (*Указание.* Использовать лемму Цорна.)

Пусть V — A-модуль, $W \leqslant V$ и $I \trianglelefteq_r A$. Обозначим через WI аддитивную подгруппу группы V, порождённую всевозможными произведениями вида wx, где $w \in W$, $x \in I$. Легко видеть, что WI — A-подмодуль модуля V. В случае $V = A^\circ$, данное определение произведения WI согласуется с определением произведения идеалов (2.6).

(4.14) Теорема (лемма Накаямы). *Пусть V — A-модуль и $W \leqslant V$. Предположим, что фактормодуль V/W конечно порождён. Если $W + V\mathrm{J}(A) = V$, то $W = V$.*

Доказательство. Достаточно доказать лемму для случая, когда $W = 0$ и затем применить утверждение к фактормодулю V/W. Итак, считаем, что V — конечно порождённый A-модуль и $V\mathrm{J}(A) = V$. Требуется доказать, что $V = 0$. Допустим, что $V \neq 0$. Тогда по предложению (4.13) модуль V содержит максимальный подмодуль U. Фактормодуль V/U неприводим, поэтому $(V/U)\mathrm{J}(A) = 0$, откуда следует, что $V\mathrm{J}(A) \leqslant U \neq V$. Противоречие. □

Положив $W = 0$ в теореме (4.14), получаем важное следствие (также часто называемое леммой Накаямы).

(4.15) Следствие. *Если V — ненулевой конечно порождённый A-модуль, то $V\mathrm{J}(A) < V$.*

Отметим, что требование конечной порождённости модуля V в лемме Накаямы является существенным. Например, в качестве V можно взять поле $\mathbb{Q}$ рациональных чисел, а в качестве A — его подкольцо $\mathbb{Z}[\pi^{-1}]$, где π — множество нечётных простых чисел, см. (2.5). Тогда V не является конечно порождённым A-модулем. Однако, $\mathrm{J}(A) = 2A$ и имеет место равенство $V\mathrm{J}(A) = V$.

В качестве примера использования леммы Накаямы докажем следующее утверждение.

(4.16) Предложение. *Пусть S — кольцо и R — подкольцо центра $\mathrm{Z}(S)$. Предположим, что S является конечно порождённым как R-модуль. Тогда $\mathrm{J}(R) \leqslant \mathrm{J}(S) \cap R$.*

Доказательство. Рассмотрим S как R-алгебру. Достаточно показать, что для произвольного неприводимого S-модуля V справедливо равенство $V\mathrm{J}(R) = 0$. Поскольку S конечно порождено как R-модуль, можно записать $S = s_1R + \ldots + s_nR$ для некоторых $s_i \in S$. Выберем ненулевой элемент $v \in V$. Тогда

$$V = vS = vs_1R + \ldots + vs_nR,$$

откуда следует, что V — (ненулевой) конечно порождённый R-модуль. Из (4.15) следует, что $V\mathrm{J}(R) < V$. Однако $V\mathrm{J}(R)$ является S-подмодулем модуля V, поскольку $\mathrm{J}(R)$ состоит из центральных элементов кольца S. Значит, $V\mathrm{J}(R) = 0$ в силу неприводимости V. $\square$

Отметим, что в условиях предложения (4.16) справедливо и обратное включение, т. е. имеет место равенство $\mathrm{J}(R) = \mathrm{J}(S) \cap R$.

Следующее вспомогательное утверждение нам потребуется в дальнейшем.

(4.17) Предложение. *Пусть G — конечная группа и $\varphi : R \to S$ — гомоморфизм коммутативных колец такой, что $\operatorname{Ker}\varphi \subseteq \mathrm{J}(R)$. Рассмотрим естественное поднятие φ до кольцевого гомоморфизма $\tilde{\varphi} : RG \to SG$ групповых алгебр. Пусть $e \in RG$ — идемпотент и $x \in e(RG)e$. Если $x\tilde{\varphi} = e\tilde{\varphi}$, то x обратим в кольце $e(RG)e$.*

Доказательство. Обозначим $A = e(RG)e$. Из (2.19)(ii) вытекает, что A действительно является кольцом и e — его единицей. По (4.7) достаточно показать, что $e - x \in \mathrm{J}(A)$. Из (4.10) следует, что $\mathrm{J}(A) = \mathrm{J}(RG) \cap A$ и, значит, достаточно проверить, что $e - x \in \mathrm{J}(RG)$. По условию $e - x \in \operatorname{Ker}\tilde{\varphi}$ и мы покажем, что $\operatorname{Ker}\tilde{\varphi} \subseteq \mathrm{J}(RG)$, откуда будет следовать требуемое.

В силу (3.11) любой элемент $u \in \operatorname{Ker}\tilde{\varphi}$ имеет вид $u = \sum_{g\in G} u_g g$ для подходящих $u_g \in \operatorname{Ker}\varphi$. Значит, ввиду замечания (3.3), достаточно показать, что $\operatorname{Ker}\varphi \subseteq \mathrm{J}(RG)$. По условию $\operatorname{Ker}\varphi \subseteq \mathrm{J}(R)$. Кроме того, $R \leqslant \mathrm{Z}(RG)$ и RG является конечно порождённым R-модулем. Поэтому из (4.16) следует, что $\mathrm{J}(R) \subseteq \mathrm{J}(RG)$ и, тем самым, утверждение доказано. $\square$

Кольцо называется *локальным*, если оно содержит единственный максимальный правый идеал.

(4.18) Предложение. *Пусть S — кольцо. Тогда следующие условия эквивалентны.*

(i) *S содержит единственный максимальный правый идеал I_r.*

(ii) *S содержит единственный максимальный левый идеал I_l.*

(iii) *Существует собственный идеал $I \trianglelefteqslant S$ такой, что любой элемент из $S \setminus I$ обратим.*

Кроме того, если выполнены условия (i)–(iii), то $I_r = I_l = I = \mathrm{J}(S)$.

✎ Доказать предложение (4.18).

✎ **(4.19)** Доказать, что единственными идемпотентами локального кольца являются 0 и 1.

✎ **(4.20)** Пусть p — простое число, и π — множество всех простых чисел, отличных от p. Показать, что кольцо $\mathbb{Z}[\pi^{-1}]$ является локальным, см. (2.5).

Для локальных колец из леммы Накаямы вытекает следующее утверждение.

(4.21) Следствие (лемма Накаямы для локальных колец). *Пусть S — локальное кольцо с максимальным идеалом I, M — конечно порождённый правый S-модуль, N — подмодуль модуля M такой, что $M = N + MI$. Тогда $M = N$.*

Доказательство. Как мы замечали, S можно рассматривать как R-алгебру для подходящего коммутативного кольца R и тогда M и N будут модулями над R-алгеброй S. Кроме того, радикал $\mathrm{J}(S)$, очевидно, равен I. Значит, $M = N$ по лемме Накаямы, поскольку фактормодуль M/N конечно порождённого модуля M также конечно порождён. $\square$

5. Конечномерные алгебры над полем

Начиная с этого раздела, если не оговорено особо, мы будем предполагать, что $R = F$ — поле, а все рассматриваемые F-модули (в том числе и F-алгебра A) конечномерны как векторные пространства над F. В частности, любой A-модуль обладает композиционным рядом, а также, как мы уже отмечали, в этом случае можем предполагать, что $F \leqslant \mathrm{Z}(A)$, поскольку отображение $\alpha \mapsto \alpha 1_A$ будет мономорфизмом колец.

(5.1) Предложение. *Пусть A — F-алгебра. Существует лишь конечное число попарно неизоморфных неприводимых A-модулей, т. е. $|\mathscr{M}(A)| < \infty$.*

✎ Доказать предложение (5.1). (*Указание.* Воспользоваться предложением (3.43) и теоремой Жордана-Гёльдера (3.33).)

(5.2) Предложение. *Пусть A — F-алгебра. Тогда $\mathrm{J}(A)$ — нильпотентный идеал.*

✎ Доказать предложение (5.2).

✓ Отметим, что для произвольных R-алгебр, где R — кольцо, заключение предложения (5.2) вообще говоря неверно.

Из предложений (4.11) и (5.2) следует, что среди нильпотентных правых идеалов F-алгебры A существует единственный максимальный идеал, и этот идеал совпадает с радикалом $\mathrm{J}(A)$. Также из предложения (5.2) следует, что радикал F-алгебры состоит из нильпотентных элементов. Значит, по предложению (4.12) справедливо следующее утверждение, дающее характеризацию радикала F-алгебр в коммутативном случае.

(5.3) Следствие. *Пусть A — коммутативная F-алгебра. Тогда радикал $\mathrm{J}(A)$ совпадает с множеством нильпотентных элементов.*

(5.4) Предложение. *Пусть A — F-алгебра. Тогда имеет место равенство $\mathrm{J}(\mathrm{Z}(A)) = \mathrm{J}(A) \cap \mathrm{Z}(A)$.*

✎ Доказать предложение (5.4).

✎ **(5.5)** Найти радикалы следующих алгебр.

1. $\mathrm{M}_n(F)$, где F — поле.
2. $\mathbb{Z}_n$ как $\mathbb{Z}$-алгебра.
3. $\mathbb{F}_p\mathbb{Z}_p$ для простого p.
4. $\mathbb{F}_2 S_3$.
5. $\mathbb{F}_3 S_3$.

(*Указание.* 3. Рассмотреть идеал, порождённый элементом $1 - a$, где a — порождающий группы $\mathbb{Z}_p$. 4. Сначала рассмотреть двусторонние идеалы I_1, I_2, порождённые, соответственно, элементами $e_1 = 1 + (123) + (132)$ и $e_2 = (123) + (132)$. Воспользоваться предложениями (2.17) и (4.3). Рассмотреть дополнительно правые идеалы J_1, J_2, J_3, порождённые элементами $v_1 = e_2(1 + (23))$, $v_2 = e_2(1 + (13))$, $v_3 = e_2(1 + (12))$. 5. Рассмотреть правые идеалы I_1, I_2, порождённые, соответственно, элементами $e_1 = 1 + (12)$ и $e_2 = 1 - (12)$. Показать, что модуль I_i содержит единственный максимальный подмодуль J_i, где $i = 1, 2$. Сравнить радикал с суммой $J_1 + J_2$.)

6. Вполне приводимые модули

Напомним, что F всюду обозначает некоторое поле и A — конечномерную алгебру над F. Все рассматриваемые A-модули считаются конечномерными пространствами над F.

Будем называть A-модуль V *вполне приводимым* или *полупростым*, если он является прямой суммой неприводимых A-модулей.

✓ Подчеркнём, что, в частности, нулевой и неприводимый модуль вполне приводимы.

(6.1) Предложение. *Если A — F-алгебра и V — A-модуль, то следующие условия эквивалентны.*

(*i*) *Модуль V вполне приводим.*

(ii) *Для любого A-подмодуля $U \leqslant V$ существует A-подмодуль $W \leqslant V$ такой, что $V = U \oplus W$.*

(iii) *Модуль V является суммой (необязательно прямой) неприводимых модулей.*

Доказательство. $(i) \Rightarrow (ii)$ Пусть $V = \bigoplus V_i$ и $U \leqslant V$. В силу конечномерности можно выбрать подмодуль $W \leqslant V$, максимальный среди тривиально пересекающихся с U. Тогда $W + U = W \oplus U$ и достаточно показать, что эта сумма совпадает с V. Пусть, напротив, $W + U < V$. Тогда существует V_j, не содержащийся в $W + U$. В силу неприводимости V_j получаем $(U + W) \cap V_j = 0$. Но тогда $W + V_j > W$ и подмодуль $W + V_j$ тривиально пересекается с U вопреки выбору W.

$(ii) \Rightarrow (iii)$ Пусть W — максимальный подмодуль в V, являющийся суммой неприводимых подмодулей. Если $W < V$, то $V = W \oplus U$ для ненулевого подмодуля $U \leqslant V$. Но тогда, ввиду конечномерности, U содержит неприводимый подмодуль M. Значит, $W + M > W$ и подмодуль $W + M$ — сумма неприводимых подмодулей. Это противоречит выбору W.

$(iii) \Rightarrow (i)$ Пусть $V = \sum V_i$, где подмодули V_i неприводимы. Пусть $W \leqslant V$ — максимальный подмодуль, представимый как прямая сумма некоторых из подмодулей V_i. Если $W \neq V$, то существует V_j, не лежащий в W. Но тогда $W \cap V_j = 0$ в силу неприводимости V_j и сумма $W + V_j$ прямая вопреки максимальности W. $\square$

Отметим, что при доказательстве импликации $(iii) \Rightarrow (i)$ мы получили следующее более сильное утверждение.

(6.2) Следствие. *Пусть V — A-модуль и $V = \sum V_i$, где V_i — неприводимые подмодули. Тогда V — прямая сумма некоторых из подмодулей V_i.*

Ещё одним очевидным следствием предложения (6.1) является тот факт, что вполне приводимый A-модуль неприводим тогда и только тогда, когда он неразложим.

✎ **(6.3)** Является ли вполне приводимым естественный подстановочный модуль для алгебры

1. $\mathbb{F}_2 S_4$,
2. $\mathbb{F}_3 S_4$?

Очевидно, что прямая сумма вполне приводимых модулей вполне приводима. Следующее утверждение показывает, что полная приводимость наследуется также при переходе к подмодулям и фактормодулям.

(6.4) Предложение. *Пусть V — вполне приводимый A-модуль. Если U — A-подмодуль из V, то A-модули U и V/U вполне приводимы.*

✎ Доказать предложение (6.4).

✎ **(6.5)** Доказать, что пересечение всех максимальных подмодулей вполне приводимого A-модуля равно нулю.

Пусть V — вполне приводимый A-модуль и M — неприводимый A-модуль. *M-однородной компонентой* модуля V (или *компонентой Веддерберна*) называется сумма всех подмодулей из V, изоморфных M. Будем обозначать её через $\mathrm{W}_M(V)$. Сразу отметим, что если V не содержит подмодулей, изоморфных M, то $\mathrm{W}_M(V) = 0$. Кроме того, если неприводимые A-модули M и N неизоморфны, то $\mathrm{W}_M(V) \cap \mathrm{W}_N(V) = 0$, как следует из теоремы Жордана-Гёльдера (3.33).

(6.6) Предложение. *Пусть $V = \bigoplus V_i$ — прямая сумма неприводимых A-модулей V_i и M — произвольный неприводимый A-модуль. Тогда*

(i) $\mathrm{W}_M(V)$ *является* $\mathrm{End}_A(V)$*-подмодулем модуля* V,

(ii) $\mathrm{W}_M(V) = \bigoplus_{V_i \cong M} V_i$,

(iii) *число подмодулей V_i, изоморфных M, является инвариантом модуля V, т. е. не зависит от данного разложения $V = \bigoplus V_i$.*

✎ Доказать предложение (6.6).

Для вполне приводимого A-модуля V и неприводимого A-модуля M будем обозначать через $\mathrm{n}_M(V)$ число неприводимых прямых слагаемых, изоморфных M, в некотором разложении $V = \bigoplus V_i$, где V_i неприводимы. В силу (iii) предложения (6.6) число $\mathrm{n}_M(V) = \dim_F(\mathrm{W}_M(V))/\dim_F(M)$ зависит только от M и V. Кроме того, числа $\mathrm{n}_M(V)$ определяют модуль V с точностью до изоморфизма. Более строго, вполне приводимые A-модули V и W изоморфны тогда и только тогда, когда $\mathrm{n}_M(V) = \mathrm{n}_M(W)$ для всех $M \in \mathscr{M}(A)$.

7. Полупростые F-алгебры

(7.1) Определение. F-алгебра A называется *полупростой*, если $\mathrm{J}(A) = 0$, и *простой*, если она ненулевая и не имеет собственных ненулевых двусторонних идеалов.

Очевидно, что простая F-алгебра является полупростой.

(7.2) Предложение. *Пусть A — F-алгебра. Тогда факторалгебра $A/\mathrm{J}(A)$ полупроста.*

✎ Доказать предложение (7.2).

Полупростота F-алгебры и её модулей тесно связаны.

(7.3) Предложение. *Пусть A — F-алгебра. Тогда следующие условия эквивалентны.*

(*i*) *Алгебра A полупроста.*

(*ii*) *Регулярный модуль A° вполне приводим.*

(*iii*) *Каждый A-модуль вполне приводим.*

Доказательство. $(i) \Rightarrow (ii)$ Достаточно показать, что существует конечный набор максимальных правых идеалов $M_1, \ldots, M_n$ алгебры A такой, что $\cap_i M_i = 0$. В самом деле, если это верно, то A° можно изоморфно вложить во вполне приводимый модуль $A^\circ/M_1 \oplus \ldots \oplus A^\circ/M_n$ с помощью отображения $a \mapsto (a+M_1, \ldots, a+M_n)$. Тогда по предложению (6.4) модуль A° будет вполне приводимым.

Пусть N — подмодуль из A°, являющийся пересечением конечного числа максимальных правых идеалов алгебры A и имеющий минимальную размерность среди всевозможных таких пересечений. Достаточно показать, что $N = 0$. Пусть, напротив, $N \neq 0$. По условию $\mathrm{J}(A) = 0$. С другой стороны $\mathrm{J}(A)$ совпадает с пересечением всех максимальных правых идеалов из A по предложению (4.2). Значит, существует максимальный правый идеал M такой, что $M \cap N < N$, вопреки выбору N.

$(ii) \Rightarrow (i)$ Поскольку модуль A° вполне приводим, то он равен сумме неприводимых подмодулей — минимальных правых идеалов алгебры A. Поскольку $\mathrm{J}(A)$ аннулирует каждый простой модуль, то $0 = A^\circ\mathrm{J}(A) = \mathrm{J}(A)$. Значит, алгебра A полупроста.

$(ii) \Rightarrow (iii)$ Пусть V — A-модуль. В силу полной приводимости модуля A° мы можем записать $A^\circ = \sum_i I_i$, где I_i — некоторые минимальные правые идеалы алгебры A. Тогда

$$V = \sum_{v \in V} vA = \sum_{v \in V} \sum_i vI_i.$$

(Вообще говоря, эта сумма может иметь бесконечное число слагаемых, однако, ввиду конечномерности модуля V, ей легко придать строгий смысл.) Отображение $I_i \to vI_i$, действующее по правилу $a \mapsto va$, $a \in I_i$, является эпиморфизмом A-модулей. Поскольку модуль I_i неприводим, то $vI_i \cong I_i$ или $vI_i \cong 0$. Значит, V — сумма неприводимых модулей.

$(iii) \Rightarrow (ii)$ Очевидно. □

Поскольку регулярный модуль факторалгебры изоморфен фактормодулю регулярного модуля исходной алгебры, из предложений (6.4) и (7.3) вытекает следующее утверждение.

(7.4) Следствие. *Если F-алгебра A полупроста и $B \trianglelefteq A$, то факторалгебра A/B полупроста.*

✓ Отметим, что, в отличие от факторалгебры, подалгебра полупростой алгебры может не быть полупростой. В качестве примера можно рассмотреть подалгебру верхнетреугольных матриц в алгебре $\mathrm{M}_n(F)$, $n \geqslant 2$. Эта подалгебра содержит ненулевой нильпотентный идеал, состоящий из матриц с нулевой диагональю.

(7.5) Следствие. *Если F-алгебра A полупроста, то любой неприводимый A-модуль изоморфен минимальному правому идеалу из A.*

✎ **(7.6)** Доказать следствие (7.5).

✎ **(7.7)** Пусть V — произвольный A-модуль. Доказать, что

(*i*) если $V\mathrm{J}(A) = 0$, то V вполне приводим,

(*ii*) фактормодуль $V/(V\mathrm{J}(A))$ вполне приводим,

(*iii*) $V\mathrm{J}(A)$ совпадает с пересечением максимальных подмодулей модуля V.

Исследуем теперь вопрос о полупростоте в важном для нас случае групповых алгебр.

(7.8) Предложение. *Пусть G — конечная группа, p — простой делитель порядка $|G|$, и F — поле характеристики p. Тогда $\sum_{g\in G} g \in \mathrm{J}(FG)$. В частности, в этом случае групповая алгебра FG не полупроста.*

✎ Доказать предложение (7.8).

Справедливо также утверждение, обратное к предложению (7.8). Для его доказательства нам понадобится следующее вспомогательное утверждение, являющееся несложным упражнением по линейной алгебре.

(7.9) Лемма. *Пусть φ — линейное преобразование конечномерного векторного пространства V над полем F. Если $\varphi^2 = \varphi$, то $V = \operatorname{Im}\varphi \oplus \operatorname{Ker}\varphi$.*

✎ **(7.10)** Доказать лемму (7.9).

(7.11) Теорема (Машке). *Пусть G — конечная группа и F — поле, характеристика которого не делит порядок $|G|$ (в частности, может быть равна нулю). Тогда групповая алгебра FG полупроста.*

Доказательство. По предложению (7.3) достаточно показать, что произвольный FG-модуль V вполне приводим. Пусть U — подмодуль из V. Найдём подмодуль $W \leqslant V$ такой, что $V = U \oplus W$. Векторное пространство V можно представить в виде прямой суммы $U \oplus U_0$ для некоторого подпространства $U_0 \leqslant V$. Пусть $\pi : V \to V$ — линейное отображение, являющееся проекцией V на U параллельно U_0. Рассмотрим отображение $\tilde{\pi} : V \to V$, которое строится по π следующим образом:

$$v\tilde{\pi} = \frac{1}{|G|}\sum_{g\in G} vg\pi g^{-1}.$$

Другими словами $\tilde{\pi}$ является «усреднением» всех отображений, сопряжённых с π элементами группы G, причём деление на $|G|$ возможно ввиду ограничения на характеристику поля F. Заметим, что $\tilde{\pi}$ является F-линейным и $\operatorname{Im}\tilde{\pi} \subseteq U$, поскольку U — FG-подмодуль. Кроме того, для любого $h \in G$ выполнено

$$vh\tilde{\pi} = \frac{1}{|G|}\sum_{g\in G} (vhg\pi g^{-1}h^{-1})h = v\tilde{\pi}h,$$

откуда следует, что $\tilde{\pi} \in \operatorname{End}_{FG}(V)$. Более того, для любого $u \in U$ имеем $u\tilde{\pi} = u$. Поэтому $U = \operatorname{Im}\tilde{\pi}$ и $\tilde{\pi}^2 = \tilde{\pi}$. По лемме (7.9) получаем $V = U \oplus W$, где $W = \operatorname{Ker}\tilde{\pi}$ — FG-подмодуль модуля V. □

Объединяя утверждения (7.8) и (7.11), получаем критерий полупростоты групповой алгебры.

(7.12) Следствие. *Пусть G — конечная группа и F — поле. Групповая алгебра FG полупроста тогда и только тогда, когда характеристика поля F не делит порядок группы G.*

✎ **(7.13)** Доказать следующее обобщение теоремы Машке. Пусть G — конечная группа, $H \leqslant G$, F — поле характеристики, не делящей индекс $|G : H|$. Если V — FG модуль такой, что FH-модуль V_H вполне приводим, то FG-модуль V также вполне приводим. (*Указание.* Следовать рассуждению из доказательства теоремы Машке.)

✎ **(7.14)** Доказать следующий аналог теоремы Машке. Пусть V — конечная абелева группа и G — такая подгруппа группы $\operatorname{Aut} V$, что $(|V|, |G|) = 1$. Пусть $V = U \oplus U_0$, где U — G-инвариантная подгруппа. Тогда существует G-инвариантная подгруппа $W \leqslant V$ такая, что $V = U \oplus W$. (*Указание.* Доказать аналог леммы (7.9) для случая, когда V — конечная абелева группа и $\varphi \in \operatorname{End} V$. Далее следовать рассуждению из доказательства теоремы Машке.)

Пусть V — A-модуль. Рассмотрим для любого элемента $a \in A$ отображение $a_V : V \to V$, действующее по правилу $a_V : v \mapsto va$. Тогда $a_V \in \operatorname{End}_F(V)$ и отображение $a \mapsto a_V$ является гомоморфизмом F-алгебр $A \to \operatorname{End}_F(V)$. Ядром этого гомоморфизма, как легко видеть, является аннулятор $\operatorname{Ann}(V)$. Обозначим через A_V образ этого гомоморфизма. Таким образом, $A_V \cong A/\operatorname{Ann}(V)$.

(7.15) Предложение. *Для вполне приводимого A-модуля V алгебра A_V полупроста.*

✎ Доказать предложение (7.15).

Оказывается, структуру полупростой алгебры A можно описать, определив однородные компоненты регулярного модуля A°.

(7.16) Теорема (Веддерберна). *Пусть A — полупростая алгебра и M — неприводимый A-модуль.*

(i) $\mathrm{W}_M(A^\circ)$ *— минимальный двусторонний идеал алгебры A.*

(ii) *Пусть U — неприводимый A-модуль. Если $M \ncong U$, то $\mathrm{W}_M(A^\circ) \leqslant \mathrm{Ann}(U)$, а если $M \cong U$, то $\mathrm{W}_M(A^\circ) \cap \mathrm{Ann}(U) = 0$. В частности, справедливо разложение в прямую сумму идеалов*

(7.17)
$$A = \mathrm{W}_M(A^\circ) \oplus \mathrm{Ann}(M).$$

(iii) $\mathrm{W}_M(A^\circ)$ *является простой F-алгеброй, и отображение $a \mapsto a_M$ осуществляет изоморфизм F-алгебр $\mathrm{W}_M(A^\circ) \cong A_M \leqslant \mathrm{End}_F(M)$.*

(iv) *Алгебра A является прямой суммой простых алгебр*

$$A = \bigoplus_{U \in \mathscr{M}(A)} \mathrm{W}_U(A^\circ).$$

Доказательство. Сразу отметим, что $\mathrm{W}_M(A^\circ) \neq 0$, т. к. по следствию (7.5) модуль A° содержит подмодуль, изоморфный M. Мы сначала покажем, что $\mathrm{W}_M(A^\circ)$ — идеал. Его минимальность будет установлена чуть ниже. Легко видеть, что для любого $a \in A$ отображение $a_l : x \mapsto ax$ принадлежит алгебре $\mathrm{End}_A(A^\circ)$. По пункту (i) предложения (6.6) выполнено включение $\mathrm{W}_M(A^\circ)a_l \subseteq \mathrm{W}_M(A^\circ)$, т. е. правый идеал $\mathrm{W}_M(A^\circ)$ выдерживает умножения слева на элементы из A и, значит, является двусторонним.

Если $U \ncong M$, то, как мы уже отмечали, $\mathrm{W}_U(A^\circ) \cap \mathrm{W}_M(A^\circ) = 0$. Поскольку $\mathrm{W}_U(A^\circ)$ и $\mathrm{W}_M(A^\circ)$ — идеалы, имеет место равенство $\mathrm{W}_U(A^\circ)\mathrm{W}_M(A^\circ) = 0$. По определению $\mathrm{W}_U(A^\circ)$ — сумма подмодулей из A°, изоморфных U. Пусть $U_0 \leqslant \mathrm{W}_U(A^\circ)$ — один из них. Тогда $\mathrm{W}_M(A^\circ) \subseteq \mathrm{Ann}(U_0)$. Однако $\mathrm{Ann}(U_0) = \mathrm{Ann}(U)$, ввиду изоморфизма $U_0 \cong U$.

Пусть $U \cong M$. Предположим, что $I = \mathrm{W}_M(A^\circ) \cap \mathrm{Ann}(U) \neq 0$. Тогда любой неприводимый подмодуль из I является подмодулем $\mathrm{W}_M(A^\circ)$ и, значит, изоморфен U. Пусть U_0 — один из таких подмодулей. Тогда $U_0 \leqslant \mathrm{Ann}(U) = \mathrm{Ann}(U_0)$, откуда следует, что $U_0^2 = 0$, т. е. идеал U_0 нильпотентен. По предложению (4.11) получаем $U_0 \leqslant \mathrm{J}(A)$ вопреки полупростоте алгебры A. Отсюда следует, что сумма $\mathrm{W}_M(A^\circ) + \mathrm{Ann}(M)$ прямая. Кроме того, $\mathrm{W}_M(A^\circ) + \mathrm{Ann}(M) = A$, поскольку полупростой модуль A° является суммой своих однородных компонент. Отсюда вытекает (ii).

Ввиду (ii) всякий элемент $a \in A$ представим в виде $a = b + c$, где $b \in \mathrm{W}_M(A^\circ)$ и $c \in \mathrm{Ann}(M)$. Поэтому $a_M = b_M$ и, значит, гомоморфизм $a \mapsto a_M$ сюръективно отображает $\mathrm{W}_M(A^\circ)$ на A_M. Если $a \in \mathrm{W}_M(A^\circ)$ и $a_M = 0$, то в силу (ii) получаем $a \in \mathrm{W}_M(A^\circ) \cap \mathrm{Ann}(A) = 0$. Таким образом, отображение $a \mapsto a_M$ осуществляет изоморфизм F-алгебр $\mathrm{W}_M(A^\circ)$ и A_M.

Докажем минимальность идеала $\mathrm{W}_M(A^\circ)$. Пусть $I \leqslant \mathrm{W}_M(A^\circ)$ — идеал алгебры A. Если $I < \mathrm{W}_M(A^\circ)$, то ввиду полупростоты модуля $\mathrm{W}_M(A^\circ)$, существует минимальный правый идеал $I_0 \leqslant \mathrm{W}_M(A^\circ)$ алгебры A такой, что $I \cap I_0 = 0$. Заметим, что $I_0 \cong M$, т. к. любой композиционный фактор модуля $\mathrm{W}_M(A^\circ)$ изоморфен M по пункту (ii) предложения (6.6). Тогда $I_0 I \leqslant I_0 \cap I = 0$, т. е. $I \leqslant \mathrm{Ann}(I_0) = \mathrm{Ann}(M)$, но с другой стороны $I \leqslant \mathrm{W}_M(A^\circ)$. По пункту (ii) имеем $\mathrm{Ann}(M) \cap \mathrm{W}_M(A^\circ) = 0$, т. е. $I = 0$. Отсюда следует (i).

Разложение в (iv) следует из (7.17) и того, что полупростой модуль A° является суммой всех компонент $\mathrm{W}_U(A^\circ)$. Эта сумма прямая в силу (ii).

Отметим, наконец, что что любой идеал алгебры $\mathrm{W}_M(A^\circ)$ будет также идеалом в A, что вытекает из разложения в (iv) и доказанного выше равенства $\mathrm{W}_{M_1}(A^\circ)\mathrm{W}_{M_2}(A^\circ) = 0$ для неизоморфных неприводимых A-модулей M_1 и M_2. Отсюда следует простота алгебры $\mathrm{W}_M(A^\circ)$, и тем самым полностью доказаны (iii) и (iv). □

Таким образом, теорема Веддерберна по существу сводит изучение полупростых F-алгебр к простым.

(7.18) Предложение. *Пусть A — F-алгебра и V — неприводимый A-модуль. Тогда алгебра A_V простая. В частности, $|\mathscr{M}(A_V)| = 1$.*

✎ Доказать предложение (7.18).

✎ **(7.19)** *Группой кватернионов* называется группа

$$Q_8 = \langle x, y \mid x^4 = 1, \;\; y^2 = x^2, \;\; x^y = x^{-1} \rangle.$$

Сколько различных двусторонних идеалов в алгебре $\mathbb{C}Q_8$?

(7.20) Теорема (о двойном централизаторе). *Пусть A — простая F-алгебра и $I \neq 0$— правый идеал из A. Обозначим $B = \mathrm{End}_A(I)$. Тогда для любого $a \in A$ преобразование a_I является эндоморфизмом B-модуля I. Кроме того, $A_I = \mathrm{End}_B(I)$ и отображение $a \mapsto a_I$ является изоморфизмом F-алгебр $A \to \mathrm{End}_B(I)$.*

Доказательство. Мы уже отмечали (см. упражнение (3.21)), что B является F-алгеброй и I — B-модулем. Поэтому $\mathrm{End}_B(I)$ снова является F-алгеброй. Для произвольного элемента $a \in A$ выполнены равенства

$$(x\varphi)a_I = (x\varphi)a = (xa)\varphi = (xa_I)\varphi$$

при любых $x \in I$, $\varphi \in B$. Поэтому $a_I \in \mathrm{End}_B(I)$.

Покажем, что отображение $a \mapsto a_I$ является изоморфизмом алгебр. Перед формулировкой теоремы Веддерберна (7.16) мы отметили, что оно является гомоморфизмом алгебр с ядром $\mathrm{Ann}(I)$. Из простоты алгебры A следует, что $\mathrm{Ann}(I) = 0$ и, значит, это отображение инъективно.

Прежде, чем доказывать сюръективность, сделаем одно замечание. Для произвольного $u \in I$ рассмотрим отображение $u_l : I \to I$, действующее по правилу $x \mapsto ux$ для любого $x \in I$. Поскольку для всех $x \in I$ и $a \in A$ выполнено

$$(xu_l)a = (ux)a = u(xa) = (xa)u_l,$$

имеем $u_l \in B$. В частности, действие u_l на I перестановочно с действием произвольного элемента $\varphi \in \mathrm{End}_B(I)$.

Итак, нам осталось показать, что $A_I = \{\, a_I \mid a \in A\} = \mathrm{End}_B(I)$. Заметим, что $A = AI$, поскольку AI — ненулевой двусторонний идеал в A и алгебра A простая. Поскольку $1_I \in A_I$ — единица в $\mathrm{End}_B(I)$, достаточно показать, что $A_I = (AI)_I$ — правый идеал в $\mathrm{End}_B(I)$. Пусть $a \in A$, $x \in I$, $\varphi \in \mathrm{End}_B(I)$. Поскольку элементы из AI — это суммы произведений вида ax, то достаточно показать, что $(ax)_I\varphi \in (AI)_I$. Учитывая предыдущее замечание о перестановочности действия φ с операторами левого умножения на элементы из I, получаем следующую цепочку равенств для произвольного $y \in I$

$$y((ax)_I\varphi) = (y(ax)_I)\varphi = (yax)\varphi = (x(ya)_l)\varphi = (x\varphi)(ya)_l = ya(x\varphi) = y(a(x\varphi))_I,$$

поскольку $ya \in I$. В силу произвольности y, имеет место требуемое включение $(ax)_I\varphi = (a(x\varphi))_I \in (AI)_I$. □

Объясним, почему предыдущее утверждение носит название «теорема о двойном централизаторе». Если S — некоторая алгебра и $X \subseteq S$ — произвольное подмножество, то *централизатором* X в S называется множество

$$\mathrm{C}_S(X) = \{s \in S \mid sx = xs \ \text{ для всех } x \in X\}$$

которое, как легко видеть, является подалгеброй в S. В частности, $\mathrm{Z}(S) = \mathrm{C}_S(S)$.

Теперь в обозначениях теоремы (7.20) мы можем записать $B = \mathrm{End}_A(I) = \mathrm{C}_{\mathrm{End}_F(I)}(A_I)$ и $\mathrm{End}_B(I) = \mathrm{C}_{\mathrm{End}_F(I)}(B)$. Поэтому основное утверждение теоремы состоит в том, что для простой F-алгебры A и её ненулевого правого идеала I выполнено равенство

$$A_I = \mathrm{C}_{\mathrm{End}_F(I)}(\mathrm{C}_{\mathrm{End}_F(I)}(A_I)).$$

Важным следствием из теоремы (7.20) является описание строения простых алгебр над алгебраически замкнутым полем.

(7.21) Следствие. *Пусть A — простая F-алгебра и F — алгебраически замкнутое поле. Если V — неприводимый A-модуль, то $A \cong \mathrm{End}_F(V)$. В частности, $\dim_F A = (\dim_F V)^2$ и имеет место изоморфизм A-модулей*

$$A^\circ \cong \underbrace{V \oplus \ldots \oplus V}_{\dim_F V}.$$

Доказательство. В силу следствия (7.5) можно считать, что V — минимальный правый идеал из A. Изоморфизм $A \cong \mathrm{End}_F(V)$ вытекает теоремы (7.20) и следствия (3.41) из леммы Шура. Разложение регулярного модуля A° следует из теоремы (7.16) и пункта (ii) предложения (6.6). □

(7.22) Следствие. *Пусть A — полупростая F-алгебра и F — алгебраически замкнутое поле. Тогда*

(i) $\dim_F A = \sum_{M \in \mathscr{M}(A)} (\dim_F M)^2$,

(ii) $\dim_F Z(A) = |\mathscr{M}(A)|$.

✎ **(7.23)** Доказать следствие (7.22)

Для групповых алгебр, учитывая предложения (3.7) и (7.11), следствие (7.22) можно переформулировать так:

(7.24) Следствие. *Пусть G — конечная группа и F — алгебраически замкнутое поле, характеристика которого не делит $|G|$. Тогда*

(i) $|G| = \sum_{M \in \mathscr{M}(FG)} (\dim_F M)^2$,

(ii) $|\mathscr{M}(FG)| = |\mathscr{K}(G)|$.

8. Представления алгебр

(8.1) Определение. *Представлением* F-алгебры A называется гомоморфизм F-алгебр

$$\mathscr{X} : A \to \mathrm{M}_n(F)$$

для некоторого $n \geqslant 1$. Число n называется *степенью представления* $\mathscr{X}$ и обозначается $\deg \mathscr{X}$. Представления степени 1 мы будем часто называть *линейными*.

✓ Символы представлений мы будем писать слева от аргумента.

Легко видеть, что если $\mathscr{X}$ — представление степени n алгебры A и P — невырожденная матрица из $\mathrm{M}_n(F)$, то отображение $a \mapsto P^{-1}\mathscr{X}(a)P$ определяет новое представление степени n алгебры A. Однако это новое представление, как мы сейчас увидим, мало отличается от исходного.

Два представления $\mathscr{X}$ и $\mathscr{Y}$ алгебры A называются *эквивалентными*, если существует невырожденная матрица P такая, что $\mathscr{Y}(a) = P^{-1}\mathscr{X}(a)P$ для всех $a \in A$.

Из представлений легко строить модули, а из модулей — представления. Пусть $V = F^n$ — пространство строк и $\mathscr{X}$ — представление степени n. Если положить $va = v\mathscr{X}(a)$ для всех $v \in V$, $a \in A$, то таким образом на V задаётся структура A-модуля. Такой A-модуль будем называть *модулем, соответствующим представлению* $\mathscr{X}$.

Обратно, пусть V — A-модуль, имеющий размерность $n \geqslant 1$ над F. Выберем базис $v_1, \ldots, v_n$ пространства V и для любого $a \in A$ запишем $v_i a = \alpha_{i1}v_1 + \ldots + \alpha_{in}v_n$. Тогда отображение $a \mapsto (\alpha_{ij})$ является представлением алгебры A степени n. Такое представление мы будем называть [13] *представлением, соответствующим модулю* V в базисе $v_1, \ldots, v_n$.

(8.2) Предложение. *Модули, соответствующие эквивалентным представлениям, изоморфны. Обратно, представления, соответствующие изоморфным модулям, эквивалентны. В частности, представления, соответствующие одному и тому же модулю в различных базисах, эквивалентны.*

✎ Доказать предложение (8.2).

Пусть V — векторное пространство размерности $n \geqslant 1$ над полем F. Изоморфизм F-алгебр $\mathrm{End}_F(V) \cong \mathrm{M}_n(F)$ позволяет также использовать термин «представление» для любого гомоморфизма $\mathscr{X} : A \to \mathrm{End}_F(V)$.

(8.3) Примеры представлений алгебр Пусть A — F-алгебра.

1. *Регулярным представлением* $\mathscr{R}$ будем называть представление, соответствующее регулярному модулю A°.

2. Если $\mathscr{X}$ — представление A и B — подалгебра в A, то ограничение $\mathscr{X}_B$ представления $\mathscr{X}$ на B является представлением алгебры B.

3. Если $I \trianglelefteqslant A$, $\varphi : A \to A/I$ — естественный гомоморфизм алгебр и $\mathscr{X}$ — представление факторалгебры A/I, то композиция $\mathscr{Y} = \mathscr{X} \circ \varphi$ является представлением алгебры A. При этом $\deg \mathscr{Y} = \deg \mathscr{X}$ и $I \subseteq \mathrm{Ker}\,\mathscr{Y}$. Обратно, если $\mathscr{Y}$ — представление алгебры A, и $I \subseteq \mathrm{Ker}\,\mathscr{Y}$, то существует единственное представление $\mathscr{X}$ факторалгебры A/I такое, что $\mathscr{Y} = \mathscr{X} \circ \varphi$.

✎ Проверить сформулированные в (8.3) утверждения.

Представление алгебры A называется *неприводимым (приводимым, вполне приводимым, неразложимым)*, если таким является соответствующий ему A-модуль.

Из сделанных выше замечаний о соответствии представлений и модулей, а также из предложения (5.1) получаем

(8.4) Следствие. *У любой F-алгебры A существует лишь конечное число попарно неэквивалентных неприводимых представлений.*

(8.5) Предложение. *Пусть A — F-алгебра и $\mathscr{X}_1, \ldots, \mathscr{X}_s$ — полная система её попарно неэквивалентных неприводимых представлений. Тогда*

$$\mathrm{J}(A) = \bigcap_{i=1}^{s} \mathrm{Ker}\,\mathscr{X}_i.$$

[13] Мы не определяем представление, соответствующее нулевому модулю.

✎ Доказать предложение (8.5).

Такие свойства представлений, как неприводимость, полная приводимость и т. д. можно выразить на матричном языке, не переходя к соответствующим модулям.

Пусть $\mathscr{X}$ — приводимое представление алгебры A и V — соответствующий ему модуль. Тогда V содержит нетривиальный собственный подмодуль U. Выберем в V базис так, чтобы последние его векторы образовывали базис U. Тогда в этом «согласованном» с рядом

$$V > U > 0$$

базисе представление, соответствующее модулю V, имеет блочный вид

(8.6)
$$a \mapsto \begin{pmatrix} \mathscr{X}_1(a) & * \\ \mathbf{0} & \mathscr{X}_2(a) \end{pmatrix}, \quad a \in A,$$

где $\mathscr{X}_1$ и $\mathscr{X}_2$ — некоторые представления алгебры A. При этом $\mathscr{X}_2$ соответствует A-модулю U, а $\mathscr{X}_1$ — фактормодулю V/U. Таким образом, приводимое представление $\mathscr{X}$ эквивалентно представлению (8.6), которое в дальнейшем для краткости мы будем записывать в виде

$$\begin{pmatrix} \mathscr{X}_1 & * \\ \mathbf{0} & \mathscr{X}_2 \end{pmatrix}.$$

Обратно, представление алгебры A, эквивалентное представлению такого вида, очевидно, приводимо.

Аналогично, представление $\mathscr{X}$ разложимо тогда и только тогда, когда оно эквивалентно представлению блочного вида

$$\begin{pmatrix} \mathscr{X}_1 & \mathbf{0} \\ \mathbf{0} & \mathscr{X}_2 \end{pmatrix}.$$

В этом случае мы будем писать $\mathscr{X} = \mathscr{X}_1 \oplus \mathscr{X}_2$ и говорить, что $\mathscr{X}$ является *прямой суммой представлений* $\mathscr{X}_1$ и $\mathscr{X}_2$.

Если $\mathscr{X}$ — произвольное представление, то оно эквивалентно блочно-верхнетреугольному представлению

$$\begin{pmatrix} \mathscr{X}_1 & * & \cdots & * \\ \mathbf{0} & \mathscr{X}_2 & \cdots & * \\ \cdots & \cdots & \cdots & \cdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathscr{X}_k \end{pmatrix}$$

с неприводимыми представлениями $\mathscr{X}_1, \ldots, \mathscr{X}_k$ на диагонали. Чтобы показать это, достаточно, как и выше, взять у модуля V, соответствующего $\mathscr{X}$, взять композиционный ряд

$$V = V_0 > V_1 > \ldots > V_k = 0,$$

и «согласованный» с ним базис. Неприводимые представления $\mathscr{X}_i$, соответствующие факторам V_{i-1}/V_i, $i = 1, \ldots, k$, будем называть *неприводимыми (простыми) компонентами* представления $\mathscr{X}$. Из теоремы Жордана-Гёльдера (3.33) следует, что набор неприводимых компонент представления $\mathscr{X}$ определён однозначно с точностью до эквивалентности. В используемых обозначениях неприводимую компоненту $\mathscr{X}_1$ (компоненту $\mathscr{X}_k$) мы будем называть *верхней* (*нижней*). Верхняя (нижняя) неприводимая компонента представления соответствует неприводимому фактормодулю (подмодулю) модуля V и, вообще говоря неверно, что она определена однозначно с точностью до эквивалентности, как можно увидеть на примере регулярного представления полупростой, но не простой алгебры.

Пусть $\mathscr{X}$ — вполне приводимое представление алгебры A. Поскольку модуль V, соответствующий $\mathscr{X}$, изоморфен прямой сумме неприводимых модулей $V_1, \ldots, V_k$, то $\mathscr{X}$ эквивалентно блочно-диагональному представлению

$$\begin{pmatrix} \mathscr{X}_1 & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathscr{X}_2 & \cdots & \mathbf{0} \\ \cdots & \cdots & \cdots & \cdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathscr{X}_k \end{pmatrix},$$

где $\mathscr{X}_i$ — неприводимое представление, соответствующее модулю V_i, $i = 1, \ldots, k$. Обратно, если некоторое представление $\mathscr{X}$ эквивалентно представлению такого вида с неприводимыми компонентами $\mathscr{X}_i$, то оно вполне приводимо.

9. Характеры представлений алгебр

Следом $n \times n$-матрицы $B = (\beta_{ij})$ называется сумма $\operatorname{tr} B = \beta_{11} + \ldots + \beta_{nn}$ её диагональных элементов.

✎ **(9.1)** Пусть B, C — $n \times n$-матрицы над полем F. Доказать, что $\operatorname{tr}(BC) = \operatorname{tr}(CB)$. В частности, следы сопряжённых матриц совпадают.

Пусть A — F-алгебра. *Характером представления* $\mathscr{X}$ *алгебры* A называется отображение $\chi : A \to F$, заданное соотношением $\chi(a) = \operatorname{tr} \mathscr{X}(a)$, для всех $a \in A$.

Соответствие между представлениями и модулями и предложение (8.2) позволяют говорить об характерах для произвольных A-модулей.

✓ Отметим, что характер χ некоторого представления $\mathscr{X}$ алгебры A является F-линейным отображением $A \to F$, но если $\deg \mathscr{X} > 1$, то, вообще говоря, не является гомоморфизмом F-алгебр.

Если χ_1 и χ_2 — характеры представлений $\mathscr{X}_1$ и $\mathscr{X}_2$, то их сумма $\chi_1 + \chi_2$ также является характером, например, представления $\mathscr{X}_1 \oplus \mathscr{X}_2$. Поэтому множество характеров алгебры замкнуто относительно сложения.

✎ **(9.2)** Доказать, что характеры эквивалентных представлений совпадают.

(9.3) Вообще говоря, неэквивалентные представления F-алгебры A могут обладать одинаковыми характерами. Например, в качестве A можно рассмотреть групповую алгебру FG, где F — поле характеристики 2 и G — циклическая группа порядка 2, порождённая элементом g. Пусть представления $\mathscr{X}$ и $\mathscr{Y}$ алгебры A задаются на порождающем элементе g равенствами

$$\mathscr{X}(g) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathscr{Y}(g) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Тогда представления $\mathscr{X}$ и $\mathscr{Y}$, очевидно, неэквивалентны, в то время как их характеры тождественно равны нулю. Однако, имеет место следующее утверждение.

(9.4) Предложение. *Пусть A — F-алгебра, где F — алгебраически замкнутое поле. Пусть $\mathscr{X}_1, \ldots, \mathscr{X}_s$ — некоторые попарно неэквивалентные неприводимые представления алгебры A и $\chi_1, \ldots, \chi_s$ — соответствующие им характеры. Тогда*

(*i*) *все представления $\mathscr{X}_i$ сюръективны,*

(*ii*) *существуют элементы $a_1, \ldots, a_s \in A$ такие, что $\chi_i(a_j) = \delta_{ij}$,*

(*iii*) *характеры $\chi_1, \ldots, \chi_s$ являются линейно независимыми. В частности, они все ненулевые и попарно различны.*

Доказательство. (*i*) Пусть M — неприводимый A-модуль, соответствующий представлению $\mathscr{X}_i$. Достаточно показать, что $A_M = \operatorname{End}_F(M)$. Заметим, что M также является неприводимым A_M-модулем, и A_M — простая алгебра в силу (7.18). Поэтому по следствию (7.21) получаем $A_M = \operatorname{End}_F(M)$.

(*ii*) Так как для всех неприводимых A-модулей M_j имеет место включение $\mathrm{J}(A) \leqslant \operatorname{Ann}(M_j)$, из предложения (3.42)(*iv*) следует, что модули M_j можно рассматривать как (неприводимые) модули полупростой алгебры $A/\mathrm{J}(A)$.

Пусть теперь M_i — неприводимый A-модуль, а χ_i — характер, соответствующие представлению $\mathscr{X}_i$. Выберем элемент $a_i \in A$ так, чтобы его образ при гомоморфизме $A \to A/\mathrm{J}(A)$ лежал в M_i-однородной компоненте алгебры $A/\mathrm{J}(A)$ и действовал на M_i как какое-нибудь наперёд заданное преобразование из $\operatorname{End}_F(M_i)$ со следом 1 (последнее возможно в силу (*i*)). Тогда a_i аннулирует все неприводимые модули M_j, не изоморфные M_i, что следует из теоремы (7.16)(*ii*). Поэтому получаем $\chi_j(a_i) = \delta_{ij}$.

(*iii*) Если для некоторых $\alpha_j \in F$ выполнено равенство $\alpha_1\chi_1 + \ldots + \alpha_s\chi_s = 0$, то, взяв значение обеих частей на элементе a_j, определённом в (*ii*), получим $\alpha_j = 0$. $\square$

(9.5) Предложение. *Пусть $\mathscr{X} : A \to \mathrm{M}_n(F)$ — неприводимое представление алгебры A над алгебраически замкнутым полем F. Если $M \in \mathrm{M}_n(F)$ удовлетворяет $\mathscr{X}(a)M = M\mathscr{X}(a)$ для всех $a \in A$, то M — скалярная матрица. В частности, для любого $z \in \mathrm{Z}(A)$ образ $\mathscr{X}(z)$ — скалярная матрица. Следовательно, если алгебра A коммутативна, то $\deg \mathscr{X} = 1$.*

✎ Доказать предложение (9.5).

Из предложения (3.43) вытекает

(9.6) Предложение. *Всякое неприводимое представление F-алгебры A является верхней неприводимой компонентой её регулярного представления.*

10. Представления и характеры групп

(10.1) Определение. Пусть G — конечная группа. *Представлением* группы G над полем F (или F-*представлением*) называется гомоморфизм групп

$$\mathscr{X} : G \to \mathrm{GL}_n(F)$$

для некоторого $n \geqslant 1$.

Представление $\mathscr{X}$ группы G однозначно продолжается по линейности до представления степени n алгебры FG, которое мы, как правило, будем обозначать тем же символом $\mathscr{X}$. Наоборот, если $\mathscr{X}$ — представление алгебры FG, то его ограничение на G будет представлением группы. Поэтому все понятия, определённые для представлений алгебр (степень, эквивалентность, неприводимость, и т. д.) можно перенести на представления групп.

Ядро представления $\mathscr{X}$ группы G будем обозначать через $\ker \mathscr{X}$, чтобы подчеркнуть его отличие от ядра $\operatorname{Ker} \mathscr{X}$ представления $\mathscr{X}$ алгебры FG.

Пусть $\mathscr{X}$ — F-представление степени n группы G и K — подкольцо поля F. Будем говорить, что $\mathscr{X}$ *записано над* K, если $\mathscr{X}(g) \in \mathrm{M}_n(K)$ для всех $g \in G$. Также будем говорить, что $\mathscr{X}$ *может быть записано над* K, если оно эквивалентно некоторому F-представлению, записанному над K.

✎ **(10.2)** Показать, что группа кватернионов Q_8 имеет единственное неприводимое $\mathbb{C}$-представление $\mathscr{X}$ степени 2, и это представление не может быть записано над $\mathbb{R}$.

Пусть $\mathscr{X}$ — представление группы G над полем F. Отображение $\chi : G \to F$, задаваемое правилом $\chi(g) = \operatorname{tr} \mathscr{X}(g)$ для всех $g \in G$ называется *F-характером представления $\mathscr{X}$ группы G* или просто *F-характером группы G*.

Как следует из определения, F-характер представления $\mathscr{X}$ группы G над полем F совпадает с ограничением на G характера представления $\mathscr{X}$ алгебры FG.

Отметим, что, как и в случае алгебр, F-характеры групп, вообще говоря, не являются гомоморфизмами групп.[14)]

(10.3) Примеры представлений и характеров групп

1. У любой группы G есть *тривиальное n-мерное представление*, заданное по правилу $\mathscr{X}(g) = \mathbf{1}_n$ для всех $g \in G$. Это представление соответствует тривиальному n-мерному FG-модулю.

2. Будем называть *линейным* F-характер 1-мерного представления группы G. Всякий линейный F-характер является гомоморфизмом групп $G \to F^{\times}$.

3. Тривиальное 1-мерное F-представление группы G будем называть *главным*, а его характер 1_G — *главным* F-характером группы G. При этом $1_G(g) = 1$ для всех $g \in G$. Главное представление соответствует главному FG-модулю, см. (3.19).

4. Характер ρ регулярного F-представления $\mathscr{R}$ группы G будем называть *регулярным характером группы G*. При этом для любого $g \in G$
$$\rho(g) = \begin{cases} 0_F, & g \neq 1; \\ |G| \cdot 1_F, & g = 1. \end{cases}$$

5. Если $\mathscr{X}$ — F-представление группы G и $H \leqslant G$, то обозначим через $\mathscr{X}_H$ ограничение представления $\mathscr{X}$ на H. Тогда $\mathscr{X}_H$ является F-представлением группы H, и если V — FG-модуль, соответствующий представлению $\mathscr{X}$, то V_H — FH-модуль, соответствующий $\mathscr{X}_H$.

6. Если $N \trianglelefteqslant G$, $\varphi : G \to G/N$ — естественный гомоморфизм групп и $\mathscr{X}$ — F-представление факторгруппы G/N, то композиция $\mathscr{Y} = \mathscr{X} \circ \varphi$ является F-представлением группы G. При этом $\deg \mathscr{Y} = \deg \mathscr{X}$ и $N \subseteq \ker \mathscr{Y}$. Обратно, если $\mathscr{Y}$ — F-представление группы G, и $N \subseteq \ker \mathscr{Y}$, то существует единственное F-представление $\mathscr{X}$ факторгруппы G/N такое, что $\mathscr{Y} = \mathscr{X} \circ \varphi$. (Ср. (8.3), пример 3.)

7. Пусть $\mathscr{X}$ — F-представление группы G и V — соответствующий ему FG-модуль. Представление, соответствующее контрагредиентному модулю V^* называется *контрагредиентным представлением* и

[14)] См., однако, (10.3), пример 2.

обозначается $\mathscr{X}^*$. В двойственном базисе[15] модуля V^* контрагредиентное представление $\mathscr{X}^*$ задаётся равенством[16]

$$\mathscr{X}^*(g) = \mathscr{X}(g)^{\iota},$$

а характеры χ и χ^* представлений $\mathscr{X}$ и $\mathscr{X}^*$ связаны соотношением

$$\chi^*(g) = \chi(g^{-1})$$

для всех $g \in G$.

✎ Проверить сформулированные в (10.3) утверждения.

Неприводимым F-характером группы G мы будем называть F-характер её неприводимого представления над полем F. Множество всех неприводимых F-характеров группы G будем обозначать $\mathrm{Irr}_F(G)$. Из сделанных выше замечаний о приведении произвольного представления к блочно-верхнетреугольному виду с неприводимыми компонентами на диагонали следует, что всякий F-характер ψ группы представляется в виде

(10.4)
$$\psi = \sum_{\chi \in \mathrm{Irr}_F(G)} n_\chi \chi,$$

для некоторых неотрицательных целых чисел n_χ.

Из (9.1) следует, что F-характеры группы являются примерами так называемых классовых функций. *Классовой функцией* на группе G со значениями в поле F называется отображение $\varphi : G \to F$, принимающее для любого класса сопряжённости группы G одинаковые значения на всех элементах этого класса. Множество всех классовых функций на группе G со значениями в поле F будем обозначать через $\mathrm{cf}_F(G)$.

(10.5) Предложение. *Пусть G — группа и F — поле. Имеют место следующие утверждения.*

(i) $\mathrm{cf}_F(G)$ *является подалгеброй в F-алгебре $\mathrm{f}_F(G)$ всех F-значных функций на G.*

(ii) $\dim_F \mathrm{cf}_F(G) = |\mathscr{K}(G)|$.

✎ Доказать предложение (10.5).

Алгебру $\mathrm{cf}_F(G)$ будем называть *F-алгеброй классовых функций на группе G со значениями в поле F.*

Всякую классовую функцию $\varphi \in \mathrm{cf}_F(G)$ $\big($как и вообще любую функцию из $\mathrm{f}_F(G)\big)$ можно естественным образом продолжить до F-линейного отображения из FG в F, которое мы без специальных оговорок будем обозначать тем же символом φ. Подчеркнём, что для произвольного элемента $x \in FG$ равенство $(\varphi\psi)(x) = \varphi(x)\psi(x)$, вообще говоря, уже не имеет места.

Из предложения (9.4)(iii), следствия (7.24), теоремы (7.11) и замечаний после предложения (6.6) вытекает

(10.6) Предложение. *Пусть G — конечная группа и F — алгебраически замкнутое поле характеристики, не делящей $|G|$. Тогда справедливы следующие утверждения.*

(i) $|G| \cdot 1_F = \sum_{\chi \in \mathrm{Irr}_F(G)} \chi(1)^2$.

(ii) $\mathrm{Irr}_F(G)$ — *базис алгебры* $\mathrm{cf}_F(G)$. *В частности, в разложении* (10.4) *произвольного F-характера ψ образы коэффициентов n_χ в поле F (т. е. элементы $n_\chi \cdot 1_F \in F$) определяются однозначно.*

(iii) *Неэквивалентные F-представления группы G обладают различными F-характерами.*

Таким образом, предложение (9.4) демонстрирует ключевую идею теории характеров. Хотя значение F-характера представления $\mathscr{X}$ на каждом конкретном элементе $g \in G$ несёт мало информации о матрице $\mathscr{X}(g)$, совокупность этих значений по всем элементам группы G может по существу целиком определять представление $\mathscr{X}$.

Как и для алгебр, множество F-характеров группы замкнуто относительно сложения. Покажем, что оно также замкнуто относительно умножения. Для этого нам понадобится конструкция тензорного произведения модулей групповой алгебры.

[15] См. (2.33).

[16] Напомним, что $M^{\iota} = (M^{-1})^{\top}$ для квадратной невырожденной матрицы M.

11. Тензорное произведение FG-модулей

Пусть V и W — FG-модули. Мы построим новый FG-модуль $V\otimes W$, называемый *тензорным произведением модулей V и W*. Выберем F-базисы $v_1,\ldots,v_n$ и $w_1,\ldots,w_m$ модулей V и W, соответственно. Пусть $V\otimes W$ обозначает векторное пространство над полем F размерности nm, базисом которого являются векторы, обозначаемые $v_j\otimes w_j$. Другими словами, $V\otimes W$ — это множество всевозможных формальных линейных комбинаций $\sum\alpha_{ij}(v_j\otimes w_j)$, где $\alpha_{ij}\in F$. Если $v\in V$ и $w\in W$, то пусть $v=\sum\alpha_i v_i$ и $w=\sum\beta_j w_j$ и положим по определению

$$v\otimes w=\sum_{i,j}\alpha_i\beta_j(v_i\otimes w_j)\in V\otimes W.$$

Отметим, что, вообще говоря, не любой элемент из $V\otimes W$ имеет вид $v\otimes w$ для некоторых $v\in V$ и $w\in W$. Определим действие группы G на $V\otimes W$, полагая

$$(v_i\otimes w_j)g=v_ig\otimes w_jg$$

для всех $g\in G$ и продолжая это действие по линейности на всё пространство $V\otimes W$ и всю групповую алгебру FG. В частности, $(v\otimes w)g=vg\otimes wg$ для любых $v\in V$, $w\in W$ и $g\in G$. Таким образом на $V\otimes W$ задаётся структура FG-модуля.

(11.1) Проверить корректность данного определения. Доказать, что FG-модуль $V\otimes W$ определяется модулями V и W с точностью до изоморфизма, т. е. не зависит от выбора базисов пространств V и W.

Важно отметить, что не для любого $a\in FG$ выполнено равенство $(v\otimes w)a=va\otimes wa$. Поэтому мы сначала задали действие на $V\otimes W$ для групповых элементов, и затем продолжили его по линейности. Если A – произвольная алгебра, а V и W — её модули, то задать на пространстве $V\otimes W$ структуру A-модуля удаётся, вообще говоря, не всегда.

Переведём понятие тензорного произведения FG-модулей на язык представлений.

Напомним, что *кронекеровым произведением* матриц $A=(\alpha_{ij})\in\mathrm{M}_m(F)$ и $B=(\beta_{kl})\in\mathrm{M}_n(F)$ называется $mn\times mn$-матрица

$$A\otimes B=\begin{pmatrix}\alpha_{11}B & \ldots & \alpha_{1m}B\\ \ldots & \ldots & \ldots\\ \alpha_{m1}B & \ldots & \alpha_{mm}B\end{pmatrix}.$$

(11.2) Предложение. *Показать, что для любых $A,C\in\mathrm{M}_m(F)$, $B,D\in\mathrm{M}_n(F)$, $\alpha\in F$*

(i) $\operatorname{tr}(A\otimes B)=\operatorname{tr}A\cdot\operatorname{tr}B$;

(ii) $\det(A\otimes B)=(\det A)^n\cdot(\det B)^m$;

(iii) $(A\otimes B)(C\otimes D)=AC\otimes BD$;

(iv) $(A+C)\otimes B=A\otimes B+C\otimes B,\quad B\otimes(A+C)=B\otimes A+B\otimes C$;

(v) $(\alpha A)\otimes B=A\otimes(\alpha B)=\alpha(A\otimes B)$;

(vi) если $\mu_1,\ldots,\mu_m$ и $\nu_1,\ldots,\nu_n$ — характеристические значения матриц A и B, соответственно, то все характеристическими значения матрицы $A\otimes B$ исчерпываются величинами $\mu_i\nu_j$ при $i=1,\ldots,m$ и $j=1,\ldots,n$.

Доказать предложение (11.2).

Пусть $\mathscr{X}$ и $\mathscr{Y}$ — F-представления группы G степеней m и n, соответственно. Положим

$$(\mathscr{X}\otimes\mathscr{Y})(g)=\mathscr{X}(g)\otimes\mathscr{Y}(g)$$

для всех $g\in G$. Из (11.2) следует, что таким образом определено отображение

$$\mathscr{X}\otimes\mathscr{Y}:G\to\mathrm{GL}_{mn}(F),$$

которое является F-представлением группы G. Назовём $\mathscr{X}\otimes\mathscr{Y}$ *тензорным произведением* представлений $\mathscr{X}$ и $\mathscr{Y}$.

(11.3) Предложение. *Пусть V и W — FG-модули с базисами $v_1,\ldots,v_m$ и $w_1,\ldots,w_n$ и характерами χ и ψ, соответственно. Пусть $\mathscr{X}$ и $\mathscr{Y}$ — представления группы G, соответствующие FG-модулям V и W в выбранных базисах. Тогда верны следующие утверждения.*

(i) F-представление группы G, соответствующее модулю $V\otimes W$ в базисе

$$v_1\otimes w_1,\ \ldots,\ v_1\otimes w_n,\ \ldots,\ v_m\otimes w_1,\ \ldots,\ v_m\otimes w_n,$$

совпадает с $\mathscr{X}\otimes\mathscr{Y}$.

(*ii*) *Характер представления $\mathscr{X} \otimes \mathscr{Y}$ равен $\chi\psi$.*

В частности, произведение F-характеров группы G является характером.

✎ Доказать предложение (11.3).

Несмотря на то, что множество характеров группы G замкнуто относительно сложения и умножения, кольцом оно не является, поскольку разность характеров, вообще говоря, не является характером. Иногда удобно рассматривать *кольцо обобщённых F-характеров* $\mathbb{Z}[\mathrm{Irr}_F(G)]$ — множество целочисленных линейных комбинаций неприводимых F-характеров группы G.

✎ **(11.4)** Доказать, что классовая функция $\varphi \in \mathrm{cf}_F(G)$ является обобщённым F-характером тогда и только тогда, когда $\varphi = \chi - \theta$ для некоторых F-характеров χ и θ группы G.

12. Индуцированные модули

Пусть V — FG-модуль и предположим, что $V = W_1 \oplus \ldots \oplus W_k$, где $W_1, \ldots, W_k$ — подпространства пространства V, и на множестве $\{W_i \mid i = 1, \ldots, k\}$ группа G действует транзитивно. В этом случае набор подпространств $W_1, \ldots, W_k$ называется *системой импримитивности степени* k модуля V. Неприводимый FG-модуль V называется *примитивным*, если он не имеет системы импримитивности степени, большей 1, в противном случае он называется *импримитивным*.

Подчеркнём, что если $W_1, \ldots, W_k$ — система импримитивности модуля V степени, большей 1, то подпространства W_i не являются FG-подмодулями.

(12.1) Предложение. *Пусть V — FG-модуль с системой импримитивности $W_1, \ldots, W_k$. Обозначим через W одно из подпространств W_i, и через B — некоторый его базис. Пусть $I = \{g \in G \,|\, Wg = W\}$ — стабилизатор подпространства W. Тогда имеют место следующие утверждения.*

(*i*) *$I \leqslant G$ и W является FI-подмодулем модуля V_I.*

(*ii*) *$k = |G : I|$.*

(*iii*) *Для любой системы $r_1, \ldots, r_k$ представителей правых смежных классов G по I множество $Br_1 \cup \ldots \cup Br_k$ является базисом пространства V.*

(*iv*) *Обозначим через $\mathscr{X}$ представление группы I, соответствующее FI-подмодулю W в базисе B, и для любого $g \in G$ положим*[17]

$$\mathscr{X}^\circ(g) = \begin{cases} \mathscr{X}(g), & g \in I; \\ \mathbf{0}, & g \notin I. \end{cases}$$

Выберем представители $r_1, \ldots, r_k$ правых смежных классов G по I. Представление $\mathscr{Y}$ группы G, соответствующее FG-модулю V в базисе $Br_1 \cup \ldots \cup Br_k$, задаётся равенством

$$\mathscr{Y}(g) = \begin{pmatrix} \mathscr{X}^\circ(r_1 g r_1^{-1}) & \ldots & \mathscr{X}^\circ(r_1 g r_k^{-1}) \\ \ldots & \ldots & \ldots \\ \mathscr{X}^\circ(r_k g r_1^{-1}) & \ldots & \mathscr{X}^\circ(r_k g r_k^{-1}) \end{pmatrix}.$$

(*v*) *Представление группы G, соответствующее модулю V в некотором базисе, с точностью до эквивалентности определяется представлением $\mathscr{X}$ группы I.*

✎ Доказать предложение (12.1)

(12.2) Предложение. *Пусть $H \leqslant G$ и W — FH-модуль. Тогда существует единственный с точностью до изоморфизма FG-модуль V, имеющий систему импримитивности $W_1, \ldots, W_k$ такую, что стабилизатор одного из подпространств этой системы (которое мы обозначим через W_0) совпадает с H и имеет место изоморфизм FH-модулей $W_0 \cong W$.*

Доказательство. Пусть V — внешняя прямая сумма $|G : H|$ копий пространства W. Мы обозначим эти подпространства через $W \otimes r$, где r пробегает набор R представителей правых смежных классов G по H, т. е. $V = \bigoplus_{r \in R} W \otimes r$. Элементы пространства $W \otimes r$ будем записывать $w \otimes r$, т. е. $W \otimes r = \{w \otimes r \,|\, w \in W\}$.

Теперь для $g \in G$ и $w \in W$ определим $w \otimes g \in V$ следующим образом. Пусть $g = hr$, где $h \in H$ и $r \in R$. Тогда положим $w \otimes g = wh \otimes r$. Отметим, что $w \otimes hg = wh \otimes g$ для любых $w \in W$, $h \in H$, $g \in G$. В частности,

[17] Отметим, что $\mathscr{X}^\circ$, вообще говоря, не является представлением группы G.

если $s \in Hr$, то $W \otimes s = W \otimes r$, и поэтому наша конструкция не зависит от выбора набора представителей R правых смежных классов.[18)]

Пусть $g \in G$. Положим $(w \otimes r)g = w \otimes rg$ для всех $w \in W$ и $r \in R$ и продолжим это действие элемента g по линейности на всё пространство V. Заметим, что $(w \otimes g_1)g_2 = w \otimes g_1 g_2$. Отсюда, как легко видеть, вытекает, что на V задано действие группы G. Продолжив это действие по линейности на всю алгебру FG, мы получаем структуру FG-модуля. При этом $\{W \otimes r \mid r \in R\}$ является системой импримитивности модуля V.

Ясно, что стабилизатор подпространства $W_0 = W \otimes 1$ совпадает с H, и изоморфизм векторных пространств $\varphi : W \to W_0$, действующий по правилу $w\varphi = w \otimes 1$, является изоморфизмом FH-модулей, поскольку для всех $h \in H$, $w \in W$

$$(w\varphi)h = (w \otimes 1)h = wh \otimes 1 = (wh)\varphi.$$

Из (12.1)(iv) следует, что всякий FG-модуль, удовлетворяющий условию предложения, изоморфен построенному модулю V. □

Модуль V, существование которого утверждается в предложении (12.2), называется FG-модулем, *индуцированным* FH-модулем W и обозначается W^G.

✎ **(12.3)** Показать, что модуль, индуцированный неприводимым модулем, может не быть даже вполне приводимым. (*Указание.* Рассмотреть группу G порядка, делящегося на характеристику поля F, и её единичную подгруппу E. Сравнить FG-модуль, индуцированный главным FE-модулем, с регулярным FG-модулем. Воспользоваться предложениями (7.8) и (7.3).)

✎ **(12.4)** Пусть $H \leqslant G$ и F — поле, характеристика которого не делит порядок $|H|$.

(i) Пусть V — главный FH-модуль и $e = \dfrac{1}{|H|}\sum\limits_{h \in H} h$. Показать, что e — идемпотент алгебры FG, и имеет место изоморфизм FG-модулей $eFG \cong V^G$.

(ii) Пусть V — одномерный FH-модуль с F-характером λ и $e = \dfrac{1}{|H|}\sum\limits_{h \in H} \lambda(h^{-1})h$. Чему изоморфен FG-модуль eFG?

(12.5) Предложение. (i) *Пусть V — FG-модуль. Тогда $V^G \cong V$.*

(ii) *Пусть $K \leqslant H \leqslant G$ и U — FK-модуль. Тогда имеет место изоморфизм FG-модулей $(U^H)^G \cong U^G$.*

(iii) *Пусть $H \leqslant G$ и $U \leqslant V$ — включение FH-модулей. Показать, что $U^G \leqslant V^G$, причём $U < V$ тогда и только тогда, когда $U^G < V^G$.*

✎ Доказать предложение (12.5).

(12.6) Определение. Пусть G — группа, $H \leqslant G$, $\mathscr{X}$ — F-представление группы H, обладающее характером χ и W — FH-модуль, соответствующий представлению $\mathscr{X}$. Тогда представление $\mathscr{X}^G$ группы G, соответствующее индуцированному FG-модулю W^G в некотором базисе, называется *представлением, индуцированным представлением* $\mathscr{X}$, а F-характер χ^G представления $\mathscr{X}^G$ называется *характером, индуцированным F-характером* χ.

Отметим, что в силу предложения (12.1)(v) представление $\mathscr{Y}$, индуцированное F-представлением $\mathscr{X}$ подгруппы H группы G определено с точностью до эквивалентности, и одно из его явных выражений приведено в (12.1)(iv).

Строго говоря, определение индуцированного F-характера χ^G зависит от представления $\mathscr{X}$, характером которого является χ, а такое представление, как мы видели, не всегда определяется характером χ однозначно с точностью до эквивалентности. Однако из следующего утверждения вытекает, что характер χ^G определяется только характером χ и, значит, данное выше определение корректно.

(12.7) Предложение. *Пусть G — группа, $H \leqslant G$, и χ — F-характер группы H. Для произвольного $g \in G$ определим*

$$\chi^\circ(g) = \begin{cases} \chi(g), & g \in H; \\ 0, & g \notin H. \end{cases}$$

Тогда для любого набора R представителей всех правых смежных классов G по H

$$\chi^G(g) = \sum_{r \in R} \chi^\circ(rgr^{-1}). \qquad \textbf{(12.8)}$$

[18)] На тензорном языке $V = W \otimes_{FH} FG$.

✎ Доказать предложение (12.7).

По аналогии с формулой (12.8) для произвольной классовой функции $\varphi \in \mathrm{cf}_F(H)$ подгруппы H группы G можно определить понятие *индуцированной функции* φ^G, задав её равенством

(12.9) $$\varphi^G(g) = \sum_{r \in R} \varphi^\circ(rgr^{-1}),$$

где R — набор представителей всех правых смежных классов G по H, а функция $\varphi^\circ : G \to F$ совпадает с φ на H и тождественно равна нулю вне H.

(12.10) Предложение. *Пусть G — группа, $H \leqslant G$ и $\varphi \in \mathrm{cf}_F(H)$.*

(*i*) *Функция φ^G, определяемая в* (12.9)*, не зависит от выбора системы представителей правых смежных классов и $\varphi^G \in \mathrm{cf}_F(G)$.*

(*ii*) $|H|\varphi^G(g) = \sum_{x \in G} \varphi^\circ(xgx^{-1})$.

(*iii*) *Если характеристика поля F не делит $|H|$, то для любого $g \in G$*
$$\varphi^G(g) = |\mathrm{C}_G(g)| \sum_{x \in R_g} \frac{\varphi(x)}{|\mathrm{C}_H(x)|},$$
где R_g — набор представителей всех классов сопряжённости группы H, содержащихся в классе g^G.

✎ Доказать предложение (12.10).

Нам также потребуется операция ограничения классовой функции, которая в определённом смысле является двойственной к операции индуцирования. Если $H \leqslant G$ и $\psi \in \mathrm{cf}_F(G)$, то обозначим через ψ_H ограничение функции ψ на подгруппу H. Очевидно, что $\psi_H \in \mathrm{cf}(H)$.

✎ **(12.11)** Пусть V — FG-модуль, χ — F-характер представления группы G, соответствующего модулю V, и $H \leqslant G$. Показать, что F-характер представления группы H, соответствующего FH-модулю V_H совпадает с χ_H.

13. Сопряжённые представления

Если две подгруппы конечной группы сопряжены, то между их представлениями можно установить естественное взаимно однозначное соответствие.

Пусть $H \leqslant G$ и $\mathscr{X}$ — F-представление группы H над произвольным полем F. Для элемента $g \in G$ определим *сопряжённое представление* $\mathscr{X}^g$ группы H^g по правилу $\mathscr{X}^g(h^g) = \mathscr{X}(h)$. Легко видеть, что $\mathscr{X}^g$ действительно является F-представлением группы H, $\deg \mathscr{X}^g = \deg \mathscr{X}$ и $\mathscr{X}^g$ неприводимо тогда и только тогда, когда неприводимо $\mathscr{X}$. Кроме того, представления $\mathscr{X}_1$ и $\mathscr{X}_2$ группы H эквивалентны тогда и только тогда, когда эквивалентны представления $\mathscr{X}_1^g$ и $\mathscr{X}_2^g$ группы H^g. Будем говорить, что F-характер представления $\mathscr{X}^g$ группы H^g *сопряжён* с F-характером χ представления $\mathscr{X}$ группы H и будем обозначать его через χ^g. Аналогично, FH-модуль W и FH^g-модуль U называются сопряжёнными, если соответствующие им представления групп H и H^g сопряжены.

(13.1) Предложение. *Пусть V — FG-модуль, $H \leqslant G$, и W — подмодуль FH-модуля V_H.*

(*i*) *Если $g \in G$, то Wg — FH^g-подмодуль модуля V_{H^g}. Кроме того, модули W и Wg сопряжены.*

(*ii*) *Если $g \in G$ и M — FH^g-подмодуль модуля V_{H^g}, сопряжённый с W, то $M \cong Wt$ для некоторого элемента t из смежного класса $\mathrm{N}_G(H)g$.*

(*iii*) *Если M — FH-подмодуль модуля V_H, изоморфный W, то для всех $g \in G$ имеет место изоморфизм FH^g-модулей $Mg \cong Wg$.*

✎ Доказать предложение (13.1).

Пусть $H \leqslant G$, $g \in G$, $\mathscr{X}$ — F-представление группы H, и W — FH-модуль, соответствующий $\mathscr{X}$. Символом Wg будем обозначать FH^g-модуль, сопряжённый с W и соответствующий сопряжённому представлению $\mathscr{X}^g$. В силу (13.1)(*i*) это обозначение хорошо согласуется со случаем, когда W и Wg — содержатся в некотором FG-модуле.

✎ **(13.2)** Пусть $H \leqslant G$, $g \in G$, W — FH-модуль. Показать, что $W^G \cong (Wg)^G$.

Пусть H, K — подгруппы группы G и $t \in G$. *Двойным смежным классом* группы G по подгруппам H и K с представителем t называется множество

$$HtK = \{htk \,|\, h \in H,\ k \in K\}.$$

Любые два двойных смежных класса либо не пересекаются, либо совпадают, и группа G является объединением своих двойных смежных классов.

(13.3) Предложение (Теорема Макки). *Пусть $H, K \leqslant G$ и T — множество представителей всех двойных смежных классов группы G по H и K. Пусть W — FH-модуль. Тогда имеет место изоморфизм FK-модулей*

$$(W^G)_K \cong \bigoplus_{t \in T} ((Wt)_{H^t \cap K})^K.$$

✎ Доказать предложение (13.3).

Читателю было бы полезно перевести формулировку теоремы Макки на язык представлений.

Отметим важные частные случаи теоремы (13.3).

(13.4) Следствие. (*i*) *Пусть V — регулярный FG-модуль и $K \leqslant G$. Тогда V_K — прямая сумма $|G : K|$ регулярных FK-модулей.*

(*ii*) *Пусть $H \trianglelefteq G$, T — множество представителей всех смежных классов группы G по H. Пусть W — FH-модуль. Тогда*

$$(W^G)_H \cong \bigoplus_{t \in T} Wt.$$

14. Ограничение на нормальные подгруппы

Если FG-модуль V неприводим, то о структуре FH-модуля V_H для произвольной подгруппы $H \leqslant G$ в общем случае можно сказать немного. Однако, ситуация меняется в важном частном случае, когда подгруппа H нормальна.

(14.1) Теорема (Клиффорда). *Пусть $H \trianglelefteq G$ и V — неприводимый FG-модуль. Пусть U — неприводимый FH-подмодуль модуля V_H. Тогда*

(*i*) *$V_H = \sum_{g \in G} Ug$, где U — произвольный неприводимый FH-подмодуль модуля V_H. В частности, модуль V_H вполне приводим и любой неприводимый FH-подмодуль из V_H сопряжён с U.*

(*ii*) *$V_H = \oplus_M \mathrm{W}_M(V_H)$, где M пробегает сопряжённые с U попарно неизоморфные подмодули из V_H. Группа G действует транзитивно на однородных компонентах $\mathrm{W}_M(V_H)$. В частности, для любого неприводимого FH-подмодуля $M \leqslant V_H$ имеет место равенство $\mathrm{n}_M(V_H) = \mathrm{n}_U(V_H)$.*

(*iii*) *Обозначим $W = \mathrm{W}_U(V_H)$ и $I = \{g \in G \,|\, Ug \cong U\}$. Тогда $I \leqslant G$, W — неприводимый FI-модуль и $V \cong W^G$.*

Доказательство. (*i*) Поскольку $\sum_{g \in G} Ug$ — ненулевое G-инвариантное подпространство, то $V_H = \sum_{g \in G} Ug$ ввиду неприводимости модуля V. Значит, V_H вполне приводим по предложению (6.1)(*iii*). Из предложений (6.2) и (6.6)(*ii*) следует, что всякий неприводимый подмодуль из V_H изоморфен какому либо слагаемому Ug и, значит, сопряжён с U по предложению (13.1).

(*ii*) Разложение $V_H = \oplus_M \mathrm{W}_M(V_H)$ следует из (*i*) и предложения (6.6)(*ii*). Установим транзитивность действия группы G. Пусть $M = Ug$ для подходящего $g \in G$. Достаточно показать, что $\mathrm{W}_U(V_H)g = \mathrm{W}_M(V_H)$. Так как $\mathrm{W}_U(V_H)$ — сумма FH-подмодулей, изоморфных U, то из предложения (13.1)(*iii*) следует, что $\mathrm{W}_U(V_H)g$ — сумма подмодулей, изоморфных M. Поэтому $\mathrm{W}_U(V_H)g \subseteq \mathrm{W}_M(V_H)$. Обратное включение получается аналогично.

В силу (*i*) все неприводимые FH-подмодули M из V_H сопряжены с U и поэтому имеют одинаковую размерность. Кроме того, из транзитивности действия G на однородных компонентах следует, что все $\mathrm{W}_M(V_H)$ также имеют одинаковую размерность. Значит, число $\mathrm{n}_M(V_H) = \dim_F(\mathrm{W}_M(V_H))/\dim_F(M)$ не зависит от модуля M.

(*iii*) Из доказанного выше следует, что однородные компоненты FH-модуля V_H образуют систему импримитивности для V. Поскольку I — стабилизатор одной из компонент W, то из предложения (12.2) вытекает изоморфизм $V \cong W^G$. Поэтому неприводимость FI-модуля W следует из предложения (12.5)(*ii*) и неприводимости FG-модуля V. □

Подгруппа $I \leqslant G$, определённая в (14.1)(*iii*), называется *группой инерции* неприводимого FH-подмодуля U модуля V_H.

15. Расширение основного поля

В этом разделе мы будем преимущественно говорить о групповых F-алгебрах, хотя многое факты и определения можно было бы перенести и на произвольные F-алгебры.

Пусть $F \subseteq F$ — расширение полей и $\mathscr{X}$ — F-представление группы G. Тогда $\mathscr{X}$ также является E-представлением, и мы в этом случае будем обозначать его $\mathscr{X}^E$. Если F-представления $\mathscr{X}$ и $\mathscr{Y}$ эквивалентны, то также эквивалентны и E-представления $\mathscr{X}^E$ и $\mathscr{Y}^E$. Поэтому, если $\mathscr{X}$ соответствует FG-модулю V, то существует однозначно определённый (с точностью до изоморфизма) EG-модуль V^E, соответствующий представлению $\mathscr{X}^E$. (На тензорном языке имеют место изоморфизмы $EG \cong E \otimes_F FG$ и $V^E \cong E \otimes_F V$.)

Если представление $\mathscr{X}^E$ неприводимо, то также неприводимо и представление $\mathscr{X}$. Однако, $\mathscr{X}^E$ может оказаться приводимым, даже если $\mathscr{X}$ неприводимо.

✎ **(15.1)** Пусть $G = \langle g \mid g^3 = 1 \rangle$ — циклическая группа порядка 3 и $\mathscr{X}$ — её $\mathbb{R}$-представление, определённое равенством

$$\mathscr{X}(g) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Показать, что $\mathscr{X}$ неприводимо, а $\mathscr{X}^{\mathbb{C}} = \mathscr{X}_1 \oplus \mathscr{X}_2$, где $\mathscr{X}_1$ и $\mathscr{X}_2$ — неэквивалентные неприводимые $\mathbb{C}$-представления.

✎ **(15.2)** Пусть $\mathbb{R}$-представление группы кватернионов

$$Q_8 = \langle a, b \mid a^4 = b^4 = 1, \quad a^2 = b^2, \quad a^b = a^{-1} \rangle$$

определено равенством

$$\mathscr{X}(a) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \mathscr{X}(b) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

Показать, что $\mathscr{X}$ неприводимо, а $\mathscr{X}^{\mathbb{C}} = \mathscr{Y} \oplus \mathscr{Y}$, где $\mathscr{Y}$ — неприводимое $\mathbb{C}$-представление.

(15.3) Предложение. *Пусть $F \subseteq E$ — расширение полей и $\mathscr{Y}$ — неприводимое E-представление группы G. Тогда существует неприводимое F-представление $\mathscr{X}$ такое, что $\mathscr{Y}$ является неприводимой компонентой представления $\mathscr{X}^E$.*

✎ Доказать предложение (15.3). (*Указание.* Использовать предложение (9.6).)

Отметим, что далее мы покажем единственность с точностью до эквивалентности F-представления $\mathscr{X}$ из предложения (15.3) (см. замечание после следствия (15.10)).

(15.4) Определение. F-представление $\mathscr{X}$ группы G называется *абсолютно неприводимым*, если представление $\mathscr{X}^E$ неприводимо для любого расширения E поля F.

(15.5) Предложение. *Пусть $\mathscr{X}$ — неприводимое F-представление степени n группы G. Тогда следующие условия эквивалентны.*

(*i*) *$\mathscr{X}$ абсолютно неприводимо.*

(*ii*) *$\mathscr{X}^E$ неприводимо для всякого конечного расширения $F \subseteq E$.*

(*iii*) *Централизатор образа $\mathscr{X}(G)$ в алгебре $\mathrm{M}_n(F)$ состоит из скалярных матриц.*

(*iv*) *$\mathscr{X}(FG) = \mathrm{M}_n(F)$.*

Доказательство. (*i*) $\Rightarrow$ (*ii*) Очевидно.

(*ii*) $\Rightarrow$ (*iii*) Пусть матрица $M \in \mathrm{M}_n(F)$ удовлетворяет $\mathscr{X}(g)M = M\mathscr{X}(g)$ для всех $g \in G$. Выберем конечное расширение E поля F, в котором M имеет собственное значение λ. Тогда подпространство $U \leqslant E^n$, состоящее из всех собственных векторов, отвечающих собственному значению λ, ненулевое. Но U инвариантно относительно любой матрицы $\mathscr{X}(g)$, поскольку $u\mathscr{X}(g)M = uM\mathscr{X}(g) = \lambda u\mathscr{X}(g)$ для всех $u \in U$, $g \in G$. Из неприводимости представления $\mathscr{X}^E$ следует, что $U = E^n$, т. е. M — скалярная матрица и, в частности, $\lambda \in F$.

(*iii*) $\Rightarrow$ (*iv*) Перейдём на язык модулей. Пусть $A = FG$ и $V = F^n$ — A-модуль, соответствующий представлению $\mathscr{X}$. Тогда образу $\mathscr{X}(FG)$ соответствует алгебра A_V и требуется показать, что $A_V = \mathrm{End}_F(V)$.

По предложению (7.18) алгебра A_V простая. Поскольку V — неприводимый A_V-модуль, то из теоремы о двойном централизаторе (7.20) следует, что $A_V = \mathrm{C}_{\mathrm{End}_F(V)}(\mathrm{C}_{\mathrm{End}_F(V)}(A_V))$. Однако из (iii) следует, что $\mathrm{C}_{\mathrm{End}_F(V)}(A_V)$ состоит из скалярных преобразований пространства V. Поэтому $A_V = \mathrm{End}_F(V)$.

$(iv) \Rightarrow (i)$ Пусть $F \subseteq L$ — расширение полей. Поскольку любая матрица из $\mathrm{M}_n(L)$ является L-линейной комбинацией матриц из $\mathrm{M}_n(F)$, то $\mathscr{X}^L(LG) = \mathrm{M}_n(L)$. Но тогда представление $\mathscr{X}^L$ не может быть эквивалентно представлению вида

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$$

и, значит, неприводимо. □

Как видно из (iii) и (iv) предложения (15.5), абсолютную неприводимость F-представления можно проверить, не рассматривая расширения поля F.

(15.6) Определение. Поле F называется *полем разложения* группы G, если любое неприводимое F-представление группы G абсолютно неприводимо.

Поле, не имеющее собственных подполей, называется *простым*. Легко видеть, что простые поля — это, в точности, поля $\mathbb{Q}$ и $\mathbb{F}_p$ для простого p.

✎ **(15.7)** Доказать, что для группы S_3 любое простое поле является полем разложения.

Поскольку любое конечное расширение алгебраически замкнутого поля F совпадает с F, то из предложения (15.5) получаем

(15.8) Следствие. *Алгебраически замкнутое поле F является полем разложения для любой группы.*

Следующее утверждение оказывается полезным при проверке эквивалентности неприводимых F-представлений, а также в других ситуациях.

(15.9) Предложение. *Пусть $\mathscr{X}$ — неприводимое представление групповой алгебры FG и $a \in FG$. Тогда существует элемент $b \in FG$ такой, что $\mathscr{X}(b) = \mathscr{X}(a)$ и $\mathscr{Y}(b) = 0$ для всех неприводимых представлений $\mathscr{Y}$ алгебры FG, не эквивалентных $\mathscr{X}$.*

Доказательство. Следующее рассуждение является видоизменением идеи из доказательства пункта (ii) предложения (9.4).

Пусть $\mathscr{X}_1, \dots, \mathscr{X}_s$ — полный набор представителей классов эквивалентности неприводимых FG-представлений. Тогда $\mathrm{J}(FG) = \cap_i \mathrm{Ker}\, \mathscr{X}_i$ по предложению (8.5), и $\mathscr{X}_1, \dots, \mathscr{X}_s$ также является полным набором неприводимых представлений полупростой алгебры $A = FG/\mathrm{J}(FG)$ (см. предложение (7.2)). В силу (ii) теоремы (7.16) имеет место разложение $A = \mathrm{W}_M(A^\circ) \oplus \mathrm{Ann}(M)$, где M — неприводимый A-модуль, соответствующий представлению $\mathscr{X}$. Запишем $a = b + c$, где $b \in \mathrm{W}_M(A^\circ)$ и $c \in \mathrm{Ann}(M)$. Тогда, переформулировав на языке представлений утверждение (ii) теоремы (7.16), получим $\mathscr{X}(b) = \mathscr{X}(a)$ и $\mathscr{Y}(b) = 0$ для всех неприводимых представлений $\mathscr{Y}$ алгебры A, не эквивалентных $\mathscr{X}$. □

(15.10) Следствие. *Пусть $F \subseteq E$ — расширение полей, $\mathscr{X}$ и $\mathscr{Y}$ — неприводимые F-представления такие, что $\mathscr{X}^E$ и $\mathscr{Y}^E$ имеют общую неприводимую компоненту. Тогда представления $\mathscr{X}$ и $\mathscr{Y}$ эквивалентны.*

Доказательство. Предположим, что $\mathscr{X}$ и $\mathscr{Y}$ не эквивалентны. По предложению (15.9) существует элемент $b \in FG$ такой, что $\mathscr{X}(b) = \mathscr{X}(1) = \mathbf{1}_{\deg \mathscr{X}}$ — единичная матрица и $\mathscr{Y}(b) = \mathbf{0}_{\deg \mathscr{Y}}$ — нулевая матрица. Тогда $\mathscr{X}^E(b) = \mathbf{1}_{\deg \mathscr{X}}$ и $\mathscr{Y}^E(b) = \mathbf{0}_{\deg \mathscr{Y}}$, и поэтому для любой общей неприводимой компоненты $\mathscr{Z}$ представлений $\mathscr{X}^E$ и $\mathscr{Y}^E$ должно быть выполнено, с одной стороны, $\mathscr{Z}(b) = \mathbf{1}_{\deg \mathscr{Z}}$, а с другой стороны $\mathscr{Z}(b) = \mathbf{0}_{\deg \mathscr{Z}}$. Противоречие. □

Отметим, что из этого следствия вытекает единственность с точностью до эквивалентности неприводимого представления $\mathscr{X}$, существование которого утверждается в предложении (15.3).

(15.11) Предложение. *Пусть F — поле разложения группы G и $\mathscr{X}_1, \dots, \mathscr{X}_s$ — набор представителей всех классов эквивалентности неприводимых F-представлений группы G. Если $F \subseteq E$ — расширение полей, то $\mathscr{X}_1^E, \dots, \mathscr{X}_s^E$ — набор представителей всех неприводимых E-представлений группы G. В частности, любое неприводимое E-представление может быть записано над полем F.*

Доказательство. Поскольку представления $\mathscr{X}_i$ абсолютно неприводимы, то также абсолютно неприводимы и представления $\mathscr{X}_i^E$. Они попарно неэквивалентны по следствию (15.10). Пусть $\mathscr{Y}$ — некоторое неприводимое E-представление. Из предложения (15.3) и неприводимости представлений $\mathscr{X}_i^E$ вытекает, что $\mathscr{Y}$ эквивалентно некоторому $\mathscr{X}_i^E$. □

(15.12) Следствие. *В предложении* (10.6) *вместо алгебраической замкнутости поля F достаточно потребовать выполнения более слабого условия — чтобы F было полем разложения группы G.*

Доказательство. Это следует из (15.11), поскольку любое поле вложено в своё алгебраическое замыкание, □

В следующем разделе будут обсуждаться представления групп над полем $\mathbb{C}$ комплексных чисел. Отметим здесь одно полезное следствие, касающееся таких представлений.

(15.13) Следствие. *Пусть $\overline{\mathbb{Q}}$ — алгебраическое замыкание поля $\mathbb{Q}$ рациональных чисел (т. е. поле всех алгебраических чисел, см. приложение A). Любое $\mathbb{C}$-представление группы G может быть записано над полем $\overline{\mathbb{Q}}$.*

✎ **(15.14)** Доказать следствие (15.13).

16. Обыкновенные представления

В этом разделе мы остановимся более подробно на классическом частном случае — когда основное поле F является полем $\mathbb{C}$ комплексных чисел. В этом случае часто говорят об *обыкновенных* представлениях и характерах групп.

Пусть G — конечная группа. Обозначим $\mathrm{Irr}(G) = \mathrm{Irr}_{\mathbb{C}}(G)$. Каждому обыкновенному характеру $\chi \in \mathrm{Irr}(G)$ соответствует единственный с точностью до изоморфизма неприводимый $\mathbb{C}G$-модуль $M_\chi \in \mathscr{M}(\mathbb{C}G)$. Выберем базис в каждом модуле M_χ и обозначим через $\mathscr{X}_\chi$ соответствующее представление.

Мы знаем из (7.24)(ii), что число неприводимых обыкновенных характеров $|\mathrm{Irr}(G)|$ группы G выражается только в групповых терминах и совпадает с количеством классов сопряжённости $|\mathscr{K}(G)|$.

Для группы G *таблицей (обыкновенных) характеров* $\mathrm{X}(G)$ называется квадратная матрица, строки которой индексированы неприводимыми характерами $\chi \in \mathrm{Irr}(G)$, а столбцы — классами сопряжённости $K \in \mathscr{K}(G)$. При этом элемент χ-й строки и K-го столбца таблицы $\mathrm{X}(G)$ равен $\chi(x_{_K})$. Напомним, что $x_{_K}$ обозначает представитель класса K. Например, ниже приведена таблица характеров группы S_3.

$\mathrm{X}(S_3)$	1	(12)	(123)
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

✓ Отметим, что задача вычисления таблицы характеров произвольной группы является достаточно сложной. Особое значение имеет нахождение неприводимых характеров конечных простых групп. Для многих простых и близких к ним групп «небольшого» порядка (в частности, для всех спорадических групп) таблицы характеров и другая важная информация могут быть найдены в Атласе [8]. Таблицы характеров некоторых групп приведены также в приложении B.

Из (9.4)(iii) следует, что для любой группы G матрица $\mathrm{X}(G)$ является невырожденной и два обыкновенных представления группы G эквивалентны тогда и только тогда, когда их характеры совпадают.

Из (10.6)(i) вытекает важная формула

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2.$$

(16.1) Предложение. *Группа G абелева тогда и только тогда, когда* $\deg\chi = 1$ *для любого* $\chi \in \mathrm{Irr}(G)$.

✎ Доказать предложение (16.1)

Для комплексного числа $\alpha \in \mathbb{C}$ пусть $\overline{\alpha}$ обозначает число, комплексно-сопряжённое с α. Пусть $\mathbb{Q}_m$ обозначает *m-е круговое поле*, т. е. подполе $\mathbb{Q}(\zeta)$ поля $\mathbb{C}$, где ζ — *примитивный корень степени m из* 1, т. е. элемент порядка m из группы $\mathbb{C}^\times$.

(16.2) Предложение. *Пусть ζ — примитивный корень степени m из 1. Для любого $\sigma \in \mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q})$ существует целое k, взаимно простое с m, для которого $\zeta^\sigma = \zeta^k$, и наоборот, для любого такого k существует единственный автоморфизм $\sigma \in \mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q})$ для которого $\zeta^\sigma = \zeta^k$.*

✎ Доказать предложение (16.2).

(16.3) Предложение. *Пусть $\mathscr{X}$ — обыкновенное представление группы G степени n с характером χ, $g \in G$ и $|g| = k$. Тогда верны следующие утверждения.*

(i) *Матрица $\mathscr{X}(g)$ подобна диагональной матрице* $\mathrm{diag}(\zeta_1, \ldots, \zeta_n)$.

(ii) $\zeta_i^k = 1$. *В частности,* $|\zeta_i| = 1$, $\overline{\zeta_i} = \zeta_i^{-1}$ *и* $\zeta_i \in \mathbb{Q}_k$.

(iii) $\chi(g) = \sum \zeta_i$. *В частности,* $|\chi(g)| \leqslant n$ *и* $\chi(g) \in \mathbb{Q}_k$.

(iv) $\chi(g^{-1}) = \overline{\chi(g)}$.

✎ Доказать предложение (16.3)

(16.4) Определение. Пусть χ — обыкновенный характер группы G и $\mathscr{X}$ — представление с характером χ. *Ядром* $\ker\chi$ *характера* χ называется $\ker\mathscr{X}$.

Определение (16.4) корректно, поскольку, как мы уже заметили, обыкновенные представления, соответствующие одному и тому же характеру, эквивалентны.

✓ Отметим, что для произвольных F-характеров, аналогично определяемое понятие ядра, вообще говоря, некорректно, поскольку могут существовать F-представления с одинаковыми F-характерами, но различными ядрами.

✎ **(16.5)** Привести пример таких представлений.

(16.6) Предложение. *Пусть χ — обыкновенный характер группы G. Тогда*

(i) $\ker\chi = \{g \in G \mid \chi(g) = \chi(1)\}$.

(ii) *Если* $\chi = \sum_{\tau\in\mathrm{Irr}(G)} n_\tau \tau$, *где* n_τ *— неотрицательные целые числа, то*

$$\ker\chi = \bigcap_{\substack{\tau\in\mathrm{Irr}(G),\\ n_\tau>0}} \ker\tau.$$

(iii) *Имеет место равенство*

$$\bigcap_{\tau\in\mathrm{Irr}(G)} \ker\tau = 1.$$

✎ Доказать предложение (16.6).

✎ **(16.7)** Доказать, что

(i) нормальные подгруппы конечной группы — это, в точности, пересечения ядер неприводимых обыкновенных характеров;

(ii) по таблице характеров группы можно найти таблицы характеров всех её факторгрупп.

Напомним, что *экспонентой* $\exp G$ группы G называется наименьшее общее кратное порядков её элементов.

(16.8) Следствие. (i) *Пусть χ — обыкновенный характер группы G. Тогда $\chi(g)$ является целым алгебраическим числом*[19] *для любого $g \in G$.*

(ii) *Значения всех обыкновенных характеров группы G лежат в $\mathbb{Q}_m$, где $m = \exp G$.*

Доказательство. (i) Из (16.3) вытекает, что $\chi(g)$ является суммой корней многочлена $x^k - 1$, где $k = |g|$. Поскольку корни многочлена $x^k - 1$ являются целыми алгебраическими числами и в силу (A.5)(i) множество целых алгебраических чисел замкнуто относительно сложения, то отсюда следует требуемое.

(ii) следует из (16.3)(iii). □

Пусть G — группа экспоненты m, χ — её обыкновенный характер и $\sigma \in \mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q})$. Обозначим через $\overline{\chi}$ и χ^σ классовые функции, определённые для любого $g \in G$ равенствами

$$\overline{\chi}(g) = \overline{\chi(g)}, \qquad \chi^\sigma(g) = \chi(g)^\sigma.$$

Поле $\mathbb{Q}_m$ является полем разложения многочлена $x^m - 1$ и, значит, расширение полей $\mathbb{Q} \subseteq \mathbb{Q}_m$ является нормальным. Поэтому комплексное сопряжение оставляет поле $\mathbb{Q}_m$ инвариантным и существует автоморфизм из $\mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q})$, действие которого на $\mathbb{Q}_m$ совпадает с комплексным сопряжением. В частности, $\overline{\chi} \in \{\chi^\sigma \mid \sigma \in \mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q})\}$ для любого характера χ группы G.

[19] Определение и необходимые сведения о целых алгебраических числах приведены в приложении A

(16.9) Предложение. *Пусть G — группа, $m = \exp G$ и $\sigma \in \mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q})$. Тогда*

(i) *для любого обыкновенного характера χ группы G функция χ^σ является характером, причём χ^σ неприводим тогда и только тогда, когда χ неприводим;*

(ii) *существует такое целое число k, взаимно простое с m, что $\chi^\sigma(g) = \chi(g^k)$ для любого обыкновенного характера χ и любого $g \in G$.*

Доказательство. (i) Пусть $\mathscr{X}$ — обыкновенное представление группы G с характером χ. По (15.13) существует $\overline{\mathbb{Q}}$-представление $\mathscr{Y}$ такое, что $\mathscr{Y}^{\mathbb{C}}$ эквивалентно $\mathscr{X}$. Поэтому χ будет характером $\overline{\mathbb{Q}}$-представления $\mathscr{Y}$. В силу алгебраичности расширения $\mathbb{Q} \subseteq \mathbb{Q}_m$ автоморфизм σ поля $\mathbb{Q}_m$ продолжается до автоморфизма алгебраического замыкания $\overline{\mathbb{Q}}$, который также обозначим через σ. Пусть $g \in G$ и $\mathscr{Y}(g) = (\alpha_{ij})$, где $\alpha_{ij} \in \overline{\mathbb{Q}}$. Легко видеть, что отображение $\mathscr{Y}^\sigma : g \mapsto (\alpha_{ij}^\sigma)$ является $\overline{\mathbb{Q}}$-представлением группы G, и его характер совпадает с χ^σ. Поскольку σ является автоморфизмом поля $\overline{\mathbb{Q}}$, представление $\mathscr{Y}^\sigma$ неприводимо тогда и только тогда, когда неприводимо представление $\mathscr{Y}$. Таким образом, утверждения о неприводимости характеров χ и χ^σ равносильны в силу (15.11).

(ii) Пусть $\zeta \in \mathbb{C}$ — примитивный корень степени m из 1. По (16.2) для некоторого $k \in \mathbb{Z}$, взаимно простого с m, справедливо равенство $\zeta^\sigma = \zeta^k$. Пусть χ — характер группы G и $g \in G$. Рассмотрим обыкновенное представление $\mathscr{X}$ с характером χ. Так как $|g|$ делит m, то из (16.3) следует, что матрица $\mathscr{X}(g)$ подобна диагональной матрице $\mathrm{diag}(\zeta_1, \ldots, \zeta_n)$, где ζ_i — степени числа ζ и $n = \chi(1)$. Тогда $\mathscr{X}(g^k)$ подобна $\mathrm{diag}(\zeta_1^k, \ldots, \zeta_n^k)$ и, значит,

$$\chi(g^k) = \mathrm{tr}\,\mathscr{X}(g^k) = \zeta_1^k + \ldots + \zeta_n^k = (\zeta_1 + \ldots + \zeta_n)^\sigma = \chi^\sigma(g).$$

□

В предыдущих обозначениях будем называть $\overline{\chi}$ и χ^σ характерами, *комплексно сопряжённым* и *алгебраически сопряжённым* с характером χ, соответственно.

✎ **(16.10)** Пусть $\mathscr{X}$ — обыкновенное представление группы G с характером χ. Показать, что $\overline{\chi}$ является характером контрагредиентного представления $\mathscr{X}^*$.

(16.11) Предложение. *Пусть G — группа и $g \in G$.*

(i) *Элементы g и g^{-1} сопряжены в G тогда и только тогда, когда $\chi(g) \in \mathbb{R}$ для всех $\chi \in \mathrm{Irr}(G)$.*

(ii) *Элемент g сопряжён с g^k для всех целых k, взаимно простых с $|g|$, тогда и только тогда, когда $\chi(g) \in \mathbb{Q}$ для всех $\chi \in \mathrm{Irr}(G)$.*

(iii) *Таблица характеров симметрической группы S_n целочисленна.*

✎ Доказать предложение (16.11).

Напомним, что через ρ обозначается регулярный характер групповой алгебры $\mathbb{C}G$. Из (10.3), пример 3, следует, что для любого $g \in G$

(16.12)
$$\rho(g) = \begin{cases} 0, & g \neq 1; \\ |G|, & g = 1. \end{cases}$$

(16.13) Предложение. *Справедливо равенство*

$$\rho = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi.$$

✎ Доказать предложение (16.13).

(16.14) Из (7.16)(iv) и (2.17) следует, что единица алгебры $\mathbb{C}G$ представима в виде суммы

$$1 = \sum_{\chi \in \mathrm{Irr}(G)} e_\chi$$

где e_χ — попарно ортогональные центральные идемпотенты из $\mathbb{C}G$, причём e_χ — единица простой алгебры $\mathrm{W}_{M_\chi}(\mathbb{C}G)$, а также

$$\mathrm{W}_{M_\chi}(\mathbb{C}G) = e_\chi \mathbb{C}G$$

для всех $\chi \in \mathrm{Irr}(G)$. Будем называть e_χ *центральным идемпотентом алгебры $\mathbb{C}G$, соответствующим неприводимому характеру χ.*

✓ Отметим, что e_χ — примитивный идемпотент алгебры $\mathrm{Z}(\mathbb{C}G)$, но, вообще говоря, не является примитивным идемпотентом алгебры $\mathbb{C}G$.

Нам потребуется явное выражение идемпотентов e_χ через естественный базис алгебры $\mathbb{C}G$, состоящий из групповых элементов, а также базис центра $\mathrm{Z}(\mathbb{C}G)$, состоящий из классовых сумм.

(16.15) Предложение. *Имеет место разложение*

$$e_\chi = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g = \frac{\chi(1)}{|G|}\sum_{K\in\mathscr{K}(G)}\chi(x_{_K}^{-1})\widehat{K}.$$

Доказательство. Достаточно доказать лишь первое равенство. Пусть $e_\chi = \sum_{g\in G}\alpha_g g$ для подходящих коэффициентов $\alpha_g\in\mathbb{C}$. Из (16.12) следует, что $\rho(e_\chi g^{-1}) = \alpha_g|G|$ для любого $g\in G$. Тогда (16.13) влечёт

$$\alpha_g|G| = \sum_{\theta\in\mathrm{Irr}(G)}\theta(1)\theta(e_\chi g^{-1}).$$

Отметим, что ввиду (7.16)(ii) однородная компонента $\mathrm{W}_{M_\chi}(\mathbb{C}G)$ алгебры $\mathbb{C}G$ аннулирует любой модуль M_θ при $\theta\ne\chi$ и поэтому $\mathscr{X}_\theta(e_\chi)=\mathbf{0}$, а в силу (16.14) также $\mathscr{X}_\theta(e_\theta)=\mathscr{X}_\theta(1)=\mathbf{1}$. Поэтому

$$\mathscr{X}_\theta(e_\chi g^{-1}) = \mathscr{X}_\theta(e_\chi)\mathscr{X}_\theta(g^{-1}) = \begin{cases}\mathbf{0}, & \theta\ne\chi;\\ \mathscr{X}_\chi(g^{-1}), & \theta=\chi,\end{cases}$$

и, значит, $\theta(e_\chi g^{-1}) = \delta_{\theta,\chi}\chi(g^{-1})$. Следовательно $\alpha_g|G| = \chi(1)\chi(g^{-1})$, что и требовалось показать. □

Условие ортогональности идемпотентов e_χ позволяет вывести важное соотношение между неприводимыми характерами.

(16.16) Предложение (Обобщённое соотношение ортогональности). *Для произвольных* $h\in G$, $\chi,\theta\in\mathrm{Irr}(G)$ *имеет место равенство*

$$\frac{1}{|G|}\sum_{g\in G}\chi(gh)\theta(g^{-1}) = \delta_{\chi,\theta}\frac{\chi(h)}{\chi(1).}$$

Доказательство. Подставим в соотношение $e_\chi e_\theta = \delta_{\chi,\theta}\, e_\chi$ выражение для идемпотентов e_χ и e_θ из предложения (16.15) и сравним коэффициенты при групповых элементах в обеих частях равенства.

Зафиксируем $h\in G$. Коэффициент при h справа равен

$$\delta_{\chi,\theta}\frac{\chi(1)}{|G|}\chi(h^{-1}),$$

а слева —

$$\frac{\chi(1)\theta(1)}{|G|^2}\Big(\sum_{\substack{f,g\in G\\ fg=h}}\chi(f^{-1})\theta(g^{-1})\Big) = \frac{\chi(1)\theta(1)}{|G|^2}\Big(\sum_{g\in G}\chi(gh^{-1})\theta(g^{-1})\Big).$$

Требуемое равенство получается приравниванием этих коэффициентов и заменой h на h^{-1}. □

Подстановка $h=1$ в (16.16) даёт

(16.17) Следствие (Первое соотношение ортогональности). *Для произвольных* $\chi,\theta\in\mathrm{Irr}(G)$ *имеет место равенство*

$$\frac{1}{|G|}\sum_{g\in G}\chi(g)\theta(g^{-1}) = \delta_{\chi,\theta}.$$

Обозначим $\mathrm{cf}(G)=\mathrm{cf}_{\mathbb{C}}(G)$. Для произвольных классовых функций $\varphi,\psi\in\mathrm{cf}(G)$ введём *скалярное произведение*

$$(\varphi,\psi)_{_G} = \frac{1}{|G|}\sum_{g\in G}\varphi(g)\overline{\psi(g)}.$$

✎ **(16.18)** Проверить, что для любых $\varphi,\psi,\tau\in\mathrm{cf}(G)$, $\alpha\in\mathbb{C}$ выполнены свойства

(i) $\mathbb{R}\ni(\varphi,\varphi)_{_G}>0$ если $\varphi\ne 0$;

(ii) $(\varphi+\psi,\tau)_{_G} = (\varphi,\tau)_{_G}+(\psi,\tau)_{_G}$;

(iii) $(\alpha\varphi,\psi)_{_G} = \alpha(\varphi,\psi)_{_G}$;

(iv) $(\varphi,\psi)_{_G} = \overline{(\psi,\varphi)_{_G}}$.

Другими словами, $(\cdot,\cdot)_G$ является обычным скалярным произведением, относительно которого $\mathrm{cf}(G)$ становится унитарным пространством.

Мы знаем из (10.6)(ii), что $\mathrm{Irr}(G)$ является базисом пространства $\mathrm{cf}(G)$. В силу (16.17) и (16.3)(iv) для любых $\chi,\theta\in\mathrm{Irr}(G)$ имеет место равенство

$$(\chi,\theta)_G=\delta_{\chi,\theta},$$

т. е. базис $\mathrm{Irr}(G)$ ортонормированный. Отсюда получается простой метод нахождения коэффициентов в разложении произвольной классовой функции $\varphi\in\mathrm{cf}(G)$ по базису $\mathrm{Irr}(G)$. Если $(\varphi,\chi)_G=\alpha_\chi$, где $\chi\in\mathrm{Irr}(G)$, то $\varphi=\sum_{\chi\in\mathrm{Irr}(G)}\alpha_\chi\chi$.

(16.19) Следствие. *Пусть $\varphi,\psi\in\mathrm{cf}(G)$.*

(i) *Функция φ является обобщённым характером тогда и только тогда, когда $(\varphi,\chi)_G$ — целое число для всех $\chi\in\mathrm{Irr}(G)$.*

(ii) *Функция φ является характером тогда и только тогда, когда $(\varphi,\chi)_G$ — неотрицательное целое число для всех $\chi\in\mathrm{Irr}(G)$.*

(iii) *Если φ и ψ — характеры, то $(\varphi,\psi)_G=(\psi,\varphi)_G$ — неотрицательное целое число.*

(iv) *Если φ — характер, то он неприводим тогда и только тогда, когда $(\varphi,\varphi)_G=1$.*

✎ **(16.20)** Доказать следствие (16.19).

Скалярное произведение проясняет двойственность между операциями ограничения и индуцирования классовых функций.

(16.21) Предложение (Закон взаимности Фробениуса). *Пусть $H\leqslant G$, $\varphi\in\mathrm{cf}(H)$ и $\psi\in\mathrm{cf}(G)$. Тогда*

$$(\varphi^G,\psi)_G=(\varphi,\psi_H)_H$$

✎ Доказать предложение (16.21).

Напомним, что для матрицы A её транспонированная матрица обозначается через $A^\top$. Если $A=(\alpha_{ij})\in\mathrm{M}_n(\mathbb{C})$, то положим $\overline{A}=(\overline{\alpha_{ij}})$.

(16.22) Предложение (Второе соотношение ортогональности). *Для любых $g,h\in G$*

$$\sum_{\chi\in\mathrm{Irr}(G)}\chi(g)\overline{\chi(h)}=\begin{cases}0, & \text{если } g \text{ и } h \text{ не сопряжены в } G;\\ |\mathrm{C}_G(g)|, & \text{иначе.}\end{cases}$$

Доказательство. Поскольку характеры являются классовыми функциями, первое соотношение ортогональности (16.17) можно переписать в виде

(16.23)
$$|G|\delta_{\chi,\theta}=\sum_{K\in\mathscr{K}(G)}|K|\chi(x_K)\overline{\theta(x_K)}.$$

Пусть $\mathrm{X}=\mathrm{X}(G)$ и D — целочисленная диагональная матрица, индексированная классами сопряжённости и состоящая из элементов $\delta_{K,L}|K|$. Тогда система равенств (16.23) при $\chi,\theta\in\mathrm{Irr}(G)$ эквивалентна матричному соотношению

$$|G|\mathbf{1}=\mathrm{X}D\overline{\mathrm{X}}^\top.$$

Поскольку взаимно обратные матрицы перестановочны, то мы получаем

$$|G|\mathbf{1}=D\overline{\mathrm{X}}^\top\mathrm{X},$$

а это эквивалентно системе

$$|G|\delta_{K,L}=|K|\sum_{\chi\in\mathrm{Irr}(G)}\overline{\chi(x_K)}\chi(x_L)$$

при $K,L\in\mathscr{K}(G)$. Отметим, что $|G|/|K|=|\mathrm{C}_G(x_K)|$. Переобозначив $g=x_K$, $h=x_L$ и взяв комплексное сопряжение, получим требуемое равенство. □

Сделаем несколько замечаний о характерах прямых произведений групп.

Пусть H,K — группы, $G=H\times K$, $\varphi\in\mathrm{cf}(H)$, $\psi\in\mathrm{cf}(K)$. Определим отображение $\varphi\times\psi:G\to\mathbb{C}$ по правилу $(\varphi\times\psi)(hk)=\varphi(h)\psi(k)$ для всех $h\in H$ и $k\in K$. Легко видеть, что $\varphi\times\psi\in\mathrm{cf}(G)$.

(16.24) Предложение. *Пусть $G = H \times K$.*

(i) *Если χ и θ — характеры групп H и K, соответственно, то $\chi \times \theta$ — характер группы G*

(ii) $\mathrm{Irr}(G) = \{\, \chi \times \theta \mid \chi \in \mathrm{Irr}(H),\ \theta \in \mathrm{Irr}(K)\}$.

Доказательство. (i) Используя естественные эпиморфизмы $G/K \cong H$ и $G/H \cong K$, характеры χ и θ групп H и K, соответственно, можно «поднять» до характеров $\widetilde{\chi}$ и $\widetilde{\theta}$ группы G, положив $\widetilde{\chi}(hk) = \chi(h)$ и $\widetilde{\theta}(hk) = \theta(k)$ для всех $h \in H$, $k \in K$. Тогда $\chi \times \theta = \widetilde{\chi}\,\widetilde{\theta}$ — характер группы G.

(ii) Пусть $\chi_1, \chi_2 \in \mathrm{Irr}(H)$ и $\theta_1, \theta_2 \in \mathrm{Irr}(K)$. Тогда

$$
\begin{aligned}
(\chi_1 \times \theta_1, \chi_2 \times \theta_2)_{G} &= \frac{1}{|G|}\sum_{g\in G}(\chi_1 \times \theta_1)(g)\overline{(\chi_2 \times \theta_2)(g)} = \frac{1}{|H||K|}\sum_{\substack{h\in H\\ k\in K}} \chi_1(h)\theta_1(k)\overline{\chi_2(h)\theta_2(k)} \\
&= \left(\frac{1}{|H|}\sum_{h\in H}\chi_1(h)\overline{\chi_2(h)}\right)\left(\frac{1}{|K|}\sum_{k\in K}\theta_1(k)\overline{\theta_2(k)}\right) = (\chi_1, \chi_2)_{H}(\theta_1, \theta_2)_{K}
\end{aligned}
$$

В силу (i) отсюда следует, что характеры $\chi \times \theta$ попарно различны и неприводимы при различных выборах $\chi \in \mathrm{Irr}(H)$, $\theta \in \mathrm{Irr}(K)$.

Поскольку

$$
\sum_{\substack{\chi\in \mathrm{Irr}(H)\\ \theta\in\mathrm{Irr}(K)}} (\chi \times \theta)(1)^2 = \sum_{\substack{\chi\in \mathrm{Irr}(H)\\ \theta\in\mathrm{Irr}(K)}} \chi(1)^2\theta(1)^2 = \left(\sum_{\chi\in\mathrm{Irr}(H)}\chi(1)^2\right)\left(\sum_{\theta\in\mathrm{Irr}(K)}\theta(1)^2\right) = |H||K| = |G|,
$$

отсюда следует, что характеры $\chi \times \theta$ исчерпывают всё множество $\mathrm{Irr}(G)$. □

Пусть G — группа и $\chi \in \mathrm{Irr}(G)$. Определим отображения $\omega_\chi : \mathrm{Z}(\mathbb{C}G) \to \mathbb{C}$. Пусть $\mathscr{X}$ — некоторое $\mathbb{C}$-представление с характером χ. Из предложения (9.5) вытекает, что для любого $z \in \mathrm{Z}(\mathbb{C}G)$ матрица $\mathscr{X}(z)$ скалярна. Пусть $\mathscr{X}(z) = \varepsilon\mathbf{1}$ для $\varepsilon \in \mathbb{C}$. Поскольку скалярная матрица совпадает с любой своей сопряжённой, число ε не зависит от выбора представления $\mathscr{X}$ с характером χ. Мы положим $\omega_\chi(z) = \varepsilon$. Другими словами, для всех $z \in \mathrm{Z}(\mathbb{C}G)$

$$\mathscr{X}(z) = \omega_\chi(z)\mathbf{1}.$$

Так как $\mathscr{X}$ — гомоморфизм алгебр, легко видеть, что $\omega_\chi : \mathrm{Z}(\mathbb{C}G) \to \mathbb{C}$ также является гомоморфизмом алгебр, который мы будем называть *центральным гомоморфизмом, соответствующим неприводимому характеру* χ. В частности, этот гомоморфизм полностью определяется своими значениями на базисе алгебры $\mathrm{Z}(\mathbb{C}G)$. Одним из таких базисов является набор центральных идемпотентов.

(16.25) Предложение. (i) *Пусть $\chi \in \mathrm{Irr}(G)$. Тогда для любого $\theta \in \mathrm{Irr}(G)$*

$$\omega_\chi(e_\theta) = \delta_{\chi,\theta},$$

где e_θ — центральный идемпотент, соответствующий характеру θ. В частности, гомоморфизмы ω_χ попарно различны.

(ii) *Все гомоморфизмы $\mathbb{C}$-алгебр $\mathrm{Z}(\mathbb{C}G) \to \mathbb{C}$ исчерпываются множеством $\{\omega_\chi \mid \chi \in \mathrm{Irr}(G)\}$.*

(iii) *Пусть $K \in \mathscr{K}(G)$. Тогда имеет место представление*

$$\widehat{K} = \sum_{\chi\in\mathrm{Irr}(G)} \omega_\chi(\widehat{K})e_\chi.$$

✎ Доказать предложение (16.25).

Другим естественным базисом алгебры $\mathrm{Z}(\mathbb{C}G)$, как мы знаем из (3.7)(ii), являются классовые суммы группы G. Пусть $K \in \mathscr{K}(G)$ и $g \in K$. Взяв след обеих частей равенства $\mathscr{X}(\widehat{K}) = \omega_\chi(\widehat{K})\mathbf{1}$, получим

$$\chi(1)\omega_\chi(\widehat{K}) = \chi(\widehat{K}) = \sum_{x\in K}\chi(x) = |K|\chi(g),$$

откуда следует

(16.26) Предложение. *Имеем*

$$\omega_\chi(\widehat{K}) = \frac{|K|\chi(x_{K})}{\chi(1)}.$$

В частности, центральные гомоморфизмы ω_χ полностью определяются по таблице характеров группы G.

Ясно, что одноэлементные классы сопряжённости образуют центр группы G и имеет место включение $\mathrm{Z}(G) \subseteq \mathrm{Z}(\mathbb{C}G)$. В частности, из (16.26) следует соотношение

$$\chi(z) = \chi(1)\omega_\chi(z)$$

для произвольных $\chi \in \mathrm{Irr}(G)$ и $z \in \mathrm{Z}(G)$. Это соотношение обобщается следующим утверждением.

(16.27) Предложение. *Пусть $\chi \in \mathrm{Irr}(G)$ и $z \in \mathrm{Z}(G)$.*

(*i*) $\omega_\chi(z)^{|z|} = 1$.

(*ii*) *Для произвольного $g \in G$ справедливы соотношения*

$$\chi(zg) = \omega_\chi(z)\chi(g) = \frac{\chi(z)\chi(g)}{\chi(1)}.$$

✎ Доказать предложение (16.27).

По аналогии с таблицей характеров $\mathrm{X}(G)$ определим *таблицу $\Omega(G)$ центральных гомоморфизмов, соответствующих неприводимым обыкновенным характерам группы G* как квадратную матрицу, строки которой индексированы центральными гомоморфизмами ω_χ по всем $\chi \in \mathrm{Irr}(G)$, а столбцы — классами сопряжённости $K \in \mathscr{K}(G)$. При этом элемент χ-й строки и K-го столбца матрицы $\Omega(G)$ равен $\omega_\chi(\widehat{K})$. Например, ниже приведена таблица $\Omega(S_3)$.

$\Omega(S_3)$	1	(12)	(123)
ω_{χ_1}	1	3	2
ω_{χ_2}	1	-3	2
ω_{χ_3}	1	0	-1

Следующее утверждение показывает, что матрица $\Omega(G)$ лежит в кольце $\mathrm{M}_{|\,\mathrm{Irr}(G)|}(\boldsymbol{R})$.

(16.28) Предложение. *Пусть $\chi \in \mathrm{Irr}(G)$ и $K \in \mathscr{K}(G)$. Тогда значение $\omega_\chi(\widehat{K})$ является целым алгебраическим числом.*

Доказательство. В (3.7)(*iv*) показано, что для любых классов $K, L \in \mathscr{K}(G)$ имеет место равенство $\widehat{K}\widehat{L} = \sum_{M \in \mathscr{K}(G)} a_{KLM}\widehat{M}$, где $a_{KLM} \in \mathbb{Z}$. Поскольку ω_χ — гомоморфизм алгебр $\mathrm{Z}(\mathbb{C}G) \to \mathbb{C}$, отсюда следует, что

$$\omega_\chi(\widehat{K})\omega_\chi(\widehat{L}) = \sum_{M \in \mathscr{K}(G)} a_{KLM}\omega_\chi(\widehat{M}). \tag{16.29}$$

Пусть W — $\mathbb{Z}$-модуль, порождённый значениями $\{\omega_\chi(L) \mid L \in \mathscr{K}(G)\}$. Тогда W — конечно порождённый $\mathbb{Z}$-модуль и в силу (16.29) для любого $K \in \mathscr{K}(G)$ выполнено включение $\omega_\chi(\widehat{K})W \subseteq W$. Из предложения (A.4) вытекает, что $\omega_\chi(\widehat{K})$ — целое алгебраическое число. □

Важным следствием предложения (16.28) является

(16.30) Предложение. *Если $x \in \mathrm{Irr}(G)$, то $\chi(1)$ делит $|G|$.*

Доказательство. Из первого соотношения ортогональности (16.17) вытекает, что

$$|G| = \sum_{g \in G} \chi(g)\chi(g^{-1}).$$

Перепишем это равенство в терминах центрального гомоморфизма ω_χ. Из (16.26) следует, что

$$|G| = \sum_{K \in \mathscr{K}(G)} |K|\chi(x_K)\chi(x_K^{-1}) = \sum_{K \in \mathscr{K}(G)} \chi(1)\omega_\chi(\widehat{K})\chi(x_K^{-1}).$$

Поэтому

$$\frac{|G|}{\chi(1)} = \sum_{K \in \mathscr{K}(G)} \omega_\chi(\widehat{K})\chi(x_K^{-1}).$$

В силу (16.28), (16.26) и (A.5)(*i*) выражение справа является целым алгебраическим числом, а поскольку выражение слева — рациональное число, то по (A.1) обе части являются целыми рациональными числами. □

В действительности имеет место даже более сильный результат. Теорема Ито [6, (6.15)] утверждает, что степень неприводимого обыкновенного характера группы G делит индекс любой её нормальной абелевой подгруппы.

С помощью центральных гомоморфизмов можно получить явную формулу для структурных констант a_{KLM} центра $\mathrm{Z}(\mathbb{C}G)$.

(16.31) Предложение. *Пусть $K, L, M \in \mathscr{K}(G)$. Тогда для чисел a_{KLM} таких, что*

$$\widehat{K}\widehat{L} = \sum_{M\in\mathscr{K}(G)} a_{KLM}\widehat{M}$$

имеет место выражение

$$a_{KLM} = \frac{|K||L|}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(x_K)\chi(x_L)\overline{\chi(x_M)}}{\chi(1)}.$$

✎ Доказать предложение (16.31). (*Указание.* Воспользоваться (16.26) и (16.22)).

✎ **(16.32)** Пусть $K_1, \ldots, K_s \in \mathscr{K}(G)$. Показать, что число наборов $(x_{K_1}, \ldots, x_{K_s})$, где $x_{K_i} \in K_i$, таких, что

$$x_{K_1}\cdot\ldots\cdot x_{K_s} = 1$$

равно

$$\frac{|K_1|\cdot\ldots\cdot|K_s|}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(x_{K_1})\cdot\ldots\chi(x_{K_s})}{\chi(1)^{s-2}}.$$

(*Указание.* Применить индукцию по s.)

Пусть $\varphi \in \mathrm{cf}(G)$. Обсудим вкратце методы определения принадлежности функции φ множеству характеров или кольцу обобщённых характеров группы G.

Положим $\mathbb{Z}[\mathrm{Irr}(G)] = \mathbb{Z}[\mathrm{Irr}_{\mathbb{C}}(G)]$. Если известно множество $\mathrm{Irr}(G)$, то из свойств скалярного произведения вытекает, что $\varphi \in \mathbb{Z}[\mathrm{Irr}(G)]$ тогда и только тогда, когда $(\varphi, \chi)_G \in \mathbb{Z}$ для всех $\chi \in \mathrm{Irr}(G)$. Более типичной является ситуация, когда имеется некоторый класс $\mathscr{H}$ подгрупп группы G такой, что $\varphi_H \in \mathbb{Z}[\mathrm{Irr}(H)]$ для всех $H \in \mathscr{H}$. Суть характеризационной теоремы Брауэра (16.34)(i) состоит в том, что для определённого семейства подгрупп $\mathscr{H}$ последнее условие является достаточным для включения $\varphi \in \mathbb{Z}[\mathrm{Irr}(G)]$.

(16.33) Определение. Группа E называется *p-элементарной (брауэровой)*, где p — простое число, если она является прямым произведением циклической группы и p-группы. Будем говорить, что E *элементарная (брауэрова)*, если она p-элементарна для некоторого простого числа p.

Заметим, что p-элементарную подгруппу можно было бы также определить как прямое произведение p-группы и циклической p'-группы.

Напомним, что характеры степени 1 называются линейными.

(16.34) Теорема (Брауэра). *Пусть $\varphi \in \mathrm{cf}(G)$. Тогда следующие условия эквивалентны.*

(i) $\varphi \in \mathbb{Z}[\mathrm{Irr}(G)]$

(ii) *$\varphi_E \in \mathbb{Z}[\mathrm{Irr}(E)]$ для всякой элементарной подгруппы $E \leqslant G$.*

(iii) *φ является $\mathbb{Z}$-линейной комбинацией характеров вида λ^G, где λ — линейный характер некоторой элементарной подгруппы $E \leqslant G$.*

Доказательство. См. [2, Теорема 40.1] или [6, Теорема 8.4]. □

Зафиксируем до конца этого раздела некоторое простое число p.

(16.35) Определение. Пусть n — натуральное число. Назовём *p-частью* числа n максимальную степень p, делящую n, и обозначим её через n_p, а *p'-частью* числа n — величину n/n_p, которую будем обозначать через $n_{p'}$.

По определению характер $\chi \in \mathrm{Irr}(G)$ имеет *p-дефект d*, если $|G|_p = p^d|\chi(1)|_p$.

Мы используем теорему Брауэра для изучения значений неприводимых обыкновенных характеров p-дефекта 0.

(16.36) Определение. Пусть $\chi \in \mathrm{Irr}(G)$ и d — p-дефект характера χ. Определим отображение $\dot\chi : G \to \mathbb{C}$ по правилу

$$\dot\chi(g) = \begin{cases} p^d\chi(g), & \text{если} p \nmid |g|; \\ 0, & \text{иначе.} \end{cases}$$

для любого $g \in G$.

Легко видеть, что $\dot\chi \in \mathrm{cf}(G)$. Покажем, что в действительности $\dot\chi$ является обобщённым характером.

(16.37) Предложение. *Если* $\chi \in \mathrm{Irr}(G)$, *то* $\dot\chi \in \mathbb{Z}[\mathrm{Irr}(G)]$.

Доказательство. Пусть E — элементарная подгруппа из G и $\theta \in \mathrm{Irr}(E)$. По теореме (16.34) достаточно проверить, что $(\dot\chi_E, \theta)_E \in \mathbb{Z}$, где $\dot\chi_E$ обозначает $(\dot\chi)_E$.

Поскольку E нильпотентна, мы можем записать $E = P \times Q$, где P — p-группа и $p \nmid |Q|$. Пусть $x \in E$. Если $p \nmid |x|$, то $x \in Q$. Поэтому функция $\dot\chi$ тождественно равна нулю на $E \setminus Q$ и $\dot\chi_Q = p^d\chi_Q$. Имеем

(16.38) $$(\dot\chi_Q, \theta)_E = \frac{1}{|E|}\sum_{x\in E}\dot\chi(x)\overline{\theta(x)} = \frac{p^d}{|E|}\sum_{x\in Q}\chi(x)\overline{\theta(x)} = \frac{p^d}{|P|}(\chi_Q, \theta_Q)_Q,$$

поскольку $|E| = |P||Q|$.

Рассмотрим центральный гомоморфизм ω_χ. Из (16.26) следует, что если $g \in G$, то

$$\chi(g) = \frac{\omega_\chi(\widehat{g^G})\chi(1)}{|g^G|} = \frac{\omega_\chi(\widehat{g^G})\chi(1)|\mathrm{C}_G(g)|}{|G|}.$$

Тогда

(16.39) $$(\dot\chi_Q, \theta)_E = \frac{p^d}{|E|}\sum_{x\in Q}\chi(x)\overline{\theta(x)} = \frac{p^d\chi(1)}{|E||G|}\sum_{x\in Q}\omega_\chi(\widehat{x^G})|\mathrm{C}_G(x)|\overline{\theta(x)} = \frac{p^d\chi(1)}{|Q||G|}\sum_{x\in Q}\omega_\chi(\widehat{x^G})|\mathrm{C}_G(x) : P|\overline{\theta(x)},$$

где последнее равенство следует из того, что $P \leqslant \mathrm{C}_G(x)$ для любого $x \in Q$.

Из (16.38) следует, во-первых, что $(\dot\chi_Q, \theta)_E \in \mathbb{Q}$, а во-вторых, что $|P|(\dot\chi_Q, \theta)_E \in \mathbb{Z}$. Из (16.39) следует, что величина

$$\frac{|Q||G|}{p^d\chi(1)}(\dot\chi_Q, \theta)_E$$

также является целой, т. к. с одной стороны она рациональна, а с другой — целое алгебраическое число в силу (16.8)(i) и (16.28). Однако по условию $|Q|\frac{|G|}{p^d\chi(1)}$ является целым числом, не делящимся на p, а $|P|$ — степень p. Поэтому $(\dot\chi_Q, \theta)_E \in \mathbb{Z}$, что и требовалось доказать. □

(16.40) Предложение. *Пусть* $\chi \in \mathrm{Irr}(G)$ *— характер p-дефекта* 0. *Тогда* $\chi(g) = 0$ *для любого элемента* $g \in G$ *порядка, делящегося на* p.

Доказательство. Из предложения (16.37) следует, что $\dot\chi$ является обобщённым характером. В частности, $(\dot\chi, \chi)_G \in \mathbb{Z}$. С другой стороны $\dot\chi(g) = \chi(g)$ при $p \nmid |g|$ т. к. p-дефект характера χ равен 0, и поэтому

$$(\dot\chi, \chi)_G = \frac{1}{|G|}\sum_{g\in G,\, p\nmid|g|}|\chi(g)|^2.$$

Отсюда следует, что $0 < (\dot\chi, \chi)_G \leqslant (\chi, \chi)_G = 1$ и, значит, $(\dot\chi, \chi)_G = (\chi, \chi)_G$. Но тогда

$$0 = (\dot\chi - \chi, \chi)_G = \frac{1}{|G|}\sum_{g\in G,\, p\,|\,|g|}|\chi(g)|^2,$$

откуда вытекает, что $\chi(g) = 0$ для всех $g \in G$ таких, что $p \mid |g|$. □

17. Брауэровы характеры

Начиная с этого раздела, мы будем изучать модулярные представления конечных групп, т. е. представления над полем простой характеристики.

Пусть $\boldsymbol{R}$ — кольцо целых алгебраических чисел. Всюду далее мы фиксируем простое число p и некоторый максимальный идеал M кольца $\boldsymbol{R}$, содержащий идеал $p\boldsymbol{R}$. Положим $F = \boldsymbol{R}/M$ и пусть

$$^\star : \boldsymbol{R} \to F$$

— естественный эпиморфизм колец.

✎ **(17.1)** Показать, что F — поле характеристики p.

(17.2) Предложение. *$M \cap \mathbb{Z} = p\mathbb{Z}$. В частности, $\mathbb{Z}^\star \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.*

Доказать предложение (17.2).

Положим

$$U = \{\zeta \in \mathbb{C} \,|\, \zeta^m = 1 \ \text{ для некоторого } \ m \in \mathbb{Z} \ \text{ такого, что } \ p \nmid m\}.$$

Другими словами, U — группа корней из 1 степени, взаимно простой с p. Ясно, что $U \subseteq \boldsymbol{R}$.

(17.3) Предложение. *Имеют место следующие утверждения.*

(*i*) *Ограничение отображения * на U является изоморфизмом групп $U \to F^\times$.*

(*ii*) *Поле F совпадает с алгебраическим замыканием своего простого подполя $\mathbb{F}_p$.*

Доказательство. Будем обозначать ограничение отображения * на U тем же символом. Покажем инъективность гомоморфизма групп $^\star : U \to F^\times$. Пусть $1 \neq \zeta \in U$. Тогда $m = |\zeta| > 1$ и $p \nmid m$. Допустим, что $\zeta^\star = 1$. Имеет место тождество в кольце $\boldsymbol{R}[x]$

$$1 + x + \ldots + x^{m-1} = \frac{x^m - 1}{x - 1} = \prod_{i=1}^{m-1} (x - \zeta^i).$$

Сравнив правую и левую часть при $x = 1$, получим, что в кольце $\boldsymbol{R}$ элемент $1 - \zeta$ делит m. Но раз $\zeta^\star = 1$, то $(1-\zeta)^\star = 0$ и, значит, $m^\star = 0$. Тогда $m \in M$. В силу (17.2) число m кратно p. Противоречие. Значит, отображение * инъективно на U.

Пусть $f \in F^\times$. Выберем элемент $\alpha \in \boldsymbol{R}$ такой, что $\alpha^\star = f$. Так как α — целое алгебраическое число, то

$$\alpha^n + b_1\alpha^{n-1} + b_2\alpha^{n-1} + \ldots + b_n = 0$$

для некоторых $b_1, b_2, \ldots, b_n \in \mathbb{Z}$. Тогда

$$f^n + b_1^\star f^{n-1} + b_2^\star f^{n-1} + \ldots + b_n^\star = 0$$

и f является алгебраическим над $\mathbb{F}_p$ в силу (17.2). То есть расширение $\mathbb{F}_p \subseteq F$ является алгебраическим. Для завершения доказательства достаточно показать, что если $F \subseteq K$ — алгебраическое расширение полей, то $K^\times \subseteq U^\star$. Отсюда будет следовать сюръективность отображения * и алгебраическая замкнутость поля F.

Пусть $k \in K^\times$. Тогда, как известно из теории полей, элемент k алгебраичен над $\mathbb{F}_p$. То есть k является ненулевым элементом конечного поля $\mathbb{F}_p(k)$ характеристики p. Поэтому $k^s = 1$, где $s = |\mathbb{F}_p(k)| - 1$ и, значит, $p \nmid s$. Но мы видели, что в $U^\star$ уже есть s различных корней многочлена $x^s - 1$ — это степени элемента $\xi^\star$, где $\xi \in U$ — элемент порядка s. Значит, k совпадает с одним из этих корней, т. е. лежит в $U^\star$. □

Элемент $g \in G$ называется *p-регулярным* или *p'-элементом*, если $p \nmid |g|$. Класс сопряжённости g^G произвольного p-регулярного элемента g мы будем также называть *p-регулярным*. Ясно, что p-регулярный класс состоит из p-регулярных элементов. Обозначим через $G_{p'}$ множество всех p-регулярных элементов группы G, а через $\mathscr{K}(G_{p'})$ — множество всех её p-регулярных классов.

(17.4) Лемма. *Пусть $g \in G$. Тогда существуют однозначно определённые элементы $g_{p'}, g_p \in G$ такие, что $g_{p'}$ является p-регулярным, g_p является p-элементом и $g = g_p g_{p'} = g_{p'} g_p$. При этом $g_{p'}, g_p \in \langle g \rangle$ и имеет место равенство $\mathrm{C}_G(g) = \mathrm{C}_G(g_p) \cap \mathrm{C}_G(g_{p'})$.*

(17.5) Доказать лемму (17.4).

Элементы g_p и $g_{p'}$ из леммы (17.4) называются, соответственно, *p-частью* и *p'-частью* элемента g.

Пусть π — подмножество множества всех простых чисел. Через π' обозначается множество простых чисел, не принадлежащих π. Элемент $g \in G$ называется π-элементом, если все простые делители его порядка принадлежат π. Множество всех π-элементов группы G обозначается через G_π.

Следующее упражнение обобщает лемму (17.4).

(17.6) Пусть $g \in G$ и π — произвольное множество простых чисел. Тогда существуют однозначно определённые элементы $g_\pi, g_{\pi'} \in G$ такие, что $g_\pi \in G_\pi$, $g_{\pi'} \in G_{\pi'}$ и $g = g_\pi g_{\pi'} = g_{\pi'} g_\pi$. При этом $g_\pi, g_{\pi'} \in \langle g \rangle$.

(17.7) Определение. Пусть $\mathscr{X} : G \to \mathrm{GL}_n(F)$ — F-представление группы G. Пусть $g \in G_{p'}$. По (17.3)(*i*) все характеристические значения матрицы $\mathscr{X}(g)$ имеют вид $\zeta_1^\star, \ldots, \zeta_n^\star$ для однозначно определённых элементов $\zeta_1, \ldots, \zeta_n \in U$. *Брауэровым* или *$p$-модулярным характером* F-представления $\mathscr{X}$ называется отображение $\varphi : G_{p'} \to \mathbb{C}$, заданное для $g \in G_{p'}$ правилом

$$\varphi(g) = \zeta_1 + \ldots + \zeta_n.$$

Функцию $G_{p'} \to \mathbb{C}$, принимающую постоянное значение на каждом p-регулярном классе, будем называть *p-регулярной классовой функцией*. Множество всех p-регулярных классовых функций группы G будем обозначать через $\mathrm{cf}(G_{p'})$. На этом множестве, как и на $\mathrm{cf}(G)$, задаётся структура $\mathbb{C}$-алгебры относительно естественных операций.

Определим для произвольной функции $\theta \in \mathrm{cf}(G_{p'})$ *комплексно-сопряжённую* функцию $\overline{\theta}$ по правилу $\overline{\theta}(g) = \overline{\theta(g)}$ для всех $g \in G_{p'}$. Если $H \leqslant G$ и $\theta \in \mathrm{cf}(G_{p'})$, то обозначим через θ_H ограничение θ на $H_{p'}$. Ясно, что $\theta_H \in \mathrm{cf}(H_{p'})$.

(17.8) Предложение. *Пусть φ — брауэров характер F-представления $\mathscr{X}$ группы G.*

(i) *φ — брауэров характер любого F-представления, эквивалентного $\mathscr{X}$ (при фиксированном выборе идеала M).*

(ii) *$\varphi \in \mathrm{cf}(G_{p'})$.*

(iii) *$\varphi(g^{-1}) = \overline{\varphi(g)}$ для любого $g \in G_{p'}$.*

(iv) *$\overline{\varphi}$ является брауэровым характером контрагредиентного F-представления $\mathscr{X}^*$.*

(v) *Если $H \leqslant G$, то φ_H — брауэров характер группы H.*

✎ Доказать предложение (17.8).

Следует подчеркнуть, что для произвольной p-регулярной классовой функции $\varphi \in \mathrm{cf}(G_{p'})$ вообще говоря некорректно спрашивать, будет ли φ брауэровым характером группы G или нет, поскольку ответ на этот вопрос может существенно зависеть от выбора максимального идеала M кольца $\boldsymbol{R}$, содержащего простое число p. Есть примеры, показывающие, что брауэров характер φ при одном выборе M может перестать быть таковым, если идеал M изменить. Кроме того, если M фиксирован, φ — брауэров характер и σ — автоморфизм поля $\mathbb{C}$, то классовая функция $\varphi^\sigma \in \mathrm{cf}(G_{p'})$, заданная правилом, $\varphi^\sigma(g) = \varphi(g)^\sigma$ при всех $g \in G_{p'}$ может не быть брауэровым характером группы G (см. предложение (19.12)).

Как и для F-характеров, *степенью* брауэрова характера φ назовём степень представления $\mathscr{X}$. Ясно, что она равна $\varphi(1)$. Брауэров характер главного F-представления называется *главным*. Будем обозначать его через $1_{G_{p'}}$.

(17.9) Предложение. *Пусть $\mathscr{X}$ и $\mathscr{Y}$ — F-представления группы G с брауэровыми характерами φ и ψ. Тогда брауэровы характеры F-представлений $\mathscr{X} \oplus \mathscr{Y}$ и $\mathscr{X} \otimes \mathscr{Y}$ равны, соответственно, $\varphi+\psi$ и $\varphi\psi$. В частности, множество брауэровых характеров группы G замкнуто относительно сложения и умножения.*

✎ Доказать предложение (17.9). (*Указание.* Воспользоваться предложением (11.2)(iv).)

Назовём брауэров характер φ представления $\mathscr{X}$ *неприводимым*, если неприводимо $\mathscr{X}$. Множество всех неприводимых брауэровых характеров группы G относительно максимального идеала M будем обозначать через $\mathrm{IBr}_M(G)$. Если ясно, о каком идеале M идёт речь, но нужно подчеркнуть, что характеристика поля F равна p, то будем обозначать это множество через $\mathrm{IBr}_p(G)$. Но в большинстве случаев будем просто использовать обозначение $\mathrm{IBr}(G)$. Из (8.4) вытекает, что это множество конечно.

(17.10) Предложение. *Справедливы следующие утверждения.*

(i) *Если два F-представления $\mathscr{X}$ и $\mathscr{Y}$ группы G имеют один и тот же набор неприводимых компонент (с учётом кратностей), то их брауэровы характеры совпадают.*

(ii) *Если $\psi \in \mathrm{cf}(G_{p'})$ является брауэровым, то*

(17.11)
$$\psi = \sum_{\varphi \in \mathrm{IBr}(G)} a_\varphi \varphi,$$

где a_φ — неотрицательные целые числа.

Доказательство. Поскольку $\mathscr{X}$ и $\mathscr{Y}$ эквивалентны блочно-верхнетреугольным представлениям с одинаковыми (с точностью до перестановки) неприводимыми компонентами на диагонали, то брауэровы характеры $\mathscr{X}$ и $\mathscr{Y}$ равны сумме брауэровых характеров неприводимых компонент. Отсюда также следует, что любой брауэров характер является суммой элементов из $\mathrm{IBr}(G)$ с неотрицательными целыми коэффициентами. ☐

Как мы вскоре увидим (см. следствие (17.15)), утверждение (17.10)(i) можно обратить.

Следующее предложение объясняет, почему достаточно определять брауэровы характеры только на множестве p-регулярных элементов: зная брауэров характер представления $\mathscr{X}$, можно восстановить его F-характер.

(17.12) Предложение. *Имеем*

(i) *пусть $\mathscr{X}$ — F-представление группы G с F-характером χ и брауэровым характером φ. Тогда $\chi(g) = \chi(g_{p'}) = \varphi(g_{p'})^\star$ любого $g \in G$;*

(ii) *пусть χ — обыкновенный характер группы G. Тогда $\chi(g)^\star = \chi(g_{p'})^\star$ для любого $g \in G$.*

(iii) $\mathrm{Irr}_F(G) = \{\varphi^\star \mid \varphi \in \mathrm{IBr}(G)\}$, *где $\varphi^\star(g) = \varphi(g_{p'})^\star$ для всех $g \in G$.*

Доказательство. (i) Пусть $g \in G$. Ограничим представление $\mathscr{X}$ на циклическую группу $\langle g\rangle$. Пусть $\mathscr{X}_i$ — неприводимые компоненты этого ограничения. По (9.5) все $\mathscr{X}_i$ одномерны. Так как $g_p, g_{p'} \in \langle g\rangle$, то $\mathscr{X}_i(g) = \mathscr{X}_i(g_p)\mathscr{X}_i(g_{p'})$. Но $\mathscr{X}_i(g_p) \in F^\times$ — p-элемент, откуда следует, что $\mathscr{X}_i(g_p) = 1$. Поэтому $\chi(g) = \sum_i \mathscr{X}_i(g) = \sum_i \mathscr{X}_i(g_{p'}) = \chi(g_{p'})$.

(ii) Пусть $\mathscr{X}$ — обыкновенное представление с характером χ. Рассуждая, как в (i), получаем $\chi(g) = \sum_i \mathscr{X}_i(g_p)\mathscr{X}_i(g_{p'})$, где $\mathscr{X}_i$ — неприводимые компоненты ограничения $\mathscr{X}$ на $\langle g\rangle$. Так как $\mathscr{X}_i(g_p) \in \boldsymbol{R}$ — p-элемент, то $\mathscr{X}_i(g_p)^\star = 1$. Значит, $\chi(g)^\star = \sum_i \mathscr{X}_i(g_{p'})^\star = \chi(g_{p'})^\star$.

(iii) Из (i) вытекает, что $\varphi^\star$ совпадает с F-характером любого F-представления, брауэровым характером которого является φ. □

(17.13) Следствие. *Имеем*

(i) *брауэровы характеры неэквивалентных неприводимых F-представлений различны;*

(ii) $|\mathrm{IBr}(G)| = |\mathscr{M}(FG)|$.

Доказательство. (i) Если брауэровы характеры двух неприводимых F-представлений совпадают, то в силу (17.12)(i) совпадают и их F-характеры. Тогда сами представления эквивалентны по (9.4)(iii).

(ii) Следует из (i). □

Имеет место даже более сильный результат.

(17.14) Предложение. *Пусть $\varphi_1, \ldots, \varphi_s \in \mathrm{IBr}(G)$ попарно различны.*

(i) *Если $\alpha_1, \ldots, \alpha_s \in \boldsymbol{R}$ такие, что $\sum_i \alpha_i\varphi_i(x) \in M$ для всех $x \in G_{p'}$, то $\alpha_i \in M$ для всех i.*

(ii) *Характеры $\varphi_1, \ldots, \varphi_s$ линейно независимо над $\mathbb{C}$. В частности, всё множество $\mathrm{IBr}(G)$ линейно независимо над $\mathbb{C}$.*

Доказательство. (i) Пусть $\mathscr{X}_i$ — неприводимое F-представление с брауэровым характером φ_i и его F-характер равен ψ_i. Так как $\sum_i \alpha_i\varphi_i(x) \in M$ для всех $x \in G_{p'}$, то из (17.12)(i) следует, что $\sum_i \alpha_i^\star\psi_i(x) = 0$ для всех $x \in G$. Однако мы знаем из (9.4)(iii), что F-характеры ψ_i линейно независимы, т. е. $a_i^\star = 0$ и, значит, $a_i \in M$.

(ii) Достаточно доказать линейную независимость множества $\varphi_1, \ldots, \varphi_s$ над $\overline{\mathbb{Q}}$, поскольку отсюда с помощью элементарной линейной алгебры будет следовать линейная независимость над любым расширением поля $\overline{\mathbb{Q}}$ и, в частности, над $\mathbb{C}$.

Пусть $\gamma_1, \ldots, \gamma_s \in \overline{\mathbb{Q}}$ такие, что $\sum_i \gamma_i\varphi_i = 0$. Предположим, что не все γ_i равны нулю. Из следствия (A.22) вытекает существование элемента $\beta \in \overline{\mathbb{Q}}$ такого, что все произведения $\beta\gamma_i$ лежат в $\boldsymbol{R}$, но не все лежат в M. Поскольку $\sum_i(\beta\gamma_i)\varphi_i = 0$, то это противоречит ($i$). □

Из линейной независимости неприводимых брауэровых характеров вытекает, что коэффициенты a_φ в разложении (17.11) произвольного брауэрова характера ψ по характерам из $\mathrm{IBr}(G)$ определяются однозначно. Будем называть a_φ *кратностью вхождения* неприводимого брауэрова характера φ в характер ψ. Отметим, что если V и W — FG-модули, соответствующие представления которых имеют брауэровы характеры ψ и φ, то a_φ совпадает с числом композиционных факторов модуля V, изоморфных W. Переформулировав это на языке представлений, получаем следующее обращение утверждения (17.10)(i).

(17.15) Следствие. *Если два F-представления группы G имеют одинаковые брауэровы характеры, то у них один и тот же набор неприводимых компонент (с учётом кратностей).*

✓ Отметим, что равенство брауэровых характеров, вообще говоря, не влечёт эквивалентность F-представлений. Неэквивалентные F-представления циклической группы порядка 2, приведённые в (9.3), не только имеют равные F-характеры, но, как легко видеть, и равные брауэровы характеры (при любом выборе идеала M).

Ещё одним следствием линейной независимости является тот факт, что брауэров характер неприводим тогда и только тогда, когда он не представим в виде суммы $\varphi + \psi$ для некоторых брауэровых характеров φ и ψ. В частности, в силу (17.8)(iv) получаем

(17.16) Предложение. $\varphi \in \mathrm{IBr}(G)$ *тогда и только тогда, когда* $\overline{\varphi} \in \mathrm{IBr}(G)$.

Отметим, что этот факт также следует из (3.29).

18. Связь с обыкновенными характерами

Брауэровы характеры важны тем, что осуществляют связь между обыкновенными характерами группы G и её F-характерами в характеристике p. Чтобы объяснить это подробнее, нам потребуется ещё несколько определений и вспомогательных утверждений.

Определим подкольцо поля $\overline{\mathbb{Q}}$ и идеал в этом подкольце следующим образом.

$$\widetilde{\boldsymbol{R}} = \left\{ \frac{\alpha}{\beta} \,\Big|\, \alpha \in \boldsymbol{R},\ \beta \in \boldsymbol{R} \setminus M \right\}, \qquad \widetilde{M} = \left\{ \frac{\alpha}{\beta} \,\Big|\, \alpha \in M,\ \beta \in \boldsymbol{R} \setminus M \right\}.$$

✎ **(18.1)** Показать, что $\widetilde{\boldsymbol{R}}$ — локальное кольцо с максимальным идеалом $\widetilde{M}$. В частности, $\mathrm{J}(\widetilde{\boldsymbol{R}}) = \widetilde{M}$.

✎ **(18.2)** Описать кольцо $\widetilde{\boldsymbol{R}} \cap \mathbb{Q}$ и его идеал $\widetilde{M} \cap \mathbb{Q}$.

Отображение * может быть естественно продолжено на кольцо $\widetilde{\boldsymbol{R}}$. Если $\alpha \in \boldsymbol{R}$ и $\beta \in \boldsymbol{R} \setminus M$, то

$$\left(\frac{\alpha}{\beta}\right)^\star = \frac{\alpha^\star}{\beta^\star}.$$

✎ **(18.3)** Показать, что введённое отображение $^\star : \widetilde{\boldsymbol{R}} \to F$ определено корректно и является гомоморфизмом колец с ядром $\widetilde{M}$. В частности, $\boldsymbol{R} \cap \widetilde{M} = M$.

(18.4) Лемма. *Пусть V — векторное пространство над полем $\overline{\mathbb{Q}}$ и W — конечно порождённый $\widetilde{\boldsymbol{R}}$-подмодуль $\widetilde{\boldsymbol{R}}$-модуля V. Тогда существуют элементы $w_1, \ldots, w_s \in W$, которые линейно независимы над $\overline{\mathbb{Q}}$ и такие, что $W = \widetilde{\boldsymbol{R}}w_1 \oplus \ldots \oplus \widetilde{\boldsymbol{R}}w_s$.*

Доказательство. Пусть

$$\tau : W \to W/\widetilde{M}W$$

— естественный эпиморфизм $\widetilde{\boldsymbol{R}}$-модулей. Фактормодуль $W\tau$ можно рассматривать как векторное пространство над полем $F = \widetilde{\boldsymbol{R}}/\widetilde{M}$, положив $\alpha^\star(w\tau) = (\alpha w)\tau$ для всех $\alpha \in \widetilde{\boldsymbol{R}}$. Поскольку $\widetilde{\boldsymbol{R}}$-модуль W конечно порождён, размерность $\dim_F W\tau$ конечна. Пусть $w_1\tau, \ldots, w_s\tau$ — базис пространства $W\tau$, где $w_i \in W$. Положим $T = \widetilde{\boldsymbol{R}}w_1 + \ldots + \widetilde{\boldsymbol{R}}w_s$. Тогда T — $\widetilde{\boldsymbol{R}}$-подмодуль модуля W, и имеет место равенство $W = T + \widetilde{M}W$. Из следствия (4.21) вытекает, что $W = T$.

Остаётся проверить, что элементы $w_1, \ldots, w_s$ линейно независимы над $\overline{\mathbb{Q}}$. Если $\sum_i \gamma_i w_i = 0$, где $\gamma_i \in \overline{\mathbb{Q}}$ не все равны нулю, то по следствию (A.22) существует элемент $\beta \in \overline{\mathbb{Q}}$ такой, что все произведения $\beta\gamma_i$ лежат в $\boldsymbol{R}$, но не все лежат в M. Тогда $\sum_i \beta\gamma_i w_i = 0$. Применив гомоморфизм τ, получим $\sum_i (\beta\gamma_i)^\star (w_i\tau) = 0$, где не все коэффициенты $(\beta\gamma_i)^\star$ равны нулю. Это противоречит линейной независимости над F элементов $w_i\tau$. □

(18.5) Предложение. *Любое обыкновенное представление группы G может быть записано над кольцом $\widetilde{\boldsymbol{R}}$.*

Доказательство. Пусть $\mathscr{X}$ — обыкновенное представление группы G. В силу следствия (15.13) можно считать, что $\mathscr{X}$ записано над $\overline{\mathbb{Q}}$. Пусть V — $\overline{\mathbb{Q}}G$-модуль, соответствующий $\mathscr{X}$, и $v_1, \ldots, v_n$ — его базис. Рассмотрим $\widetilde{\boldsymbol{R}}$-подмодуль W модуля V, порожденный всевозможными произведениями $v_i g$, где $i = 1, \ldots, n$ и $g \in G$. Тогда W является конечно порождённым $\widetilde{\boldsymbol{R}}$-модулем, который инвариантен относительно действия группы G. По лемме (18.4) существуют линейно независимые над $\overline{\mathbb{Q}}$ элементы $w_1, \ldots, w_s \in W$, которые линейно независимы над $\overline{\mathbb{Q}}$ и такие, что $W = \widetilde{\boldsymbol{R}}w_1 \oplus \ldots \oplus \widetilde{\boldsymbol{R}}w_s$. В частности, $s \leqslant n$. Обратно, $s \geqslant n$, поскольку W содержит $\overline{\mathbb{Q}}$-базис $v_1, \ldots, v_n$. Значит, $w_1, \ldots, w_n$ — базис пространства V, и $\overline{\mathbb{Q}}$-представление $\mathscr{Y}$, соответствующее модулю V в этом базисе, записано над $\widetilde{\boldsymbol{R}}$ ввиду того, что $w_i g$ является $\widetilde{\boldsymbol{R}}$-линейной комбинацией элементов w_j для всех $g \in G$. □

Продолжим отображение * на кольца $\mathrm{M}_n(\widetilde{\boldsymbol{R}})$ и $\widetilde{\boldsymbol{R}}[x]$ следующим образом. Пусть $A \in \mathrm{M}_n(\widetilde{\boldsymbol{R}})$ и $A = (\alpha_{ij})$. Положим $A^\star = (\alpha_{ij}^\star)$. Ясно, что отображение

$$^\star : \mathrm{M}_n(\widetilde{\boldsymbol{R}}) \to \mathrm{M}_n(F)$$

является гомоморфизмом колец. Кроме того, $\det(A^\star) = \det(A)^\star$ для всех $A \in \mathrm{M}_n(\widetilde{\boldsymbol{R}})$. Мы также можем естественно продолжить отображение * до гомоморфизма колец многочленов

$$^\star : \widetilde{\boldsymbol{R}}[x] \to F[x],$$

причём заметим, что если корни ζ_i некоторого многочлена $f \in \widetilde{\boldsymbol{R}}[x]$ лежат в $\widetilde{\boldsymbol{R}}$, то корнями многочлена $f^\star \in F[x]$ будут элементы $\zeta_i^\star$ поля F.

Пусть $\mathscr{X}$ — обыкновенное представление группы G, записанное над $\widetilde{\boldsymbol{R}}$. Обозначим через $\mathscr{X}^\star$ отображение $g \mapsto \mathscr{X}(g)^\star$. Тогда $\mathscr{X}^\star$ является F-представлением группы G.

Для произвольной классовой функции $\theta \in \mathrm{cf}(G)$ обозначим через $\hat{\theta}$ ограничение θ на $G_{p'}$. Легко видеть, что $\hat{\theta} \in \mathrm{cf}(G_{p'})$ для всех $\theta \in \mathrm{cf}(G)$, и отображение $\hat{}: \mathrm{cf}(G) \to \mathrm{cf}(G_{p'})$ является $\mathbb{C}$-линейным и сюръективным.

(18.6) Предложение. *Пусть χ — обыкновенный характер группы G.*

(*i*) *$\hat{\chi}$ — брауэров характер группы G (для любого выбора максимального идеала M).*

(*ii*) *Если $\mathscr{X}$ — обыкновенное представление с характером χ, записанное над $\widetilde{\boldsymbol{R}}$, то $\hat{\chi}$ является брауэровым характером F-представления $\mathscr{X}^\star$.*

Доказательство. Докажем сразу оба утверждения. Пусть $\mathscr{X}$ — обыкновенное представление группы G с характером χ. В силу (18.5) можно считать, что $\mathscr{X}$ записано над $\widetilde{\boldsymbol{R}}$. Пусть φ обозначает брауэров характер F-представления $\mathscr{X}^\star$. Достаточно показать, что $\varphi = \hat{\chi}$. Пусть $g \in G_{p'}$ и $f \in \widetilde{\boldsymbol{R}}[x]$ — характеристический многочлен матрицы $\mathscr{X}(g)$. Имеем

$$f^\star(x) = \det(\mathscr{X}(g) - x\mathbf{1})^\star = \det(\mathscr{X}(g)^\star - x\mathbf{1}) = \det(\mathscr{X}^\star(g) - x\mathbf{1})$$

и, значит, $f^\star$ — характеристический многочлен матрицы $\mathscr{X}^\star(g)$.

Заметим, что корни ζ_i многочлена f являются корнями из 1 степени $|g|$, т. е. лежат в $U \subseteq \boldsymbol{R} \subseteq \widetilde{\boldsymbol{R}}$. Поэтому элементами $\zeta_i^\star$ исчерпываются все корни многочлена $f^\star$ и, следовательно, характеристическими значениями матрицы $\mathscr{X}^\star(g)$. Таким образом, по определению брауэрова характера $\varphi(g) = \sum_i \zeta_i = \chi(g) = \hat{\chi}(g)$. В силу произвольности g получаем $\varphi = \hat{\chi}$.

Поскольку p-регулярная классовая функция $\hat{\chi}$ не зависит от максимального идеала M и приведённое выше рассуждение верно для для любого выбора M, то $\hat{\chi}$ является брауэровым характером группы G при любом M. □

Следует подчеркнуть, что если обыкновенные представления $\mathscr{X}$ и $\mathscr{Y}$ эквивалентны и записаны над $\widetilde{\boldsymbol{R}}$, то F-представления $\mathscr{X}^\star$ и $\mathscr{Y}^\star$, вообще говоря, могут не быть эквивалентны. Например, пусть обыкновенные представления $\mathscr{X}$ и $\mathscr{Y}$ циклической группы $\langle a \mid a^2 = 1\rangle$ заданы по правилу

$$\mathscr{X}(a) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \mathscr{Y}(a) = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Эти представления эквивалентны, поскольку их $\mathbb{C}$-характеры равны. Однако при $p = 2$ соответствующие F представления

$$\mathscr{X}^\star(a) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathscr{Y}^\star(a) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

неэквивалентны над F (независимо от выбора идеала M). Отметим тем не менее, что $\mathscr{X}^\star$ и $\mathscr{Y}^\star$ имеют одинаковый набор неприводимых компонент. Как видно из следующего утверждения это верно и в общем случае.

(18.7) Следствие. *Пусть $\mathscr{X}$ и $\mathscr{Y}$ — эквивалентные обыкновенные представления группы G, записанные над $\widetilde{\boldsymbol{R}}$. Тогда F-представления $\mathscr{X}^\star$ и $\mathscr{Y}^\star$ имеют одинаковый набор неприводимых компонент (с учётом кратностей).*

Доказательство. Пусть χ — общий характер представлений $\mathscr{X}$ и $\mathscr{Y}$. Из (18.6)(*ii*) вытекает, что F-представления $\mathscr{X}^\star$ и $\mathscr{Y}^\star$ имеют один и тот же брауэров характер $\hat{\chi}$. Требуемое следует из (17.15). □

Сформулируем ещё два важных следствия.

(18.8) Следствие. *Справедливы следующие утверждения.*

(*i*) *Множество $\mathrm{IBr}(G)$ является базисом пространства $\mathrm{cf}(G_{p'})$.*

(*ii*) $|\mathrm{IBr}(G)| = |\mathscr{K}(G_{p'})|$.

(*iii*) *Пусть E — поле характеристики p, являющееся полем разложения группы G. Тогда число попарно неэквивалентных неприводимых E-представлений группы G равно $|\mathscr{K}(G_{p'})|$.*

Доказательство. (*i*) Ввиду (17.14)(*ii*) множество $\mathrm{IBr}(G)$ линейно независимо. Поэтому достаточно выразить любую p-регулярную классовую функцию в виде $\mathbb{C}$-линейной комбинации неприводимых брауэровых характеров. Пусть $\theta \in \mathrm{cf}(G_{p'})$. В силу сюръективности отображения $\hat{}: \mathrm{cf}(G) \to \mathrm{cf}(G_{p'})$ существует функция $\eta \in \mathrm{cf}(G)$ такая, что $\hat{\eta} = \theta$. Тогда $\eta = \sum_{\chi \in \mathrm{Irr}(G)} \alpha_\chi \chi$ для некоторых $\alpha_\chi \in \mathbb{C}$. Применив $\hat{}$, получим

$\theta = \sum_{\chi \in \mathrm{Irr}(G)} \alpha_\chi \hat{\chi}$. Но каждый $\hat{\chi}$ является брауэровым характером по (18.6)(i) и, значит, представим в виде линейной комбинации элементов из $\mathrm{IBr}(G)$ по (17.10)(ii).

(ii) Это следует из (i), т. к. размерность пространства $\mathrm{cf}(G_{p'})$, как легко видеть, совпадает с $|\mathscr{K}(G_{p'})|$.

(iii) По предложению (15.11) число попарно неэквивалентных неприводимых E-представлений группы G совпадает с числом попарно неэквивалентных неприводимых $\overline{E}$-представлений, где $\overline{E}$ — алгебраическое замыкание поля E, а поскольку $\overline{E}$ содержит F, это же число равно по (15.11) также и числу попарно неэквивалентных неприводимых F-представлений. Значит, требуемое следует из (ii) ввиду (17.13)(i). □

Напомним, что через $\mathrm{O}_p(G)$ обозначается наибольшая нормальная p-подгруппа группы G.

(18.9) Следствие. *Справедливы следующие утверждения.*

(i) *Единственным неприводимым F-представлением p-группы является её главное F-представление.*

(ii) *Если $\mathscr{X}$ — неприводимое F-представление группы G, то $\mathrm{O}_p(G) \leqslant \ker \mathscr{X}$.*

(iii) *Пусть $\mathscr{X}_1, \ldots, \mathscr{X}_s$ — полный набор попарно неэквивалентных неприводимых F-представлений группы G. Тогда*

$$\bigcap_{i=1}^{s} \ker \mathscr{X}_i = \mathrm{O}_p(G).$$

Доказательство. (i) Любая p-группа P имеет единственный p-регулярный класс. Значит, в силу (18.8)(ii) единственным неприводимым F-представлением группы P является её главное представление.

(ii) Обозначим $P = \mathrm{O}_p(G)$. По теореме Клиффорда (14.1)(i) ограничение $\mathscr{X}_P$ является вполне приводимым F-представлением группы P. Из (i) вытекает, что $\mathscr{X}_P$ — прямая сумма главных F-представлений, т. е. $P \leqslant \ker \mathscr{X}$.

(iii) Обозначим $N = \bigcap_i \ker \mathscr{X}_i$. Включение $\mathrm{O}_p(G) \leqslant N$ следует из (ii). Поскольку $N \trianglelefteqslant G$, для доказательства обратного включения достаточно установить, что N состоит из p-элементов. Пусть $g \in N$. Тогда элемент $1 - g \in FG$ лежит в $\mathrm{Ker}\, \mathscr{X}_i$ для любого $i = 1, \ldots, s$, где $\mathscr{X}_i$ рассматривается как представление алгебры FG. Поскольку $\mathscr{X}_1, \ldots, \mathscr{X}_s$ образуют полный набор её неприводимых представлений, из (8.5) следует, что $1 - g \in \mathrm{J}(FG)$. Поэтому $(1-g)^n = 0$ для некоторого натурального n в силу (5.2). Пусть k — произвольное натуральное число такое, что $n \leqslant p^k$. Тогда $0 = (1-g)^{p^k} = 1 - g^{p^k}$, т. е. $g^{p^k} = 1$. Отсюда следует требуемое. □

19. Таблица брауэровых характеров. Числа разложения. Инварианты Картана

Таблицей брауэровых характеров $\Phi_M(G)$ группы G (относительно максимального идеала M) называется квадратная матрица, строки которой индексированы неприводимыми брауэровыми характерами $\varphi \in \mathrm{IBr}(G)$, а столбцы — p-регулярными классами сопряжённости $K \in \mathscr{K}(G_{p'})$. Элемент φ-й строки и K-го столбца равен $\varphi(x_{\kappa})$. Если идеал M фиксирован, то вместо $\Phi_M(G)$ будем просто писать $\Phi(G)$ или же $\Phi_p(G)$, если нужно подчеркнуть, что характеристика основного поля равна p. Например, ниже приведена таблица брауэровых характеров группы S_3 в характеристике 2.

$\Phi_2(S_3)$	1	(123)
φ_1	1	1
φ_2	2	-1

Пусть $\Phi = \Phi(G)$. Из (17.14)(ii) следует, что Φ является невырожденной матрицей. Так как элементы матрицы Φ лежат в $\boldsymbol{R}$, мы можем рассмотреть её образ относительно отображения *.

(19.1) Предложение. *Матрица $\Phi^\star$ является невырожденной.*

Доказательство. В силу (17.12)(iii) множество $\{\varphi^\star \mid \varphi \in \mathrm{IBr}(G)\}$, где $\varphi^\star(g) = \varphi(g_{p'})^\star$ для всех $g \in G$, совпадает с множеством всех неприводимых F-характеров, которое линейно независимо над F ввиду (9.4)(iii). Но любой F-характер однозначно определяются своими значениями на множестве представителей p-регулярных классов, см. (17.12)(i). Из этих замечаний следует, что матрица $\Phi^\star$, которая и состоит из таких значений, является невырожденной. □

(19.2) Определение. Пусть $\chi \in \mathrm{Irr}(G)$. Ввиду (18.6)(i) мы можем записать

(19.3)
$$\hat{\chi} = \sum_{\varphi \in \mathrm{IBr}(G)} d_{\chi\varphi} \varphi.$$

Однозначно определённые неотрицательные целые числа $d_{\chi\varphi}$ называются *числами разложения* группы G в характеристике p. Матрица

$$\mathrm{D} = (d_{\chi\varphi})_{\chi\in\mathrm{Irr}(G),\varphi\in\mathrm{IBr}(G)}$$

называется *матрицей разложения* и, очевидно, является матрицей отображения $\hat{}: \mathrm{cf}(G) \to \mathrm{cf}(G_{p'})$ в базисах $\mathrm{Irr}(G)$ и $\mathrm{IBr}(G)$.

Если положить $\mathrm{X} = \mathrm{X}(G)$ и $\Phi = \Phi(G)$, а также обозначить через $\widehat{\mathrm{X}}$ матрицу, состоящую из столбцов матрицы X, соответствующих p-регулярным классам, то равенство (19.3) можно переписать в матричном виде

$$\widehat{\mathrm{X}} = \mathrm{D}\Phi.$$

✓ Несмотря на то, что формально определение матрицы разложения также зависит от выбора максимального идеала M, мы покажем в (19.12)(i.2), что при другом выборе M, содержащего $p\boldsymbol{R}$, полученная матрица разложения будет отличаться от данной лишь перестановкой строк и столбцов.

(19.4) Предложение. *Имеем*

(i) *ранг матрицы разложения равен* $|\mathrm{IBr}(G)|$;

(ii) *столбцы матрицы разложения линейно независимы.*

Доказательство. Поскольку отображение $\hat{}: \mathrm{cf}(G) \to \mathrm{cf}(G_{p'})$ сюръективно, $\dim \mathrm{cf}(G_{p'}) = |\mathrm{IBr}(G)|$ и $\mathrm{Irr}(G)$ — базис пространства $\mathrm{cf}(G)$, отсюда следует, что среди $\{\hat{\chi} \mid \chi \in \mathrm{Irr}(G)\}$ найдётся $|\mathrm{IBr}(G)|$ линейно независимых характеров. Поэтому у матрицы разложения имеется $|\mathrm{IBr}(G)|$ линейно независимых строк. Так как число её столбцов также равно $|\mathrm{IBr}(G)|$, то отсюда следуют оба утверждения. □

Следующее утверждение показывает, что все строки и столбцы матрицы разложения ненулевые.

(19.5) Предложение. *Имеем*

(i) *если* $\varphi \in \mathrm{IBr}(G)$, *то существует* $\chi \in \mathrm{Irr}(G)$ *такой, что* $d_{\chi\varphi} \neq 0$;

(ii) *если* $\chi \in \mathrm{Irr}(G)$, *то существует* $\varphi \in \mathrm{IBr}(G)$ *такой, что* $d_{\chi\varphi} \neq 0$.

Доказательство. Пункт (i) вытекает из утверждения (19.4)(ii). Пункт (ii) очевиден, поскольку $0 \neq \chi(1) = \sum_{\varphi\in\mathrm{IBr}(G)} d_{\chi\varphi}\varphi(1)$. □

Следующее утверждение показывает, что в теории брауэровых характеров интересен только случай, когда простое число p является делителем порядка $|G|$.

(19.6) Предложение. *Если* $p \nmid |G|$, *то* $\mathrm{IBr}(G) = \mathrm{Irr}(G)$.

Доказательство. Предположим, что $p \nmid |G|$. Из (7.24)(i) следует, что в этом случае

$$|G| = \sum_{\varphi\in\mathrm{IBr}(G)} \varphi(1)^2. \tag{19.7}$$

С другой стороны

$$|G| = \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)^2 = \sum_{\chi\in\mathrm{Irr}(G)} \left(\sum_{\varphi\in\mathrm{IBr}(G)} d_{\chi\varphi}\varphi(1)\right)^2 = \sum_{\chi\in\mathrm{Irr}(G)} \sum_{\varphi,\psi\in\mathrm{IBr}(G)} d_{\chi\varphi}d_{\chi\psi}\varphi(1)\psi(1)$$

$$= \sum_{\varphi,\psi\in\mathrm{IBr}(G)} a_{\varphi,\psi}\,\varphi(1)\psi(1) \geqslant \sum_{\varphi\in\mathrm{IBr}(G)} \varphi(1)^2, \tag{19.8}$$

где $a_{\varphi,\psi} = \sum_{\chi\in\mathrm{Irr}(G)} d_{\chi\varphi}d_{\chi\psi}$ совпадает с произведением φ-го и ψ-го столбцов матрицы разложения и поэтому последнее неравенство вытекает из того, что $a_{\varphi,\psi} \geqslant 0$ при $\varphi \neq \psi$ и $a_{\varphi,\varphi} \geqslant 1$ ввиду (19.5)(i). Сравнивая (19.7) и (19.8), получаем, что в действительности $a_{\varphi,\psi} = \delta_{\varphi,\psi}$, т. е. каждому φ соответствует ровно один χ такой что, $d_{\chi\varphi} \neq 0$ (и в этом случае $d_{\chi\varphi} = 1$), причём разным φ соответствуют разные χ. Другими словами D — это матрица подстановки, и $\chi = \hat{\chi} = \varphi$ для любой пары соответствующих характеров φ и χ. Отсюда следует требуемое. □

(19.9) Следствие. *Пусть* φ *— брауэров характер группы* G, $H \leqslant G$ *и* $p \nmid |H|$. *Тогда* φ_H *— обыкновенный характер группы* H.

Доказательство. Из (17.8)(v) следует, что φ_H — брауэров характер группы H. Поэтому он является суммой элементов из $\mathrm{IBr}(H)$, и требуемое вытекает из (19.6) и условия $p \nmid |H|$. □

✎ **(19.10)** Считая известной таблицы обыкновенных характеров знакопеременной группы A_5 и её подгрупп (см. приложение B), найти её таблицы брауэровых характеров в характеристиках 2, 3, и 5. (*Указание.* Использовать изоморфизм $A_5 \cong \mathrm{SL}_2(4)$ в случае характеристики 2.)

Для любой функции $\theta \in \mathrm{cf}(G_{p'})$ определим отображение $\check{\theta} : G \to \mathbb{C}$ по правилу

$$\check{\theta}(g) = \theta(g_{p'})$$

для всех $g \in G$. Легко видеть, что $\check{\theta} \in \mathrm{cf}(G)$. Ясно также, что для любой функции $\theta \in \mathrm{cf}(G_{p'})$ если $\eta = \check{\theta}$, то $\hat{\eta} = \theta$.

Любой брауэров характер является $\mathbb{C}$-линейной комбинацией брауэровых характеров вида $\hat{\chi}$, где $\chi \in \mathrm{Irr}(G)$, что следует из (19.4)(i). В действительности имеет место более сильный факт.

(19.11) Предложение. *Пусть* $\varphi \in \mathrm{IBr}(G)$. *Тогда*

(i) $\check{\varphi} \in \mathbb{Z}[\mathrm{Irr}(G)]$;

(ii) *φ является $\mathbb{Z}$-линейной комбинацией брауэровых характеров $\hat{\chi}$, где* $\chi \in \mathrm{Irr}(G)$.

Доказательство. (i) Воспользуемся характеризацией Брауэра обобщённых характеров. Пусть $E \leqslant G$ — элементарная брауэрова подгруппа. Запишем $E = P \times Q$, где P — p-группа и Q — p'-группа. Если $g \in E$, то существуют элементы $x \in P$ и $y \in Q$ такие, что $g = xy = yx$. По лемме (17.4) имеем $x = g_p$ и $y = g_{p'}$. Значит, $\check{\varphi}(g) = \varphi(g'_p) = \varphi(y) = \varphi_Q(y)$. Но φ_Q — обыкновенный характер группы Q в силу (19.9), и он продолжается до обыкновенного характера $1_P \times \varphi_Q$ группы E по (16.24)(i). Другими словами, ограничение $\check{\varphi}$ на E совпадает с $1_P \times \varphi_Q$ и требуемое вытекает из теоремы (16.34).

(ii) Это следует из (i), поскольку на множестве $G_{p'}$ функции φ и $\check{\varphi}$ тождественно равны. □

Напомним, что для натурального числа n и простого p выражения n_p и $n_{p'}$ обозначают, соответственно, p-часть и p'-часть числа n.

Пусть $m = \exp G$. Поскольку значение произвольного брауэрова характера φ группы G являются суммой комплексных корней степени $m_{p'}$ из 1, то для любого $\sigma \in \mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$ можно определить p-регулярную классовую функцию φ^σ по правилу

$$\varphi^\sigma(g) = \varphi(g)^\sigma$$

для всех $g \in G_{p'}$. В отличие от обыкновенных характеров, функция φ^σ, вообще говоря, может не быть брауэровым характером относительно того же выбора максимального идеала M, а если $\varphi \in \mathrm{IBr}(G)$ и φ^σ — брауэров характер, то не всегда $\varphi^\sigma \in \mathrm{IBr}(G)$.

Например, пусть $G = J_1$ — простая спорадическая группа Янко и $p = 11$. Рассмотрим элемент $\sigma \in \mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$, который на элементе $\xi = e^{2\pi i/5}$ действует по правилу $\sigma : \xi \mapsto \xi^2$ и оставляет неподвижными все примитивные корни из 1 степени, взаимно простой с 5. Существуют неприводимые брауэровы характеры $\varphi_1, \varphi_2, \varphi_3 \in \mathrm{IBr}(G)$ степеней 7, 49 и 56, соответственно, такие, что φ_1^σ и φ_2^σ не являются брауэровыми характерами, в то время как $\varphi_3^\sigma = \varphi_1 + \varphi_2$.

В связи с этим представляет интерес следующее утверждение о поведении брауэровых характеров под действием автоморфизмов поля $\overline{\mathbb{Q}}$ или при смене максимального идеала M.

(19.12) Предложение. *Пусть* $m = \exp G$.

(i) *Предположим, что M_1 и M_2 — максимальные идеалы кольца $\boldsymbol{R}$, содержащие $p\boldsymbol{R}$. Тогда*

($i.1$) *существует автоморфизм $\sigma \in \mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$ такой, что отображение $\varphi \mapsto \varphi^\sigma$ является биекцией между множествами $\mathrm{IBr}_{M_1}(G)$ и $\mathrm{IBr}_{M_2}(G)$;*

($i.2$) *этот автоморфизм σ однозначно поднимается до элемента из $\mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q}_{m_p})$ (который также обозначим через σ) такое, что $d_{\chi^\sigma\varphi^\sigma} = d_{\chi\varphi}$ для любых $\chi \in \mathrm{Irr}(G)$ и $\varphi \in \mathrm{IBr}_{M_1}(G)$, и, в частности, матрица разложения группы G в характеристике p определяется однозначно с точностью до перестановки строк и столбцов.*

(ii) *Предположим, что φ — брауэров характер группы G относительно некоторого выбора максимального идеала M_1 кольца $\boldsymbol{R}$, содержащего $p\boldsymbol{R}$, и $\sigma \in \mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$. Тогда существует максимальный идеал M_2 кольца $\boldsymbol{R}$, содержащий $p\boldsymbol{R}$, относительно которого φ^σ является брауэровым характером. При этом φ неприводим относительно M_1 тогда и только тогда, когда φ^σ неприводим относительно M_2.*

Доказательство. (i) Положим $F_1 = \boldsymbol{R}/M_1$ и $F_2 = \boldsymbol{R}/M_2$. Существует изоморфизм полей $\rho : F_1 \to F_2$ в силу (17.3)(ii) и единственности с точностью до изоморфизма алгебраического замыкания поля $\mathbb{F}_p$.

Пусть ${}^{\star_1} : \boldsymbol{R} \to F_1$ и ${}^{\star_2} : \boldsymbol{R} \to F_2$ — естественные эпиморфизмы. Обозначим через σ автоморфизм группы U, который действует так, что $(\xi^{\star_1})^\rho = (\xi^\sigma)^{\star_2}$ для любого $\xi \in U$, делая коммутативной следующую диаграмму.

$$\begin{tikzcd} U \arrow[r, "\star_1"] \arrow[d, dotted, "\sigma"'] & F_1^\times \arrow[d, "\rho"] \\ U \arrow[r, "\star_2"] & F_2^\times \end{tikzcd}$$

Такой автоморфизм существует ввиду (17.3)(i). Отображение σ можно поднять до однозначно определённого элемента из группы $\mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$. В самом деле, так как σ — автоморфизм группы U, то существует целое число k, взаимно простое с $m_{p'}$ такое, что $\zeta^\sigma = \zeta^k$, где ζ — примитивный корень степени $m_{p'}$ из 1. Поэтому отображение σ определяет автоморфизм из $\mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$, который мы будем также обозначать через σ.

Пусть $\mathscr{X}$ — F_1-представление группы G с брауэровым характером φ относительно M_1. Поскольку значения φ являются суммами корней из 1 степени $m_{p'}$, они лежат в $\mathbb{Q}_{m_{p'}}$ и, значит, определена p-регулярная классовая функция φ^σ. Покажем, что брауэров характер F_2-представления $\mathscr{X}^\rho$ группы G относительно M_2 равен φ^σ, причём φ неприводим относительно M_1 тогда и только тогда, когда φ^σ неприводим относительно M_2. Отсюда будет следовать утверждение (i.1).

Пусть $g \in G_{p'}$ и $\zeta_1^{\star_1}, \ldots, \zeta_s^{\star_1}$ — корни характеристического многочлена $f(x) = \det(\mathscr{X}(g) - x\mathbf{1}_s) \in F_1[x]$ для подходящих $\zeta_1, \ldots, \zeta_s \in U$. Тогда $\varphi(g) = \zeta_1 + \ldots + \zeta_s$. Поскольку ρ индуцирует изоморфизм колец многочленов $F_1[x] \to F_2[x]$, отсюда следует, что характеристическими значениями матрицы $\mathscr{X}^\rho(g)$ будут корни $(\zeta_1^{\star_1})^\rho, \ldots, (\zeta_s^{\star_1})^\rho$ многочлена $f^\rho(x)$. По выбору отображения σ имеем $(\zeta_i^{\star_1})^\rho = (\zeta_i^\sigma)^{\star_2}$, и поэтому значение брауэрова характера F_2-представления X^ρ относительно M_2 на элементе g равно $\zeta_1^\sigma + \ldots + \zeta_s^\sigma = \varphi^\sigma(g)$, что и требовалось показать.

Равносильность неприводимости брауэровых характеров φ и φ^σ относительно идеалов M_1 и M_2, соответственно, вытекает из того, что F_1 — представление $\mathscr{X}$ неприводимо тогда и только тогда, когда неприводимо F_2 — представление $\mathscr{X}^\rho$. В самом деле, если $\mathscr{X}$ эквивалентно блочно-верхнетреугольному F_1-представлению $\mathscr{Y}$, то применив изоморфизм ρ получим, что $\mathscr{X}^\rho$ эквивалентно блочно-верхнетреугольному F_2-представлению $\mathscr{Y}^\rho$, и наоборот.

Теперь докажем утверждение (б). Известно, что σ однозначно продолжается до автоморфизма из группы $\mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q}_{m_p})$. Пусть $\chi \in \mathrm{Irr}(G)$. Тогда $(\hat{\chi})^\sigma = \widehat{\chi^\sigma}$. Однако

$$(\hat{\chi})^\sigma = \left(\sum_{\varphi \in \mathrm{IBr}_{M_1}(G)} d_{\chi\varphi}\varphi \right)^\sigma = \sum_{\varphi \in \mathrm{IBr}_{M_1}(G)} d_{\chi\varphi}\varphi^\sigma,$$

а также

$$\widehat{\chi^\sigma} = \sum_{\varphi \in \mathrm{IBr}_{M_1}(G)} d_{\chi^\sigma\varphi^\sigma}\varphi^\sigma.$$

Сравнив коэффициенты в правых частях, получим $d_{\chi^\sigma\varphi^\sigma} = d_{\chi\varphi}$, как и утверждалось в ($i$.2).

(ii) Пусть $F_1 = \boldsymbol{R}/M_1$, ${}^{\star_1} : \boldsymbol{R} \to F_1$ — естественный эпиморфизм и $\mathscr{X}_1$ — F_1-представление группы G, брауэровым характером которого (относительно идеала M_1) является φ.

Автоморфизм σ допускает продолжение до элемента из $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$, который также обозначим через σ. Положим $M_2 = M_1^\sigma$. Ясно, что $\boldsymbol{R}^\sigma = \boldsymbol{R}$ и M_2 — максимальный идеал кольца $\boldsymbol{R}$, содержащий $p\boldsymbol{R}$. Обозначим $F_2 = \boldsymbol{R}/M_2$ и пусть ${}^{\star_2} : \boldsymbol{R} \to F_2$ — естественный гомоморфизм. Тогда σ определяет отображение $\rho : F_1 \to F_2$, заданное правилом $(\alpha^{\star_1})^\rho = (\alpha^\sigma)^{\star_2}$ для всех $\alpha \in \boldsymbol{R}$. Рассуждая, как в начале доказательства пункта (i), получим совпадение отображения φ^σ с брауэровым характером F_2-представления $\mathscr{X}_2 = \mathscr{X}_1^\rho$ относительно M_2, а также равносильность неприводимости φ относительно M_1 и неприводимости φ^σ относительно M_2. □

Тем не менее в группе $\mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$ существует циклическая подгруппа, элементы которой действуют на множестве $\mathrm{IBr}(G)$.

(19.13) Предложение. *Пусть $m = \exp G$ и автоморфизм $\sigma \in \mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$ переводит примитивный корень ζ степени $m_{p'}$ из 1 в ζ^p. Тогда $\varphi \in \mathrm{IBr}(G)$ если и только если $\varphi^\sigma \in \mathrm{IBr}(G)$. Порядок подгруппы $\langle\sigma\rangle \leqslant \mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$ совпадает с порядком p по модулю $m_{p'}$.*

✎ Доказать предложение (19.13). (*Указание.* Использовать автоморфизм Фробениуса поля F.)

Пусть D — матрица разложения группы G. Произведение

$$\mathrm{C} = \mathrm{D}^\top \mathrm{D}$$

называется *матрицей Картана* группы G (в характеристике p). Очевидно, что C является симметрической квадратной $|\operatorname{IBr}(G)| \times |\operatorname{IBr}(G)|$-матрицей с неотрицательными целыми элементами. Поскольку D имеет ранг $|\operatorname{IBr}(G)|$, из элементарной линейной алгебры вытекает, что C положительно определена. Положим $\mathrm{C} = (c_{\varphi\psi})_{\varphi,\psi\in\operatorname{IBr}(G)}$. Тогда

$$c_{\varphi\psi} = \sum_{\chi\in\operatorname{Irr}(G)} d_{\chi\varphi} d_{\chi\psi}$$

— скалярное произведение φ-го и ψ-го столбцов матрицы разложения D. Элементы $c_{\varphi\psi}$ называют *инвариантами Картана* группы G.

(19.14) Предложение. *Матрица Картана группы G определяется однозначно с точностью до перестановки строк и столбцов. В частности, набор инвариантов Картана группы G определён однозначно.*

✎ Доказать предложение (19.14). (*Указание.* Воспользоваться (19.12)(i.2).)

(19.15) Определение. Для произвольного $\varphi \in \operatorname{IBr}(G)$ определим обыкновенный характер

$$\theta_\varphi = \sum_{\chi\in\operatorname{Irr}(G)} d_{\chi\varphi}\chi,$$

который называется *главным неразложимым характером*, соответствующим брауэрову характеру φ.

Из определения вытекает, что

(19.16)
$$\widehat{\theta_\varphi} = \sum_{\chi\in\operatorname{Irr}(G)} d_{\chi\varphi}\hat{\chi} = \sum_{\chi\in\operatorname{Irr}(G)} \sum_{\psi\in\operatorname{IBr}(G)} d_{\chi\varphi} d_{\chi\psi}\psi = \sum_{\psi\in\operatorname{IBr}(G)} c_{\varphi\psi}\psi.$$

Пусть Θ — *таблица значений главных неразложимых характеров на $G_{p'}$*, т. е. квадратная матрица, строки которой индексированы характерами $\varphi \in \operatorname{IBr}(G)$, а столбцы — p-регулярными классами сопряжённости $K \in \mathscr{K}(G_{p'})$. Элемент φ-й строки и K-го столбца матрицы Θ равен $\theta_\varphi(x_{\scriptscriptstyle K})$. Тогда из (19.16) следует, что

$$\Theta = \mathrm{C}\Phi.$$

Чуть ниже (предложение (19.18)(i)) мы покажем, что матрица Θ полностью определяет значения главных неразложимых характеров.

Пусть $\mu, \nu \in \operatorname{cf}(G) \cup \operatorname{cf}(G_{p'})$. Положим

$$(\mu,\nu)_{G_{p'}} = \frac{1}{|G|} \sum_{g\in G_{p'}} \mu(g)\overline{\nu(g)}.$$

Обозначим через $\operatorname{cf}^\circ(G)$ множество функций из $\operatorname{cf}(G)$, тождественно равных нулю вне $G_{p'}$. Легко видеть, что $\operatorname{cf}^\circ(G)$ — идеал алгебры $\operatorname{cf}(G)$. Заметим также, что $\operatorname{cf}^\circ(G)$ является $\mathbb{C}$-алгеброй, и ограничение отображения $\hat{}: \operatorname{cf}(G) \to \operatorname{cf}(G_{p'})$ на $\operatorname{cf}^\circ(G)$ будет изоморфизмом $\mathbb{C}$-алгебр.

✎ **(19.17)** Проверить, что $\operatorname{cf}^\circ(G)$ и $\operatorname{cf}(G_{p'})$ являются унитарными пространствами со скалярным произведением $(\cdot,\cdot)_{G_{p'}}$.

Основные свойства главных неразложимых характеров перечислены в следующем утверждении.

(19.18) Предложение. *Имеем*

(i) $\theta_\varphi \in \operatorname{cf}^\circ(G)$ *для любого* $\varphi \in \operatorname{IBr}(G)$. *В частности, значения главных неразложимых характеров определяются матрицей* Θ*;*

(ii) $(\varphi,\theta_\psi)_{G_{p'}} = \delta_{\varphi,\psi}$ *для любых* $\varphi,\psi \in \operatorname{IBr}(G)$*;*

(iii) *множество* $\{\theta_\varphi \mid \varphi \in \operatorname{IBr}(G)\}$ *является базисом пространства* $\operatorname{cf}^\circ(G)$*;*

(iv) *если* $\chi \in \operatorname{cf}^\circ(G)$ *— обыкновенный характер, то* χ *является целочисленной линейной комбинацией главных неразложимых характеров.*

(v) $\mathrm{C}^{-1} = \big((\varphi,\psi)_{G_{p'}}\big)_{\varphi,\psi\in\operatorname{IBr}(G)}$.

(vi) $(\theta_\varphi,\theta_\psi)_G = (\theta_\varphi,\theta_\psi)_{G_{p'}} = c_{\varphi\psi}$ *для любых* $\varphi,\psi \in \operatorname{IBr}(G)$.

(vii) $|G|_p$ *делит* $\theta_\varphi(1)$ *для любого* $\varphi \in \operatorname{IBr}(G)$.

Доказательство. (i) Пусть $x \in G$ и $y \in G_{p'}$. Обозначим $K = x^G$, $L = y^G$. Из второго соотношения ортогональности (16.22) вытекает
$$\sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(x)}\chi(y) = \delta_{K,L}|\mathrm{C}_G(x)|.$$
Поскольку y — p-регулярный элемент, имеем $\chi(y) = \sum_{\varphi\in\mathrm{IBr}(G)} d_{\chi\varphi}\varphi(y)$. Значит,
$$\sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(x)}\chi(y) = \sum_{\chi \in \mathrm{Irr}(G)} \sum_{\varphi\in\mathrm{IBr}(G)} d_{\chi\varphi}\overline{\chi(x)}\varphi(y) = \sum_{\varphi\in\mathrm{IBr}(G)} \overline{\theta_\varphi(x)}\varphi(y),$$
и, следовательно,

(19.19)
$$\sum_{\varphi\in\mathrm{IBr}(G)} \overline{\theta_\varphi(x)}\varphi(y) = \delta_{K,L}|\mathrm{C}_G(x)|.$$

Предположим теперь, что $x \notin G_{p'}$. Тогда $K \neq L$ и в силу произвольности y получаем
$$\sum_{\varphi\in\mathrm{IBr}(G)} \overline{\theta_\varphi(x)}\varphi = 0.$$
По (18.8)(i) неприводимые брауэровы характеры линейно независимы. Значит, $\theta_\varphi(x) = 0$ и $\theta_\varphi \in \mathrm{cf}^\circ(G)$.

(ii) Обозначим через Q целочисленную диагональную матрицу, индексированную p-регулярными классами и состоящую из элементов $\delta_{K,L}|\mathrm{C}_G(x_K)|$. В этих обозначениях равенство (19.19) для $x \in G_{p'}$ можно переписать в матричном виде
$$\overline{\Theta}^\top \Phi = Q.$$
Отсюда следует, что
$$\mathbf{1} = \overline{\Theta}^\top(\Phi Q^{-1}) = (\Phi Q^{-1})\overline{\Theta}^\top.$$
Выбрав произвольные $\varphi, \psi \in \mathrm{IBr}(G)$, получаем
$$\delta_{\varphi,\psi} = \sum_{K\in\mathscr{K}(G_{p'})} \varphi(x_K)\frac{1}{|\mathrm{C}_G(x_K)|}\overline{\theta_\psi(x_K)} = \sum_{g\in G_{p'}} \frac{\varphi(g)\overline{\theta_\psi(g)}}{|G|} = (\varphi, \theta_\psi)_{G_{p'}}.$$

(iii) Размерность $\dim \mathrm{cf}^\circ(G)$ очевидно равна $|\mathscr{K}(G_{p'})|$, что совпадает с числом главных неразложимых характеров по (18.8)(ii). Линейная независимость этих характеров следует из (ii) и, значит, они образуют базис пространства $\mathrm{cf}^\circ(G)$.

(iv) Из (iii) следует, что
$$\chi = \sum_{\varphi\in\mathrm{IBr}(G)} a_\varphi\theta_\varphi$$
для некоторых $a_\varphi \in \mathbb{C}$. Тогда
$$a_\varphi = (\varphi, \chi)_{G_{p'}} = (\check{\varphi}, \chi)_G \in \mathbb{Z},$$
где первое равенство следует из (ii), второе — из того, что $\chi \in \mathrm{cf}^\circ(G)$, а включение — из (19.11)(i).

(v) Пусть $\varphi, \psi \in \mathrm{IBr}(G)$. Мы уже отмечали, что

(19.20)
$$\widehat{\theta_\psi} = \sum_{\eta\in\mathrm{IBr}(G)} c_{\psi\eta}\eta.$$

Поскольку $c_{\psi\eta} = c_{\eta\psi}$, из (ii) следует, что
$$\delta_{\varphi,\psi} = (\varphi, \theta_\psi)_{G_{p'}} = (\varphi, \widehat{\theta_\psi})_{G_{p'}} = \sum_{\eta\in\mathrm{IBr}(G)} c_{\eta\psi}(\varphi, \eta)_{G_{p'}},$$
т. е. матрица $\big((\varphi,\psi)_{G_{p'}}\big)_{\varphi,\psi\in\mathrm{IBr}(G)}$ обратна к матрице Картана C.

(vi) В силу (i), (19.20) и (ii) получаем
$$(\theta_\varphi, \theta_\psi)_G = (\theta_\varphi, \theta_\psi)_{G_{p'}} = (\widehat{\theta_\varphi}, \theta_\psi)_{G_{p'}} = \sum_{\eta\in\mathrm{IBr}(G)} c_{\eta\varphi}(\eta, \theta_\psi)_{G_{p'}} = c_{\psi\varphi} = c_{\varphi\psi}$$

(vii) Пусть $\varphi \in \mathrm{IBr}(G)$ и $P \in \mathrm{Syl}_p(G)$.[20)]

[20)] Напомним, что через $\mathrm{Syl}_p(G)$ обозначается множество p-силовских подгрупп группы G.

Поскольку $(\theta_\varphi)_P$ и 1_P — обыкновенные характеры группы P, то число

$$\big((\theta_\varphi)_P, 1_P\big)_{_P} = \frac{1}{|P|}\,\theta_\varphi(1)$$

является целым, а равенство следует из того, что $\theta_\varphi(g) = 0$ для любого неединичного $g \in P$ в силу (i). Отсюда вытекает (vii). $\square$

Пусть $\eta \in \mathrm{cf}(G_{p'})$. Определим отображение $\widetilde{\eta} : G \to \mathbb{C}$ по правилу

$$\widetilde{\eta}(g) = \begin{cases} |G|_p\,\eta(g), & \text{если } \ g \in G_{p'};\\ 0, & \text{иначе}\end{cases}$$

для любого $g \in G$ (ср. определение (16.36)). Легко видеть, что $\widetilde{\eta} \in \mathrm{cf}^\circ(G)$ и отображение$\,\widetilde{}\,$: $\mathrm{cf}(G_{p'}) \to \mathrm{cf}^\circ(G)$ является $\mathbb{C}$-линейным и сюръективным.

(19.21) Предложение. *Если* $\varphi \in \mathrm{IBr}(G)$, *то* $\widetilde{\varphi} \in \mathbb{Z}[\mathrm{Irr}(G)]$.

Доказательство. В силу теоремы Брауэра (16.34) достаточно проверить, что если E — элементарная брауэрова подгруппа, то $\widetilde{\varphi}_{_E}$ — её обобщённый характер. Запишем $E = P \times Q$, где P — p-группа и Q — p'-группа. Тогда

$$\widetilde{\varphi}_{_E}(g) = \begin{cases} |G|_p\,\varphi_{_Q}(g), & \text{если } \ g \in Q;\\ 0, & \text{иначе}\end{cases}$$

для всех $g \in E$. Заметим, что $\varphi_{_Q}$ — обыкновенный характер группы Q ввиду (19.9). Пусть $\rho_{_P}$ — регулярный характер группы P и положим $\tau = \rho_{_P} \times \varphi_{_Q}$. Из (16.24)$(i)$ следует, что τ — обыкновенный характер группы E, и ввиду (16.12) получаем, что

$$\tau(g) = \begin{cases} |P|\,\varphi_{_Q}(g), & \text{если } \ g \in Q;\\ 0, & \text{иначе}\end{cases}$$

для всех $g \in E$. Поэтому $\widetilde{\varphi}_{_E} = \dfrac{|G|_p}{|P|}\,\tau$ — обыкновенный характер группы E. $\square$

Используя классовые функции вида $\widetilde{\varphi}$, можно получить дополнительную информацию о матрице Картана.

(19.22) Предложение. *Пусть* C *— матрица Картана группы* G. *Тогда*

(19.23)
$$\det(\mathrm{C}) = \prod_{K \in \mathscr{K}(G_{p'})} |\mathrm{C}_G(x_{_K})|_p.$$

В частности, определитель матрицы Картана является степенью числа p.

Доказательство. Сначала докажем, что $\det(\mathrm{C})$ — степень числа p.

Из определения отображения$\,\widetilde{}\,$: $\mathrm{cf}(G_{p'}) \to \mathrm{cf}^\circ(G)$ следует, что для любых $\varphi, \psi \in \mathrm{IBr}(G)$ имеет место соотношение

$$(\widetilde{\varphi}, \widetilde{\psi})_{_G} = |G|_p^2(\varphi, \psi)_{_{G_{p'}}}.$$

Пусть $A = \big((\widetilde{\varphi}, \widetilde{\psi})_{_G}\big)_{\varphi,\psi\in \mathrm{IBr}(G)}$. Тогда, учитывая (19.18)(v), предыдущее соотношение можно переписать в матричном виде

$$A = |G|_p^2\,\mathrm{C}^{-1}.$$

Значит, $A\mathrm{C} = |G|_p^2\mathbf{1}$. Но в силу (19.21) матрица A целочисленная, и поэтому $\det(\mathrm{C})$ — степень числа p.

Теперь докажем равенство (19.23). Как мы видели, имеет место матричное равенство

$$\Theta = \mathrm{C}\Phi.$$

Кроме того, в доказательстве (19.18)(ii) было установлено, что

$$\overline{\Theta}^\top \Phi = Q,$$

где Q — диагональная матрица с элементами $\delta_{_{K,L}}|\mathrm{C}_G(x_{_K})|$, индексированными p-регулярными классами. Отсюда вытекает, что

$$\overline{\Phi}^\top \mathrm{C}\Phi = Q,$$

поскольку матрица C целочисленная и симметрическая. Заметим, что ввиду предложения (17.16) матрица $\overline{\Phi}$ отличается от Φ возможно лишь перестановкой строк, и поэтому $\det(\overline{\Phi}^{\top}) = \det(\overline{\Phi}) = \pm\det(\Phi)$. Значит,

$$\det(\Phi)^2 = \pm\frac{\prod_{K\in\mathscr{K}(G_{p'})}|\mathrm{C}_G(x_{_K})|}{\det(\mathrm{C})}. \tag{19.24}$$

Поскольку значения брауэровых характеров лежат в $\boldsymbol{R}$, из предыдущего равенства следует, что

$$\det(\Phi)^2 \in \boldsymbol{R}\cap\mathbb{Q} = \mathbb{Z}.$$

Предположим, что p делит $\det(\Phi)^2$. Тогда

$$0 = (\det(\Phi)^2)^\star = (\det(\Phi)^\star)^2 = (\det(\Phi^\star))^2$$

и, значит, матрица $\Phi^\star$ вырожденная, вопреки (19.1). Итак, $\det(\Phi)^2$ не делится на p, и поскольку $\det(\mathrm{C})$ — степень p, требуемое следует из равенства (19.24). $\square$

20. Блоки характеров

В этом разделе мы определим понятие p-блока — одного из ключевых объектов в теории модулярных представлений, введённых Р. Брауэром.

По аналогии с центральными гомоморфизмами ω_χ, определёнными ранее для любых $\chi\in\mathrm{Irr}(G)$, введём также отображения $\lambda_\varphi : Z(FG)\to F$ для любого $\varphi\in\mathrm{IBr}(G)$. Пусть $\mathscr{X}$ — F-представление с брауэровым характером φ. В силу неприводимости $\mathscr{X}$ из (9.5) следует, что для любого $z\in\mathrm{Z}(FG)$ матрица $\mathscr{X}(z)$ равна $a\mathbf{1}$ для некоторого $a\in F$. Мы положим $\lambda_\varphi(z)=a$.

В (16.28) мы показали, что для любых $\chi\in\mathrm{Irr}(G)$ и $K\in\mathscr{K}(G)$ значение центрального гомоморфизма $\omega_\chi:\mathrm{Z}(\mathbb{C}G)\to\mathbb{C}$ на $\widehat{K}$ является целым алгебраическим числом. Как мы отмечали в (3.10) отображение $^\star:\boldsymbol{R}\to F$ можно естественно поднять до эпиморфизма колец $\mathrm{Z}(\boldsymbol{R}G)\to\mathrm{Z}(FG)$ и что значения центрального гомоморфизма ω_χ на элементах из $\mathrm{Z}(\boldsymbol{R}G)$ лежат в $\boldsymbol{R}$. Ясно также, что ограничение ω_χ на $\mathrm{Z}(\boldsymbol{R}G)$ является гомоморфизмом $\boldsymbol{R}$-алгебр. Из (2.14)(i) вытекает[21] существование и единственность гомоморфизма колец $\lambda_\chi:\mathrm{Z}(FG)\to F$, для которого коммутативна следующая диаграмма.

$$\begin{tikzcd}
\mathrm{Z}(\boldsymbol{R}G) \arrow[r, "\omega_\chi"] \arrow[d, "\star"'] \arrow[dr, "\omega_\chi^\star"] & \boldsymbol{R} \arrow[d, "\star"] \\
\mathrm{Z}(FG) \arrow[r, dotted, "\lambda_\chi"'] & F
\end{tikzcd}$$

Здесь $\omega_\chi^\star$ обозначает композицию отображений $\omega_\chi:\mathrm{Z}(\boldsymbol{R}G)\to\boldsymbol{R}$ и $^\star:\boldsymbol{R}\to F$.

(20.1) Предложение. *Для любого $\eta\in\mathrm{Irr}(G)\cup\mathrm{IBr}(G)$ отображение $\lambda_\eta:\mathrm{Z}(FG)\to F$ является гомоморфизмом F-алгебр.*

Доказать предложение (20.1).

Из предложения (20.1), в частности, вытекает, что для любого $\chi\in\mathrm{Irr}(G)$ отображение λ_χ однозначно задаётся своими значениями

$$\lambda_\chi(\widehat{K}) = \omega_\chi(\widehat{K})^\star \tag{20.2}$$

на базисных элементах $\widehat{K}$ алгебры $\mathrm{Z}(FG)$. Отметим, что $\widehat{K}$ в левой части равенства (20.2) является элементом из FG, а в правой — из $\mathbb{C}G$. В дальнейшем мы будем преимущественно пользоваться равенством (20.2) для вычисления значений центрального гомоморфизма λ_χ.

(20.3) Напомним, что ранее мы продолжили отображение $^\star:\boldsymbol{R}\to F$ на локальное кольцо $\widetilde{\boldsymbol{R}}$. В дальнейшим нам понадобится рассмотреть ограничение ω_χ не только на $\mathrm{Z}(\boldsymbol{R}G)$, но также и на $\mathrm{Z}(\widetilde{\boldsymbol{R}}G)$. Соображения, аналогичные приведённым выше, показывают, что $\omega_\chi(\mathrm{Z}(\widetilde{\boldsymbol{R}}G))\subseteq\widetilde{\boldsymbol{R}}$, и позволяют поднять отображение * до эпиморфизма колец $\mathrm{Z}(\widetilde{\boldsymbol{R}}G)\to\mathrm{Z}(FG)$.

[21] Предложение (2.14)(i) применимо, поскольку ядро гомоморфизма * на $\mathrm{Z}(\boldsymbol{R}G)$ содержится в $\mathrm{Ker}\,\omega_\chi^\star$. В самом деле, ядро * на $\mathrm{Z}(\boldsymbol{R}G)$ состоит из всевозможных линейных комбинаций $\sum_{K\in\mathscr{K}(G)}\alpha_{_K}\widehat{K}$, где $\alpha_{_K}\in M$. Однако образ такой линейной комбинации под действием ω_χ равен $\sum_{K\in\mathscr{K}(G)}\alpha_{_K}\omega_\chi(\widehat{K})\in M$ и, значит, обращается в 0 под действием *.

(20.4) Предложение. *Во введённых обозначениях для любого $\chi \in \operatorname{Irr}(G)$ коммутативна следующая диаграмма*

$$\begin{tikzcd} \mathrm{Z}(\widetilde{\boldsymbol{R}}G) \arrow[r, "\omega_\chi"] \arrow[d, "\star"] & \widetilde{\boldsymbol{R}} \arrow[d, "\star"] \\ \mathrm{Z}(FG) \arrow[r, "\lambda_\chi"] & F \end{tikzcd}$$

✎ Доказать предложение (20.4).

В отличие от центральных гомоморфизмов ω_χ, введённые гомоморфизмы λ_χ при $\chi \in \operatorname{Irr}(G)$, равно как и λ_φ при $\varphi \in \operatorname{IBr}(G)$, вообще говоря, не являются попарно различными. Для характеров $\mu, \nu \in \operatorname{Irr}(G) \cup \operatorname{IBr}(G)$ будем писать $\mu \sim \nu$ тогда и только тогда, когда $\lambda_\mu = \lambda_\nu$. Очевидно, что $\sim$ является отношением эквивалентности.

✎ **(20.5)** Показать, что $1_G \sim 1_{G_{p'}}$.

(20.6) Определение. Классы эквивалентности множества $\operatorname{Irr}(G) \cup \operatorname{IBr}(G)$ относительно отношения $\sim$ называются *p-блоками* группы G. Множество p-блоков обозначается через $\operatorname{Bl}_p(G)$ или просто $\operatorname{Bl}(G)$.

Пусть $B \in \operatorname{Bl}(G)$. Из определения следует, что p-блок B имеет «обыкновенную часть» и «брауэрову часть». Положим $\operatorname{Irr}(B) = B \cap \operatorname{Irr}(G)$ — *p-блок обыкновенных характеров* и $\operatorname{IBr}(B) = B \cap \operatorname{IBr}(G)$ — *p-блок брауэровых характеров*. Далее в (20.9) мы увидим, что для любого p-блока B множества $\operatorname{Irr}(B)$ и $\operatorname{IBr}(B)$ непусты.

Обозначим через $\lambda_{_B}$ однозначно определённый гомоморфизм F-алгебр $\mathrm{Z}(FG) \to F$, равный λ_η для произвольного $\eta \in B$ и будем называть его *центральным гомоморфизмом, соответствующим блоку B*.

Главным p-блоком группы G называется (единственный) p-блок, содержащий характеры 1_G и $1_{G_{p'}}$.

Разбиение множества $\operatorname{Irr}(G)$ на p-блоки обыкновенных характеров можно осуществить, исходя из таблицы обыкновенных характеров группы G. Из предложений (20.1) и (16.26) следует, что два характера $\chi, \tau \in \operatorname{Irr}(G)$ лежат в одном p-блоке тогда и только тогда, когда выполнены равенства

$$\left(\frac{|K|\chi(x_{_K})}{\chi(1)}\right)^\star = \left(\frac{|K|\tau(x_{_K})}{\tau(1)}\right)^\star$$

для всех $K \in \mathscr{K}(G)$. Строго говоря, эти равенства определяют эквивалентность $\chi \sim \tau$ при фиксированном выборе идеала M, содержащего число p. Следующее утверждение показывает, однако, что эта эквивалентность на множестве $\operatorname{Irr}(G)$ не зависит от M.

(20.7) Предложение. *Пусть $\chi, \tau \in \operatorname{Irr}(G)$. Для того чтобы χ и τ лежали в одном p-блоке необходимо и достаточно, чтобы для любого $K \in \mathscr{K}(G)$ величина $\omega_\chi(\widehat{K}) - \omega_\tau(\widehat{K})$ лежала в каждом максимальном идеале кольца $\boldsymbol{R}$, содержащем $p\boldsymbol{R}$. В частности, разбиение множества $\operatorname{Irr}(G)$ на p-блоки обыкновенных характеров не зависит от M.*

Доказательство. Достаточность очевидна. Покажем необходимость. Допустим, что $\chi \sim \tau$ и $K \in \mathscr{K}(G)$. Обозначим $\alpha = \omega_\chi(\widehat{K}) - \omega_\tau(\widehat{K})$. Если мы покажем, что для некоторого натурального числа n имеет место включение $\alpha^n \in p\boldsymbol{R}$, то отсюда будет следовать требуемое. В самом деле, если α не содержится в некотором максимальном идеале I из $\boldsymbol{R}$, то и никакая степень элемента α не лежит в I ввиду того, что поле $\boldsymbol{R}/I$ не имеет ненулевых нильпотентных элементов.

Пусть $m = \exp G$ и $\sigma \in \operatorname{Gal}(\mathbb{Q}_m, \mathbb{Q})$. В силу (16.9)$(ii)$ существует целое число k, взаимно простое с m, такое, что $\eta(g)^\sigma = \eta(g^k)$ для любого обыкновенного характера η и любого $g \in G$. Заметим, что для такого k имеет место равенство $|g^G| = |(g^k)^G|$, где $g \in G$ — произвольный элемент, поскольку g и g^k порождают одну и ту же циклическую подгруппу и, значит, имеют одинаковые централизаторы в G. Учитывая это, получаем

$$\alpha^\sigma = \left(\frac{|K|\chi(x_{_K})}{\chi(1)} - \frac{|K|\tau(x_{_K})}{\tau(1)}\right)^\sigma = \frac{|L|\chi(x_{_K}^k)}{\chi(1)} - \frac{|L|\tau(x_{_K}^k)}{\tau(1)} = \omega_\chi(\widehat{L}) - \omega_\tau(\widehat{L}) \in M,$$

где L — класс сопряжённости, содержащий элемент $x_{_K}^k$, а последнее включение вытекает из соотношения $\chi \sim \tau$.

Рассмотрим многочлен

$$f(x) = \prod_{\sigma \in \operatorname{Gal}(\mathbb{Q}_m, \mathbb{Q})} (x - \alpha^\sigma) \in \boldsymbol{R}[x].$$

Его коэффициенты инвариантны относительно всех элементов группы $\mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q})$ и, следовательно, лежат в $\mathbb{Q}$. Поскольку $\boldsymbol{R} \cap \mathbb{Q} = \mathbb{Z}$, имеем $f(x) \in \mathbb{Z}[x]$. С другой стороны мы показали, что $\alpha^\sigma \in M$ для всех $\sigma \in \mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q})$. Поэтому все коэффициенты многочлена $f(x)$, кроме старшего, лежат в $\mathbb{Z} \cap M = p\mathbb{Z}$. Подставив α в f, получим $0 = f(\alpha) \equiv \alpha^n \mod p\boldsymbol{R}$, где $n = |\,\mathrm{Gal}(\mathbb{Q}_m, \mathbb{Q})|$, что и требовалось доказать. ☐

Поле того, как множество $\mathrm{Irr}(G)$ разбито на p-блоки обыкновенных характеров, мы можем также разбить множество $\mathrm{IBr}(G)$ на p-блоки брауэровых характеров, если известна матрица разложения.

(20.8) Предложение. *Имеем*

(*i*) *пусть* $\chi \in \mathrm{Irr}(G)$ *и* $\varphi \in \mathrm{IBr}(G)$. *Если* $d_{\chi\varphi} \neq 0$, *то* $\lambda_\chi = \lambda_\varphi$;

(*ii*) $\mathrm{IBr}(B) = \{\varphi \in \mathrm{IBr}(G) \,|\, d_{\chi\varphi} \neq 0$ *для некоторого* $\chi \in \mathrm{Irr}(B)\}$.

Доказательство. Пусть $\chi \in \mathrm{Irr}(G)$ и $\mathscr{X}$ — обыкновенное представление с характером χ. В силу (18.5) можно считать, что $\mathscr{X}$ записано над $\widetilde{\boldsymbol{R}}$. Тогда $\hat{\chi}$ является брауэровым характером F-представления $\mathscr{X}^\star$ ввиду (18.6)(*ii*).

Пусть $K \in \mathscr{K}(G)$. По определению центрального гомоморфизма ω_χ имеем $\mathscr{X}(\widehat{K}) = \omega_\chi(\widehat{K})\mathbf{1}$. Отсюда

$$\mathscr{X}^\star(\widehat{K}) = \omega_\chi(\widehat{K})^\star \mathbf{1} = \lambda_\chi(\widehat{K})\mathbf{1}.$$

Обозначим через $\mathscr{Y}$ блочно-верхнетреугольное F-представление с неприводимыми компонентами на главной диагонали, эквивалентное представлению $\mathscr{X}^\star$. Поскольку матрица $\mathscr{X}^\star(\widehat{K})$ скалярная, получаем

$$\mathscr{Y}(\widehat{K}) = \mathscr{X}^\star(\widehat{K}) = \lambda_\chi(\widehat{K})\mathbf{1}.$$

Так как любая неприводимая компонента $\mathscr{Z}$ представления $\mathscr{X}^\star$ эквивалентна некоторой неприводимой компоненте представления $\mathscr{Y}$, значение которой на $\widehat{K}$ — скалярная матрица, отсюда вытекает, что $\mathscr{Z}(\widehat{K}) = \lambda_\chi(\widehat{K})\mathbf{1}$. В частности, если $d_{\chi\varphi} \neq 0$ для некоторого $\varphi \in \mathrm{IBr}(G)$, то φ является брауэровым характером некоторой неприводимой компоненты представления $\mathscr{X}^\star$, и поэтому $\lambda_\varphi(\widehat{K}) = \lambda_\chi(\widehat{K})$. Отсюда, в силу произвольности K и того, что гомоморфизмы λ_φ и λ_χ определяются своими значениями на классовых суммах, получаем равенство $\lambda_\varphi = \lambda_\chi$, а также включение

$$\{\, \varphi \in \mathrm{IBr}(G) \,|\, d_{\chi\varphi} \neq 0 \text{ для некоторого } \chi \in \mathrm{Irr}(B) \,\} \subseteq \mathrm{IBr}(B).$$

Обратно, если $\varphi \in \mathrm{IBr}(B)$, то ввиду (19.5)(*i*) существует характер $\chi \in \mathrm{Irr}(G)$, для которого $d_{\chi\varphi} \neq 0$, и из только что доказанного вытекает, что p-блок, которому принадлежит χ должен совпадать с B. ☐

(20.9) Следствие. *Для любого* $B \in \mathrm{Bl}(G)$ *имеем* $\mathrm{Irr}(B) \neq \varnothing$ *и* $\mathrm{IBr}(B) \neq \varnothing$.

Доказательство. Пусть $B \in \mathrm{Bl}(G)$. Тогда либо $\chi \in B$ для некоторого $\chi \in \mathrm{Irr}(G)$, либо $\varphi \in B$ для некоторого $\varphi \in \mathrm{IBr}(G)$. В силу (19.5) существуют, соответственно, $\varphi \in \mathrm{IBr}(G)$ и $\chi \in \mathrm{Irr}(G)$, такие, что $d_{\chi\varphi} \neq 0$, и тогда, соответственно, $\varphi \in \mathrm{IBr}(B)$ и $\chi \in \mathrm{Irr}(B)$. ☐

✎ **(20.10)** Найти 2- и 3-блоки группы S_3.

В приложении В приведены таблицы обыкновенных характеров и матрицы разложения для некоторых конечных групп по всем простым делителям p их порядка. Исходя из этих данных, можно определить p-блоки таких групп, используя предложения (20.7) и (20.8).

(20.11) Определение. *Графом Брауэра* группы G называется граф с множеством вершин $\mathrm{Irr}(G)$, в котором два характера $\chi, \tau \in \mathrm{Irr}(G)$ соединены ребром тогда и только тогда, когда существует характер $\varphi \in \mathrm{IBr}(G)$ такой, что $d_{\chi\varphi} \neq 0$ и $d_{\tau\varphi} \neq 0$.

Из предложения (20.8) вытекает, что если характеры $\chi, \tau \in \mathrm{Irr}(G)$ соединены ребром в графе Брауэра, то они лежат в одном p-блоке. Отсюда получаем

(20.12) Следствие. *Для любого* $B \in \mathrm{Bl}(G)$ *множество* $\mathrm{Irr}(B)$ *является объединением компонент связности*[22] *графа Брауэра.*

Существуют примеры, показывающие, что смежность вершин в графе Брауэра зависит от выбора максимального идеала M, содержащего число p. Однако компоненты связности графа Брауэра, как мы увидим в (20.18)(*i*), в точности совпадают множествами $\mathrm{Irr}(B)$ и поэтому не зависят от идеала M ввиду (20.7). Чтобы показать это, сформулируем несколько вспомогательных утверждений.

[22]Здесь и далее под компонентой связности графа Брауэра мы подразумеваем множество вершин некоторой компоненты связности этого графа.

(20.13) Предложение. *Пусть* $\mathscr{A} \subseteq \mathrm{Irr}(G)$ *— объединение компонент связности графа Брауэра. Положим*

$$\mathscr{B} = \{\varphi \in \mathrm{IBr}(G) \mid d_{\chi\varphi} \neq 0 \text{ для некоторого } \chi \in \mathscr{A}\}.$$

Тогда для любых $x \in G_{p'}$ *и* $y \in G$ *выполнено равенство*

$$\sum_{\chi \in \mathscr{A}} \chi(x)\overline{\chi(y)} = \sum_{\varphi \in \mathscr{B}} \varphi(x)\overline{\theta_\varphi(y)}.$$

Доказательство. Для любого $\chi \in \mathscr{A}$ по условию имеем

$$\chi(x) = \sum_{\varphi \in \mathrm{IBr}(G)} d_{\chi\varphi}\varphi(x) = \sum_{\varphi \in \mathscr{B}} d_{\chi\varphi}\varphi(x).$$

Также для любого $\varphi \in \mathscr{B}$

$$\theta_\varphi(y) = \sum_{\chi \in \mathrm{Irr}(G)} d_{\chi\varphi}\chi(y) = \sum_{\chi \in \mathscr{A}} d_{\chi\varphi}\chi(y).$$

Поэтому

$$\sum_{\chi \in \mathscr{A}} \chi(x)\overline{\chi(y)} = \sum_{\substack{\chi \in \mathscr{A} \\ \varphi \in \mathscr{B}}} d_{\chi\varphi}\varphi(x)\overline{\chi(y)} = \sum_{\varphi \in \mathscr{B}} \varphi(x)\overline{\theta_\varphi(y)},$$

что и требовалось доказать. □

Одним из следствий предложения (20.13) является частичное обобщение второго соотношения ортогональности для обыкновенных характеров.

(20.14) Следствие (Слабая ортогональность в блоке). *Пусть* $x \in G_{p'}$, $y \in G \setminus G_{p'}$. *Тогда*

$$\sum_{\chi \in \mathrm{Irr}(B)} \chi(x)\overline{\chi(y)} = 0$$

для любого $B \in \mathrm{Bl}(G)$.

Доказательство. Поскольку $\mathrm{Irr}(B)$ — компонента связности графа Брауэра, требуемое следует из (20.13), ввиду того, что $\theta_\varphi(y) = 0$ для всех φ по (19.18)(*i*). □

Напомним, что через e_χ обозначается центральный идемпотент алгебры $\mathbb{C}G$, соответствующий неприводимому обыкновенному характеру χ, определённый в (16.14). Пусть $\mathscr{A}$ — произвольное подмножество из $\mathrm{Irr}(G)$. Определим центральный идемпотент алгебры $\mathbb{C}G$

$$f_{\mathscr{A}} = \sum_{\chi \in \mathscr{A}} e_\chi.$$

Поскольку классовые суммы образуют базис центра $\mathrm{Z}(\mathbb{C}G)$, для всякого $\mathscr{A} \subseteq \mathrm{Irr}(G)$ однозначно определены константы $\alpha_{\mathscr{A}}(K) \in \mathbb{C}$, где $K \in \mathscr{K}(G)$, такие, что

$$f_{\mathscr{A}} = \sum_{K \in \mathscr{K}(G)} \alpha_{\mathscr{A}}(K)\widehat{K}.$$

(20.15) Предложение. *Пусть* $\mathscr{A}$ *— объединение компонент связности графа Брауэра. Тогда для всех* $K \in \mathscr{K}(G)$ *имеем*

(*i*) $\alpha_{\mathscr{A}}(K) = \dfrac{1}{|G|} \sum_{\chi \in \mathscr{A}} \chi(1)\overline{\chi(x_K)}$;

(*ii*) $\alpha_{\mathscr{A}}(K) = 0$, *если* $K \notin \mathscr{K}(G_{p'})$;

(*iii*) $\alpha_{\mathscr{A}}(K) \in \widetilde{\boldsymbol{R}}$.

Доказательство. (*i*) Это равенство является прямым следствием предложения (16.15).

(*ii*) Из (*i*) и предложения (20.13) вытекает

$$\alpha_{\mathscr{A}}(K) = \frac{1}{|G|} \sum_{\chi \in \mathscr{A}} \chi(1)\overline{\chi(x_K)} = \frac{1}{|G|} \sum_{\varphi \in \mathscr{B}} \varphi(1)\overline{\theta_\varphi(x_K)},$$

где $\mathscr{B} = \{\varphi \in \mathrm{IBr}(G) \mid d_{\chi\varphi} \neq 0$ для некоторого $\chi \in \mathscr{A}\}$. Если $K \notin \mathscr{K}(G_{p'})$, то в силу (19.18)$(i)$ имеем $\theta_\varphi(x_{K}) = 0$ для всех $\varphi \in \mathscr{B}$.

(iii) Ввиду (ii) можем считать, что $K \in \mathscr{K}(G_{p'})$. Тогда из (i) и предложения (20.13) следует, что

$$\alpha_{\mathscr{A}}(K) = \frac{1}{|G|}\sum_{\chi\in\mathscr{A}} \chi(1)\overline{\chi(x_{K})} = \frac{1}{|G|}\sum_{\varphi\in\mathscr{B}} \overline{\varphi(x_{K})}\theta_\varphi(1).$$

Заметим, что по (19.18)(vii) для всех $\varphi \in \mathscr{B}$ имеет место делимость $|G|_p \mid \theta_\varphi(1)$ и значения $\overline{\varphi(x_{K})}$ лежат в $\boldsymbol{R}$. Поэтому $\alpha_{\mathscr{A}}(K)$ является частным от деления числа из $\boldsymbol{R}$ на $|G|_{p'} \in \mathbb{Z}\setminus M$ (см. предложение (17.2)). Отсюда следует требуемое. ☐

(20.16) Предложение. *Если $\mathscr{A} \subseteq \mathrm{Irr}(G)$ и $f_{\mathscr{A}} \in \widetilde{\boldsymbol{R}}G$, то $\mathscr{A}$ является объединением некоторых p-блоков обыкновенных характеров.*

Доказательство. Мы отмечали в (20.3), что отображение * можно поднять до гомоморфизма колец * : $\mathrm{Z}(\widetilde{\boldsymbol{R}}G) \to \mathrm{Z}(FG)$. Заметим, что в силу (3.8) имеет место включение $f_{\mathscr{A}} \in \mathrm{Z}(\mathbb{C}G) \cap \widetilde{\boldsymbol{R}}G = \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$. Рассмотрим значения на $f_{\mathscr{A}}^\star$ центральных гомоморфизмов λ_χ, $\chi \in \mathrm{Irr}(G)$. Из (20.4) следует, что

$$\lambda_\chi(f_{\mathscr{A}}^\star) = \omega_\chi(f_{\mathscr{A}})^\star = \sum_{\tau\in\mathscr{A}} \omega_\chi(e_\tau)^\star = \begin{cases} 1, & \chi \in \mathscr{A}, \\ 0, & \chi \notin \mathscr{A}, \end{cases} \tag{20.17}$$

где последнее равенство вытекает из (16.25)(i).

Предположим, что $\mathscr{A}$ не является объединением p-блоков обыкновенных характеров. Тогда существуют p-блок $B \in \mathrm{Bl}(G)$ и характеры $\chi, \tau \in \mathrm{Irr}(B)$ такие, что $\chi \in \mathscr{A}$ и $\tau \notin \mathscr{A}$. Из (20.17) следует, что $\lambda_\chi(f_{\mathscr{A}}^\star) = 1$ и $\lambda_\tau(f_{\mathscr{A}}^\star) = 0$. Но $\lambda_\chi = \lambda_\tau$, поскольку χ и τ лежат в одном p-блоке. Противоречие. Отсюда следует требуемое утверждение. ☐

Теперь для p-блоков обыкновенных характеров кроме определения мы получаем ещё две характеризации.

(20.18) Следствие. *Имеем*

(i) *множество $\{\mathrm{Irr}(B) \mid B \in \mathrm{Bl}(G)\}$ совпадает с множеством компонент связности графа Брауэра;*

(ii) *p-блоки обыкновенных характеров — это, в точности, минимальные непустые подмножества $\mathscr{A} \subseteq \mathrm{Irr}(G)$, для которых $f_{\mathscr{A}} \in \widetilde{\boldsymbol{R}}G$.*

Доказательство. (i) В силу (20.12) достаточно показать, что любая компонента связности $\mathscr{A}$ графа Брауэра является объединением p-блоков обыкновенных характеров. Из (20.15)(iii) следует, что $f_{\mathscr{A}} \in \widetilde{\boldsymbol{R}}G$. Поэтому требуемое вытекает из (20.16).

(ii) Это вытекает из (i), (20.15)(iii) и (20.16). ☐

(20.19) Предложение. *Пусть $B \in \mathrm{Bl}(G)$. Тогда*

(i) *для любого $x \in G_{p'}$*

$$\sum_{\chi\in\mathrm{Irr}(B)} \overline{\chi(x)}\,\chi = \sum_{\varphi\in\mathrm{IBr}(B)} \overline{\varphi(x)}\,\theta_\varphi;$$

(ii) *для любого $x \in G$*

$$\sum_{\chi\in\mathrm{Irr}(B)} \overline{\chi(x)}\,\hat{\chi} = \sum_{\varphi\in\mathrm{IBr}(B)} \overline{\theta_\varphi(x)}\,\varphi;$$

(iii) *для любого $x \in G_{p'}$*

$$\sum_{\varphi\in\mathrm{IBr}(B)} \overline{\varphi(x)}\,\widehat{\theta_\varphi} = \sum_{\varphi\in\mathrm{IBr}(B)} \overline{\theta_\varphi(x)}\,\varphi.$$

Доказательство. В силу (20.18)(i) получаем, что $\mathrm{Irr}(B)$ — компонента связности графа Брауэра и

$$\{\varphi \in \mathrm{IBr}(G) \mid d_{\chi\varphi} \neq 0 \text{ для некоторого } \chi \in B\} = \mathrm{IBr}(B)$$

в силу (20.8)(ii). Поэтому, положив $\mathscr{A} = B$ в (20.13), получаем (i) и (ii). Рассмотрев образ относительно отображения $\hat{}\colon \mathrm{cf}(G) \to \mathrm{cf}(G_{p'})$ в (i) и взяв $x \in G_{p'}$ в (ii), получим (iii). ☐

✓ Отметим, что равенство (20.19)(ii) обобщает слабую ортогональность в блоке (20.14), поскольку в случае $x \in G \setminus G_{p'}$ имеем $\theta_\varphi(x) = 0$ в силу (19.18)(i).

Для $B \in \mathrm{Bl}(G)$ положим $f_{B} = f_{\mathrm{Irr}(B)}$. Иногда в литературе элементы f_{B} называют *идемпотентами Осимы* алгебры $\mathbb{C}G$. Из (20.18)(ii) следует, что

$$f_{B} \in \mathrm{Z}(\widetilde{\boldsymbol{R}}G) \tag{20.20}$$

для любого $B \in \mathrm{Bl}(G)$.

Опишем строение групповой алгебры $\widetilde{\boldsymbol{R}}G$.

(20.21) Предложение. *Имеем*

(i) *справедливо разложение*

$$\widetilde{\boldsymbol{R}}G = \bigoplus_{B\in \mathrm{Bl}(G)} f_{{}_B}\widetilde{\boldsymbol{R}}G;$$

(ii) $\mathrm{Z}(f_{{}_B}\widetilde{\boldsymbol{R}}G) = f_{{}_B}\mathrm{Z}(\widetilde{\boldsymbol{R}}G)$.

✎ Доказать предложение (20.21).

Пусть $\mathrm{Bl}(G) = \{B_1, \ldots, B_k\}$. Упорядочив множества $\mathrm{Irr}(G)$ и $\mathrm{IBr}(G)$ таким образом, чтобы вначале шли характеры из B_1, затем из B_2, и т. д., в соответствии с предложением (20.8) мы можем записать матрицу D в виде

(20.22)
$$\mathrm{D} = \begin{pmatrix} \mathrm{D}_{B_1} & 0 & \ldots & 0 \\ 0 & \mathrm{D}_{B_2} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \mathrm{D}_{B_k} \end{pmatrix},$$

где D_{B_i} обозначает подматрицу, стоящую на пересечении строк и столбцов, соответствующих характерам из блока B_i. Будем называть D_{B_i} *матрицей разложения p-блока B_i*, а её элементы — *числами разложения p-блока B_i*.

(20.23) Предложение. *Для любого $B \in \mathrm{Bl}(G)$*

(i) *ранг матрицы D_B равен $|\,\mathrm{IBr}(B)|$;*

(ii) $|\,\mathrm{Irr}(B)| \geqslant |\,\mathrm{IBr}(B)|$.

✎ Доказать предложение (20.23).

Пусть D записана в виде (20.22). Тогда матрица Картана примет блочно диагональный вид

$$\mathrm{C} = \mathrm{D}^{\top}\mathrm{D} = \begin{pmatrix} \mathrm{C}_{B_1} & 0 & \ldots & 0 \\ 0 & \mathrm{C}_{B_2} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \mathrm{C}_{B_k} \end{pmatrix},$$

где $\mathrm{C}_{B_i} = (\mathrm{D}_{B_i})^{\top}\mathrm{D}_{B_i}$ — *матрица Картана p-блока B_i*. Покажем, что для любого p-блока его матрица разложения и матрица Картана не представимы в блочно-диагональном виде.

(20.24) Предложение. *Для любого $B \in \mathrm{Bl}(G)$ матрица разложения D_B и матрица Картана C_B не могут быть представлены в блочном виде*

$$\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$$

путём перестановки характеров из $\mathrm{Irr}(B)$ и $\mathrm{IBr}(B)$, которыми индексируются строки и столбцы матриц D_B и C_B.

Доказательство. Пусть для некоторого $B \in \mathrm{Bl}(G)$ матрица D_B имеет указанный вид и $\mathrm{Irr}(B) = \mathscr{A}_1 \cup \mathscr{A}_2$ — соответствующее разбиение характеров, индексирующих строки D_B. Тогда для любой пары характеров $\chi_1 \in \mathscr{A}_1$ и $\chi_2 \in \mathscr{A}_2$ не существует брауэрова характера $\varphi \in \mathrm{IBr}(G)$ такого, что $d_{\chi_1\varphi} \neq 0$ и $d_{\chi_2\varphi} \neq 0$. Значит, $\mathscr{A}_1$ и $\mathscr{A}_2$ лежат в разных компонентах связности графа Брауэра вопреки (20.18)(i).

Теперь предположим, что для некоторого $B \in \mathrm{Bl}(G)$ матрица Картана C_B имеет указанный вид и $\mathrm{IBr}(B) = \mathscr{B}_1 \cup \mathscr{B}_2$ — соответствующее разбиение брауэровых характеров. Тогда для любых $\varphi_1 \in \mathscr{B}_1$ и $\varphi_2 \in \mathscr{B}_2$ выполнено $0 = c_{\varphi_1\varphi_2} = \sum_{\chi\in \mathrm{Irr}(B)} d_{\chi\varphi_1}d_{\chi\varphi_2}$, т. е. φ_1-й и φ_2-й столбцы матрицы D_B ортогональны. Рассмотрим столбцы матрицы D_B, индексированные характерами из $\mathscr{B}_1$. Эти столбцы образуют матрицу, ненулевые строки которой индексированы некоторым подмножеством $\mathscr{A}_1 \subseteq \mathrm{Irr}(B)$, а нулевые — подмножеством $\mathscr{A}_2 \subseteq \mathrm{Irr}(B)$. Заметим, что $\mathscr{A}_1 \neq \varnothing$, т. к. иначе D_B имеет нулевой столбец, вопреки (19.5)(i). Можно считать, что матрица D_B имеет блочный вид

$$\begin{array}{cc} & \begin{array}{cc} \mathscr{B}_1 & \mathscr{B}_2 \end{array} \\ \begin{array}{c} \mathscr{A}_1 \\ \mathscr{A}_2 \end{array} & \left(\begin{array}{c|c} D_{11} & D_{12} \\ \hline \mathbf{0} & D_{22} \end{array}\right) \end{array}$$

Покажем, что D_{12} — нулевая подматрица. В самом деле, если в какой-то её χ-й строке есть ненулевой элемент $d_{\chi\varphi_2}$, то поскольку χ-я строка из D_{11} ненулевая, существует $\varphi_1 \in \mathscr{B}_1$ такой, что $d_{\chi\varphi_1} \neq 0$ и, значит, $c_{\varphi_1\varphi_2} \geqslant d_{\chi\varphi_1} d_{\chi\varphi_2} > 0$, вопреки ортогональности столбцов. Таким образом, в случае $\mathscr{A}_2 \neq \varnothing$ матрица D_B может быть приведена к блочно-диагональному виду, что противоречит доказанному выше, а если $\mathscr{A}_2 = \varnothing$, то D_B имеет нулевой столбец из D_{12} вопреки (19.5)(i). □

Разбиение неприводимых характеров на блоки позволяет доказать следующее усиление утверждения (19.11)(ii).

(20.25) Предложение. *Пусть $B \in \mathrm{Bl}(G)$ и $\varphi \in \mathrm{IBr}(B)$. Тогда φ является $\mathbb{Z}$-линейной комбинацией брауэровых характеров $\hat{\chi}$, где $\chi \in \mathrm{Irr}(B)$.*

Доказательство. В силу (19.11)(ii) для некоторых $a_\chi \in \mathbb{Z}$ мы можем записать

$$\varphi = \sum_{\chi \in \mathrm{Irr}(G)} a_\chi \hat{\chi} = \varphi_B + \varphi_0,$$

где

$$\varphi_B = \sum_{\chi \in \mathrm{Irr}(B)} a_\chi \hat{\chi}, \qquad \varphi_0 = \sum_{\chi \in \mathrm{Irr}(G) \setminus \mathrm{Irr}(B)} a_\chi \hat{\chi}$$

Выразив $\hat{\chi}$ через брауэровы характеры, ввиду (20.8) получаем, что φ_B является $\mathbb{Z}$-линейной комбинацией характеров из $\mathrm{IBr}(B)$, а φ_0 — характеров из $\mathrm{IBr}(G) \setminus \mathrm{IBr}(B)$. Значит, из линейной независимости брауэровых характеров следует, что равенство $\varphi - \varphi_B = \varphi_0$ возможно лишь если обе части равны нулю. Отсюда получаем требуемое. □

21. Блоки групповой алгебры

Изучим подробнее связь примитивных идемпотентов алгебр $\mathrm{Z}(\mathbb{C}G)$ и $\mathrm{Z}(FG)$.

Согласно (20.15)(iii) для произвольного $B \in \mathrm{Bl}(G)$ идемпотент f_B лежит в $\mathrm{Z}(\widetilde{\boldsymbol{R}}G)$. Назовём *центральным идемпотентом алгебры FG, соответствующим p-блоку B*, элемент $e_B = f_B^{\star}$.

(21.1) Предложение. *Справедливы следующие утверждения.*

- (i) *Элементы e_B, где $B \in \mathrm{Bl}(G)$, являются попарно ортогональными центральными идемпотентами алгебры FG.*
- (ii) *e_B — F-линейная комбинация классовых сумм p-регулярных классов.*
- (iii) *$\lambda_B(e_{B'}) = \delta_{B,B'}$ для любых $B, B' \in \mathrm{Bl}(G)$.*
- (iv) *Множество $\{e_B \mid B \in \mathrm{Bl}(G)\}$ линейно независимо над F. В частности, все e_B ненулевые и попарно различны.*
- (v) *$\sum_{B \in \mathrm{Bl}(G)} e_B = 1$.*
- (vi) *Пусть $z \in \mathrm{Z}(FG)$. Если $\lambda_B(z) = 0$ для всех $B \in \mathrm{Bl}(G)$, то z — нильпотентный элемент.*
- (vii) *Все гомоморфизмы F-алгебр $\mathrm{Z}(FG) \to F$ исчерпываются множеством $\{\lambda_B \mid B \in \mathrm{Bl}(G)\}$.*
- $(viii)$ *Любой идемпотент алгебры $\mathrm{Z}(FG)$ является суммой некоторых различных e_B.*
- (ix) *Все e_B являются примитивными идемпотентами алгебры $\mathrm{Z}(FG)$.*

Доказательство. (i) Это следует из того, что ${}^\star : \mathrm{Z}(\widetilde{\boldsymbol{R}}G) \to \mathrm{Z}(FG)$ — эпиморфизм колец и идемпотенты $f_B \in \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$ попарно ортогональны.

(ii) Это вытекает из (20.15)(ii).

(iii) Пусть $\chi \in \mathrm{Irr}(G)$. Из (16.25)(i) следует, что значение $\omega_\chi(f_{B'})$ равно 1 если $\chi \in \mathrm{Irr}(B')$ и 0 если $\chi \notin \mathrm{Irr}(B')$. Поэтому, выбрав χ из $\mathrm{Irr}(B)$, ввиду (20.4) получим

$$\lambda_B(e_{B'}) = \lambda_\chi(f_{B'}^{\star}) = \omega_\chi(f_{B'})^{\star} = \delta_{B,B'}.$$

(iv) Это вытекает из (iii).

(v) Это следует из равенств $\sum_{B \in \mathrm{Bl}(G)} f_B = \sum_{\chi \in \mathrm{Irr}(G)} e_\chi = 1$ ввиду того, что отображение ${}^\star : \mathrm{Z}(\widetilde{\boldsymbol{R}}G) \to \mathrm{Z}(FG)$ является гомоморфизмом колец.

(vi) Покажем, что $\mathscr{X}(z) = \mathbf{0}$ для любого неприводимого представления $\mathscr{X}$ алгебры FG. Пусть φ — брауэров характер $\mathscr{X}$, рассматриваемого как (неприводимое) F-представление группы G и пусть B — p-блок, содержащий φ. По условию имеем

$$\mathscr{X}(z) = \lambda_\varphi(z)\mathbf{1} = \lambda_B(z)\mathbf{1} = 0.$$

Значит, z лежит в ядре любого неприводимого представления $\mathscr{X}$ алгебры FG и поэтому $z \in \mathrm{J}(FG)$ ввиду (8.5). Из предложения (5.2) следует, что z — нильпотентный элемент.

(vii) Пусть $\lambda : \mathrm{Z}(FG) \to F$ — гомоморфизм F-алгебр. Тогда ядро $\operatorname{Ker}\lambda$ является подпространством в $\mathrm{Z}(FG)$ коразмерности 1 и $\mathrm{Z}(FG) = \operatorname{Ker}\lambda \oplus F1$. Поэтому λ однозначно задаётся своим ядром. Если $\lambda \neq \lambda_B$, то $\operatorname{Ker}\lambda_B \nsubseteq \operatorname{Ker}\lambda$, и существует элемент $z_B \in \operatorname{Ker}\lambda_B \setminus \operatorname{Ker}\lambda$.

Предположим, что $\lambda \notin \{\lambda_B \mid B \in \mathrm{Bl}(G)\}$. Рассмотрим элемент

$$z = \prod_{B \in \mathrm{Bl}(G)} z_B \in \mathrm{Z}(FG).$$

Тогда $\lambda_B(z) = 0$ для всех $B \in \mathrm{Bl}(G)$, и из (vi) следует, что z — нильпотентный элемент. Отсюда вытекает, что $\lambda(z) = 0$ как нильпотентный элемент поля F. Но это противоречит тому, что $\lambda(z) = \prod \lambda(z_B) \neq 0$. Отсюда следует требуемое.

($viii$) Пусть $e \in \mathrm{Z}(FG)$ — идемпотент. Предположим, что $ee_B \neq 0$ для некоторого $B \in \mathrm{Bl}(G)$. Покажем, что в этом случае $ee_B = e_B$.

Так как элемент ee_B — ненулевой идемпотент, он не является нильпотентным. С другой стороны для любого p-блока B', отличного от B, имеем $\lambda_{B'}(ee_B) = \lambda_{B'}(e)\lambda_{B'}(e_B) = 0$. Поэтому из ($vi$) следует, что $\lambda_B(ee_B) \neq 0$. Но $\lambda_B(ee_B)$ — идемпотент из F, значит, $\lambda_B(ee_B) = 1$ Получаем, что $\lambda_B(e_B - ee_B) = 1 - 1 = 0$ и $\lambda_{B'}(e_B - ee_B) = \lambda_{B'}(1-e)\lambda_{B'}(e_B) = 0$ Для всех $B' \neq B$. Тогда из (vi) следует, что элемент $e_B - ee_B$ нильпотентный. Но он, очевидно, также идемпотент. Поэтому $e_B - ee_B = 0$.

Итак, из доказанного следует, что $e = e(\sum e_B) = \sum ee_B$ — сумма некоторых (различных) e_B.

(ix) Пусть идемпотент e_B не является примитивным. Тогда $e_B = e_1 + e_2$, где $e_1, e_2 \in \mathrm{Z}(FG)$ — ненулевые ортогональные идемпотенты и мы получаем

$$e_1 = e_1^2 = e_1(e_B - e_2) = e_1 e_B = e_B,$$

где последнее равенство следует из доказательства предыдущего пункта. Но тогда $e_2 = e_B - e_1 = 0$. Противоречие. □

✓ Отметим, что в алгебре FG идемпотенты e_B могут не быть примитивными.

(21.2) Предложение. *Имеет место равенство*

$$\mathrm{J}(\mathrm{Z}(FG)) = \bigcap_{B \in \mathrm{Bl}(G)} \operatorname{Ker}\lambda_B.$$

✎ Доказать предложение (21.2).

Алгебра FG допускает в силу (2.18)(iii) разложение в прямую сумму своих двусторонних идеалов

(21.3)
$$FG = \bigoplus_{B \in \mathrm{Bl}(G)} e_B FG,$$

причём из примитивности e_B как идемпотентов алгебры $\mathrm{Z}(FG)$ и предложения (2.17)(iii) следует, что идеал $e_B FG$ не представим в виде прямой суммы ненулевых двусторонних идеалов алгебры FG. Мы можем рассматривать (21.3) как обобщение разложения (7.16)(iv) из теоремы Веддерберна на случай, когда алгебра FG не обязательно является полупростой. Для $B \in \mathrm{Bl}(G)$ будем обозначать соответствующую неразложимую компоненту $e_B FG$ через $\mathrm{W}_B(FG)$ или просто W_B и называть её *блоком алгебры FG, соответствующим p-блоку B*. Ясно, что блок W_B является F-алгеброй с единицей e_B.

✓ Отметим, что в некоторой литературе часто именно компоненты W_B называют p-блоками группы G. В силу (2.22) набор блоков $\{\mathrm{W}_B \mid B \in \mathrm{Bl}(G)\}$ определяется однозначно алгеброй FG как набор неразложимых двусторонних идеалов.

(21.4) Предложение. *Имеем*

(i) *Алгебра $\mathrm{Z}(FG)$ допускает разложение в прямую сумму своих идеалов*

$$\mathrm{Z}(FG) = \bigoplus_{B \in \mathrm{Bl}(G)} \mathrm{Z}(\mathrm{W}_B).$$

Пусть $B \in \mathrm{Bl}(G)$. Тогда выполнены следующие утверждения.

(ii) $\mathrm{Z}(\mathrm{W}_B) = e_B \mathrm{Z}(FG)$.

(*iii*) *Единственным неприводимым представлением F-алгебры* $\mathrm{Z}(\mathrm{W}_B)$ *является ограничение на неё гомоморфизма* λ_B.

(*iv*) $\mathrm{Z}(\mathrm{W}_B) = Fe_B \oplus \mathrm{J}(\mathrm{Z}(\mathrm{W}_B))$.

(*v*) $\mathrm{Z}(\mathrm{W}_B)$ *— локальное кольцо.*

(*vi*) $\mathrm{J}(\mathrm{Z}(\mathrm{W}_B)) = e_B\mathrm{J}(\mathrm{Z}(FG))$.

(*vii*) *Если I, J — идеалы алгебры* $\mathrm{Z}(FG)$ *и $e_B \in I + J$, то либо $e_B \in I$ либо $e_B \in J$.*

Доказательство. (*i*) Это следует из (2.21)(*i*).

(*ii*) Это следует из (2.18)(*iv*).

(*iii*) Из (9.5) следует, что всякое неприводимое представление алгебры $\mathrm{Z}(\mathrm{W}_B)$ одномерно. Пусть $\lambda : \mathrm{Z}(\mathrm{W}_B) \to F$ — одно из таких представлений. Ввиду разложения (*i*) можно продолжить λ до неприводимого представления $\mathrm{Z}(FG) \to F$. Тогда из (21.1)(*vii*) следует, что $\lambda = \lambda_{B'}$ для некоторого $B' \in \mathrm{Bl}(G)$. Но если $B' \neq B$, то $\lambda_{B'}(\mathrm{W}_B) = 0$ в силу (21.1)(*iii*). Значит, $B' = B$, откуда следует требуемое.

(*iv*) Пусть λ — ограничение на $\mathrm{Z}(\mathrm{W}_B)$ гомоморфизма λ_B. Так как λ — единственное неприводимое представление алгебры $\mathrm{Z}(\mathrm{W}_B)$, то $\mathrm{J}(\mathrm{Z}(\mathrm{W}_B)) = \mathrm{Ker}\,\lambda$ — F-подпространство в $\mathrm{Z}(\mathrm{W}_B)$ коразмерности 1. Поскольку $\lambda(e_B) = 1 \neq 0$, имеем требуемое разложение $\mathrm{Z}(\mathrm{W}_B) = Fe_B \oplus \mathrm{Ker}\,\lambda$.

(*v*) В силу (*iv*) радикал $\mathrm{J}(\mathrm{Z}(\mathrm{W}_B))$ имеет в W_B коразмерность 1 и содержится в любом максимальном идеале. Поэтому любой максимальный идеал совпадает с $\mathrm{J}(\mathrm{Z}(\mathrm{W}_B))$. Следовательно, $\mathrm{Z}(\mathrm{W}_B)$ — локальное кольцо.

(*vi*) Из (*ii*) и (4.10) получаем

$$\mathrm{J}(\mathrm{Z}(\mathrm{W}_B)) = \mathrm{J}(e_B\mathrm{Z}(FG)) = e_B\mathrm{J}(\mathrm{Z}(FG)).$$

(*vii*) Так как $e_B I$ — идеал в $\mathrm{Z}(FG)$ и $e_B \in \mathrm{Z}(\mathrm{W}_B)$, то $e_B I \trianglelefteq \mathrm{Z}(\mathrm{W}_B)$. Если $e_B I = \mathrm{Z}(\mathrm{W}_B)$, то

$$e_B \in \mathrm{Z}(\mathrm{W}_B) = e_B I \subseteq I.$$

Поэтому можем считать, что $e_B I$ — собственный идеал в $\mathrm{Z}(\mathrm{W}_B)$. Аналогично, $e_B J$ — собственный идеал в $\mathrm{Z}(\mathrm{W}_B)$. В силу локальности кольца $\mathrm{Z}(\mathrm{W}_B)$ получаем $e_B I \subseteq \mathrm{J}(\mathrm{Z}(W_B))$ и $e_B J \subseteq \mathrm{J}(\mathrm{Z}(W_B))$. По условию $e_B = x + y$ для некоторых $x \in I$ и $y \in J$. Поэтому

$$e_B = e_B^2 = e_B x + e_B y \in e_B I + e_B J \subseteq \mathrm{J}(\mathrm{Z}(W_B)).$$

Но e_B — единица алгебры. Противоречие. □

Подобно неприводимым обыкновенным и брауэровым характерам группы G неприводимые $\mathbb{C}G$- и FG-модули естественно разбиваются на классы эквивалентности, соответствующие p-блокам группы G. Следующее утверждение даёт критерий принадлежности модуля такому классу.

(21.5) Предложение. *Пусть* $B \in \mathrm{Bl}(G)$.

(*i*) *Если M_χ — неприводимый $\mathbb{C}G$-модуль с обыкновенным характером* $\chi \in \mathrm{Irr}(G)$, *то*

$$M_\chi f_B = \begin{cases} M_\chi, & \text{если } \chi \in B; \\ 0, & \text{если } \chi \notin B. \end{cases}$$

(*ii*) *Если M_φ — неприводимый FG-модуль с брауэровым характером* $\varphi \in \mathrm{IBr}(G)$, *то*

$$M_\varphi e_B = \begin{cases} M_\varphi, & \text{если } \varphi \in B; \\ 0, & \text{если } \varphi \notin B. \end{cases}$$

Доказательство. (*i*) Идемпотент e_χ действует тождественно на M_χ в силу (7.16)(*iii*), поскольку является единицей компоненты Веддерберна $\mathrm{W}_{M_\chi}(\mathbb{C}G^\circ)$. Значит, $M_\chi = M_\chi e_\chi$. Осталось заметить, что произведение $e_\chi f_B$ равно e_χ, если $\chi \in B$, и 0, если $\chi \notin B$. Отсюда следует требуемое.

(*ii*) Так как $\sum_{B\in\mathrm{Bl}(G)} e_B = 1$, имеем $M_\varphi = \bigoplus_{B\in\mathrm{Bl}(G)} M_\varphi e_B$ в силу (2.37)(*iii*). Из неприводимости модуля M_φ следует, что существует единственный $B \in \mathrm{Bl}(G)$ для которого $M_\varphi = M_\varphi e_B$ и $M_\varphi e_{B'} = 0$ для всех $B' \neq B$. В частности, e_B действует тождественно на M_φ, т. е. если $\mathscr{X}$ — F-представление, соответствующее M_φ, то $\mathscr{X}(e_B) = \mathbf{1}$. Но $e_B \in \mathrm{Z}(FG)$ и, значит, $\mathscr{X}(e_B) = \lambda_\varphi(e_B)\mathbf{1}$. Поэтому $1 = \lambda_\varphi(e_B) = \lambda_{B'}(e_B)$, где B' — p-блок, содержащий φ. Из (21.1)(*iii*) следует, что $B' = B$. □

(21.6) Следствие. *Для всякого $B \in \mathrm{Bl}(G)$ брауэров характер любого композиционного фактора блока W_B принадлежит B.*

Доказательство. Поскольку $\mathrm{W}_B = e_B FG$, идемпотент e_B действует как тождественное преобразование на блоке W_B, а, значит, и на любом его композиционном факторе V. Из (21.5)(*ii*) следует, что брауэров характер FG-модуля V лежит в B. □

Естественно спросить, каковы брауэров характер и размерность блока W_B.

(21.7) Предложение. *Пусть* $B \in \mathrm{Bl}(G)$.

(i) *Брауэров характер* FG*-модуля* W_B *равен*

$$\sum_{\chi\in\mathrm{Irr}(B)} \chi(1)\hat{\chi} = \sum_{\varphi\in\mathrm{IBr}(B)} \theta_\varphi(1)\varphi = \sum_{\varphi\in\mathrm{IBr}(B)} \varphi(1)\widehat{\theta_\varphi}.$$

(ii) $\dim_F W_B = \sum_{\chi\in\mathrm{Irr}(B)} \chi(1)^2 = \sum_{\varphi\in\mathrm{IBr}(B)} \theta_\varphi(1)\varphi(1)$.

Доказательство. (i) Пусть η_B — брауэров характер блока W_B. Поскольку

$$FG = \bigoplus_{B\in\mathrm{Bl}(G)} \mathrm{W}_B,$$

брауэров характер регулярного модуля FG° равен $\sum_{B\in\mathrm{Bl}(G)} \eta_B$.

Пусть $\mathscr{R}$ — регулярное $\mathbb{C}$-представление группы G относительно базиса из групповых элементов и ρ — его характер. Поскольку $\mathscr{R}$ записано над $\mathbb{Z} \subseteq \utilde{\boldsymbol{R}}$, из (18.6)$(ii)$ получаем, что брауэров характер регулярного F-представления $\mathscr{R}^\star$ группы G равен $\hat{\rho}$.

Итак, в силу (16.13) имеем

$$\sum_{B\in\mathrm{Bl}(G)} \eta_B = \hat{\rho} = \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)\hat{\chi} = \sum_{B\in\mathrm{Bl}(G)} \left(\sum_{\chi\in\mathrm{Irr}(B)} \chi(1)\hat{\chi} \right).$$

Поскольку неприводимые компоненты брауэрова характера η_B лежат в $\mathrm{IBr}(B)$ по (21.6), и неприводимые компоненты брауэрова характера $\sum_{\chi\in\mathrm{Irr}(B)} \chi(1)\hat{\chi}$ лежат в $\mathrm{IBr}(B)$ по (20.8)(i), получаем

$$\eta_B = \sum_{\chi\in\mathrm{Irr}(B)} \chi(1)\hat{\chi}$$

для всех $B \in \mathrm{Bl}(G)$. Далее, положив $x = 1$ в (20.19)$(i), (ii)$, получаем (i).

(ii) Это следует из (i). □

Пусть $B \in \mathrm{Bl}(G)$ и $\eta \in \mathrm{cf}(G)$. Тогда функция

$$\eta_B = \sum_{\chi\in\mathrm{Irr}(B)} (\eta, \chi)_G\, \chi$$

называется B*-частью* классовой функции η. Легко видеть, что $\eta = \sum_{B\in\mathrm{Bl}(G)} \eta_B$, и для любого $B \in \mathrm{Bl}(G)$ отображение $\eta \mapsto \eta_B$ является $\mathbb{C}$-линейным преобразованием алгебры $\mathrm{cf}(G)$.

(21.8) Предложение. *Пусть* $B \in \mathrm{Bl}(G)$, $\eta \in \mathrm{cf}(G)$. *Тогда*

$$\eta_B(x) = \eta(f_B x)$$

для всех $x \in \mathbb{C}G$.

Доказательство. В силу линейности можно считать, что $\eta \in \mathrm{Irr}(G)$. Тогда

(21.9)
$$\eta_B = \begin{cases} \eta, & \text{если } \eta \in B; \\ 0, & \text{если } \eta \notin B. \end{cases}$$

Пусть $M = M_\eta$ и $\mathscr{X} = \mathscr{X}_\eta$. Из (21.5)$(i)$ следует, что если $\eta \in B$, то $M = M f_B$ и, значит, f_B действует на M тождественно, т. е. $\mathscr{X}(f_B) = \mathbf{1}$, а если $\eta \notin B$, то $M f_B = 0$, т. е. $\mathscr{X}(f_B) = \mathbf{0}$. Поэтому

$$\eta(f_B x) = \mathrm{tr}\,\mathscr{X}(f_B x) = \mathrm{tr}\left(\mathscr{X}(f_B)\mathscr{X}(x)\right) = \begin{cases} \mathrm{tr}\,\mathscr{X}(x) = \eta(x), & \text{если } \eta \in B; \\ \mathrm{tr}\,\mathbf{0} = 0, & \text{если } \eta \notin B. \end{cases}$$

Сравнив с (21.9), получаем $\eta_B(x) = \eta(f_B x)$. □

✎ **(21.10)** Доказать, что отображение $\eta \mapsto \eta_B$ является эндоморфизмом

22. Дефект блока. Дефектная группа

Существует тесная связь между p-блоками и p-подгруппами группы G, к описанию которой мы приступаем.

Для произвольных подмножеств X, Y группы G определим отношение *G-включения*. Будем говорить, что X *G-содержится* в Y и записывать $X \leqslant_G Y$, если некоторое G-сопряжённое с X подмножество содержится в Y или, что эквивалентно, X содержится в некотором G-сопряжённом с Y подмножестве.

Пусть $K \in \mathscr{K}(G)$ — произвольный класс сопряжённости. Положим

$$\Delta_p(K) = \bigcup_{x \in K} \mathrm{Syl}_p(\mathrm{C}_G(x)).$$

Как правило мы будем писать $\Delta(K)$ вместо $\Delta_p(K)$. Легко видеть, что множество $\Delta(K)$ является классом сопряжённых p-подгрупп группы G. Его элементы будем называть *p-дефектными группами класса K*. Для любого $K \in \mathscr{K}(G)$ зафиксируем некоторый представитель $\delta(K) \in \Delta(K)$. Будем также иногда писать $\delta_p(K)$ вместо $\delta(K)$. *Дефектом класса K* (или, точнее, его *p-дефектом*) называется число $\mathrm{d}(K)$, определяемое равенством $|\delta(K)| = p^{\,\mathrm{d}(K)}$.

Пусть P — произвольная p-подгруппа группы G. Мы можем рассмотреть совокупность всех классов $K \in \mathscr{K}(G)$, p-дефектные группы которых G-содержатся в P. Символом $\mathrm{Z}_P(FG)$ обозначим F-линейную оболочку классовых сумм таких классов. Другими словами,

$$\mathrm{Z}_P(FG) = \bigoplus_{\substack{K \in \mathscr{K}(G),\\ \delta(K) \leqslant_G P}} F\widehat{K}.$$

Из данных определений сразу вытекает

(22.1) Предложение. *Справедливы следующие утверждения.*

(i) *Пусть $P, Q \leqslant G$ — p-подгруппы и $P \leqslant_G Q$. Тогда $\mathrm{Z}_P(FG) \subseteq \mathrm{Z}_Q(FG)$.*

(ii) *Если p-подгруппы P и Q сопряжены в G, то $\mathrm{Z}_P(FG) = \mathrm{Z}_Q(FG)$.*

(iii) *Для любого $K \in \mathscr{K}(G)$ имеем $\widehat{K} \in \mathrm{Z}_{\delta(K)}(FG)$.*

(22.2) Предложение. *Справедливы следующие утверждения.*

(i) *Для любой p-подгруппы $P \leqslant G$ имеем $\mathrm{Z}_P(FG) \trianglelefteqslant \mathrm{Z}(FG)$.*

(ii) *Для любых p-подгрупп $P, Q \leqslant G$ выполнено равенство*

$$\mathrm{Z}_P(FG) \cap \mathrm{Z}_Q(FG) = \sum_{x,y \in G} \mathrm{Z}_{P^x \cap Q^y}(FG).$$

Доказательство. (i) Из (3.7)(iv) следует, что для произвольных классов $K, L \in \mathscr{K}(G)$ соответствующие классовые суммы из $\mathrm{Z}(FG)$ перемножаются по правилу

$$\widehat{K}\widehat{L} = \sum_{M \in \mathscr{K}(G)} a^{\star}_{KLM} \widehat{M},$$

где a_{KLM} — число всевозможных пар $(x, y) \in K \times L$ таких, что $xy = z$ для фиксированного (но произвольного) представителя $z \in M$. Если z выбран так, что $\delta(M) \leqslant \mathrm{C}_G(z)$, то на множестве таких пар (x, y) можно определить действие группы $\delta(M)$, положив $(x, y)^d = (x^d, y^d)$ для любого $d \in \delta(M)$. Поскольку $\delta(M)$ — p-группа, её орбиты при этом действии будут иметь мощность, равную степени числа p.

Предположим, что $a^{\star}_{KLM} \neq 0$ для некоторого класса M. Из предыдущего замечания следует, что $\delta(M)$ имеет одноэлементную орбиту, т. е. существует пара элементов $x \in K$ и $y \in L$, централизуемых группой $\delta(M)$. Другими словами, при нашем предположении имеем $\delta(M) \leqslant_G \delta(K)$ и $\delta(M) \leqslant_G \delta(L)$.

Пусть теперь K — класс, для которого $\delta(K) \leqslant_G P$, и L — произвольный класс. Из доказанного выше следует, что произведение $\widehat{K}\widehat{L}$ является линейной комбинацией классовых сумм $\widehat{M}$, соответствующих классам M, для которых, в частности, $\delta(M) \leqslant_G \delta(K) \leqslant_G P$, т. е. $\widehat{K}\widehat{L} \in \mathrm{Z}_P(FG)$. Поэтому $\mathrm{Z}_P(FG)$ — идеал в $\mathrm{Z}(FG)$.

(ii) Включение $\sum_{x,y \in G} \mathrm{Z}_{P^x \cap Q^y}(FG) \subseteq \mathrm{Z}_P(FG) \cap \mathrm{Z}_Q(FG)$ следует из соотношений $P^x \cap Q^y \leqslant_G P$ и $P^x \cap Q^y \leqslant_G Q$ для всех $x, y \in G$. Докажем обратное включение. Пусть $z \in \mathrm{Z}_P(FG) \cap \mathrm{Z}_Q(FG)$. Тогда

$$z = \sum_{K \in \mathscr{K}(G)} a_K \widehat{K}$$

для некоторых $a_K \in F$. Поскольку $z \in \mathrm{Z}_P(FG)$, получаем, что если $a_K \neq 0$, то $\delta(K) \leqslant_G P$. Аналогично, если $a_K \neq 0$, то $\delta(K) \leqslant_G Q$. То есть для каждого $K \in \mathscr{K}(G)$ такого, что $a_K \neq 0$, найдутся $x, y \in G$, для которых $\delta(K) \subseteq P^x \cap Q^y$. Но тогда $\widehat{K} \in \mathrm{Z}_{P^x \cap Q^y}(FG)$ и, значит, $z \in \sum_{x,y \in G} \mathrm{Z}_{P^x \cap Q^y}(FG)$, что и требовалось доказать. $\square$

Как соотносятся идеалы алгебры $\mathrm{Z}(FG)$ вида $\mathrm{Z}_P(FG)$ с идеалами $\mathrm{Z}(W_B)$? Оказывается, что для каждого $B \in \mathrm{Bl}(G)$ существует единственный класс сопряжённых минимальных по включению p-подгрупп P, для которых $\mathrm{Z}(W_B)$ лежит в $\mathrm{Z}_P(FG)$.

(22.3) Предложение. *Пусть $B \in \mathrm{Bl}(G)$. Существует единственный класс сопряжённых p-подгрупп P, для которых выполнены следующие два условия.*

(*i*) $\mathrm{Z}(W_B) \subseteq \mathrm{Z}_P(FG)$;

(*ii*) *если $\mathrm{Z}(W_B) \subseteq \mathrm{Z}_Q(FG)$ для некоторой p-подгруппы Q, то $P \leqslant_G Q$.*

✎ Доказать предложение (22.3). (*Указание.* Воспользоваться (21.4)(*vii*).)

(22.4) Определение. Пусть $B \in \mathrm{Bl}(G)$. Класс сопряжённых p-подгрупп, существование и единственность которого утверждается в (22.3), будем обозначать через $\Delta(B)$, а его элементы называть *дефектными группами p-блока B*. Для любого $B \in \mathrm{Bl}(G)$ зафиксируем некоторый представитель $\delta(B) \in \Delta(B)$.

Из определения следует

(22.5) Предложение. *Для любого $B \in \mathrm{Bl}(G)$ имеем $e_{B} \in \mathrm{Z}_{\delta(B)}(FG)$.*

Ввиду важности введённого понятия, мы дадим другое, эквивалентное определение дефектной группы p-блока.

Пусть $B \in \mathrm{Bl}(G)$. Запишем

(22.6)
$$e_{B} = \sum_{K \in \mathscr{K}(G)} a_{B}(K)\widehat{K},$$

где $a_{B} : \mathscr{K}(G) \to F$ — однозначно определённое отображение. Из (20.15)(*i*), (*iii*) следует, что

(22.7)
$$a_{B}(K) = \left(\frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(B)} \chi(1)\overline{\chi(x_{K})}\right)^{\star}.$$

Кроме того, в силу (20.15)(*ii*) имеем $a_{B}(K) = 0$ если $K \notin \mathscr{K}(G_{p'})$. Поэтому

(22.8)
$$e_{B} = \sum_{K \in \mathscr{K}(G_{p'})} a_{B}(K)\widehat{K}.$$

Поскольку
$$1 = \lambda_{B}(e_{B}) = \sum_{K \in \mathscr{K}(G_{p'})} a_{B}(K)\lambda_{B}(\widehat{K}),$$

существует по меньшей мере один класс $K \in \mathscr{K}(G)$ для которого $a_{B}(K) \neq 0$ и $\lambda_{B}(\widehat{K}) \neq 0$. Любой такой K мы назовём *дефектным классом p-блока B*. Из определения сразу вытекает

(22.9) Предложение. *Дефектный класс любого p-блока является p-регулярным.*

Мы покажем, что p-дефектные группы дефектных классов p-блока B — это в точности его дефектные группы.

(22.10) Теорема (Min-Max). *Пусть $B \in \mathrm{Bl}(G)$ и $K \in \mathscr{K}(G)$.*

(*i*) *Если $\lambda_{B}(\widehat{K}) \neq 0$, то $\delta(B) \leqslant_G \delta(K)$.*

(*ii*) *Если $a_{B}(K) \neq 0$, то $\delta(K) \leqslant_G \delta(B)$.*

Доказательство. (*i*) Рассмотрим идеалы $\mathrm{Z}_{\delta(K)}(FG)$ и $\operatorname{Ker} \lambda_{B}$ алгебры $\mathrm{Z}(FG)$. Имеем $\widehat{K} \in \mathrm{Z}_{\delta(K)}(FG)$, но с другой стороны $\widehat{K} \notin \operatorname{Ker} \lambda_{B}$, поскольку $\lambda_{B}(\widehat{K}) \neq 0$. Значит, $\mathrm{Z}_{\delta(K)}(FG) \nsubseteq \operatorname{Ker} \lambda_{B}$. Однако идеал $\operatorname{Ker} \lambda_{B}$ имеет коразмерность 1 в $\mathrm{Z}(FG)$. Поэтому
$$\mathrm{Z}(FG) = \mathrm{Z}_{\delta(K)}(FG) + \operatorname{Ker} \lambda_{B}.$$

В частности, из (21.4)(*vii*) следует, что идемпотент e_{B} лежит либо в $\mathrm{Z}_{\delta(K)}(FG)$, либо в $\operatorname{Ker} \lambda_{B}$. Но последнее невозможно, поскольку $\lambda_{B}(e_{B}) = 1 \neq 0$. Значит, $e_{B} \in \mathrm{Z}_{\delta(K)}(FG)$, откуда получаем $\mathrm{W}_B = e_{B}\mathrm{Z}(FG) \subseteq \mathrm{Z}_{\delta(K)}(FG)$. Поэтому $\delta(B) \leqslant_G \delta(K)$.

(*ii*) Из условия следует, что классовая сумма $\widehat{K}$ входит в разложение (22.8) с ненулевым коэффициентом. Однако e_{B} лежит в идеале $\mathrm{Z}_{\delta(B)}(FG)$. По определению этого идеала получаем, что $\delta(K) \leqslant_G \delta(B)$. ☐

(22.11) Следствие. *Для любого $B \in \mathrm{Bl}(G)$ и произвольного дефектного класса K блока B имеем $\Delta(B) = \Delta(K)$.*

Доказательство. Пусть K — дефектный класс p-блока B. Тогда $a_{B}(K) \neq 0$ и $\lambda_{B}(\widehat{K}) \neq 0$. Из теоремы (22.10) следует, что группы $\delta(K)$ и $\delta(B)$ сопряжены, т. е. $\delta(K) \in \Delta(B)$ и $\delta(B) \in \Delta(K)$. $\square$

Какие p-подгруппы группы G могут быть дефектными группами её p-блоков? Оказывается,[23] что любая дефектная группа имеет вид $P \cap Q$ для некоторых $P, Q \in \mathrm{Syl}_p(G)$. Нашей ближайшей целью является установить более слабый результат, который утверждает, что дефектная группа произвольного p-блока содержит любую нормальную p-подгруппу группы G.

Докажем вспомогательное утверждение.

(22.12) Предложение. *Пусть $K \in \mathscr{K}(G)$ и $K \nsubseteq \mathrm{C}_G(\mathrm{O}_p(G))$. Тогда $\widehat{K}$ — нильпотентный элемент алгебры FG.*

Доказательство. Обозначим $P = \mathrm{O}_p(G)$. Группа P действует сопряжением на K. Пусть O — одна из орбит этого действия. Заметим, что O содержится в одном смежном классе G по P, поскольку любые два её представителя сопряжены элементом из P и, значит, имеют одинаковые образы в факторгруппе G/P. Кроме того, из условия следует, что $K \cap \mathrm{C}_G(\mathrm{O}_p(G)) = \varnothing$. Поэтому $|O| > 1$ и, в частности, $p \bigm| |O|$.

Пусть $\mathscr{X}$ — неприводимое F-представление группы G. Ввиду (18.9)(ii) имеем $P \subseteq \ker \mathscr{X}$, т. е. $\mathscr{X}$ принимает постоянное значение на каждом смежном классе G по P. Из сделанных выше замечаний получаем

$$\sum_{y \in O} \mathscr{X}(y) = |O|^{\star} \mathscr{X}(x) = 0,$$

поскольку $p \bigm| |O|$, где $x \in O$ — произвольный представитель. Просуммировав по всем орбитам, имеем $\mathscr{X}(\widehat{K}) = 0$ для любого неприводимого представления $\mathscr{X}$. Поэтому элемент $\widehat{K}$ лежит в $\mathrm{J}(FG)$ в силу (8.5) и, значит, является нильпотентным. $\square$

(22.13) Предложение. *Для любого $B \in \mathrm{Bl}(G)$ имеем $\mathrm{O}_p(G) \leqslant \delta(B)$.*

Доказательство. Пусть K — дефектный класс блока B. Тогда $\lambda_{B}(\widehat{K}) \neq 0$ и, значит, элемент $\widehat{K}$ не является нильпотентным. Тогда из (22.12) следует, что $K \subseteq \mathrm{C}_G(\mathrm{O}_p(G))$. Поэтому $\mathrm{O}_p(G) \subseteq \delta(K)$. Но $\delta(K) \in \Delta(B)$ ввиду (22.11), и мы получаем требуемое. $\square$

(22.14) Определение. Пусть $B \in \mathrm{Bl}(G)$ и $|\delta(B)| = p^d$. Число d, которое мы обозначим через $\mathrm{d}(B)$, называется *дефектом p-блока B*.

Это определение корректно, поскольку все дефектные группы p-блока B сопряжены и, значит, имеют одинаковые порядки. Мы покажем, что дефект $\mathrm{d}(B)$ можно определить, зная лишь степени характеров из $\mathrm{Irr}(B)$ или $\mathrm{IBr}(B)$.

✎ **(22.15)** Доказать, что если $\mathrm{O}_p(G) \neq 1$, то G не имеет p-блоков дефекта 0.

✎ **(22.16)** Каковы дефекты блоков абелевой группы?

(22.17) Предложение. *Пусть $B \in \mathrm{Bl}(G)$ и $d = \mathrm{d}(B)$. Запишем $|G|_p = p^a$. Тогда*

(i) *p^{a-d} — максимальная степень числа p, делящая $\chi(1)$ для всех $\chi \in \mathrm{Irr}(B)$;*

(ii) *p^{a-d} — максимальная степень числа p, делящая $\varphi(1)$ для всех $\varphi \in \mathrm{IBr}(B)$.*

Доказательство. (i) Пусть K — дефектный класс p-блока B. В силу (22.11) имеем $\delta(K) \in \Delta(B)$, и поэтому из условия получаем

$$p^d = |\delta(K)| = |\mathrm{C}_G(x_{K})|_p = \frac{|G|_p}{|K|_p} = \frac{p^a}{|K|_p},$$

т. е. $|K|_p = p^{a-d}$.

Пусть $\chi \in \mathrm{Irr}(B)$. Так как K — дефектный класс p-блока B, то

$$0 \neq \lambda_{B}(\widehat{K}) = \lambda_{\chi}(\widehat{K}) = \omega_{\chi}(\widehat{K})^{\star} = \left(\frac{|K|\chi(x_{K})}{\chi(1)}\right)^{\star}. \qquad (*)$$

[23] См.(25.12)

Но $\chi(x_{\scriptscriptstyle K}) \in \boldsymbol{R}$ и, значит, $\dfrac{|K|}{\chi(1)} \notin \widetilde{M}$ в силу $(*)$. Отсюда следует, что $\chi(1)_p \geqslant |K|_p = p^{a-d}$, т. е. $p^{a-d} \mid \chi(1)$.

С другой стороны

$$0 \neq a_{\scriptscriptstyle B}(K) = \left(\frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(B)} \chi(1) \overline{\chi(x_{\scriptscriptstyle K})} \right)^{\star} = \left(\frac{1}{|G|} \sum_{\varphi \in \mathrm{IBr}(B)} \theta_\varphi(1) \overline{\varphi(x_{\scriptscriptstyle K})} \right)^{\star}, \qquad (**)$$

где последнее равенство следует из (20.13), поскольку $x_{\scriptscriptstyle K} \in G_{p'}$ в силу (22.9). Так как $|G|_p \mid \theta_\varphi(1)$ ввиду (19.18)(vii), имеем $\dfrac{\theta_\varphi(1)}{|G|} \in \widetilde{\boldsymbol{R}}$ для всех φ и, значит, из $(**)$ следует, что найдётся характер $\varphi \in \mathrm{IBr}(B)$ для которого $\overline{\varphi(x_{\scriptscriptstyle K})} \notin \widetilde{M}$.

Вследствие (20.25) характер φ является $\mathbb{Z}$-линейной комбинацией брауэровых характеров $\{\hat{\tau} \mid \tau \in \mathrm{Irr}(B)\}$. Поэтому $\overline{\hat{\tau}(x_{\scriptscriptstyle K})} = \overline{\tau(x_{\scriptscriptstyle K})} \notin \widetilde{M}$ для некоторого $\tau \in \mathrm{Irr}(B)$. Однако число $\alpha = \dfrac{|K|\overline{\tau(x_{\scriptscriptstyle K})}}{\tau(1)}$ лежит в $\boldsymbol{R}$ и $\overline{\tau(x_{\scriptscriptstyle K})} = \alpha\dfrac{\tau(1)}{|K|}$, откуда следует, что $\dfrac{\tau(1)}{|K|} \notin \widetilde{M}$. Поэтому $\tau(1)_p \leqslant |K|_p = p^{a-d}$.

(ii) В действительности имеет место более сильный факт: множества натуральных чисел

$$\{\chi(1) \mid \chi \in \mathrm{Irr}(B)\}, \qquad \{\varphi(1) \mid \varphi \in \mathrm{IBr}(B)\}$$

имеют одинаковый наибольший общий делитель. Это следует из того, что $\chi(1) = \hat{\chi}(1)$ — целочисленная линейная комбинация значений $\varphi(1)$ с коэффициентами, являющимися числами разложения p-блока B, а в свою очередь $\varphi(1)$ — целочисленная линейная комбинация значений $\chi(1)$ в силу (20.25). ☐

✓ В связи с предложением (22.17) отметим, что в общем случае степени неприводимых брауэровых характеров не делят порядок группы G. Более того, если $\varphi \in \mathrm{IBr}(G)$, то p-часть $\varphi(1)_p$, вообще говоря, может превосходить $|G|_p$. Так, например, простая спорадическая группа Маклафлина McL порядка $2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$ обладает неприводимым 2-модулярным характером степени $2^9 \cdot 7$.

В условиях предложения (22.17) для произвольного характера $\eta \in B$ можно записать

$$\eta(1)_p = p^{a-d+h},$$

где $h \geqslant 0$ — однозначно определённое целое число, которое называется *p-высотой* (или просто *высотой*) характера η.

Напомним, что ранее (см. стр. 47) мы определили p-дефект произвольного неприводимого обыкновенного характера. Очевидно, что если $B \in \mathrm{Bl}(G)$, то для любого характера из $\mathrm{Irr}(B)$ сумма его p-дефекта и p-высоты совпадает с $\mathrm{d}(B)$.

Из предложения (22.17) следует, что каждый p-блок содержит по крайней мере один обыкновенный и один брауэров характер высоты 0. В связи с этим отметим следующую известную гипотезу.

(22.18) Гипотеза (Брауэра о нулевой высоте[24]). *Если $B \in \mathrm{Bl}_p(G)$, то все характеры из $\mathrm{Irr}(B)$ имеют p-высоту 0 тогда и только тогда, когда $\delta(B)$ — абелева группа.*

Справедливость этой гипотезы установлена в классе p-разрешимых групп (напомним, что группа называется *p-разрешимой*, если каждый её композиционный фактор является p- или p'-группой).

✎ **(22.19)** Найти 2-высоту всех неприводимых обыкновенных и 2-модулярных характеров группы A_5. Проиллюстрировать для этого случая справедливость гипотезы (22.18).

23. Блоки дефекта 0

Наиболее простое описание имеют p-блоки нулевого дефекта (ср. предложение (16.40)).

(23.1) Предложение. *Пусть $B \in \mathrm{Bl}(G)$. Тогда следующие условия эквивалентны.*

(i) $|\mathrm{Irr}(B)| = |\mathrm{IBr}(B)|$.

(ii) *$\chi(g) = 0$ для любого $\chi \in \mathrm{Irr}(B)$ и любого $g \in G \setminus G_{p'}$.*

(iii) *$\chi(g) = 0$ для любого $\chi \in \mathrm{Irr}(B)$ и любого неединичного p-элемента g.*

(iv) $\delta(B) = 0$.

[24] Brauer's height-zero conjecture.

(*v*) *Существует* $\chi \in \operatorname{Irr}(B)$ *такой, что* $|\chi(1)|_p = |G|_p$.

(*vi*) $|\operatorname{Irr}(B)| = 1$.

Доказательство. (*i*) $\Rightarrow$ (*ii*) Из (*i*) и (20.23) следует, что матрица разложения D_B блока B обратима. Положим

$$\mathrm{D}_B^{-1} = (a_{\varphi\chi})_{\varphi\in\operatorname{IBr}(B),\,\chi\in\operatorname{Irr}(B)}.$$

Тогда для любого $\chi \in \operatorname{Irr}(B)$ получаем

$$\sum_{\varphi\in\operatorname{IBr}(B)} a_{\varphi\chi}\theta_\varphi = \sum_{\varphi\in\operatorname{IBr}(B)}\sum_{\tau\in\operatorname{Irr}(B)} a_{\varphi\chi}d_{\tau\varphi}\tau = \sum_{\tau\in\operatorname{Irr}(B)}\delta_{\chi,\tau}\tau = \chi.$$

Поэтому, в силу (19.18)(*i*), χ обращается в ноль на элементах из $G\setminus G_{p'}$.

(*ii*) $\Rightarrow$ (*iii*) Очевидно.

(*iii*) $\Rightarrow$ (*iv*) Пусть $P\in\operatorname{Syl}_p(G)$. Из (*iii*) следует, что для произвольного $\chi\in\operatorname{Irr}(B)$ выполнено равенство

$$(\chi_P, 1_P)_P = \frac{\chi(1)}{|P|}.$$

Так как левая часть — целое число и $\chi(1)$ делит $|G|$, отсюда следует, что $\chi(1)_p = |G|_p$. В силу произвольности χ, из (22.17)(*i*) вытекает, что $\delta(B) = 0$.

(*iv*) $\Rightarrow$ (*v*) Из (*iv*) и (22.17)(*i*) следует, что $\chi(1)_p = |G|_p$ для *любого* $\chi\in\operatorname{Irr}(B)$.

(*v*) $\Rightarrow$ (*vi*) Пусть $\chi\in\operatorname{Irr}(B)$ такой, что $\chi(1)_p = |G|_p$. В частности, $\chi(1)/|G| \in \widetilde{\boldsymbol{R}}$. По (16.15), для центрального идемпотента e_χ имеет место разложение

$$e_\chi = \frac{\chi(1)}{|G|}\sum_{g\in G}\chi(g^{-1})g.$$

Поэтому $e_\chi \in \widetilde{\boldsymbol{R}}G$ и из (20.16) получаем, что одноэлементное множество $\{\chi\}$ является объединением p-блоков обыкновенных характеров. Значит, $\operatorname{Irr}(B) = \{\chi\}$.

(*vi*) $\Rightarrow$ (*i*) Ввиду (20.9) и (20.23)(*ii*), имеем $1 \leqslant |\operatorname{IBr}(B)| \leqslant |\operatorname{Irr}(B)| = 1$, откуда следует (*i*). $\square$

Для натурального числа n и произвольного множества π простых чисел определим *π-часть* n_π числа n как наибольший делитель n, все простые делители которого принадлежат π (ср. определение (16.35)). Напомним, что π' обозначает множество простых чисел, не принадлежащих π.

Следующее упражнение частично обобщает предложение (23.1).

✎ **(23.2)** Пусть $\chi\in\operatorname{Irr}(G)$ и π — множество простых чисел. Доказать равносильность следующих утверждений.

(*i*) $|G|_\pi$ делит $\chi(1)$.

(*ii*) $\chi(g) = 0$ для любого неединичного $g\in G_\pi$.

(*iii*) $\chi(g) = 0$ для любого $g\in G\setminus G_{\pi'}$.

✎ **(23.3)** Доказать справедливость гипотезы (22.18) для p-блоков дефекта 0 и 1.

В связи с блоками дефекта 0 упомянем ещё одну важную гипотезу. Пусть P — некоторая p-подгруппа группы G. Назовём *p-весом* пару (P,χ), где $\chi\in\operatorname{Irr}(\mathrm{N}_G(P))$ такой характер, что $P\leqslant\ker\chi$ и $\chi(1)_p = |\mathrm{N}_G(P)/P|_p$, т. е. χ, рассматриваемый как характер группы $\mathrm{N}_G(P)/P$, принадлежит p-блоку нулевого дефекта. Если (P,χ) — p-вес, то для любого $g\in G$ пара (P^g,χ^g), как легко видеть, также является p-весом, т. е. G действует сопряжением на множестве p-весов.

(23.4) Гипотеза (Альперина о весах[25]). *Число классов сопряжённости p-весов группы G совпадает с* $|\operatorname{IBr}(G)|$.

Более точную формулировку этой гипотезы мы приведём чуть ниже, см. (24.22), когда сформулируем понятие индуцированного блока.

[25] Alperin's weight conjecture.

24. Гомоморфизм Брауэра. Индуцированные блоки

Остановимся более подробно на связи p-блоков группы и её подгрупп.

Пусть P — произвольная p-подгруппа группы G. Положим $C = \mathrm{C}_G(P)$ и $N = \mathrm{N}_G(P)$. Определим F-линейное отображение $\beta_{_P} : \mathrm{Z}(FG) \to \mathrm{Z}(FN)$, положив для произвольного $K \in \mathscr{K}(G)$

$$\beta_{_P}(\widehat{K}) = \sum_{c \in K \cap C} c$$

и продолжив это отображение по линейности на $\mathrm{Z}(FG)$. Поскольку $K \cap C$ является объединением классов сопряжённости группы N, образ $\beta_{_P}$ действительно лежит в $\mathrm{Z}(FN)$.

(24.1) Предложение. *Для любой p-подгруппы P отображение $\beta_{_P} : \mathrm{Z}(FG) \to \mathrm{Z}(FN)$, где $N = \mathrm{N}_G(P)$, является гомоморфизмом F-алгебр.*

Доказательство. Достаточно проверить, что

(24.2)
$$\beta_{_P}(\widehat{K}\widehat{L}) = \beta_{_P}(\widehat{K})\beta_{_P}(\widehat{L})$$

для любых классов $K, L \in \mathscr{K}(G)$. Зафиксируем $c \in C = \mathrm{C}_G(P)$ и обозначим

$$\mathscr{A} = \{\, (x, y) \in K \times L \mid xy = c \,\},$$
$$\mathscr{A}_0 = \{\, (x, y) \in (K \cap C) \times (L \cap C) \mid xy = c \,\}.$$

Из правила умножения классовых сумм (3.7)(iv) следует, что коэффициенты при c в левой и правой частях соотношения (24.2) равны $|\mathscr{A}|^\star$ и $|\mathscr{A}_0|^\star$, соответственно.

Достаточно показать, что $|\mathscr{A}| \equiv |\mathscr{A}_0| \mod p$. Заметим, что P действует на множестве $\mathscr{A}$ по правилу $(x, y)^u = (x^u, y^u)$ для любого $u \in P$. Легко видеть, что $\mathscr{A}_0$ — это, в точности, множество неподвижных точек группы P относительно такого действия. Отсюда следует требуемое. $\square$

(24.3) Определение. Отображение β_P называется *гомоморфизм Брауэра.*

(24.4) Предложение. *Пусть P — p-подгруппа группы G, $C = \mathrm{C}_G(P)$ и $K \in \mathscr{K}(G)$. Следующие утверждения эквивалентны.*

(i) $\beta_{_P}(\widehat{K}) \neq 0$.

(ii) $K \cap C \neq \varnothing$.

(iii) $P \leqslant_G \delta(K)$.

✎ Доказать предложение (24.4).

Изучим ядро гомоморфизма Брауэра.

(24.5) Предложение. *Пусть P — p-подгруппа группы G.*

(i) *Выполнено равенство*

$$\mathrm{Ker}\,\beta_{_P} = \sum_{\substack{K \in \mathscr{K}(G),\\ P \nleqslant_G \delta(K)}} F\widehat{K}.$$

(ii) *Для произвольного $B \in \mathrm{Bl}(G)$ имеем $\beta_{_P}(e_{_B}) = 0$ тогда и только тогда, когда $P \nleqslant_G \delta(B)$.*

Доказательство. Положим $C = \mathrm{C}_G(P)$.

(i) Пусть элемент $z \in \mathrm{Z}(FG)$ лежит в $\mathrm{Ker}\,\beta_{_P}$. Запишем

$$z = \sum_{K \in \mathscr{K}(G)} a_{_K} \widehat{K},$$

где $a_{_K} \in F$. Поскольку для различных $K \in \mathscr{K}(G)$ множества $K \cap C$ попарно не пересекаются, равенство $\beta_{_P}(z) = 0$ возможно тогда и только тогда, когда $\beta_{_P}(\widehat{K}) = 0$ для всех K таких, что $a_{_K} \neq 0$. Поэтому требуемое следует из (24.4).

(ii) Запишем

$$e_{_B} = \sum_{K \in \mathscr{K}(G)} a_{_B}(K)\widehat{K}.$$

Из (i) следует, что $\beta_{_P}(e_{_B}) = 0$ тогда и только тогда, когда для любого класса $K \in \mathscr{K}(G)$ с условием $a_{_B}(K) \neq 0$ выполнено $P \nleqslant_G \delta(K)$.

Но если это так и $P \leqslant_G \delta(B)$, то взяв в качестве K дефектный класс блока B, получим с одной стороны $a_{_B}(K) \neq 0$, а с другой $P \leqslant_G \delta(K)$, т. к. $\Delta(B) = \Delta(K)$ в силу (22.11). Противоречие.

Обратно, если $P \nleqslant_G \delta(B)$ и $a_{_B}(K) \neq 0$, то $\delta(K) \leqslant_G \delta(B)$ в силу (22.10)(ii) и, значит, $P \nleqslant_G \delta(K)$. $\square$

Таким образом, из (24.5)(ii) мы получаем ещё одну характеризацию дефектных групп p-блоков.

(24.6) Следствие. *Пусть $B \in \mathrm{Bl}(G)$. Тогда $\Delta(B)$ состоит из максимальных по включению p-подгрупп P группы G, для которых $\beta_P(e_B) \neq 0$.*

Теперь определим операцию, в некотором смысле двойственную к гомоморфизму Брауэра. Эта двойственность станет более ясной чуть ниже, когда мы с формулируем первую основную теорему Брауэра.

Пусть $H \leqslant G$ и $b \in \mathrm{Bl}(H)$. Используя центральный гомоморфизм $\lambda_b : \mathrm{Z}(FH) \to F$, определим F-линейное отображение $\lambda_b^G : \mathrm{Z}(FG) \to F$, положив

$$\lambda_b^G(\widehat{K}) = \lambda_b\left(\sum_{x \in K \cap H} x\right)$$

для произвольного $K \in \mathscr{K}(G)$. Если λ_b^G является гомоморфизмом алгебр (что, вообще говоря, бывает не всегда), то в силу (21.1)(ii) существует единственный p-блок $B \in \mathrm{Bl}(G)$ такой, что $\lambda_b^G = \lambda_B$. В этом случае будем говорить, что определён *индуцированный p-блок* B и обозначать его через b^G.

(24.7) Доказать, что для любого $B \in \mathrm{Bl}(G)$ индуцированный блок B^G определён и совпадает с B.

Приведём пример, показывающий, что для блока b подгруппы H группы G индуцированный блок b^G может быть не определён. Отметим, что в этом примере блок b является главным и одновременно имеет нулевой дефект.

(24.8) Пример. Пусть $p = 2$, $G = S_3$, $H = A_3 \leqslant G$ и b — главный 2-блок (он же блок дефекта 0) группы H. Значения гомоморфизма λ_b на классовых суммах $\widehat{L}$, где $L \in \mathscr{K}(H)$ приведены в следующей таблице.

L	L_1	L_2	L_3
x_L	1	(123)	(132)
$\omega_{1_H}(\widehat{L}) = \lvert L\rvert$	1	1	1
$\lambda_b(\widehat{L}) = \lvert L\rvert^\star$	1	1	1

Легко найти значения отображения λ_b^G на классовых суммах $\widehat{K}$, где $K \in \mathscr{K}(G)$.

K	K_1	K_2	K_3
x_K	1	(12)	(123)
$\sum_{x \in K \cap H} x$	$\widehat{L}_1$	0	$\widehat{L}_2 + \widehat{L}_3$
$\lambda_b^G(\widehat{K})$	1	0	0

Группа G имеет два 2-блока, один из которых главный (обозначим его B_1), а другой (обозначим его B_2) имеет нулевой дефект (см. приложение В). Пусть $\mathrm{Irr}(B_2) = \{\chi\}$. Определим значения гомоморфизмов λ_{B_1} и λ_{B_2}.

K	K_1	K_2	K_3
$1_G(x_K)$	1	1	1
$\omega_{1_G}(\widehat{K}) = \lvert K\rvert$	1	3	2
$\lambda_{B_1}(\widehat{K}) = \lvert K\rvert^\star$	1	1	0
$\chi(x_K)$	2	0	-1
$\omega_\chi(\widehat{K})$	1	0	-1
$\lambda_{B_2}(\widehat{K})$	1	0	1

Как видно, λ_b^G не совпадает ни λ_{B_1}, ни с λ_{B_2}. Таким образом, блок b^G не определён.

(24.9) Предложение. *Пусть $b \in \mathrm{Bl}(H)$, где $H \leqslant G$, и предположим, что определён p-блок b^G. Тогда $\delta(b) \leqslant_G \delta(b^G)$.*

Доказательство. Пусть K — дефектный класс p-блока b^G. Тогда

$$0 \neq \lambda_{b^G}(\widehat{K}) = \lambda_b^G(\widehat{K}) = \lambda_b\left(\sum_{x \in K \cap H} x\right).$$

В частности, $K \cap H \neq \varnothing$ и существует класс $L \in \mathscr{K}(H)$ такой, что $L \subseteq K$ и $\lambda_b(\widehat{L}) \neq 0$. Из теоремы Min-Max (22.10)(i) следует, что $\delta(b) \leqslant_H \delta(L)$. Поскольку $\delta(L) \in \mathrm{Syl}_p(\mathrm{C}_H(x))$ для некоторого $x \in L \subseteq K$, имеем $\delta(L) \leqslant P$ для некоторой подгруппы $P \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Так как $P \in \Delta(K) = \Delta(b^G)$, получаем $\delta(b) \leqslant_H \delta(L) \leqslant_G \delta(b^G)$, т. е. $\delta(b) \leqslant_G \delta(b^G)$. $\square$

Гомоморфизм Брауэра можно использовать для получения достаточного условия существования индуцированных p-блоков.

(24.10) Предложение. *Пусть $P \leqslant G$ — p-подгруппа и $PC_G(P) \leqslant H \leqslant N_G(P)$. Тогда справедливы следующие утверждения.*

(*i*) *Образ гомоморфизма Брауэра β_P лежит в $Z(FH)$, и для любого $b \in Bl(H)$ диаграмма*

$$\begin{tikzcd} Z(FG) \arrow[d, "\beta_P"'] \arrow[dr, "\lambda_b^G"] & \\ Z(FH) \arrow[r, "\lambda_b"'] & F \end{tikzcd}$$

коммутативна. В частности, λ_b^G — гомоморфизм F-алгебр.

(*ii*) *Для любого $b \in Bl(H)$ определён индуцированный p-блок b^G.*

(*iii*) *Для любого $B \in Bl(G)$ имеет место равенство*

$$\beta_P(e_B) = \sum_{\substack{b\in Bl(H),\\ B=b^G}} e_b.$$

(*iv*) *Пусть $B \in Bl(G)$. Тогда $B = b^G$ для некоторого $b \in Bl(H)$ в том и только в том случае, когда $P \leqslant_G \delta(B)$.*

Доказательство. (*i*) Пусть $C = C_G(P)$. Так как H нормализует C, образ гомоморфизма Брауэра β_P действительно лежит в $Z(FH)$. Проверим, что $\lambda_b \circ \beta_P = \lambda_b^G$. Для этого достаточно показать, что

$$\lambda_b\left(\sum_{x\in K\cap H} x\right) = \lambda_b\left(\sum_{x\in K\cap C} x\right)$$

для всякого $K \in \mathscr{K}(G)$, т. е. что λ_b принимает нулевое значение на сумме элементов из множества $K\cap(H\setminus C)$, которое является объединением некоторых классов $L \in \mathscr{K}(H)$, не пересекающихся с C. Поскольку $P \trianglelefteqslant H$, имеем $C_H(O_p(H)) \leqslant C$, т. е. для каждого такого класса L сумма $\widehat{L}$ — нильпотентный элемент из FH в силу (22.12). Поэтому $\lambda_b(\widehat{L}) = 0$, откуда следует требуемое.

(*ii*) Это следует из (*i*), поскольку λ_b^G — гомоморфизм F-алгебр.

(*iii*) Пусть $B \in Bl(G)$. Рассмотрим значение $\beta_P(e_B)$. Поскольку β_P — гомоморфизм F-алгебр, элемент $\beta_P(e_B) \in Z(FH)$ является идемпотентом. В силу (21.1)(*viii*) можно записать

(24.11) $$\beta_P(e_B) = e_{b_1} + \ldots + e_{b_k}$$

для некоторых различных $b_1, \ldots, b_k \in Bl(H)$. Заметим, что ввиду (*i*) равенство $B = b^G$ для некоторого $b \in Bl(H)$ имеет место тогда и только тогда, когда гомоморфизм F-алгебр $\lambda_b \circ \beta_P : Z(FG) \to F$ совпадает с λ_B, т. е. когда значение $\lambda_b \circ \beta_P$ на e_B равно 1. В силу (24.11) это выполнено тогда и только тогда, когда b совпадает в одним из b_i. Отсюда получаем требуемое.

(*iv*) Пусть $B \in Bl(G)$.

Если $B = b^G$ для некоторого $b \in Bl(H)$, то из (24.9) следует, что $\delta(b) \leqslant_G \delta(B)$, а из (22.13) получаем, что $P \leqslant O_p(H) \leqslant \delta(B)$. Поэтому $P \leqslant_G \delta(B)$.

Обратно, предположим, что $P \leqslant_G \delta(B)$. Тогда $\beta_P(e_B) \neq 0$ ввиду (24.5)(*ii*). Из (*iii*) вытекает, что существует $b \in Bl(H)$ для которого $B = b^G$. ☐

(24.12) Следствие. *Пусть блок $B \in Bl(G)$ такой, что $\delta(B)$ — нормальная подгруппа группы G. Тогда*

$$e_B = \sum_{\substack{K\in\mathscr{K}(G_{p'}),\\ \Delta(K)=\Delta(B)}} a_B(K)\widehat{K}.$$

Доказательство. Напомним, что имеет место представление

(24.13) $$e_B = \sum_{K\in\mathscr{K}(G_{p'})} a_B(K)\widehat{K},$$

см. (22.8). В силу нормальности $\delta(B)$ множество $\Delta(B)$ одноэлементно. Поэтому достаточно доказать, что если $a_B(K) \neq 0$, то $\delta(K) = \delta(B)$. Из теоремы Min-Max (22.10) следует, что если $a_B(K) \neq 0$, то $\delta(K) \leqslant \delta(B)$.

Для доказательства обратного включения применим предложение (24.10), положив $P = \delta(B)$ и $H = G$. Тогда, ввиду того, что $B = B^G$, из (24.10)(*iii*) следует равенство $\beta_P(e_B) = e_B$. Применив гомоморфизм Брауэра β_P к обеим частям соотношения (24.13), получим

$$\beta_P(e_B) = \sum_{K \in \mathscr{K}(G_{p'})} a_B(K)\beta_P(\widehat{K}).$$

Поскольку для любого K значение $\beta_P(\widehat{K})$ является суммой некоторых различных элементов из K, в силу линейной независимости получаем, что равенство $\beta_P(e_B) = e_B$ возможно лишь тогда, когда $\beta_P(\widehat{K}) = \widehat{K}$ для всех K таких, что $a_B(K) \neq 0$. В частности, если $a_B(K) \neq 0$, то $K \cap C \neq \varnothing$, где $C = \mathrm{C}_G(\delta(B))$ и, значит, $\delta(B) \leqslant \delta(K)$, что и требовалось доказать. ☐

Для доказательства ещё одного достаточного условия существования индуцированного блока нам потребуется следующее утверждение.

(24.14) Предложение. *Пусть $H \leqslant N \leqslant G$ и $b \in \mathrm{Bl}(H)$. Пусть определён индуцированный блок $b^N \in \mathrm{Bl}(N)$. Тогда блок b^G определён если и только если определён блок $(b^N)^G$, и в этом случае $b^G = (b^N)^G$.*

✎ Доказать предложение (24.14).

(24.15) Предложение. *Пусть $H \leqslant G$ и $b \in \mathrm{Bl}(H)$. Если $\mathrm{C}_G(\delta(b)) \leqslant H$, то определён индуцированный блок b^G.*

Доказательство. Пусть $P = \delta(b)$ и $T = P\mathrm{C}_G(P)$. По условию имеем $T \leqslant H$. Из (24.10)(*iv*) вытекает, что существует блок $b_0 \in \mathrm{Bl}(T)$ такой, что $b_0^H = b$. С другой стороны, в силу (24.10)(*ii*) индуцированный блок b_0^G определён. По (24.14) получаем, что блок $b^G = (b_0^H)^G$ определён и совпадает с b_0^G. ☐

Как легко видеть, условие существования индуцированного блока b^G, приведённое в (24.15), не зависит от выбора дефектной группы $\delta(b)$. Также отметим, что (24.10)(*ii*) является следствием (24.15), так как если $P\mathrm{C}_G(P) \leqslant H \leqslant \mathrm{N}_G(P)$, то для любого блока $b \in \mathrm{Bl}(H)$ выполнено включение $\mathrm{C}_G(\delta(b)) \leqslant H$, поскольку P содержится в $\delta(b)$ ввиду (22.13).

Пусть P — p-подгруппа группы G. Введём следующие обозначения

$$\mathscr{K}(G|P) = \{K \in \mathscr{K}(G) \mid P \in \Delta(K)\},$$
$$\mathrm{Bl}(G|P) = \{B \in \mathrm{Bl}(G) \mid P \in \Delta(B)\}.$$

(24.16) Предложение. *Пусть P — p-подгруппа группы G. Положим $C = \mathrm{C}_G(P)$, $N = \mathrm{N}_G(P)$. Тогда отображение $K \mapsto K \cap C$ осуществляет биекцию множеств $\mathscr{K}(G|P) \to \mathscr{K}(N|P)$.*

Доказательство. Пусть $K \in \mathscr{K}(G|P)$ и $P \in \mathrm{Syl}_p(\mathrm{C}_G(x))$ для подходящего $x \in K$. Тогда $x \in K \cap C$. Пусть $y \in K \cap C$. Тогда $P \in \mathrm{Syl}_p(\mathrm{C}_G(y))$, и поскольку $y = x^g$ для некоторого $g \in G$, также имеем $P^g \in \mathrm{Syl}_p(\mathrm{C}_G(y))$. Значит, $P = P^{gc}$ для некоторого $c \in \mathrm{C}_G(y)$. Тогда $x^{gc} = y^c = y$, т. е. x и y сопряжены элементом из N. Таким образом, $K \cap C \in \mathscr{K}(N)$. Очевидно также, что $P \in \Delta(K \cap C)$ и что отображение $K \mapsto K \cap C$ инъективно.

Докажем сюръективность. Пусть $L \in \mathscr{K}(N|P)$ и $K \in \mathscr{K}(G)$ — класс, содержащий L. Проверим, что $P \in \Delta(K)$. Пусть $x \in L$ — элемент, для которого $P \in \mathrm{Syl}_p(\mathrm{C}_N(x))$ и пусть $P \leqslant S \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Если $P < S$, то из условия $N = \mathrm{N}_G(P)$ и того, что S — p-группа следует, что $P < \mathrm{N}_S(P) = S \cap N \leqslant \mathrm{C}_N(x)$. Это противоречит тому, что $P \in \Delta(L)$. Значит, $P = S$ и $P \in \Delta(K)$. ☐

(24.17) Теорема (Первая основная теорема Брауэра). *Пусть P — p-подгруппа группы G и $N = \mathrm{N}_G(P)$.*

(*i*) *Отображение $b \mapsto b^G$ является биекцией множеств $\mathrm{Bl}(N|P) \to \mathrm{Bl}(G|P)$.*

(*ii*) *Для любого $b \in \mathrm{Bl}(N|P)$ имеем $\beta_P(e_B) = e_b$, где $B = b^G$.*

Доказательство. Обозначим $C = \mathrm{C}_G(P)$.

Сначала покажем, что образ отображения $b \mapsto b^G$, где $b \in \mathrm{Bl}(N|P)$ действительно лежит в $\mathrm{Bl}(G|P)$. Пусть $b \in \mathrm{Bl}(N|P)$. В силу (24.10) определён индуцированный p-блок $B = b^G$ и $\lambda_b \circ \beta_P = \lambda_B$. Требуется проверить, что $B \in \mathrm{Bl}(G|P)$. Пусть L — дефектный класс p-блока b. Тогда $L \in \mathscr{K}(N|P)$ ввиду (22.11). Пусть $K \in \mathscr{K}(G)$ — класс, содержащий L. Из (24.16) следует, что $K \in \mathscr{K}(G|P)$ и $L = K \cap C$. Поэтому

$$\lambda_B(\widehat{K}) = \lambda_b(\beta_P(\widehat{K})) = \lambda_b(\widehat{L}) \neq 0.$$

По теореме Min-Max (22.10)(*i*) получаем $\delta(B) \leqslant_G P$. С другой стороны, из (24.9) следует, что $P \leqslant_G \delta(B)$. Поэтому $P \in \Delta(B)$.

Теперь проверим, что отображение $b \mapsto b^G$ сюръективно. Пусть $B \in \mathrm{Bl}(G|P)$. Из (24.10)(iii) следует, что существуют p-блоки $b_1, \ldots, b_k \in \mathrm{Bl}(N)$ такие, что $b_i^G = B$ и

$$\beta_P(e_B) = e_{b_1} + \ldots + e_{b_k}.$$

Так как $P \trianglelefteqslant N$, из (22.13) вытекает, что $P \leqslant \delta(b_i)$ для всех $i = 1, \ldots, k$. Из (24.9) также получаем $\delta(b_i) \leqslant_G \delta(B) = P$ для всех $i = 1, \ldots, k$. Отсюда следует, что $P \in \Delta(b_i)$, и тем самым сюръективность отображения $b \mapsto b^G$ доказана. Более того, если докажем инъективность, то получим, что $k = 1$, т. е. выполнено (ii).

Допустим, что $b_1^G = B = b_2^G$ для некоторых $b_1, b_2 \in \mathrm{Bl}(N|P)$. Тогда $\lambda_{b_1} \circ \beta_P = \lambda_B = \lambda_{b_2} \circ \beta_P$ в силу (24.10)(i). Таким образом, для любого $K \in \mathscr{K}(G)$ имеем $\lambda_{b_1}(\widehat{L}) = \lambda_{b_2}(\widehat{L})$, где $L = K \cap C$. В частности, из (24.16) вытекает, что значения λ_{b_1} и λ_{b_2} совпадают на классовых суммах для всех классов из $\mathscr{K}(N|P)$. Из соотношения (22.6) получаем

(24.18)
$$\begin{aligned} 1 = \quad \lambda_{b_1}(e_{b_1}) &= \sum_{L \in \mathscr{K}(N)} a_{b_1}(L)\lambda_{b_1}(\widehat{L}) = \sum_{L \in \mathscr{K}(N|P)} a_{b_1}(L)\lambda_{b_1}(\widehat{L}), \\ \lambda_{b_2}(e_{b_1}) &= \sum_{L \in \mathscr{K}(N)} a_{b_1}(L)\lambda_{b_2}(\widehat{L}) = \sum_{L \in \mathscr{K}(N|P)} a_{b_1}(L)\lambda_{b_2}(\widehat{L}), \end{aligned}$$

где последние равенства в каждой цепочке выполнены, поскольку ввиду теоремы Min-Max (22.10) произведение $a_{b_1}(L)\lambda_{b_i}(\widehat{L})$, $i = 1, 2$, ненулевое только если $\delta(L) \leqslant_G P$ и $P \leqslant_G \delta(L)$, т. е. если $L \in \mathscr{K}(N|P)$. Из сделанных выше замечаний вытекает, что правые части в (24.18) совпадают. Поэтому $\lambda_{b_2}(e_{b_1}) = 1$ и $b_1 = b_2$ в силу (21.1)(ii). □

Говорят, что подгруппа P группы G является *радикальной p-подгруппой*, если $P = \mathrm{O}_p(\mathrm{N}_G(P))$.

В качестве одного из следствий теоремы (24.17) мы получаем следующее усиление утверждения (22.13), дающее необходимое условие для того, чтобы p-подгруппа была дефектной группой некоторого p-блока.

(24.19) Следствие. *Для любого $B \in \mathrm{Bl}(G)$ дефектная группа $\delta(B)$ является радикальной p-подгруппой.*

✎ **(24.20)** Доказать следствие (24.19).

Пусть $B \in \mathrm{Bl}(G)$, Говорят, что p-вес (P, χ) группы G *принадлежит* блоку B, если $B = b^G$, где $b \in \mathrm{Bl}(\mathrm{N}_G(P))$ и $\chi \in \mathrm{Irr}(b)$.

✎ **(24.21)** Доказать следующие утверждения.

(i) Если (P, χ) — p-вес, принадлежащий блоку B, то $P \in \Delta(B)$. В частности, P — радикальная p-подгруппа.

(ii) Сопряжённые p-веса принадлежат одному блоку.

Гипотеза Альперина о весах (23.4) в уточнённой формулировке звучит следующим образом.

(24.22) Гипотеза (Альперина о весах, блочная версия). *Число классов сопряжённости p-весов группы G, принадлежащих блоку $B \in \mathrm{Bl}(G)$, совпадает с $|\,\mathrm{IBr}(B)|$.*

Отметим, что имеется ряд усилений гипотезы Альперина, принадлежащих различным авторам. Одно из наиболее общих — гипотеза Дэйда — в настоящее время интенсивно изучается, см. [9]. Её доказательство сведено к случаю простых групп.

25. Теоремы Робинсона и Грина

В этом разделе мы изложим важные результаты Робинсона о числе блоков с данной дефектной группой, которые затем применим для доказательства теоремы Грина о свойстве дефектных групп.

Определим *отображение Робинсона* $\varrho : \mathrm{Z}(FG) \to \mathrm{Z}(FG)$ по правилу

$$\varrho(x) = \sum_{B \in \mathrm{Bl}(G)} \lambda_B(x) e_B$$

(25.1) Предложение. *Имеют место следующие утверждения.*

(i) *ϱ является эндоморфизмом F-алгебры $\mathrm{Z}(FG)$.*

(ii) *$\varrho(e_B) = e_B$ для любого $B \in \mathrm{Bl}(G)$.*

(iii) *$\varrho^2 = \varrho$.*

(iv) $\operatorname{Ker}\varrho = \mathrm{J}(\mathrm{Z}(FG))$.

✎ Доказать предложение (25.1).

Рассмотрим действие ϱ на классовых суммах. Пусть $L \in \mathscr{K}(G)$. Тогда

$$\varrho(\widehat{L}) = \sum_{B\in \mathrm{Bl}(G)} \lambda_B(\widehat{L})e_B = \sum_{B\in \mathrm{Bl}(G)} \lambda_B(\widehat{L}) \left(\sum_{K\in\mathscr{K}(G)} a_B(K)\widehat{K}\right) = \sum_{K\in\mathscr{K}(G)} \left(\sum_{B\in \mathrm{Bl}(G)} \lambda_B(\widehat{L})a_B(K)\right)\widehat{K}.$$

Таким образом, матрица отображения ϱ в базисе из классовых сумм равна

$$\left(\sum_{B\in \mathrm{Bl}(G)} \lambda_B(\widehat{L})a_B(K)\right)_{K,L\in\mathscr{K}(G)}.$$

Наша ближайшая цель — найти удобную формулу для вычисления сумм вида

$$\sum_{B\in \mathrm{Bl}(G)} \lambda_B(\widehat{L})a_B(K),$$

где $K, L \in \mathscr{K}(G)$.

Пусть $P \in \mathrm{Syl}_p(G)$. Для $K, L \in \mathscr{K}(G)$ положим

(25.2) $$\mathscr{A}_{K,L} = \{(x, y) \in K \times L \mid Px = Py\}.$$

(25.3) Предложение. *Пусть $K, L \in \mathscr{K}(G)$.*

(i) $|\mathscr{A}_{K,L}| = |\mathscr{A}_{L,K}|$ *и эта величина не зависит от выбора $P \in \mathrm{Syl}_p(G)$ в определении (25.2).*

(ii) $\dfrac{|\mathscr{A}_{K,L}|}{|K|} \in \widetilde{\boldsymbol{R}}$.

(iii) *Если $K \in \mathscr{K}(G_{p'})$, то*

$$\sum_{B\in \mathrm{Bl}(G)} \lambda_B(\widehat{L})a_B(K) = \left(\frac{|\mathscr{A}_{K,L}|}{|K|}\right)^{\star}$$

Доказательство. Утверждение (i) напрямую следует из определения и сопряжённости силовских подгрупп.

Из (16.31) вытекает, что для фиксированного $z \in G$

$$\big|\{(x, y) \in K \times L \mid xy = z\}\big| = \frac{|K|\,|L|}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(x_K)\chi(x_L)\overline{\chi(z)}}{\chi(1)}.$$

Обозначим $K^{-1} = (x_K^{-1})^G = \{y^{-1} \mid y \in K\}$. Тогда $|K| = |K^{-1}|$ и

$$\begin{aligned}|\mathscr{A}_{K,L}| &= \sum_{z\in P} \big|\{(x, y) \in K \times L \mid yx^{-1} = z\}\big| = \sum_{z\in P} \big|\{(x, y) \in K^{-1} \times L \mid yx = z\}\big| \\ &= \sum_{z\in P} \frac{|K^{-1}|\,|L|}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \frac{\overline{\chi(x_K)}\chi(x_L)\overline{\chi(z)}}{\chi(1)} = \frac{|K|\,|L|}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \left(\sum_{z\in P} \overline{\chi(z)}\right) \frac{\overline{\chi(x_K)}\chi(x_L)}{\chi(1)} \\ &= \frac{|K|}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} |P|(1_P, \chi_P)_P\overline{\chi(x_K)}\ \frac{|L|\chi(x_L)}{\chi(1)}.\end{aligned}$$

Поэтому

(25.4) $$\frac{|\mathscr{A}_{K,L}|}{|K|} = \frac{|P|}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} (\chi_P, 1_P)_P\overline{\chi(x_K)}\omega_\chi(\widehat{L}).$$

Поскольку $\omega_\chi(\widehat{L}), \chi(x_K) \in \boldsymbol{R}$, $(\chi_P, 1_P)_P \in \mathbb{Z}$, $|P|/|G| \in \widetilde{\boldsymbol{R}}$, отсюда следует ($ii$).

Применив $\star$ к обеим частям равенства (25.4), получим

$$\begin{aligned}\left(\frac{|\mathscr{A}_{K,L}|}{|K|}\right)^{\star} &= \left(\frac{|P|}{|G|}\right)^{\star} \sum_{B\in \mathrm{Bl}(G)} \left(\sum_{\chi\in \mathrm{Irr}(B)} (\chi_P, 1_P)_P \overline{\chi(x_K)}\right)^{\star} \lambda_B(\widehat{L}) \\ &= \sum_{B\in \mathrm{Bl}(G)} \left(\frac{1}{|G|} \sum_{\chi\in \mathrm{Irr}(B)} |P|(\chi_P, 1_P)_P \overline{\chi(x_K)}\right)^{\star} \lambda_B(\widehat{L}).\end{aligned}$$

Предположим теперь, что $K \in \mathscr{K}(G_{p'})$. Из (20.14) следует, что

$$\sum_{\chi\in \mathrm{Irr}(B)} |P|(\chi_P, 1_P)_P \overline{\chi(x_K)} = \sum_{z\in P} \sum_{\chi\in \mathrm{Irr}(B)} \chi(z)\overline{\chi(x_K)} = \sum_{\chi\in \mathrm{Irr}(B)} \chi(1)\overline{\chi(x_K)}.$$

Поэтому, в силу (22.7) получаем, что

$$\left(\frac{|\mathscr{A}_{K,L}|}{|K|}\right)^{\star} = \sum_{B\in \mathrm{Bl}(G)} \left(\frac{1}{|G|} \sum_{\chi\in \mathrm{Irr}(B)} \chi(1)\overline{\chi(x_K)}\right)^{\star} \lambda_B(\widehat{L}) = \sum_{B\in \mathrm{Bl}(G)} a_B(K)\lambda_B(\widehat{L}).$$

$\square$

Из (25.3)(ii) вытекает следующее утверждение.

(25.5) Следствие. *Пусть* $|G|_p = p^a$, $K \in \mathscr{K}(G)$, $|\delta(K)| = p^d$. *Тогда* $\dfrac{|\mathscr{A}_{K,L}|}{p^{a-d}} \in \mathbb{Z}$ *для любого* $L \in \mathscr{K}(G)$.

Для произвольной p-подгруппы P группы G по аналогии с введённым ранее обозначением $\mathscr{K}(G|P)$ положим

$$\mathscr{K}(G_{p'}|P) = \bigl\{K \in \mathscr{K}(G_{p'}) \bigm| P \in \Delta(K)\bigr\}.$$

Пусть D — нормальная p-подгруппа группы G. Запишем $|G|_p = p^a$, $|D| = p^d$. Определим

$$A(D) = \left(\frac{|\mathscr{A}_{K,L}|}{p^{a-d}}\right)_{K,L\in \mathscr{K}(G_{p'}|D)}.$$

Ввиду (25.5) и (25.3)(i) матрица $A(D)$ является целочисленной и симметрической. Отметим, что в случае, когда D не является дефектной группой никакого p-регулярного класса, матрица $A(D)$ является пустой.

Теперь мы можем приступить к определению числа блоков группы G с данной дефектной группой D. Отметим, что в силу первой основой теоремы Брауэра можно считать, что подгруппа D нормальна в G.

(25.6) Теорема (Робинсона). *Пусть D — нормальная p-подгруппа группы G. Тогда число p-блоков с дефектной группой D равно рангу матрицы* $A(D)^{\star}$.

Доказательство. Пусть U обозначает F-линейную оболочку классовых сумм $\bigl\{\widehat{L} \bigm| L \in \mathscr{K}(G_{p'}|D)\bigr\}$. Покажем, что $\varrho(U) \subseteq U$. Если $L \in \mathscr{K}(G_{p'}|D)$ и $\lambda_B(\widehat{L}) \neq 0$ для некоторого $B \in \mathrm{Bl}(G)$, то из теоремы Min-Max (22.10) вытекает, что $\delta(B) \leqslant D$. Поскольку $D \leqslant \mathrm{O}_p(G)$ и $\mathrm{O}_p(G)$ содержится в дефектной группе любого блока группы G, отсюда следует, что $D = \delta(B)$. Значит, если $B \notin \mathrm{Bl}(G|D)$, то $\lambda_B(\widehat{L}) = 0$. Поэтому для $L \in \mathscr{K}(G_{p'}|D)$ имеем

(25.7) $$\varrho(\widehat{L}) = \sum_{B\in \mathrm{Bl}(G)} \lambda_B(\widehat{L})e_B = \sum_{B\in \mathrm{Bl}(G|D)} \lambda_B(\widehat{L})e_B.$$

В силу (24.12) для любого $B \in \mathrm{Bl}(G|D)$ имеет место равенство

(25.8) $$e_B = \sum_{K\in \mathscr{K}(G_{p'}|D)} a_B(K)\widehat{K}.$$

Поэтому

$$\varrho(\widehat{L}) = \sum_{K\in \mathscr{K}(G_{p'}|D)} \left(\sum_{B\in \mathrm{Bl}(G|D)} \lambda_B(\widehat{L})a_B(K)\right) \widehat{K}$$

и, значит, $\varrho(U) \subseteq U$.

Заметим, что ранг F-линейного отображения $\varrho_U : U \to U$ совпадает с $|\operatorname{Bl}(G|D)|$. Это следует из того, что идемпотенты $\{\, e_B \mid B \in \operatorname{Bl}(G|D) \,\}$ образуют базис образа $\varrho(U)$: они линейно независимы, каждый из них лежит в образе $\varrho(U)$ по (25.1)(ii) и (25.8), и образ $\varrho(U)$ содержится в их линейной оболочке в силу (25.7).

С другой стороны ранг отображения ϱ_U совпадает с рангом его матрицы, которая в базисе из классовых сумм $\{\, \widehat{K} \mid K \in \mathscr{K}(G_{p'}|D) \,\}$ равна

$$\left(\sum_{B \in \operatorname{Bl}(G|D)} \lambda_B(\widehat{L}) a_B(K) \right)_{L,K \in \mathscr{K}(G_{p'}|D)}.$$

Как было отмечено выше, $\lambda_B(\widehat{L}) = 0$ при $B \notin \operatorname{Bl}(G|D)$, поэтому суммирование можно распространить на все блоки, т. е. ранг ϱ_U равен рангу матрицы

$$\left(\sum_{B \in \operatorname{Bl}(G)} \lambda_B(\widehat{L}) a_B(K) \right)_{L,K \in \mathscr{K}(G_{p'}|D)} = \left(\frac{|\mathscr{A}_{K,L}|}{|K|} \right)^{\star}_{L,K \in \mathscr{K}(G_{p'}|D)}$$

по (25.3)(iii), которая, как легко видеть, отличается от матрицы $A(D)^{\star}$ транспонированием и умножением на невырожденную диагональную матрицу с диагональными элементами $\left(\dfrac{1}{|K|_{p'}} \right)^{\star}$ по всем $K \in \mathscr{K}(G_{p'}|D)$. Из этих рассуждений следует, что число $|\operatorname{Bl}(G|D)|$ равно рангу матрицы $A(D)^{\star}$. □

✎ **(25.9)** Пусть $P \in \operatorname{Syl}_p(G)$. Показать, что
(i) если $P \trianglelefteqslant G$, то $|\operatorname{Bl}(G)| = \big|\{K \in \mathscr{K}(G_{p'}) \mid K \subseteq \mathrm{C}_G(P)\}\big|$;
(ii) $\big|\operatorname{Bl}(G|P)\big| = \big|\{K \in \mathscr{K}(G_{p'}) \mid K \cap \mathrm{C}_G(P) \neq \varnothing\}\big|$.

Напомним, что через $\mathrm{O}_{p'}(G)$ обозначается наибольшая нормальная p'-подгруппа группы G.

✎ **(25.10)** Пусть G — p-разрешимая группа и $\mathrm{O}_{p'}(G) = 1$. Доказать, что $|\operatorname{Bl}(G)|$=1. (*Указание.* Использовать тот факт, что $\mathrm{C}_G(\mathrm{O}_p(G)) \leqslant \mathrm{O}_p(G)$.)

Подгруппой Фраттини $\operatorname{Fr}(G)$ группы G называется пересечение всех её максимальных подгрупп.[26] В случае, когда G — p-группа, $\operatorname{Fr}(G)$ совпадает с наименьшей нормальной подгруппой, факторгруппа по которой элементарная абелева.

Следующее упражнение показывает, что нахождение числа p-блоков группы G с нормальной дефектной группой D сводится к случаю, когда D элементарная абелева.

✎ **(25.11)** Пусть D — нормальная p-подгруппа группы G. Показать, что

$$|\operatorname{Bl}(G|D)| = \big|\operatorname{Bl}\big(G/\operatorname{Fr}(D) \mid D/\operatorname{Fr}(D)\big)\big|.$$

(*Указание.* Воспользоваться тем, что если p-регулярный элемент x действует тождественно на факторах нормального ряда p-группы P или на факторгруппе $P/\operatorname{Fr}(P)$, то x действует тождественно на P.)

(25.12) Теорема (Грина). *Пусть D — дефектная группа некоторого блока группы G и P — p-силовская подгруппа, содержащая D. Тогда существует p-регулярный элемент $x \in G$ такой, что $D \in \Delta(x^G)$ и $P \cap P^x = D$.*

Доказательство. Пусть $|D| = p^d$ и $|P| = p^a$.

Сначала мы докажем утверждение в случае, когда $D \trianglelefteqslant G$. По условию $|\operatorname{Bl}(G|D)| > 0$ и из теоремы Робинсона (25.6) следует, что существуют $K, L \in \{G_{p'}|D\}$ такие, что

$$\frac{|\mathscr{A}_{K,L}|}{p^{a-d}} \not\equiv 0 \mod p.$$

Обозначим $T = \{Pg \mid g \in G\}$. Тогда

$$\mathscr{A}_{K,L} = \{(y,z) \in K \times L \mid Py = Pz\} = \bigcup_{Pg \in T} (Pg \cap K) \times (Pg \cap L),$$

[26] Обычно подгруппа Фраттини обозначается символом $\Phi(G)$, однако мы используем его для таблицы модулярных характеров.

и значит,

$$|\mathscr{A}_{K,L}| = \sum_{Pg\in T} |Pg\cap K||Pg\cap L|.$$

Заметим, что P действует на множестве T правыми умножениями. Рассмотрим мощность орбиты класса $Pg\in T$ относительно этого действия. Поскольку для $u\in P$ равенство $Pgu = Pg$ выполнено тогда и только тогда, когда $u\in P^g$, мощность орбиты класса Pg равна $|P:\,P\cap P^g|$.

Заметим также, что для $u\in P$ справедливы равенства

(25.13) $$(Pg\cap K)^u = (Pg)^u\cap K^u = Pgu\cap K,$$

и значит, $|Pg\cap K| = |Pgu\cap K|$. Аналогично, $|Pg\cap L| = |Pgu\cap L|$.

Обозначим через $\mathscr{O}$ набор представителей орбит множества T относительно действия подгруппы P правыми умножениями. Тогда из сделанных замечаний получаем

$$|\mathscr{A}_{K,L}| = \sum_{Pg\in\mathscr{O}} |P:\,P\cap P^g||Pg\cap K||Pg\cap L|.$$

Поскольку, как мы заметили, подгруппа $P\cap P^g$, действуя правыми умножениями, оставляет неподвижным смежный класс Pg, из (25.13) следует, что она же, действуя сопряжением, оставляет неподвижным пересечение $Pg\cap K$. При этом мощность орбиты произвольного элемента $x\in Pg\cap K$ равна $|P\cap P^g:\mathrm{C}_{P\cap P^g}(x)|$. В силу того, что $D\in\Delta(K)$ и $D\trianglelefteq G$, справедливо включение $\mathrm{C}_{P\cap P^g}(x)\leqslant D$. Однако, $D\leqslant P$ и $D\leqslant \mathrm{C}_G(x)$, поэтому справедливо и обратное включение, т. е. $\mathrm{C}_{P\cap P^g}(x) = D$.

Отсюда следует, что $|P\cap P^g:D|$ делит $|Pg\cap K|$ и, аналогично, $|Pg\cap L|$. А поскольку

$$p^{a-d} = |P:D| = |P:P\cap P^g||P\cap P^g:D|,$$

число

$$\frac{|P:\,P\cap P^g||Pg\cap K||Pg\cap L|}{p^{a-d}}$$

делится на $|P\cap P^g:D|$. Итак, ввиду того, что

$$\frac{|\mathscr{A}_{K,L}|}{p^{a-d}} = \sum_{Pg\in\mathscr{O}} \frac{|P:\,P\cap P^g||Pg\cap K||Pg\cap L|}{p^{a-d}} \not\equiv 0 \mod p,$$

должен существовать $g\in G$, для которого $Pg\in\mathscr{O}$, $|P\cap P^g:D| = 1$ и $|Pg\cap K|\neq 0$. Пусть $x\in Pg\cap K$. Тогда $P\cap P^x = P\cap P^g = D$, $D\in\Delta(x^G)$, и значит, x — искомый p-регулярный элемент.

Теперь рассмотрим общий случай. Обозначим $N = \mathrm{N}_G(D)$. Выберем $S\in\mathrm{Syl}_p(N)$ так, чтобы $P\cap N\leqslant S$. Из первой основной теоремы Брауэра (24.17) следует, что D является дефектной группой некоторого блока группы N. Поэтому из доказанного выше следует, что существует p-регулярный элемент $x\in N$ такой, что $D\in\Delta(x^N)$ и $S\cap S^x = D$. В силу (24.16), справедливо равенство $x^N = x^G\cap C$, где $C = \mathrm{C}_G(D)$, причём $D\in\Delta(x^G)$.

Осталось показать, что $P\cap P^x = D$. По условию имеем $D\leqslant P$. Поскольку $x\in N$, также имеем $D\leqslant P^x$, т. е. $D\leqslant P\cap P^x$. Допустим, что $D < P\cap P^x$. Тогда по известному свойству p-групп

$$D < \mathrm{N}_{P\cap P^x}(D) = P\cap P^x\cap N = (P\cap N)\cap(P\cap N)^x \leqslant S\cap S^x.$$

Это противоречие завершает доказательство теоремы. □

26. Высшие числа разложения. Вторая основная теорема Брауэра

Прежде, чем определять высшие числа разложения и формулировать теорему Брауэра, докажем ряд технических утверждений.

Напомним, что для любого $B\in\mathrm{Bl}(G)$ элемент f_B является идемпотентом алгебры $\mathrm{Z}(\widetilde{\boldsymbol{R}}G)$, см. (20.18)(*ii*). Кроме того, как мы уже отмечали, отображение отображение $^\star:\widetilde{\boldsymbol{R}}\to F$ можно естественно поднять до эпиморфизма колец $\mathrm{Z}(\widetilde{\boldsymbol{R}}G)\to\mathrm{Z}(FG)$, также обозначаемого через *.

(26.1) Предложение. *Пусть $B\in\mathrm{Bl}(G)$ и $x\in\mathrm{Z}(\widetilde{\boldsymbol{R}}G)$. Если $\lambda_B(x^\star) = 1$, то существует $y\in f_B\mathrm{Z}(\widetilde{\boldsymbol{R}}G)$ такой, что $xy = f_B$.*

Доказательство. Предположим сначала, что x лежит в кольце $f_B \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$. Тогда требуется показать, что x обратим в этом кольце. Имеем $f_B x = x$ и, значит, $e_B x^\star = x^\star$. Поэтому в силу (21.1)(iii)

$$\lambda_{B'}(x^\star - e_B) = \lambda_{B'}(x^\star) = \lambda_{B'}(e_B x^\star) = 0$$

для всех блоков $B' \neq B$. Кроме того $\lambda_B(x^\star - e_B) = 1 - 1 = 0$ по условию. Из (21.1)(vi) следует, что элемент $e_B - x^\star$, лежащий в $e_B \mathrm{Z}(FG)$, является нильпотентным. В силу (4.12) и (4.7) элемент $x^\star$ обратим в кольце $e_B \mathrm{Z}(FG)$. Значит, существует $u \in f_B \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$ такой, что

$$(xu)^\star = e_B = f_B^\star.$$

Поэтому мы можем применить утверждение (4.17) к гомоморфизму коммутативных колец $^\star : \widetilde{\boldsymbol{R}} \to F$, идемпотенту $f_B \in \widetilde{\boldsymbol{R}}G$ и элементу $xu \in f_B \mathrm{Z}(\widetilde{\boldsymbol{R}}G) \leqslant f_B \widetilde{\boldsymbol{R}}G$ (т. к. мы отмечали, что ядро отображения $^\star : \widetilde{\boldsymbol{R}} \to F$ совпадает с $\mathrm{J}(\widetilde{\boldsymbol{R}}) = \widetilde{M}$). Из (4.17) следует, что существует $v \in f_B \widetilde{\boldsymbol{R}}G$ для которого $xuv = f_B$. Таким образом, uv — обратный к x в кольце $\widetilde{\boldsymbol{R}}G$. Имеем $x \in f_B \mathrm{Z}(\widetilde{\boldsymbol{R}}G) = \mathrm{Z}(f_B \widetilde{\boldsymbol{R}}G)$ в силу (20.21)(ii). Поэтому x обратим в $\mathrm{Z}(f_B \widetilde{\boldsymbol{R}}G)$ по (2.9)(i) и, значит, $uv \in f_B \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$, что и требовалось доказать.

Теперь рассмотрим общий случай. Пусть $x \in \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$ удовлетворяет условию. Тогда $f_B x \in f_B \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$ и

$$\lambda_B\big((f_B x)^\star\big) = \lambda_B(e_B)\lambda_B(x^\star) = 1.$$

По доказанному выше существует $y \in f_B \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$ такой, что $f_B xy = f_B$, и, значит, $f_B y$ — искомый элемент из $f_B \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$. □

Пусть R — коммутативное кольцо. *Носителем* $\operatorname{supp} x$ элемента

$$x = \sum_{g \in G} a_g g, \quad a_g \in R$$

групповой алгебры RG называется подмножество $\{g \in G \mid a_g \neq 0\}$ группы G.

(26.2) Предложение. *Пусть $b \in \mathrm{Bl}(H)$, где $H \leqslant G$, и предположим, что определён p-блок $B = b^G \in \mathrm{Bl}(G)$. Тогда справедливы следующие утверждения.*

- (i) *Существует элемент $w \in f_b \widetilde{\boldsymbol{R}}G f_b$, для которого*
  - $(i.1)$ $\operatorname{supp} w \subseteq G \setminus H$;
  - $(i.2)$ *H централизует w;*
  - $(i.3)$ $(1 - f_B) f_b = (1 - f_B) w$.
- (ii) *Для любого $w \in \widetilde{\boldsymbol{R}}G$, обладающего свойствами $(i.1)$–$(i.3)$, и любого элемента $h \in H$ такого, что $\mathrm{C}_G(h_p) \leqslant H$, где h_p — p-часть элемента h, существуют элементы $w_0, \ldots, w_{p-1} \in f_b \widetilde{\boldsymbol{R}}G f_b$ такие, что $w = w_0 + \ldots w_{p-1}$ и $w_i^h = w_{i+1}$, $i = 0, \ldots, p-1$, где индексы берутся по модулю p.*

Доказательство. (i) Запишем $f_B = u - v$, где u, v — однозначно определённые элементы из $\widetilde{\boldsymbol{R}}G$ такие, что $\operatorname{supp} u \subseteq H$ и $\operatorname{supp} v \subseteq G \setminus H$. Заметим, что $u \in \mathrm{Z}(\widetilde{\boldsymbol{R}}H)$. Действительно, $f_B \in \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$ и, значит, u является линейной комбинацией сумм вида $\sum_{x \in K \cap H}$, где $K \in \mathscr{K}(G)$, а множества $K \cap H$ являются объединениями классов сопряжённости группы H.

Поскольку $B = b^G$, имеем $\lambda_B = \lambda_b^G$. Значит,

$$1 = \lambda_B(e_B) = \lambda_B(f_B^\star) = \lambda_b^G(u^\star - v^\star) = \lambda_b(u^\star),$$

ввиду того, что $\operatorname{supp} v \cap H = \varnothing$. Из (26.1) следует, что найдётся элемент $y \in f_b \mathrm{Z}(\widetilde{\boldsymbol{R}}H)$ такой, что $uy = f_b$. Покажем, что элемент $w = vy$ удовлетворяет $(i.1)$–$(i.3)$ и лежит в $f_b \widetilde{\boldsymbol{R}}G f_b$, т. е. является искомым.

Так как $\operatorname{supp} v \subseteq G \setminus H$ и $\operatorname{supp} y \subseteq H$, имеем $(i.1)$. Ввиду того, что H централизует элементы y, u, f_B и выполнено равенство $w = (u - f_B)y$, получаем $(i.2)$. Так как f_b — единица кольца $f_b \mathrm{Z}(\widetilde{\boldsymbol{R}}H)$ и y — его элемент, то

$$w f_b = v y f_b = v y = w,$$

а из $(i.2)$ получаем $f_b w = w f_b$, т. е. $w \in f_b \widetilde{\boldsymbol{R}}G f_b$. Наконец,

$$(1 - f_B)(f_b - w) = (1 - f_B)(uy - vy) = (1 - f_B)(u - v)y = (1 - f_B) f_B y = 0,$$

откуда вытекает $(i.3)$.

(ii) Поскольку группа H централизует w, она действует сопряжением на носителе $\operatorname{supp} w$ и, кроме того, коэффициент элемента w при произвольном $g \in G$ равен коэффициенту при g^u для любого $u \in H$. Заметим, что мощность любой орбиты группы $\langle h\rangle$ на $\operatorname{supp} w$ делится на p. В самом деле, если это не так, то найдётся $g \in \operatorname{supp} w$ такой, что $|\langle h\rangle : \mathrm{C}_{\langle h\rangle}(g)|$ не делится на p, т. е. $\langle h_p\rangle \leqslant \mathrm{C}_{\langle h\rangle}(g)$. Но тогда по условию $g \in \mathrm{C}_G(h_p) \leqslant H$ вопреки тому, что $g \in \operatorname{supp} w \subseteq G \setminus H$ по $(i.1)$.

Пусть $O(g)$ обозначает $\langle h\rangle$-орбиту элемента $g \in \operatorname{supp} w$ и $\mathscr{O}$ — полное множество представителей таких орбит. Тогда

$$\operatorname{supp} w = \dot{\bigcup}_{g\in\mathscr{O}} O(g).$$

Из сказанного выше следует, что для любого $g \in \operatorname{supp} w$ индекс $\big|\langle h\rangle : \mathrm{C}_{\langle h\rangle}(g)\big|$ делится на p, и поэтому $\mathrm{C}_{\langle h\rangle}(g) \leqslant \langle h^p\rangle$. Значит, обозначив $\langle h^p\rangle$-орбиту элемента g через $T(g)$, получим, что все множества $T(g)^{h^i}$, $i = 0, \ldots, p-1$, попарно не пересекаются, и

$$O(g) = T(g)\dot{\cup}T(g)^h\dot{\cup}\ldots\dot{\cup}T(g)^{h^{p-1}}.$$

Следовательно, w допускает однозначное представление в виде $w = w_0' + \ldots + w_{p-1}'$, где

$$\operatorname{supp} w_i' = \dot{\bigcup}_{g\in\mathscr{O}} T(g)^{h^i}, \quad i = 0, \ldots, p-1.$$

В частности, $(w_i')^h = w_{i+1}'$, $i = 0, \ldots, p-1$, где индексы берутся по модулю p. Так как $w \in f_b\widetilde{\boldsymbol{R}}Gf_b$, то

$$w = f_bwf_b = f_bw_0'f_b + \ldots + b_bw_{p-1}'f_b = w_0 + \ldots + w_{p-1}$$

— требуемое представление, где $w_i = f_bw_i'f_b \in f_b\widetilde{\boldsymbol{R}}Gf_b$, $i = 0, \ldots, p-1$, поскольку

$$w_i^h = (f_bw_i'f_b)^h = f_b(w_i')^hf_b = f_bw_{i+1}'f_b = w_{i+1}$$

для всех i. □

(26.3) Предложение. *Пусть $b \in \mathrm{Bl}(H)$, где $H \leqslant G$, и предположим, что определён p-блок $B = b^G \in \mathrm{Bl}(G)$. Пусть $h \in H$ такой, что $\mathrm{C}_G(h_p) \leqslant H$, где h_p — p-часть элемента h. Тогда $\chi(f_bh) = 0$ для любого $\chi \in \mathrm{Irr}(G) \setminus \mathrm{IBr}(B)$.*

Доказательство. Пусть $M = M_\chi$ — неприводимый $\mathbb{C}G$-модуль с характером χ. В силу (20.20) имеем $f_b \in \mathrm{Z}(\widetilde{\boldsymbol{R}}H)$ и, значит, из (2.37)(*iii*) следует, что модуль M, рассматриваемый как $\mathbb{C}H$-модуль, допускает разложение

$$M = Mf_b \oplus M(1 - f_b).$$

Поскольку элемент f_bh аннулирует $M(1 - f_b)$ и действует на Mf_b также, как h, величина $\chi(f_bh)$ равна сумме характеристических значений элемента h (с учётом кратности) на Mf_b.

Положим $V = Mf_b$. Пусть $\zeta = e^{\frac{2\pi i}{p}}$. Достаточно показать, что для любого $\alpha \in \mathbb{C}$ кратность α как характеристического значения элемента h на V совпадает с кратностью $\zeta\alpha$. В самом деле, если это верно, то кратности значений $\alpha, \zeta\alpha, \ldots, \zeta^{p-1}\alpha$ совпадают. А поскольку $1+\zeta+\ldots+\zeta^{p-1} = 0$, отсюда получим требуемое.

Поскольку V, рассматриваемый как $\mathbb{C}\langle h\rangle$-модуль, вполне приводим и неприводимые $\mathbb{C}\langle h\rangle$-модули одномерны, V обладает базисом из собственных векторов элемента h, в частности, каждое характеристическое значение элемента h на V является собственным. Обозначим через U_α подпространство собственных векторов элемента h, соответствующее собственному значению α. Тогда кратность α равна $\dim_{\mathbb{C}} U_\alpha$. Пусть $w, w_0, \ldots, w_{p-1} \in f_b\widetilde{\boldsymbol{R}}Gf_b$ — элементы, существование которых утверждается в предложении (26.2) для данных подгруппы H, p-блока $B = b^G$ и элемента $h \in H$. Заметим, что, поскольку f_b — единица кольца $f_b\widetilde{\boldsymbol{R}}Gf_b$, справедливы соотношения

$$Vw_i = Mf_bw_i = Mw_if_b \subseteq Mf_b = V.$$

Поэтому для элемента $s \in \widetilde{\boldsymbol{R}}G$, определённого равенством

(26.4) $$s = w_0 + \zeta^{-1}w_1 + \ldots + \zeta^{-(p-1)}w_{p-1},$$

имеем $Vs \subseteq V$. Кроме того

$$s^h = w_0^h + \zeta^{-1}w_1^h + \ldots + \zeta^{-(p-1)}w_{p-1}^h = w_1 + \zeta^{-1}w_2 + \ldots + \zeta^{-(p-1)}w_0 = \zeta s.$$

Поэтому для любого $u \in U_\alpha$ получаем

$$(us)h = uhs^h = \zeta\alpha(us).$$

Другими словами действие элемента s переводит собственное подпространство U_α в подпространство $U_{\zeta\alpha}$. Если мы покажем, что что отображение $v \mapsto vs$ инъективно на V, то получим, что

$$\dim_{\mathbb{C}} U_\alpha = \dim_{\mathbb{C}}(U_\alpha s) \leqslant \dim_{\mathbb{C}}(U_{\zeta\alpha})$$

и, аналогично,

$$\dim_{\mathbb{C}} U_\alpha \leqslant \dim_{\mathbb{C}}(U_{\zeta\alpha}) \leqslant \dim_{\mathbb{C}}(U_{\zeta^2\alpha}) \leqslant \ldots \leqslant \dim_{\mathbb{C}}(U_{\zeta^p\alpha}) = \dim_{\mathbb{C}}(U_\alpha),$$

откуда будет следовать требуемое.

Обозначим $f = (1 - f_{_B})f_b$. Тогда f — идемпотент алгебры $\widetilde{\boldsymbol{R}}G$, поскольку является произведением перестановочных идемпотентов.

Заметим, что $(1 - f_{_B})s \in f\widetilde{\boldsymbol{R}}Gf$. Действительно, с одной стороны имеем $f_b s f_b = s$, что следует из (26.4) и того, что $f_b w_i f_b = w_i$, $i = 0, \ldots, p-1$, а с другой стороны $1 - f_{_B} \in \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$ и, значит,

$$(1 - f_{_B})s = (1 - f_{_B})f_b s f_b = (1 - f_{_B})f_b\big((1 - f_{_B})s\big)(1 - f_{_B})f_b = f(1 - f_{_B})sf.$$

Также заметим, что $\zeta^\star = 1$, поскольку в группе $F^\times$ нет нетривиальных p-элементов. Поэтому $s^\star = w^\star$. Тогда из (26.2)(i.3) получаем

$$f^\star = \big((1 - f_{_B})w\big)^\star = (1 - f_{_B})^\star w^\star = (1 - f_{_B})^\star s^\star = \big((1 - f_{_B})s\big)^\star.$$

Поэтому, применяя утверждение (4.17) к гомоморфизму коммутативных колец $^\star : \widetilde{\boldsymbol{R}} \to F$, идемпотенту $f \in \widetilde{\boldsymbol{R}}G$ и элементу $(1 - f_{_B})s \in f\widetilde{\boldsymbol{R}}Gf$, заключаем, что существует $y \in \widetilde{\boldsymbol{R}}G$, для которого $(1 - f_{_B})sy = f$.

Элемент f действует тождественно на V. В самом деле, поскольку $\chi \notin B$, из (21.5)(i) следует, что идемпотент $1 - f_{_B}$ действует тождественно даже на всём модуле M, а f_b действует тождественно на V в силу равенства $V = Mf_b$.

Из сделанных замечаний следует, что для произвольного $v \in V$

$$vsy = v(1 - f_{_B})sy = vf = v,$$

и поэтому если $vs = 0$, то $v = 0$. Тем самым действие s на V инъективно и утверждение доказано. □

Теперь приступим к формулировке основных понятий и результатов этого раздела. Для определения обобщения чисел разложения докажем следующее утверждение.

(26.5) Предложение. *Пусть x — p-элемент группы G, $H = \mathrm{C}_G(x)$ и $\chi \in \mathrm{Irr}(G)$. Тогда*

(i) *для произвольного $\varphi \in \mathrm{IBr}(H)$ существует единственное число $d^x_{\chi\varphi} \in \mathbb{C}$ такое, что равенство*

$$\chi(xy) = \sum_{\varphi \in \mathrm{IBr}(H)} d^x_{\chi\varphi}\varphi(y)$$

справедливо для всех p-регулярных $y \in H$;

(ii) *$d^x_{\chi\varphi} \in \mathbb{Q}_{|x|} \cap \boldsymbol{R}$ для всех $\varphi \in \mathrm{IBr}(H)$.*

Доказательство. (i) Для ограничения χ_H запишем

$$\chi_H = \sum_{\tau \in \mathrm{Irr}(H)} a_\tau \tau,$$

где $a_\tau = (\chi_H, \tau)_{_H} \in \mathbb{Z}$. Поскольку $x \in \mathrm{Z}(H)$, из (16.27)(ii) следует, что

$$\chi(xy) = \sum_{\tau \in \mathrm{Irr}(H)} a_\tau \tau(xy) = \sum_{\tau \in \mathrm{Irr}(H)} a_\tau \omega_\tau(x)\tau(y) = \sum_{\tau \in \mathrm{Irr}(H)} \sum_{\varphi \in \mathrm{IBr}(H)} a_\tau \omega_\tau(x) d_{\tau\varphi}\varphi(y) = \sum_{\varphi \in \mathrm{IBr}(H)} d^x_{\chi\varphi}\varphi(y),$$

где

$$d^x_{\chi\varphi} = \sum_{\tau \in \mathrm{Irr}(H)} a_\tau\, d_{\tau\varphi}\, \omega_\tau(x) = \sum_{\tau \in \mathrm{Irr}(H)} \frac{(\chi_H, \tau)_{_H} d_{\tau\varphi}}{\tau(1)}\, \tau(x). \qquad \textbf{(26.6)}$$

Единственность чисел $d^x_{\chi\varphi}$ следует из линейной независимости над $\mathbb{C}$ множества $\mathrm{IBr}(H)$, см. (18.8)(i).

(ii) следует из выражения (26.6) и (16.27)(i). □

✎ **(26.7)** Показать, что $d^x_{\chi\varphi} \in \mathbb{Z}[\zeta]$, где $\zeta = e^{\frac{2\pi i}{|x|}}$, т. е. $d^x_{\chi\varphi}$ является $\mathbb{Z}$-линейной комбинацией чисел ζ^i, при $i = 0, \ldots, |x| - 1$.

(26.8) Определение. Для p-элемента $x \in G$ числа $d^x_{\chi\varphi}$, где $\chi \in \mathrm{Irr}(G)$ и $\varphi \in \mathrm{IBr}(\mathrm{C}_G(x))$, определённые в (26.5) называются *высшими числами разложения*.

Легко видеть, что обычные числа разложения $d_{\chi\varphi}$ соответствуют случаю $x = 1$.

(26.9) Теорема (Вторая основная теорема Брауэра). *Пусть $\chi \in \mathrm{Irr}(G)$ и $\varphi \in \mathrm{IBr}(H)$, где $H = \mathrm{C}_G(x)$ для некоторого p-элемента $x \in G$. Пусть $B \in \mathrm{Bl}(G)$ и $b \in \mathrm{Bl}(H)$ такие, что $\chi \in B$ и $\varphi \in b$. Тогда если $b^G \neq B$, то $d^x_{\chi\varphi} = 0$.*

Доказательство. Заметим, что блок b^G определён в силу (24.10). В силу линейной независимости брауэровых достаточно доказать, что если $b^G \neq B$, то линейная комбинация $\sum_{\psi\in\mathrm{IBr}(b)} d^x_{\chi\psi}\psi$ является нулевым элементом алгебры $\mathrm{cf}(H_{p'})$. По (26.6) имеем

$$\sum_{\psi\in\mathrm{IBr}(b)} d^x_{\chi\psi}\psi = \sum_{\psi\in\mathrm{IBr}(b)}\left(\sum_{\tau\in\mathrm{Irr}(H)} a_\tau\, d_{\tau\psi}\, \omega_\tau(x)\right)\psi = \sum_{\psi\in\mathrm{IBr}(b)}\left(\sum_{\tau\in\mathrm{Irr}(b)} a_\tau\, d_{\tau\psi}\, \omega_\tau(x)\right)\psi$$

$$= \sum_{\tau\in\mathrm{Irr}(b)} a_\tau\, \omega_\tau(x)\left(\sum_{\psi\in\mathrm{IBr}(b)} d_{\tau\psi}\psi\right) = \sum_{\tau\in\mathrm{Irr}(b)} a_\tau\, \omega_\tau(x)\, \tau,$$

где $a_\tau = (\chi_H, \tau)_H$. Достаточно проверить, что значение последнего выражения на произвольном элементе $y \in H_{p'}$ равно нулю. Поскольку $x \in \mathrm{Z}(H)$, из (16.27)(i) и (21.8) следует, что

$$\sum_{\tau\in\mathrm{Irr}(b)} a_\tau\, \omega_\tau(x)\, \tau(y) = \sum_{\tau\in\mathrm{Irr}(b)} a_\tau\, \tau(xy)$$

$$= \sum_{\tau\in\mathrm{Irr}(H)} a_\tau\, \tau_b(xy) = \sum_{\tau\in\mathrm{Irr}(H)} (\chi_H, \tau)_H \tau(f_b\, xy) = \chi(f_b\, xy).$$

Теперь применим предложение (26.3) к данной группе H и элементу $h = xy \in H$. Поскольку x и y перестановочны, имеем $h_p = x$. Поэтому, если $b^G \neq B$, то $\chi \notin b^G$, и из (26.3) вытекает, что $\chi(f_b\, xy) = \chi(f_b h) = 0$, как и требовалось. ☐

27. Следствия из второй основной теоремы Брауэра

Вторая основная теорема Брауэра является мощным и чрезвычайно полезным инструментом. Выведем из неё некоторые следствия.

(27.1) Предложение. *Пусть $\chi \in \mathrm{Irr}(G)$ и $g \in G$. Если $\chi(g) \neq 0$, то g_p принадлежит некоторой дефектной группе p-блока, содержащего χ.*

Доказательство. Пусть $x = g_p$ и запишем $g = xy$ для подходящего p-регулярного элемента $y \in C = \mathrm{C}_G(x)$. Тогда

$$\chi(g) = \chi(xy) = \sum_{\varphi\in\mathrm{IBr}(C)} d^x_{\chi\varphi}\varphi(y).$$

По условию существует характер $\varphi \in \mathrm{IBr}(C)$ такой, что $d^x_{\chi\varphi} \neq 0$. Из (26.9) следует, что если $\varphi \in b \in \mathrm{Bl}(C)$, то $\chi \in b^G$. В силу (22.13) имеем $x \in \mathrm{O}_p(C) \leqslant \delta(b)$, а из (24.9) получаем $\delta(b) \leqslant_G \delta(b^G)$. Поэтому x лежит в некоторой дефектной группе блока b^G. ☐

Отметим, что прямым следствием из (27.1) является доказанное в (23.1) утверждение о том, что обыкновенный характер из p-блока дефекта 0 обращается в 0 на всех не-p-регулярных элементах.

(27.2) Определение. Пусть $g \in G$. Множество

$$\mathrm{S}_G(g) = \{x \in G \mid (x_p)^G = (g_p)^G\}$$

назовём *p-сечением* группы G, содержащем элемент g. Другими словами, $\mathrm{S}_G(g)$ является множеством тех элементов из G, p-часть которых сопряжена с p-частью элемента g.

(27.3) Предложение. *Справедливы следующие утверждения.*

(i) $\mathrm{S}_G(1) = G_{p'}$.

(ii) $g \in \mathrm{S}_G(g) = \mathrm{S}_G(g_p)$ *для любого* $g \in G$.

(iii) *Для любого $g \in G$ множество $\mathrm{S}_G(g)$ является объединением некоторых классов сопряжённости группы G.*

(iv) *Пусть U — полное множество представителей классов сопряжённости p-элементов группы G. Тогда*

$$G = \dot{\bigcup}_{u\in U} \mathrm{S}_G(u).$$

(v) *Пусть $g \in G$ — p-элемент и T — полное множество представителей классов сопряжённости p-регулярных элементов группы $C = \mathrm{C}_G(g)$. Если $C \leqslant H \leqslant G$, то*

$$\mathrm{S}_H(g) = \dot{\bigcup}_{t \in T} (gt)^H.$$

✎ Доказать предложение (27.3).

(27.4) Предложение. *Пусть $x \in G$ и $\eta \in \mathrm{cf}(G)$. Если η тождественно равно нулю на $\mathrm{S}_G(x)$, то B-часть η_B для любого $B \in \mathrm{Bl}(G)$ также тождественно равна нулю на $\mathrm{S}_G(x)$.*

Доказательство. Пусть сначала B — произвольный блок группы G. В силу (27.3)(*ii*) можно считать, что x — p-элемент. Достаточно показать, что $\eta_B(xt) = 0$ для любого p-регулярного элемента $t \in C = \mathrm{C}_G(x)$. Справедливы соотношения

$$\textbf{(27.5)} \qquad \eta_B(xt) = \sum_{\chi \in \mathrm{Irr}(B)} (\eta, \chi)_G \chi(xt) = \sum_{\chi \in \mathrm{Irr}(B)} (\eta, \chi)_G \sum_{\varphi \in \mathrm{IBr}(C)} d^x_{\chi\varphi} \varphi(t) = \sum_{\varphi \in \mathrm{IBr}(C)} \left(\sum_{\chi \in \mathrm{Irr}(B)} (\eta, \chi)_G d^x_{\chi\varphi} \right) \varphi(t).$$

Просуммировав по всем $B \in \mathrm{Bl}(G)$, получим

$$\textbf{(27.6)} \qquad \sum_{\varphi \in \mathrm{IBr}(C)} \left(\sum_{\chi \in \mathrm{Irr}(G)} (\eta, \chi)_G d^x_{\chi\varphi} \right) \varphi(t) = \sum_{B \in \mathrm{Bl}(G)} \eta_B(xt) = \eta(xt) = 0,$$

где последнее равенство следует из условия.

Теперь фиксируем блок $B \in \mathrm{Bl}(G)$. Тогда в силу линейной независимости множества $\mathrm{IBr}(C)$ из (27.6) следует, что для любого $\varphi \in \mathrm{IBr}(C)$ выполнены равенства

$$\textbf{(27.7)} \qquad 0 = \sum_{\chi \in \mathrm{Irr}(G)} (\eta, \chi)_G d^x_{\chi\varphi} = \sum_{\chi \in \mathrm{IBr}(B)} (\eta, \chi)_G d^x_{\chi\varphi} + \sum_{\chi \in \mathrm{Irr}(G) \setminus \mathrm{IBr}(B)} (\eta, \chi)_G d^x_{\chi\varphi}.$$

Заметим, что в случае, когда $b^G = B$, где $\varphi \in b \in \mathrm{Bl}(C)$, последнее слагаемое в (27.7) равно нулю в силу теоремы (26.9), т. е. в этому случае имеем

$$\sum_{\chi \in \mathrm{IBr}(B)} (\eta, \chi)_G d^x_{\chi\varphi} = 0.$$

Однако, это равенство также справедливо и в случае, когда $b^G \neq B$, опять-таки в силу теоремы (26.9). Поэтому из (27.5) получаем $\eta_B(xt) = 0$, как и требовалось. ☐

Теперь докажем усиление утверждения (20.14).

(27.8) Предложение (Ортогональность в блоке). *Пусть $x, y \in G$ такие, что p-части x_p и y_p не сопряжены в G. Тогда*

$$\sum_{\chi \in \mathrm{Irr}(B)} \chi(x)\overline{\chi(y)} = 0$$

для любого $B \in \mathrm{Bl}(G)$.

Доказательство. Определим классовую функцию

$$\eta = \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(y)} \chi$$

и положим $u = x_p$. Если $t \in \mathrm{C}_G(u)$ — p-регулярный элемент, то элементы ut и y не сопряжены в G, поскольку не сопряжены их p-части $(ut)_p = u = x_p$ и y_p. Поэтому из второго соотношения ортогональности (16.22) следует, что $\eta(ut) = 0$. Значит, η обращается в ноль на $\mathrm{S}_G(x)$. Из (27.4) вытекает, что

$$0 = \eta_B(x) = \sum_{\chi \in \mathrm{Irr}(B)} \chi(x)\overline{\chi(y)},$$

как и требовалось. ☐

Для дальнейшего нам потребуется ещё один вспомогательный результат, который, по сути, является усилением пункта (i) теоремы Min-Max (22.10).

(27.9) Предложение. *Пусть P — p-подгруппа группы G, $B \in \mathrm{Bl}(G|P)$ и $K \in \mathscr{K}(G)$. Если $\lambda_B(\widehat{K}) \neq 0$, то существует $x \in K \cap \mathrm{C}_G(P)$ такой, что $x_p \in \mathrm{Z}(P)$.*

Доказательство. Обозначим $C = \mathrm{C}_G(P)$, $N = \mathrm{N}_G(P)$. Из первой основной теоремы Брауэра (24.17) следует, что существует блок $b \in \mathrm{Bl}(N|P)$ такой, что $B = b^G$. Если в (24.10)(i) положить $H = N$, то получим $\lambda_b \circ \beta_P = \lambda_B$ и, значит,

$$0 \neq \lambda_B(\widehat{K}) = \lambda_b\left(\sum_{x \in K\cap C} x\right).$$

Поэтому существует класс $L \in \mathscr{K}(N)$ такой, что $L \subseteq K \cap C$ и $\lambda_b(\widehat{L}) \neq 0$. Выберем произвольный элемент $x \in L$. Заметим, что $x_p \in C$, поскольку $x \in C$. Кроме того, для любого $\tau \in \mathrm{Irr}(b)$ имеем $\tau(x) \neq 0$, поскольку

$$0 \neq \lambda_b(\widehat{L}) = \lambda_\tau(\widehat{L}) = \omega_\tau(\widehat{L})^\star = \left(\frac{|L|\tau(x)}{\tau(1)}\right)^\star$$

в силу (20.2) и (16.26). Значит, из (27.1) следует, что x_p лежит в некотором элементе из $\Delta(b)$. Однако, $\Delta(b) = \{P\}$ в силу нормальности P в N. Поэтому $x_p \in P \cap C = \mathrm{Z}(P)$, т. е. x — искомый элемент из $K \cap C$. □

В (23.1) было установлено, что всякий неприводимый обыкновенный характер, обращающийся в ноль на всех неединичных p-элементах, принадлежит блоку дефекта 0. Усилением этого является следующее утверждение.

(27.10) Теорема (Кнёрра). *Пусть $\chi \in \mathrm{Irr}(G)$ и $\chi(x) = 0$ для любого $x \in G$ порядка p. Тогда χ принадлежит p-блоку дефекта 0.*

Доказательство. Пусть $\chi \in B \in \mathrm{Bl}(G)$ и пусть $P = \delta(B)$. Требуется показать, что $P = 1$. Положим

$$U = \{x \in G \mid |x| = p\}.$$

Тогда U — объединение классов сопряжённости группы G. Если K — один из таких классов, то по условию имеем

$$\lambda_B(\widehat{K}) = \omega_\chi(\widehat{K})^\star = \left(\frac{|K|\chi(x_K)}{\chi(1)}\right)^\star = 0.$$

Просуммировав по всем таким классам K, получим $\lambda_B\left(\sum_{x\in U} x\right) = 0$.

Положим $N = \mathrm{N}_G(P)$ и $C = \mathrm{C}_G(P)$. В силу первой основной теоремы Брауэра (24.17) существует блок $b \in \mathrm{Bl}(N|P)$ такой, что $B = b^G$. Кроме того, по (24.10)(i) имеем $\lambda_b \circ \beta_P = \lambda_B$. Поэтому

$$0 = \lambda_B\left(\sum_{x\in U} x\right) = \lambda_b\left(\sum_{x \in U\cap C} x\right).$$

Заметим, что $U \cap C$ — объединение некоторых классов сопряжённости группы N. Если L — один из таких классов, причём $\lambda_b(\widehat{L}) \neq 0$, то, применив (27.9) к группе N, её блоку b и классу L, получим, что существует элемент $x \in L$ такой, что $x_p \in \mathrm{Z}(P)$. Однако, $x = x_p$ и $\mathrm{Z}(P) \trianglelefteq N$, поскольку $P \trianglelefteq N$. Поэтому $L \subseteq \mathrm{Z}(P)$. Значит,

$$0 = \lambda_b\left(\sum_{x\in U\cap C} x\right) = \lambda_b\left(\sum_{x \in U\cap \mathrm{Z}(P)} x\right).$$

Обозначим

$$H = \{x \in \mathrm{Z}(P) \mid x^p = 1\}$$

и положим $\widehat{H} = \sum_{x\in H} x$. Тогда $H \leqslant \mathrm{Z}(P)$ и $\widehat{H} \in \mathrm{Z}(FN)$. Кроме того, $U \cap \mathrm{Z}(P) = H \setminus \{1\}$. В частности,

$$\lambda_b(\widehat{H}) = \lambda_b\left(\sum_{x\in H\setminus\{1\}} x\right) + \lambda_b(1) = \lambda_b\left(\sum_{x\in U\cap \mathrm{Z}(P)} x\right) + 1 = 1.$$

Кроме того, так как H — p-подгруппа, имеем

$$\widehat{H}\widehat{H} = \sum_{x\in H}\sum_{y\in H} xy = \sum_{x\in H}\widehat{H} = |H|^\star \widehat{H} = \begin{cases} 0, & \text{если } H \neq 1; \\ 1, & \text{если } H = 1. \end{cases}$$

Значит, поскольку $1 = \lambda_b(\widehat{H})^2 = \lambda_b(\widehat{H}\widehat{H})$, получаем $H = 1$, а это возможно лишь когда $P = 1$. Отсюда вытекает требуемое. □

Докажем ещё ряд вспомогательных утверждений.

(27.11) Предложение. *Пусть P — p-подгруппа группы G и $B \in \mathrm{Bl}(G|P)$. Пусть K — дефектный класс блока B и $x \in K$ — такой элемент, что $P \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Тогда справедливы следующие утверждения.*

(*i*) *Если $\chi \in \mathrm{Irr}(B)$ — характер высоты 0, то $\chi(xu)^\star \neq 0$ для любого $u \in P$.*

(*ii*) *Если $u \in \mathrm{Z}(P)$ и $L = (xu)^G$, то $\lambda_{{}_B}(\widehat{L}) \neq 0$.*

Доказательство. (*i*) По определению дефектного класса $\lambda_{{}_B}(\widehat{K}) \neq 0$. Поскольку χ — характер высоты 0, имеем $|\chi(1)|_p = |K|_p$. Значит, $\dfrac{|K|}{\chi(1)}$ — обратимый элемент кольца $\widetilde{\boldsymbol{R}}$ и поэтому

$$0 \neq \lambda_{{}_B}(\widehat{K}) = \omega_\chi(\widehat{K})^\star = \left(\frac{|K|\chi(x)}{\chi(1)}\right)^\star = \left(\frac{|K|}{\chi(1)}\right)^\star \chi(x)^\star.$$

Отсюда следует, что $\chi(x)^\star \neq 0$.

В силу (22.9) имеем $x \in G_{p'}$. Поэтому $(xu)_{p'} = x$ для любого $u \in P$. Из (17.12)(*ii*) получаем $\chi(xu)^\star = \chi(x)^\star \neq 0$.

(*ii*) Поскольку $(xu)_p = u$ и $(xu)_{p'} = x$, в силу (17.4) имеем $\mathrm{C}_G(xu) = \mathrm{C}_G(x) \cap \mathrm{C}_G(u)$. Однако, по условию P централизует x и u. Поэтому $P \leqslant \mathrm{C}_G(xu)$. Заметим, что $|\mathrm{C}_G(xu) : P|$ делит индекс $|\mathrm{C}_G(x) : P|$, который взаимно прост с p в силу условия $P \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Поэтому индекс $|\mathrm{C}_G(xu) : P|$ также взаимно прост с p и, значит, $P \in \mathrm{Syl}_p(\mathrm{C}_G(xu))$. Отсюда следует, что $|L|_p = |K|_p$.

Выберем характер $\chi \in B$ высоты 0. Тогда $|\chi(1)|_p = |K|_p = |L|_p$. Поэтому $\dfrac{|L|}{\chi(1)}$ — обратимый элемент кольца $\widetilde{\boldsymbol{R}}$. Отсюда, применив (*i*), получаем

$$\lambda_{{}_B}(\widehat{L}) = \left(\frac{|L|\chi(xu)}{\chi(1)}\right)^\star = \left(\frac{|L|}{\chi(1)}\right)^\star \chi(xu)^\star \neq 0,$$

как и утверждалось. □

Следующее утверждение устанавливает новую связь между дефектными группами блоков b и b^G (ср. (24.9)).

(27.12) Предложение. *Пусть $b \in \mathrm{Bl}(H)$, где $H \leqslant G$, и предположим, что определён p-блок $B = b^G \in \mathrm{Bl}(G)$. Тогда любой элемент из $\mathrm{Z}(\delta(B))$ сопряжён в группе G с некоторым элементом из $\mathrm{Z}(\delta(b))$.*

Доказательство. Выберем произвольный элемент $u \in \mathrm{Z}(\delta(B))$. Пусть $K = x^G$ — дефектный класс блока B, причём $\delta(B) \in \mathrm{Syl}_p(\mathrm{C}_G(x))$. Обозначим $L = (xu)^G$. Тогда $\lambda_{{}_B}(\widehat{L}) \neq 0$ в силу (27.11)(*ii*). По определению индуцированного блока имеем

$$0 \neq \lambda_{{}_B}(\widehat{L}) = \lambda_b\left(\sum_{y \in L \cap H} y\right).$$

Значит, существует класс $M \in \mathscr{K}(H)$ такой, что $M \subseteq L$ и $\lambda_b(\widehat{M}) \neq 0$. Применив (27.9) к блоку b группы H и классу M, получим, что существует $z \in M$, для которого $z_p \in \mathrm{Z}(\delta(b))$. Поскольку элементы z и xu сопряжены в G, то сопряжены и их p-части z_p и $(xu)_p = u$. Отсюда следует требуемое. □

Теперь мы можем охарактеризовать блоки, индуцирующие блок дефекта 0.

(27.13) Предложение. *Пусть $b \in \mathrm{Bl}(H)$, где $H \leqslant G$, и предположим, что определён p-блок $B = b^G \in \mathrm{Bl}(G)$. Тогда $\mathrm{d}(B) = 0$ в том и только в том случае, когда $\mathrm{d}(b) = 0$.*

Доказательство. В силу (24.9) имеем $\delta(b) \leqslant_G \delta(B)$. Поэтому, если $\mathrm{d}(B) = 0$, то $\mathrm{d}(b) = 0$. Обратно, предположим, что $\mathrm{d}(b) = 0$. Тогда из (27.12) следует, что $\mathrm{Z}(\delta(B)) = 1$, а значит, $\delta(B) = 1$, откуда следует требуемое. □

28. Обзор некоторых дальнейших результатов

В этом разделе результаты приводятся без доказательств.

Аналог утверждения (27.13) для главных блоков также имеет место, однако доказывается более сложно.

(28.1) Теорема (Третья основная теорема Брауэра). *Пусть $b \in \mathrm{Bl}(H)$, где $H \leqslant G$, и предположим, что определён p-блок $B = b^G \in \mathrm{Bl}(G)$. Тогда B — главный блок группы G в том и только в том случае, когда b — главный блок группы H.*

Рассмотрим пример, иллюстрирующий третью основную теорему Брауэра.

(28.2) Пример. Пусть $p = 2$, $G = A_5$ — знакопеременная группа подстановок множества $\{1, 2, 3, 4, 5\}$, $H \cong A_4$ — подгруппа группы G, состоящая из элементов, для которых 5 является неподвижным символом. Тогда H имеет единственный 2-блок b (главный, см. приложение В). Выясним, определён ли индуцированный блок b^G и совпадает ли он с главным 2-блоком группы G. Значения гомоморфизма λ_b на классовых суммах $\widehat{L}$, где $L \in \mathscr{K}(H)$, приведены в следующей таблице.

L	L_1	L_2	L_3	L_4
$x_{_L}$	1	(12)(34)	(123)	(132)
$\omega_{1_H}(\widehat{L}) = \lvert L\rvert$	1	3	4	4
$\lambda_b(\widehat{L}) = \lvert L\rvert^\star$	1	1	0	0

Найдём значения отображения λ_b^G на классовых суммах $\widehat{K}$, где $K \in \mathscr{K}(G)$.

K	K_1	K_2	K_3	K_4	K_5
$x_{_K}$	1	(12)(34)	(123)	(12345)	(13524)
$\sum_{x\in K\cap H} x$	$\widehat{L}_1$	$\widehat{L}_2$	$\widehat{L}_3 + \widehat{L}_4$	0	0
$\lambda_b^G(\widehat{K})$	1	1	0	0	0

Также вычислим значения $\lambda_{_B}$, где B — главный 2-блок группы G.

K	K_1	K_2	K_3	K_4	K_5
$\omega_{1_G}(\widehat{K}) = \lvert K\rvert$	1	15	20	12	12
$\lambda_{_B}(\widehat{K}) = \lvert K\rvert^\star$	1	1	0	0	0

Как видно, значения отображений λ_b^G и $\lambda_{_B}$ совпадают на всех классовых суммах группы G. Поэтому $\lambda_b^G = \lambda_{_B}$ и, значит, индуцированный блок b^G определён и совпадает с B.

Описание блоков с циклическими дефектными группами (иногда называемых *циклическими блоками*) было завершено Дэйдом и является глубоким и полезным результатом.

(28.3) Теорема (Дэйда). *Пусть* $B \in \mathrm{Bl}(G)$ *и* $\delta(B)$ *— циклическая группа. Пусть* $|\delta(B)| = p^d > 1$ *и* $|\,\mathrm{IBr}(B)| = e$*. Тогда справедливы следующие утверждения.*

(i) $e \mid p - 1$.

(ii) $|\,\mathrm{Irr}(B)| = \dfrac{p^d - 1}{e} + e$.

(iii) Если $d = 1$ *и* $e = p - 1$*, то положим* $\mathrm{Irr}(B) = \{\chi_0, \chi_1, \ldots, \chi_e\}$*. Если либо* $d > 1$*, либо* $e < p - 1$*, то выполнены следующие утверждения.*

(iii.1) Множество $\mathrm{Irr}(B)$ *однозначно разбивается на два непересекающихся подмножества*

$$\{\tau_1, \tau_2, \ldots, \tau_t\}, \qquad \{\chi_1, \chi_2, \ldots, \chi_e\},$$

где $t = \dfrac{p^d - 1}{e}$*. В этом случае характеры из первого подмножества называются* исключительными*. Любой (фиксированный) исключительный характер обозначим через* χ_0*.*

(iii.2) $\hat\tau_1 = \hat\tau_2 = \ldots = \hat\tau_t$*. В частности,* $d_{\tau_i,\varphi} = d_{\chi_0,\varphi}$ *для любого* $\varphi \in \mathrm{IBr}(B)$ *и любого* $i = 1, \ldots, t$*.*

(iv) Для любого $\varphi \in \mathrm{IBr}(B)$ *ровно два из чисел разложения* $d_{\chi_0,\varphi}, d_{\chi_1,\varphi}, \ldots, d_{\chi_e,\varphi}$ *равны* 1*, а остальные равны* 0*. В частности, все числа разложения блока* B *равны* 0 *или* 1*.*

(v) Все характеры из $\mathrm{Irr}(B)$ *имеют высоту* 0*.*

Теорема (28.3) позволяет построить *дерево Брауэра*, которое описывает строение блока B с циклической дефектной группой. Оно имеет $e+1$ вершин, взаимно однозначно соответствующих характерам χ_0, χ_1, ..., χ_e. Причём в случае, когда либо $d > 1$, либо $e < p - 1$, вершина, соответствующая характеру χ_0 называется *исключительной* и обычно выделяется особо. Количество рёбер равно e, и рёбра взаимно однозначно соответствуют характерам из $\mathrm{IBr}(B)$. Две вершины, соответствующие χ_i и χ_j, соединены ребром тогда и только тогда, когда существует характер $\varphi \in \mathrm{IBr}(B)$, для которого $d_{\chi_j,\varphi} = d_{\chi_j,\varphi} = 1$. Из свойств чисел разложения и пункта *(iv)* теоремы (28.3) легко следует, что полученный граф связен и является деревом.

В качестве примера рассмотрим главный 13-блок B простой группы Титса ${}^2F_4(2)'$ порядка $2^{11}\cdot 3^3\cdot 5^2\cdot 13$. В этом случае $|\,\mathrm{IBr}(B)| = 6$, имеется два исключительных характера, и дерево Брауэра выглядит, как показано

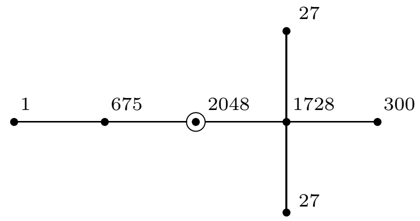

Рис. 1: Главный 13-блок группы ${}^2F_4(2)'$

на рис. 1. Вершины дерева помечены степенями соответствующих характеров, а исключительная вершина обведена.

В заключении курса сформулируем несколько глубоких теоретико-групповых теорем, вытекающих из теории обыкновенных и брауэровых характеров.

Напомним, что *обобщённой группой кватернионов* называется группа

$$Q_{2^m} = \langle x, y \mid x^{2^{m-1}} = 1,\ \ y^2 = x^{2^{m-2}},\ \ x^y = x^{-1} \rangle,$$

где $m \geqslant 3$. Легко видеть, что $|Q_{2^m}| = 2^m$ и Q_8 совпадает с обычной группой кватернионов.

Элемент порядка 2 группы G называется *инволюцией*.

✎ **(28.4)** Доказать, что обобщённая группа кватернионов содержит единственную инволюцию.

Из следующего утверждения следует, что конечная группа не может быть простой в случае, когда её 2-силовская подгруппа является обобщённой группой кватернионов.

(28.5) Теорема (Брауэра-Сузуки). *Пусть* 2*-силовская подгруппа группы* G *является обобщённой группой кватернионов. Если* $\mathrm{O}_{2'}(G) = 1$*, то* $|\mathrm{Z}(G)| = 2$.

Если 2-силовская подгруппа P группы G является обобщённой группой кватернионов порядка, большего, чем 8, то теорема Брауэра-Сузуки может быть доказана с использованием только теории обыкновенных характеров. Наиболее сложная часть теоремы — случай, когда $P \cong Q_8$ — первоначально была доказана с помощью теории блоков. Однако позже, в 1974 году, Глауберман показал, что и здесь можно обойтись только результатами из теории обыкновенных характеров. Чисто теоретико-группового доказательства теоремы Брауэра-Сузуки до сих пор не известно.

(28.6) Определение. Пусть $u \in G$ — инволюция и $u \in P \in \mathrm{Syl}_2(G)$. Инволюция u называется *изолированной*, если она не сопряжена в G ни с одним элементом из $P \setminus \{u\}$.

✎ **(28.7)** Доказать, что

(i) изолированность инволюции u не зависит от выбора 2-силовской подгруппы P в определении (28.6);

(ii) изолированная инволюция лежит в центре любой содержащей её 2-силовской подгруппы.

Для группы G обозначим через $\mathrm{Z}^*(G)$ полный прообраз в G центра факторгруппы $G/\mathrm{O}_{2'}(G)$.

Следующий фундаментальный результат является одним из наиболее важных инструментов локального анализа.

(28.8) Теорема (Z^*-теорема Глаубермана). *Пусть* G *обладает изолированной инволюцией* u*. Тогда* $u \in \mathrm{Z}^*(G)$.

Отметим, что Z^*-теорема является обобщением теоремы Брауэра-Сузуки, однако её доказательство при рассмотрении некоторых частных случаев опирается на эту теорему. Также отметим, что на сегодняшний день не известно доказательства Z^*-теоремы, которое не использовало бы теорию брауэровых характеров.

A Алгебраические числа

В этом приложении мы приведём факты из теории алгебраических чисел, используемые в основном тексте.

Комплексное число называется *алгебраическим*, если оно является корнем некоторого многочлена

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n,$$

где $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ и $a_0 \neq 0$. Комплексное число называется *целым алгебраическим*, если оно является корнем некоторого многочлена[27)]

$$x^n + b_1x^{n-1} + b_2x^{n-2} + \ldots + b_n,$$

где $b_1, b_2, \ldots, b_n \in \mathbb{Z}$.

Очевидно, что всякое целое алгебраическое число будет алгебраическим. Обратное утверждение неверно.

(A.1) Предложение. *Рациональное число $r \in \mathbb{Q}$ будет целым алгебраическим тогда и только тогда, когда $r \in \mathbb{Z}$.*

✎ Доказать предложение (A.1).

Чтобы подчеркнуть разницу с целыми алгебраическими числами, элементы кольца $\mathbb{Z}$ целых чисел мы будем иногда называть *целыми рациональными*.

Оказывается, что целые алгебраические числа образуют кольцо, а алгебраические числа — поле. Для доказательства этого нам потребуются вспомогательные утверждения.

(A.2) Лемма. (i) *Пусть α — алгебраическое число. Тогда существует $m \in \mathbb{Z}$ такое, что число $m\alpha$ целое алгебраическое.*

(ii) *Пусть ω — целое алгебраическое число. Тогда для любого $0 \neq m \in \mathbb{Z}$ число ω/m алгебраическое.*

✎ **(A.3)** Доказать лемму (A.2).

(A.4) Предложение. *Пусть $W \leqslant \mathbb{C}$ — ненулевой конечно порождённый $\mathbb{Z}$-модуль. Если элемент $\omega \in \mathbb{C}$ таков, что $\omega W \subseteq W$, то ω будет целым алгебраическим числом.*

Доказательство. Пусть W порождается как $\mathbb{Z}$-модуль элементами $\gamma_1, \ldots, \gamma_s \in \mathbb{C}$. Имеем $\omega\gamma_i \in W$ для $i = 1, \ldots, s$. Таким образом, $\omega\gamma_i = \sum_{j=1}^{s} a_{ij}\gamma_j$, где $a_{ij} \in \mathbb{Z}$. Отсюда следует, что $\sum_{j=1}^{s}(\alpha_{ij} - \delta_{ij}\omega)\gamma_j = 0$. Поскольку не все γ_j равны нулю, получаем $\det(\alpha_{ij} - \delta_{ij}\omega) = 0$. Выписывая определитель, мы видим, что ω является корнем многочлена с целыми коэффициентами, старший коэффициент которого (с точностью до знака) равен 1. Таким образом, ω — целое алгебраическое число. ☐

(A.5) Предложение. (i) *Множество целых алгебраических чисел образует кольцо.*

(ii) *Множество алгебраических чисел образует поле.*

Доказательство. (i) Пусть μ и ν – целые алгебраические числа. Легко видеть, что число $-\mu$ также целое алгебраическое, поэтому достаточно показать, что $\mu + \nu$ и $\mu\nu$ — целые алгебраические числа. Пусть μ и ν являются корнями многочленов $x^m + a_1x^{m-1} + \ldots + a_m$ и $x^n + b_1x^{n-1} + \ldots + b_n$, соответственно, где $a_i, b_j \in \mathbb{Z}$. Пусть W — $\mathbb{Z}$-модуль, порождённый произведениями $\mu^i\nu^j$, где $0 \leqslant i < m$, $0 \leqslant j < n$. Нетрудно понять, что $\mu W \subseteq W$ и $\nu W \subseteq W$, а, значит, и $(\mu+\nu)W \subseteq W$ и и $(\mu\nu)W \subseteq W$. В силу предложения (A.4) отсюда следует, что $\mu + \nu$ и $\mu\nu$ — целые алгебраические числа.

(ii) Пусть α и β — алгебраические числа. Из (A.2)(i) следует, что существуют целые алгебраические числа μ, ν и $m, n \in \mathbb{Z}$ такие, что $\alpha = \mu/m$ и $\beta = \nu/n$. Поэтому $-\alpha$, $\alpha + \beta$, $\alpha\beta$ являются алгебраическими в силу (i) и (A.2)(ii). Наконец, если $\alpha \neq 0$ и $a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$, где $a_i \in \mathbb{Q}$, то $a_n\alpha^{-n} + a_{n-1}\alpha^{-(n-1)} + \ldots + a_0 = 0$, т. е. α^{-1} также является алгебраическим, откуда и следует доказываемый результат. ☐

Таким образом множество всех алгебраических чисел совпадает с алгебраическим замыканием $\overline{\mathbb{Q}}$ поля рациональных чисел.

Кольцо всех целых алгебраических чисел мы будем обозначать через $\boldsymbol{R}$.

Полем алгебраических чисел называется конечное расширение F поля $\mathbb{Q}$ рациональных чисел. Не ограничивая общности, мы будем считать, что F является подполем поля комплексных чисел $\mathbb{C}$. Из конечности расширения $\mathbb{Q} \subseteq F$ легко следует, что элементы поля F являются алгебраическими числами.

Кольцо $D = F \cap \boldsymbol{R}$, состоящее из всех целых алгебраических чисел, содержащихся в поле алгебраических F, будем называть *кольцом целых величин поля F*.

[27)] Существенным здесь является тот факт, что старший коэффициент многочлена равен 1.

Нашей главной целью будет изучение свойств идеалов колец целых величин полей алгебраических чисел.

Напомним, что для конечно порождённой свободной абелевой группы или, что то же, для свободного $\mathbb{Z}$-модуля A имеет место изоморфизм $A \cong \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$, где число слагаемых определено однозначно и называется *$\mathbb{Z}$-рангом* модуля A. Поскольку $\mathbb{Z}$-ранг является обобщением понятия размерности векторного пространства, мы будем обозначать его $\dim_{\mathbb{Z}} A$. Известно [2, §16], что всякий подмодуль свободного $\mathbb{Z}$-модуля A ранга n также является свободным $\mathbb{Z}$-модулем ранга, не больше n.

(A.6) Предложение. *Пусть F — поле алгебраических чисел с кольцом целых величин D. Любой идеал A кольца D является конечно порождённым свободным $\mathbb{Z}$-модулем. Если $A \neq 0$, то $\dim_{\mathbb{Z}} A = \dim_{\mathbb{Q}} F$.*

Доказательство. См. [2, Теорема 17.9]. □

Коммутативное кольцо R называется *областью целостности*, если $R \neq 0$ и для любых $rs \in R$ из равенства $rs = 0$ следует, что либо $r = 0$, либо $s = 0$. Например, любое ненулевое подкольцо поля будет областью целостности. Верно и обратное: всякая область целостности вкладывается в некоторое поле, например в своё *поле частных*.

(A.7) Предложение. *Всякая конечная область целостности будет полем.*

✎ Доказать предложение (A.7).

Назовём область целостности R *целозамкнутой* в своём поле частных K, если любой элемент из K, являющийся корнем некоторого многочлена

$$x^n + b_1x^{n-1} + b_2x^{n-2} + \ldots + b_n,$$

где $b_1, b_2, \ldots, b_n \in R$, лежит в R. Например, предложение (A.1) утверждает, что кольцо $\mathbb{Z}$ целозамкнуто в $\mathbb{Q}$.

✓ Всюду далее мы будем предполагать, что F — поле алгебраических чисел с кольцом целых величин D.

(A.8) Предложение. (i) *Для любого $\alpha \in F$ существует число $m \in \mathbb{Z}$ такое, что $m\alpha \in D$. В частности, F совпадает с полем частных области целостности D.*

(ii) *Кольцо D целозамкнуто в F.*

Доказательство. (i) Поскольку α — алгебраическое число, то из (A.2)(i) следует существование числа $m \in \mathbb{Z}$ такого, что $m\alpha \in \boldsymbol{R}$. Так как $m\alpha \in F$, то $m\alpha \in D$.

(ii) Если элемент $\alpha \in F$ удовлетворяет равенству $\alpha^n + b_1\alpha^{n-1} + \ldots + b_n = 0$, где $b_i \in D$, то кольцо $D[\alpha]$ является конечно порожденным D-модулем. В силу (A.6) кольцо D является конечно-порождённым $\mathbb{Z}$-модулем, откуда следует, что и $D[a]$ является (ненулевым) конечно-порождённым $\mathbb{Z}$-модулем. Тогда $\alpha \in R$ по (A.4), откуда следует, что $\alpha \in D$. □

(A.9) Лемма. *Если A — ненулевой идеал в D, то $A \cap \mathbb{Z} \neq 0$.*

✎ **(A.10)** Доказать лемму (A.9).

(A.11) Предложение. *Если A — ненулевой идеал в D, то факторкольцо D/A конечно.*

Доказательство. В силу (A.9) существует $0 \neq a \in A \cap \mathbb{Z}$. Тогда идеал aD содержится в A. Поэтому достаточно показать, что факторкольцо D/aD конечно. На самом деле мы покажем, что оно состоит из a^n элементов, где $n = \dim_{\mathbb{Q}} F$.

Согласно предложению (A.6) существуют элементы $\omega_1, \ldots, \omega_n \in D$ такие, что $D = \omega_1\mathbb{Z} \oplus \ldots \oplus \omega_n\mathbb{Z}$, где $n = \dim_{\mathbb{Q}} F$. Отметим, что отсюда следует, что если $\omega \in aD$ и $\omega = \sum_i b_i\omega_i$, $b_i \in \mathbb{Z}$, то все коэффициенты b_i делятся на a.

Пусть $\Gamma = \{\sum_i a_i\omega_i \,|\, 0 \leqslant a_i < a\}$. Покажем, что Γ является множеством представителей для смежных классов D по aD. Пусть $\omega \in D$ тогда существуют $b_i \in \mathbb{Z}$ такие, что $\omega = \sum_i b_i\omega_i$. Запишем $b_i = q_ia + a_i$, где $0 \leqslant a_i < a$. Тогда очевидно, что $\omega D = \gamma D$, где $\gamma = \sum_i a_i\gamma_i \in \Gamma$.

Таким образом, каждый смежный класс D по aD содержит некоторый элемент из S. Если $\omega = \sum_i a_i\omega_i$ и $\omega' = \sum_i a_i'\omega_i$ — элементы из Γ, лежащие в одном классе D по aD, то $\omega - \omega' \in aD$ и, значит, целые числа $a_i - a_i'$ делятся на a. Так как $0 \leqslant a_i, a_i' < a$, отсюда следует, что $a_i = a_i'$ и $\omega = \omega'$. Таким образом, Γ есть множество представителей смежных классов D по aD и факторкольцо D/aD содержит a^n элементов, как и утверждалось. □

Кольцо R называется *нётеровым (слева)*, если любая возрастающая цепочка его (левых) идеалов $I_1 \subseteq I_2 \subseteq \ldots$ стабилизируется. Другими словами, существует натуральное число s такое, что $I_s = I_{s+1} = \ldots$

(А.12) Следствие. *Кольцо D нётерово.*

✎ **(А.13)** Доказать следствие (А.12).

Идеал I коммутативного кольца R называется *простым*, если R/I — область целостности. Это эквивалентно тому, что $I \neq R$ и множество $R \setminus I$ замкнуто относительно умножения.

✎ **(А.14)** Найти все простые идеалы кольца $\mathbb{Z}$.

✎ **(А.15)** Показать, что всякий максимальный идеал коммутативного кольца будет простым. Верно ли обратное?

(А.16) Следствие. *Каждый ненулевой простой идеал из D максимален.*

✎ **(А.17)** Доказать следствие (А.16).

Мы установили три важных свойства кольца D, которые легли в основу следующего определения.

(А.18) Определение. Область целостности, которая является нётеровой, целозамкнутой в своём поле частных и в которой всякий ненулевой простой идеал максимален называется *дедекиндовой областью*.

Таким образом, кольца целых величин полей алгебраических чисел являются дедекиндовыми областями. Замечательным свойством дедекиндовых областей является справедливость аналога основной теоремы арифметики: всякий ненулевой идеал дедекиндовой области допускает однозначное разложение в произведение простых идеалов. В этом идеалы схожи с целыми числами. Кроме того, как и для целых чисел, множество идеалов дедекиндовой области можно вложить в более широкий класс «дробных идеалов», в котором всякий ненулевой идеал будет обратим.

(А.19) Определение. *Дробным идеалом* поля F называется конечно порождённый D-подмодуль D-модуля F. Дробный идеал поля F называется *целым*, если он содержится в D.

(А.20) Предложение. *Всякий идеал кольца D является целым идеалом поля F.*

Доказательство. В силу (А.6) всякий идеал кольца D конечно порождён как $\mathbb{Z}$-модуль, а, значит, и конечно порождён как D-модуль, т. е. является дробным идеалом в F. $\square$

(А.21) Предложение. *Пусть A — дробный идеал в F. Тогда в F существует дробный идеал B такой, что $AB = D$.*

Доказательство. См. [2, Теорема 18.13]. $\square$

(А.22) Следствие. *Пусть I — собственный идеал из $\boldsymbol{R}$ и пусть $\gamma_1, \ldots, \gamma_n \in \mathbb{C}$ — алгебраические числа, не все равные нулю. Тогда в поле $\mathbb{Q}(\gamma_1, \ldots, \gamma_n)$ существует элемент β такой, что $\gamma_i\beta \in R$ для всех i, но не все элементы $\gamma_i\beta$ лежат в I.*

Доказательство. Легко видеть, что поле $F = \mathbb{Q}(\gamma_1, \ldots, \gamma_n)$ является полем алгебраических чисел. Пусть $D = F \cap \boldsymbol{R}$ — кольцо целых величин поля F. Рассмотрим D-модуль A, порождённый элементами $\gamma_1, \ldots, \gamma_n$. Тогда A — дробный идеал поля F. Из (А.21) следует, что в F существует дробный идеал B такой, что $AB = D$. В частности, $AB \nsubseteq I$ и, значит, существует элемент $\beta \in B$ такой, что $A\beta \nsubseteq I$. Но тогда $\gamma_i\beta \notin I$ для некоторого i. Отсюда следует требуемый результат. $\square$

Б Доказательства некоторых утверждений

Доказательство (2.3). Пусть I — собственный правый (левый, двусторонний) идеал кольца R и пусть $\mathscr{S}$ — множество собственных правых (левых, двусторонних) идеалов кольца R, содержащих I. Если показать, что $\mathscr{S}$ содержит максимальный элемент, то он, очевидно, будет максимальным правым (левым, двусторонним) идеалом в R, содержащим I. По лемме Цорна достаточно проверить, что любая цепь

(Б.1)
$$I_1 \leqslant I_2 \leqslant \ldots$$

элементов из $\mathscr{S}$ ограничена сверху. Пусть $L = \bigcup_{i \geqslant 1} I_i$. Тогда L — верхняя грань для цепи (Б.1) и нужно лишь проверить, что $L \in \mathscr{S}$. Если это не так, то $L = R$ поскольку L содержит I и, значит, 1_R лежит в некотором идеале I_{i_0}. Но тогда $R = I_{i_0}$, что противоречит включению $I_{i_0} \in \mathscr{S}$. $\square$

Доказательство (2.7). Пусть $I \trianglelefteqslant_r R$, $I \neq R$ и элемент $r \in I$ обратим справа, т. е. существует $s \in R$ такой, что $rs = 1$. Тогда $1 \in I$ и, значит, для любого $t \in R$ имеем $t = 1t \in I$. Следовательно, $I = R$ вопреки предположению.

Доказательство (2.9). (ii) Включение $\mathrm{Z}(R)^{\times} \leqslant \mathrm{Z}(R) \cap R^{\times}$ очевидно. Обратно, если элемент $z \in Z(R)$ обратим в R и w — его обратный, то для произвольного $r \in R$, умножив равенство $zr = rz$ справа и слева на w, получим $rw = wr$. Поэтому $w \in \mathrm{Z}(R)$ и, значит $z \in Z(R)^{\times}$.

(iii) Всякий элемент $z \in \mathrm{Z}(R)^{\times}$ лежит в $R^{\times}$ и перестановочен со всеми элементами из R. В частности, $z \in \mathrm{Z}(R^{\times})$. $\square$

Доказательство (2.10). Поскольку (i) является частным случаем (ii) при $I = \{0\}$, то докажем (ii). Пусть $a \in R \setminus I$. Существует элемент $b \in R \setminus I$ такой, что $ab = 1$. Также существует элемент $c \in R \setminus I$ такой, что $bc = 1$. Тогда $c = abc = a$ и, значит, $ba = 1$, т. е. элемент a обратим слева. $\square$

Доказательство (2.14). (i) Определим отображение $\tau : S \to T$ следующим образом. Пусть $s \in S$. В силу сюръективности гомоморфизма φ существует элемент $r \in R$ такой, что $r\varphi = s$. Тогда мы положим $s\tau = r\psi$. Проверим корректность этого определения. Пусть $r_0 \in R$ также является прообразом элемента s относительно φ. Тогда существует элемент $k \in \operatorname{Ker}\varphi$ такой, что $r_0 - r = k$. По условию $\operatorname{Ker}\varphi \subseteq \operatorname{Ker}\psi$ и, значит, $k \in \operatorname{Ker}\psi$. Поэтому $(r_0 - r)\psi = k\psi = 0$, т. е. $r_0\psi = r\psi$.

Если $s_1, s_2 \in S$ и элементы $r_1, r_2 \in R$ удовлетворяют $r_1\varphi = s_1$ и $r_2\varphi = s_2$, то $(r_1 + r_2)\varphi = s_1 + s_2$ и $(r_1r_2)\varphi = s_1s_2$. Поэтому $(s_1 + s_2)\tau = (r_1 + r_2)\psi = r_1\psi + r_2\psi = s_1\tau + s_2\tau$ и, аналогично, $(s_1s_2)\tau = s_1\tau s_2\tau$. Ясно также, что $(1_S)\tau = 1_T$, поскольку $(1_R)\varphi = 1_S$ и $(1_R)\psi = 1_T$. Итак, τ является требуемым гомоморфизмом колец.

Пусть $\tau_0 : S \to T$ — другой гомоморфизм с условием $\psi = \varphi\tau_0$. Возьмём $s \in S$. Существует элемент $r \in R$ такой, что $r\varphi = s$. Тогда $s\tau_0 = r\varphi\tau_0 = r\psi = r\varphi\tau = s\tau$. Значит, $\tau_0 = \tau$.

Утверждение (ii) доказывается вполне аналогично. $\square$

Доказательство (2.20). (i) Достаточно доказать включение $I \subseteq (I \cap I_1) \oplus \ldots \oplus (I \cap I_n)$. Пусть $r \in I$. Запишем $1 = e_1 + \ldots + e_n$, где $e_i \in I_i$. Имеем $r = r(e_1 + \ldots + e_n) = re_1 + \ldots + re_n$, и $re_i \in I_i$, так как $I_i \trianglelefteqslant R$. С другой стороны, $re_i \in I$, поскольку $I \trianglelefteqslant_r R$. Следовательно, $re_i \in I \cap I_i$, откуда следует требуемое.

(ii) Доказательство аналогично. Здесь нужно записать $r = (e_1 + \ldots + e_n)r$. Тогда $e_ir \in I \cap I_i$. $\square$

Доказательство (2.22). Так как $I_i \trianglelefteqslant R$ из (2.20)(ii) следует, что $I_i = (I_i \cap J_1) \oplus \ldots \oplus (I_i \cap J_n)$. Поскольку $I_i \cap J_j \trianglelefteqslant R$, по условию получаем, что существует индекс $i\sigma \in \{1, \ldots, n\}$ такой, что $I_i \cap J_{i\sigma} = I_i$ и $I_i \cap J_j = 0$ при $j \neq i\sigma$, т. е. $I_i \subseteq J_{i\sigma}$ для всех $i = 1, \ldots, m$. Так как $R = \bigoplus_i I_i = \bigoplus_i J_{i\sigma}$ и все идеалы J_j ненулевые, отсюда следует, что отображение $\sigma : \{1, \ldots, m\} \to \{1, \ldots, n\}$ сюръективно и, в частности, $m \geqslant n$.

Аналогично, существует сюръективное отображение $\tau : \{1, \ldots, n\} \to \{1, \ldots, m\}$ такое что $J_j \subseteq I_{j\tau}$ для всех $j = 1, \ldots, n$. В частности, $n \geqslant m$. Таким образом, $m = n$, т. е. отображение σ биективно. $\square$

Доказательство (2.29). Поскольку (i) следует из (ii), докажем (ii). Пусть отображение $\alpha : \operatorname{End}_R(eR) \to eRe$ действвет по правилу $\alpha(\varphi) = e\varphi$ для любого $\varphi \in \operatorname{End}_R(eR)$. Так как $e\varphi \in eR$, имеем $e\varphi = e(e\varphi)$. С другой стороны, $e\varphi = (ee)\varphi = (e\varphi)e$ ввиду того, что $\varphi \in \operatorname{End}_R(eR)$. Значит, $e\varphi = e(e\varphi)e$, т. е. образ α действительно лежит в eRe.

Пусть $\varphi, \psi \in \operatorname{End}_R(eR)$. Тогда

$$\alpha(\varphi + \psi) = e(\varphi + \psi) = e\varphi + e\psi = \alpha(\varphi) + \alpha(\psi),$$

т. е. отображение α аддитивно. Покажем инъективность. Пусть $\alpha(\varphi) = 0$. Тогда для любого $r \in R$ имеем

$$(er)\varphi = (e\varphi)r = \alpha(\varphi)r = 0r = 0,$$

откуда следует, что φ — нулевой элемент из $\operatorname{End}_R(eR)$.

Покажем, что α сюръективно. Пусть $r \in R$. Определим $\varphi \in \operatorname{End}_R(eR)$ по правилу $(es)\varphi = eres$ для любого $s \in R$. Легко видеть, что φ является R-линейным, т. е. действительно лежит в $\operatorname{End}_R(eR)$. Поскольку $\alpha(\varphi) = e\varphi = ere$, отсюда вытекает сюръективность α.

Пусть, наконец, $\varphi, \psi \in \operatorname{End}_R(eR)$. Тогда

$$\alpha(\varphi\psi) = e\varphi\psi = (e(e\varphi))\psi = e\psi\, e\varphi = \alpha(\psi)\,\alpha(\varphi),$$

и значит, α является антиизоморфизмом колец. $\square$

Доказательство (2.31). Пусть $z \in \mathrm{Z}(R^{\times})$. В силу (2.9)$(ii)$ достаточно показать, что $z \in \mathrm{Z}(R)$. Пусть $r \in R$. По условию $r = r_1z_1 + \ldots + r_kz_k$ для подходящих $r_i \in R^{\times}$, $z_i \in \mathrm{Z}(R)$, $i = 1, \ldots, k$. Поэтому $zr = rz$, откуда следует требуемое. $\square$

Доказательство (2.35). Пункт (ii) будем доказывать для правых идеалов. Рассуждение для левых аналогично.

$(i) \Rightarrow (ii)$ Предположим, что $eR = I_1 \oplus I_2$, где $I_1, I_2 \leqslant eR$ — правые идеалы из R. Запишем $e = e_1 + e_2$, где $e_i \in I_i$, $i = 1, 2$. Поскольку умножение слева на e действует тождественно на все элементы из eR, мы получаем $e_i = ee_i = e_1e_i + e_2e_i$. Но $e_je_i \in I_j$, $j = 1, 2$, и, ввиду однозначности разложения, отсюда следует $e_i = e_i^2$ и $e_je_i = 0$ при $j \neq i$. Значит, один из идемпотентов e_1, e_2 равен нулю. Обозначим его e_i. Тогда $e = e_j \in I_j$, где $j \neq i$, и $eR \leqslant I_j$, откуда следует $I_i = 0$.

$(ii) \Rightarrow (iii)$ Пусть, напротив, e_1 — идемпотент из eRe, отличный от 0 и e. Обозначим $e_2 = e - e_1$. Тогда e_2 также идемпотент из eRe, ортогональный e_1 и отличный от 0 и e. Поскольку $e_1 = ee_1 \in eR$ и $e_2 = ee_2 \in eR$, то $e_1R \leqslant eR$ и $e_1R \leqslant eR$. Значит, $e_1R + e_2R \leqslant eR$. Обратно, для любого $er \in eR$ имеем $er = e_1r + e_2r \in e_1R + e_2R$, т. е. $e_1R + e_2R = eR$. Осталось показать, что сумма $e_1R + e_2R$ прямая. Пусть $s \in e_1R \cap e_2R$. Тогда существуют $r_1, r_2 \in R$ такие, что $s = e_1r_1 = e_2r_2$. Но тогда $s = e_1r_1 = e_1(e_1r_1) = e_1(e_2r_1) = 0$ в силу ортогональности идемпотентов e_1 и e_2.

$(iii) \Rightarrow (i)$ Допустим, что $e = e_1 + e_2$, где $e_i \in R$, $i = 1, 2$, — ортогональные идемпотенты. Тогда $ee_i = (e_1 + e_2)e_i = e_i^2 = e_i$ и, аналогично, $e_ie = e_i$. Значит, $e_i = ee_ie \in eRe$. Тогда по условию $e_i = 0$ или e. $\square$

Доказательство (2.36). $(i) \Rightarrow (ii)$ Пусть $eR = I_1 \oplus I_2$, где $I_1, I_2 \leqslant eR$ — двусторонние идеалы из R. Запишем $e = e_1 + e_2$, где $e_i \in I_i$, $i = 1, 2$. Поскольку e — единица кольца Re, то e_i — центральные идемпотенты кольца eR по предложению (2.17). Показать, что $e_i \in \mathrm{Z}(R)$. Пусть $r \in R$. Учитывая, что $re_i, e_ir \in Re$ и $e_i \in \mathrm{Z}(Re)$, мы получаем $e_ir = e_i(e_ir) = e_ire_i = (re_i)e_i = re_i$. Из примитивности идемпотента e следует, что $e_i = 0$ для $i = 1$ или 2, то есть $e = e_j$ где $i \neq j \in \{1, 2\}$. Поэтому $eR \leqslant I_j$ и $I_i = 0$.

$(ii) \Rightarrow (i)$ Предположим, что $e = e_1 + e_2$, где $e_i \in Z(R)$, $i = 1, 2$, — ортогональные идемпотенты. Тогда $e_i = e_ie \in Re$ и, значит, идеалы $I_i = Re_i$ лежат в Re. Любой элемент $re \in Re$ можно записать как $re = re_1 + re_2$, то есть $Re = I_1 + I_2$. Покажем, что эта сумма прямая. Если $s \in I_1 \cap I_2$, то существуют $r_1, r_2 \in R$ такие, что $s = r_1e_1 = r_2e_2$. Но тогда $s = r_1e_1 = (r_1e_1)e_1 = (r_2e_2)e_1 = 0$ в силу ортогональности идемпотентов e_1 и e_2. По условию $I_i = 0$ для $i = 1$ или 2 и, значит, $e_i = 0$. $\square$

Доказательство (2.37). (i) Me_i — подгруппа аддитивной группы M, которая выдерживает умножение на любой элемент $r \in R$, поскольку $Me_ir = Mre_i \subseteq Me_i$ в силу того, что $e_i \in \mathrm{Z}(R)$. Следовательно, Me_i — R-подмодуль.

(ii) Пусть $m_1e_1 + \ldots + m_ne_n = 0$ для некоторых $m_i \in M$. Умножив справа на e_i и учитывая ортогональность идемпотентов, получим $m_ie_i = 0$ для любого i. Отсюда вытекает, что сумма $Me_1 + \ldots + Me_n$ прямая.

(iii) Для любого $m \in M$ имеем $m = m1_R = me_1 + \ldots + me_n \in Me_1 + \ldots + Me_n$. Учитывая (ii), получаем требуемое. $\square$

Доказательство (3.7). (i) Пусть $K \in \mathscr{K}(G)$. Достаточно показать, что любой элемент $g \in G$ коммутирует с $\widehat{K}$. Это следует из соотношений

$$g^{-1}\widehat{K}g = \sum_{x \in K} g^{-1}xg = \widehat{K}.$$

(ii) Пусть элемент $a = \sum_{x \in G} \alpha_x x$ лежит в $\mathrm{Z}(RG)$. Тогда для каждого $g \in G$

$$\sum_{x \in G} \alpha_x x = a = g^{-1}ag = \sum_{x \in G} \alpha_x (g^{-1}xg).$$

Сравнивая коэффициенты при элементах $x \in G$ в правой и левой частях, получим, что $\alpha_x = \alpha_{gxg^{-1}}$ для всех $g \in G$. Таким образом, коэффициенты при любых элементах одного и того же класса сопряжённости совпадают и, значит, a является R-линейной комбинацией элементов $\widehat{K}$, $K \in \mathscr{K}(G)$.

Так как классовые суммы $\widehat{K}$, где $K \in \mathscr{K}(G)$, являются суммами элементов непересекающихся подмножеств группы G, то коэффициенты в разложении любого элемента из $\mathrm{Z}(RG)$ в виде R-линейной комбинации сумм $\widehat{K}$ определяются однозначно.

(iii) Если $z_1, z_2 \in M$, то существует элемент $g \in G$ такой, что $z_2 = z_1^g$. Поэтому между множеством пар (x_1, y_1), где $x_1 \in K$, $y_1 \in L$, таких, что $x_1y_1 = z_1$, и множеством пар (x_2, y_2), где $x_2 \in K$, $y_2 \in L$, таких, что $x_2y_2 = z_2$, можно установить взаимно однозначное соответствие $(x_1, y_1) \to (x_1^g, y_1^g)$. Поэтому мощности этих множеств совпадают.

(iv) Фиксируем $z \in M$. Коэффициент при $\widehat{M}$ в произведении $\widehat{K}\widehat{L}$ равен коэффициенту при z и, значит, совпадает с числом a_{KLM} пар пар (x, y), где $x \in K$, $y \in L$, таких, что $xy = z$. $\square$

Доказательство (3.8). Включение $\mathrm{Z}(SG) \supseteq \mathrm{Z}(RG) \cap SG$ очевидно. Пусть $z \in \mathrm{Z}(SG)$ из (3.7)(ii) следует, что z является S-линейной комбинацией классовых сумм $\widehat{K}$, а, значит, и их R-линейной комбинацией. Поэтому $z \in \mathrm{Z}(RG)$ опять-таки в силу (3.7)(ii). $\square$

Доказательство (3.11). Элемент $\sum_{g\in G} a_g g$ из RG лежит в $\operatorname{Ker}\tilde{\varphi}$ тогда и только тогда, когда

$$0 = \Big(\sum_{g\in G} a_g g\Big)\tilde{\varphi} = \sum_{g\in G} a_g\varphi\ g.$$

Ввиду однозначности представления элемента $0 \in SG$ в виде S-линейной комбинации элементов группы G имеем $a_g\varphi = 0$ для всех $g \in G$. Это означает, что $a_g \in \operatorname{Ker}\varphi$ для всех $g \in G$.

Аналогично, элемент $\sum_{K\in\mathscr{K}(G)} a_{_K}\widehat{K}$ из $\mathrm{Z}(RG)$ лежит в $\operatorname{Ker}\tilde{\varphi}$ тогда и только тогда, когда $a_{_K} \in \operatorname{Ker}\varphi$ для всех $K \in \mathscr{K}(G)$. $\square$

Доказательство (3.43). Пусть $v \in V$ и $v \neq 0$. Отображение $\tau : a \mapsto va$ является гомоморфизмом A-модулей $A^\circ \to V$. Его образ ненулевой, поскольку содержит $1_A\tau = v$. Из простоты V следует, что τ — эпиморфизм. Положим $I = \operatorname{Ker}\tau$. Очевидно, что $I = \operatorname{Ann}(v)$. Но тогда I — максимальный правый идеал алгебры A и $A^\circ/I \cong V$ по теореме (3.24).

Доказательство (4.3). Как следует из замечаний после определения (2.16), алгебры A_1 и A_2 можно рассматривать как идеалы в алгебре A. По предложению (2.20) любой максимальный правый идеал из A имеет вид $I_1 \oplus A_2$ или $A_1 \oplus I_2$, где I_1 и I_2 — максимальные правые идеалы в A_1 и A_2, соответственно. Поэтому равенство $\mathrm{J}(A) = \mathrm{J}(A_1) \oplus \mathrm{J}(A_2)$ следует из предложения (4.2). $\square$

Доказательство (4.5). Пусть $a \in I$ и $1 - b$ — правый обратный для $1 - a$. Тогда

$$(1-a)(1-b) = 1, \tag{Б.2}$$

откуда следует, что $b = a(b-1) \in I$. Но тогда по предположению $1 - b$ также обратим справа. Пусть c — его правый обратный. Тогда, умножив справа на c обе части равенства (Б.2) получим $1 - a = c$. То есть $(1-b)(1-a) = 1$, что и требовалось доказать. $\square$

Доказательство (4.6). Приведём два доказательства этого предложения.

Пусть, напротив, $I \nleqslant \mathrm{J}(A)$. Из предложения (4.2) следует, что I не содержится в некотором максимальном правом идеале M. Тогда $R = I + M$ и $1 = a + m$ для некоторых $a \in I$, $m \in M$. Но по условию элемент $m = 1 - a$ обратим справа. Это противоречит тому, что он содержится в собственном правом идеале M.

Второе доказательство. Пусть, напротив, $I \nleqslant \mathrm{J}(A)$. Тогда существует неприводимый A-модуль V такой, что $VI \neq 0$, а, значит, существует элемент $0 \neq v \in V$, для которого $vI \neq 0$. В силу простоты V получаем $vI = V$. В частности, существует элемент $a \in I$, для которого $va = v$, т. е. $v(1-a) = 0$. По условию элемент $1 - a$ обратим справа, откуда следует $v = 0$, противоречие. $\square$

Доказательство (4.10). (i) Включение $e\mathrm{J}(A)e \subseteq \mathrm{J}(A) \cap eAe$ очевидно.

(ii) Докажем включение $\mathrm{J}(A) \cap eAe \subseteq \mathrm{J}(eAe)$. Легко видеть, что $\mathrm{J}(A) \cap eAe$ — идеал алгебры eAe. В силу (4.6) достаточно показать, что для всякого элемента $a \in \mathrm{J}(A) \cap eAe$ элемент $e - a$ обратим справа в eAe. Поскольку $a \in \mathrm{J}(A)$, из (4.7) следует, что существует элемент $b \in A$ такой, что $(1-a)b = 1$. Тогда

$$(e-a)(ebe) = e^2be - aebe = ebe - eabe = e(b-ab)e = e^2 = e,$$

где $ae = ea$, поскольку $a \in eAe$ и e — единица кольца eAe. Итак, ebe — правый обратный к $e - a$ в eAe, что и требовалось показать.

(iii) Докажем включение $\mathrm{J}(eAe) \subseteq e\mathrm{J}(A)e$. Пусть $a \in \mathrm{J}(eAe)$. Тогда $a = eae$ опять-таки поскольку $a \in eAe$ и e — единица кольца eAe. Достаточно показать, что $a \in \mathrm{J}(A)$, т. к. отсюда будет следовать, что $a = eae \in e\mathrm{J}(A)e$.

Рассмотрим правый идеал aA из A. Если мы покажем, что для всякого элемента $ax \in aA$, где $x \in A$, элемент $1 - ax$ обратим справа в A, то в силу (4.6) получим $a \in aA \subseteq \mathrm{J}(A)$, как и требуется.

Так как $a \in \mathrm{J}(eAe)$ и $exe \in eAe$, то $axe = aexe \in \mathrm{J}(eAe)$, и в силу (4.7) существует элемент $b \in eAe$ такой, что $(e - axe)b = e$ и, значит,

$$e = (e - axe)b = (1-ax)eb = (1-ax)b,$$

поскольку $eb = b$. Отсюда получаем

$$(1-ax)(1+bax) = (1-ax) + (1-ax)bax = 1 - ax + eax = 1,$$

поскольку $ea = a$. Итак, элемент $1 + bax$ — правый обратный к $1 - ax$ в A, что и требовалось показать. $\square$

Доказательство (4.11). (i) Пусть идеал $I \trianglelefteq_r A$ состоит из нильпотентных элементов. Поскольку для любого $a \in I$ элемент $1 - a$ обратим, то требуемое следует из леммы (4.6).

(ii) Утверждение следует из пункта (i), поскольку в нильпотентном идеале всякий элемент нильпотентен.

Приведём ещё одно доказательство. Пусть идеал $I \trianglelefteq_r A$ нильпотентен и $I^n = 0$. Для включения $I \leqslant \mathrm{J}(A)$ достаточно проверить, что I аннулирует любой неприводимый A-модуль V. Пусть, напротив, $VI \neq 0$. Тогда $VI = V$ в силу простоты V, и мы получаем

$$V = VI = (VI)I = VI^2 = \ldots = VI^n = 0,$$

противоречие. □

Доказательство (4.12). Если $a^n = 0$ и $b^m = 0$, то, используя коммутативность, получим $(a+b)^{m+n} = 0$ и $(ta)^n = 0$ для любого $t \in A$. Второе утверждение следует из обратимости элемента $1 - a$ и предложения (4.6). □

Доказательство (4.13). Пусть V — ненулевой конечно порождённый A-модуль, $v_1, \ldots, v_n$ — его порождающие и $\mathscr{S}$ — множество собственных подмодулей модуля V. По лемме Цорна достаточно показать, что любая цепь

(Б.3) $$V_1 \leqslant V_2 \leqslant \ldots$$

элементов из $\mathscr{S}$ ограничена сверху. Пусть $W = \bigcup_{i \geqslant 1} V_i$. Тогда W — верхняя грань для цепи (Б.3) и нужно лишь проверить, что $W \in \mathscr{S}$. Если это не так, то $W = V$ и, значит, каждый порождающий v_j лежит в некотором подмодуле V_{i_j}. Но тогда все порождающие содержатся в V_{i_0}, где $i_0 = \max\{i_1, \ldots, i_n\}$. Следовательно, $V = V_{i_0}$, что противоречит включению $V_{i_0} \in \mathscr{S}$.

Доказательство (4.18).. Докажем, что (iii) эквивалентно (i) и (ii).

Пусть верно (i). Поскольку максимальный правый идеал I_r единственный, то он совпадает с $\mathrm{J}(S)$ по предложению (4.2). Пусть $a \notin I_r$. Тогда, ввиду правой обратимости элемента $a + I_r$ из S/I_r существует элемент $s \in S$ такой, что $as = 1 - c$ для некоторого $c \in \mathrm{J}(S)$. Но тогда as обратим справа в S по предложению (4.7). Следовательно, и элемент a обратим справа. Поэтому в силу (2.10)(ii) имеет место (iii).

Доказательство того, что из (ii) следует (iii) проводится «симметрично».

Пусть верно (iii). Тогда любой максимальный правый (левый) идеал содержится в I, т. к. в нём нет обратимых справа (слева) элементов. Значит, имеют место пункты (i) и (ii). □

Доказательство (5.2). Заметим, что идеал $\mathrm{J}(A)^n$ является F-подпространством в A и, значит, конечномерен. Поскольку A содержит F, $\mathrm{J}(A)^n$ конечно порождён как A-модуль. Если $\mathrm{J}(A)^n \neq 0$, то по теореме (4.14) имеет место строгое включение $\mathrm{J}(A)^{n+1} < \mathrm{J}(A)^n$, и поэтому из соображения размерности ясно, что идеал $\mathrm{J}(A)$ нильпотентен. □

Доказательство (5.4). Из предложения (5.2) следует, что $\mathrm{J}(A) \cap \mathrm{Z}(A)$ — нильпотентный идеал алгебры $\mathrm{Z}(A)$. Значит, по предложению (4.11) имеется включение $\mathrm{J}(A) \cap \mathrm{Z}(A) \leqslant \mathrm{J}(\mathrm{Z}(A))$. Обратно, пусть $z \in \mathrm{J}(\mathrm{Z}(A))$. Достаточно показать, что $z \in \mathrm{J}(A)$. Правый идеал zA нильпотентен, поскольку z коммутирует со всеми элементами из A и $z^n = 0$ для некоторого n. Поэтому $z \in zA \leqslant \mathrm{J}(A)$.

Отметим, что включение $\mathrm{J}(\mathrm{Z}(A)) \leqslant \mathrm{J}(A) \cap \mathrm{Z}(A)$ также вытекает из предложения (4.16), поскольку A является конечно порождённым как F-модуль, а значит, и как $\mathrm{Z}(A)$-модуль ввиду включения $F \leqslant \mathrm{Z}(A)$ □

Доказательство (6.4). По пункту (ii) предложения (6.1) фактормодуль V/U изоморфен некоторому подмодулю из V. Поэтому достаточно доказать полную приводимость подмодуля U. Пусть $W \leqslant U$. Тогда по пункту (ii) предложения (6.1) существует подмодуль $W_0 \leqslant V$ такой, что $V = W \oplus W_0$. Тогда $U = W \oplus (U \cap W_0)$. □

Доказательство (6.6). (i) Пусть $\varphi \in \mathrm{End}_A(V)$. Достаточно показать, что $\mathrm{W}_M(V)\varphi \subseteq \mathrm{W}_M(V)$. Заметим, что если $U \leqslant V$ и $U \cong M$, to $U\varphi$ — подмодуль из V, являющийся гомоморфным образом подмодуля U. В силу неприводимости $U\varphi$ изоморфен 0 или M, т. е. $U\varphi \subseteq \mathrm{W}_M(V)$. Отсюда следует требуемое включение.

(ii) Очевидно, что правая часть содержится в $\mathrm{W}_M(V)$. Обратно, пусть $U \leqslant V$ и $U \cong M$. Пусть $\pi_i \in \mathrm{End}_A(V)$ — проекция V на прямое слагаемое V_i. Очевидно, что $U \subseteq \bigoplus_i U\pi_i$. С другой стороны, если $U\pi_i \neq 0$, то $U\pi_i \cong M$ и, значит, $U \subseteq \bigoplus_{V_i \cong M} V_i$.

(iii) Число подмодулей V_i, изоморфных M равно $\dim_F(\mathrm{W}_M(V))/\dim_F(M)$ в силу (ii). □

Доказательство (7.2). Достаточно заметить, что у алгебр A и $A/\mathrm{J}(A)$ одинаковое множество неприводимых модулей. □

Доказательство (7.5). Если V — неприводимый A-модуль, то по предложению (3.43) он изоморфен фактор модулю A°/I, где I — некоторый максимальный правый идеал алгебры A. По предложению (7.3) модуль A° вполне приводим и, значит, существует правый идеал J такой, что $A^\circ = I \oplus J$. Поскольку $J \cong A^\circ/I \cong V$ и модуль V простой, то J — минимальный правый идеал. □

Доказательство (7.9). Достаточно показать, что $\mathrm{Im}\,\varphi \cap \mathrm{Ker}\,\varphi = 0$. Пусть $u \in \mathrm{Im}\,\varphi \cap \mathrm{Ker}\,\varphi$. Тогда $u = v\varphi$ для некоторого $v \in V$. Поэтому $0 = u\varphi = v\varphi^2 = v\varphi = u$. □

Доказательство (7.8). Обозначим $t=\sum_{g\in G} g$. Легко видеть, что $t\in \mathrm{Z}(FG)$ и $t^2=|G|t=0$, т. е. элемент t нильпотентный. Из следствия (5.3) вытекает, что $t\in \mathrm{J}(\mathrm{Z}(FG))$. Тогда $t\in \mathrm{J}(FG)$ по предложению (5.4). $\square$

Доказательство (7.15). По условию $V=\sum V_i$, где V_i — неприводимые A-модули. Поскольку $\mathrm{J}(A)\leqslant \mathrm{Ann}(V_i)$ для всех i, имеем включение $\mathrm{J}(A)\leqslant \mathrm{Ann}(V)$. С другой стороны, $A_V\cong A/\mathrm{Ann}(V)$ и, значит, алгебра A_V изоморфна гомоморфному образу полупростой алгебры $A/\mathrm{J}(A)$, т. е. сама является полупростой в силу следствия (7.4). $\square$

Доказательство (7.18). Обозначим $B=A_V$. Поскольку $B\cong A/\mathrm{Ann}(V)$ и $\mathrm{J}(A)\subseteq \mathrm{Ann}(V)$, то алгебра B полупроста. Заметим, что V — неприводимый B-модуль и по теореме Веддерберна (7.16) имеет место разложение. $B=\mathrm{W}_V(B^\circ)\oplus \mathrm{Ann}_B(V)$. Но тогда $\mathrm{Ann}_B(V)=0$, т. к. B является факторалгеброй алгебры A по аннулятору $\mathrm{Ann}(V)$. Значит, B — простая алгебра и поэтому V — её единственный неприводимый модуль. $\square$

Доказательство (7.22). (i) Из теоремы Веддерберна (7.16) следует, что

$$\dim_F(A)=\sum_{M\in\mathscr{M}(A)}\dim_F \mathrm{W}_M(A^\circ),$$

где $\mathrm{W}_M(A^\circ)$ — простые F-алгебры, и, кроме того, M является единственным, с точностью до изоморфизма, неприводимым $\mathrm{W}_M(A^\circ)$-модулем. По следствию (7.21) получаем $\dim_F \mathrm{W}_M(A^\circ)=(\dim_F M)^2$.

(ii) Из теоремы (7.16) и предложения (2.21) следует, что $\mathrm{Z}(A)=\bigoplus_{M\in\mathscr{M}(A)}\mathrm{Z}(\mathrm{W}_M(A^\circ))$. По следствию (7.21) простая F-алгебра $\mathrm{W}_M(A^\circ)$ изоморфна $\mathrm{End}_F(M)\cong \mathrm{M}_n(F)$, где $n=\dim_F(M)$. Однако центр $\mathrm{Z}(\mathrm{M}_n(F))$ одномерен, поскольку, как мы отмечали в (2.2), он состоит из скалярных матриц. Значит, размерность $\dim_F \mathrm{Z}(A)$ равна $|\mathscr{M}(A)|$. $\square$

Доказательство (8.5). Пусть $\deg\mathscr{X}_i=n_i$ и $V_i=F^{n_i}$. Тогда из замечаний о соответствии представлений и модулей следует, что A-модули V_i, $i=1,\ldots,s$, с действием $va=v\mathscr{X}_i(a)$, образуют полный набор попарно неизоморфных неприводимых A-модулей. Легко видеть, что $\mathrm{Ker}\,\mathscr{X}_i=\mathrm{Ann}(V_i)$. Отсюда следует требуемое равенство. $\square$

Доказательство (9.5). Чтобы показать, что M — скалярная матрица, можно воспользоваться предложением (9.4), утверждающим, что $\mathrm{Im}\,\mathscr{X}=\mathrm{M}_n(F)$. Приведём, однако, другое доказательство, использующее, по существу, только лемму Шура.

Пусть $V=F^n$. Тогда V является A-модулем с действием $va=v\mathscr{X}(a)$. Если φ — линейное преобразование пространства V, действующее по правилу $v\varphi=vM$, то $\varphi\in\mathrm{End}_A(V)$. Из следствия (3.41) вытекает, что φ — скалярное преобразование и M — скалярная матрица.

Если $z\in Z(A)$, то матрица $\mathscr{X}(z)$ перестановочна с $\mathscr{X}(a)$ для всех $a\in A$ и поэтому скалярна по только что доказанному. Если A коммутативна, то $Z(A)=A$. Значит, любое подпространство из V будет A-инвариантным. Из неприводимости V следует, что $\deg\mathscr{X}=1$. $\square$

Доказательство (10.3). 4. Выберем в качестве базиса регулярного модуля FG° множество элементов группы G и пусть $\mathscr{R}$ — соответствующее регулярное представление. Пусть $g\in G$ и $\mathscr{R}(g)=(\alpha_{x,y})$, $x,y\in G$. Тогда $\alpha_{x,y}\neq 0$ если и только если $xg=y$, и в этом случае $\alpha_{x,y}=1_F$. Поэтому

$$\rho(g)=|\{x\in G\mid xg=x\}|\cdot 1_F=\begin{cases}0_F, & g\neq 1;\\ |G|\cdot 1_F, & g=1.\end{cases}$$

Доказательство (11.3). Пусть $g\in G$, $\mathscr{X}(g)=(\alpha_{ij})\in\mathrm{M}_n(F)$, $\mathscr{Y}(g)=(\beta_{rs})\in\mathrm{M}_m(F)$.

(i) Имеем

$$(v_i\otimes w_r)g=v_ig\otimes w_rg=\sum_{j=1}^{m}\sum_{s=1}^{n}\alpha_{ij}\beta_{rs}(v_j\otimes w_s)$$

и, значит, матрица $(\mathscr{X}\otimes\mathscr{Y})(g)$ равна $\mathscr{X}(g)\otimes\mathscr{Y}(g)$.

(ii) Имеем

$$\chi(g)=\sum_{i=1}^{m}\alpha_{ii},\qquad \psi(g)=\sum_{r=1}^{n}\beta_{rr}.$$

Пусть θ — характер представления $\mathscr{X}\otimes\mathscr{Y}$. Ввиду (i)

$$\theta(g)=\mathrm{tr}(\mathscr{X}(g)\otimes\mathscr{Y}(g))=\sum_{i=1}^{m}\sum_{r=1}^{n}\alpha_{ii}\beta_{rr}=\big(\sum_{i=1}^{m}\alpha_{ii}\big)\big(\sum_{r=1}^{n}\beta_{rr}\big)=\chi(g)\psi(g).$$

Отсюда следует требуемое. $\square$

Доказательство (12.1). (i) Очевидно.

(ii) Это следует из транзитивности действия группы G на компонентах системы импримитивности и того, что I — стабилизатор одной из компонент.

(iii) Множество $\{Wr_1, \dots, Wr_k\}$ совпадает с множеством $\{W_1, \dots, W_k\}$. Поскольку Br_i — базис подпространства Wr_i и W — прямая сумма подпространств W_i, то базис W — объединение базисов этих подпространств.

(iv) Пусть $g \in G$ и блочная $k \times k$-матрица $\mathscr{Y}(g)$ состоит из клеток A_{ij}. Покажем, что $A_{ij} = \mathscr{X}^\circ(r_i g r_j^{-1})$.

Для любого r_i существует единственный r_{i_0} такой, что $r_i g r_{i_0}^{-1} \in I$. Поэтому $\mathscr{X}^\circ(r_i g r_{i_0}^{-1}) = \mathscr{X}(r_i g r_{i_0}^{-1})$, а $\mathscr{X}^\circ(r_i g r_{i_0}^{-1}) = \mathbf{0}$ для всех $j \neq i_0$. С другой стороны, для любого $b \in B$

$$(br_i)g = b(r_i g r_{i_0}^{-1})r_{i_0} = b\mathscr{X}(r_i g r_{i_0}^{-1})r_{i_0}.$$

Поэтому $A_{i,i_0} = \mathscr{X}(r_i g r_{i_0}^{-1}) = \mathscr{X}^\circ(r_i g r_{i_0}^{-1})$ и $A_{ij} = \mathbf{0} = \mathscr{X}^\circ(r_i g r_j^{-1})$ при $j \neq i_0$.

(v) Из (iii) и (iv) следует, что у модуля V имеется базис, в котором соответствующее представление группы G однозначно определяются представлением $\mathscr{X}$ группы I. Отсюда следует требуемое. $\square$

Доказательство (12.5). (i) Очевидно.

(ii) Если $X = \{x_1, \dots, x_m\}$ — набор представителей правых смежных классов H по K и $Y = \{y_1, \dots, y_n\}$ — набор представителей правых смежных классов G по H, то $x_i y_j$ — набор представителей правых смежных классов G по K. Запишем $U^H = \bigoplus_i U \otimes x_i$. Тогда $(U^H)^G = \bigoplus_j \left(\bigoplus_i U \otimes x_i\right) \otimes y_j = \bigoplus_{ij} U \otimes x_i \otimes y_j$. С другой стороны, $U^G = \bigoplus_{ij} U \otimes x_i y_j$. Покажем, что отображение $\varphi : (U^H)^G \to U^G$, действующее по правилу $(u \otimes x_i \otimes y_j)\varphi = u \otimes x_i y_j$ для всех $u \in U$, $x_i \in X$, $y_j \in Y$, и продолженное по линейности на весь модуль $(U^H)^G$, является изоморфизмом FG-модулей. Легко видеть, что φ — изоморфизм векторных пространств. Пусть $g \in G$. Запишем $y_j g = h y_{j'}$ и $x_i h = k x_{i'}$ для подходящих $h \in H$, $k \in K$. Тогда

$$(u \otimes x_i \otimes y_j)g\varphi = (u \otimes x_i h \otimes y_{j'})\varphi = (uk \otimes x_{i'} \otimes y_{j'})\varphi = uk \otimes x_{i'} y_{j'} = u \otimes x_i y_j g = (u \otimes x_i \otimes y_j)\varphi g.$$

Отсюда следует требуемое.

(iii) Пусть R — набор представителей правых смежных классов G по H. Тогда $V^G = \bigoplus_{r \in R} V \otimes r$. Очевидно, что $U^G = \bigoplus_{r \in R} U \otimes r$ — подпространство в V^G, выдерживающее действие группы G. Если $U < V$ и $v \in V \setminus U$, то $v \otimes r \in V^G \setminus U^G$ для любого $r \in R$. Обратная импликация очевидна. $\square$

Доказательство (12.7). Пусть $\mathscr{X}$ — некоторое F-представление группы H с характером χ. Тогда χ^G — характер индуцированного представления $\mathscr{X}^G$. Если для любого $g \in G$ определить

$$\mathscr{X}^\circ(g) = \begin{cases} \mathscr{X}(g), & g \in H; \\ \mathbf{0}, & g \notin H, \end{cases}$$

то $\chi^\circ(g) = \operatorname{tr} \mathscr{X}^\circ(g)$ и из (12.1)(iv) следует, что значение характера представления $\mathscr{X}^G$ на элементе g равно $\sum_{r \in R} \chi^\circ(rgr^{-1})$, где R — произвольная система представителей всех правых смежных классов G по H.

Доказательство (12.10). (i) Отметим сначала, что для произвольных $x \in G$ и $h \in H$ имеет место равенство

$$\text{(Б.4)} \qquad \varphi^\circ(hxh^{-1}) = \varphi^\circ(x),$$

поскольку $\varphi \in \mathrm{cf}_F(H)$, и включение $hxh^{-1} \in H$ выполнено тогда и только тогда, когда $x \in H$.

Обозначим $\varphi_R^G(g)$ значение правой части равенства (12.9). Пусть R_0 — другой набор представителей всех правых смежных классов G по H. Тогда найдутся такие элементы $h_r \in H$, где $r \in R$, что $R_0 = \{h_r r \mid r \in R\}$. В силу (Б.4) имеем

$$\varphi_{R_0}^G(g) = \sum_{r_0 \in R_0} \varphi^\circ(r_0 g r_0^{-1}) = \sum_{r \in R} \varphi^\circ(h_r r g r^{-1} h_r^{-1}) = \sum_{r \in R} \varphi^\circ(rgr^{-1}) = \varphi_R^G(g).$$

(ii) Поскольку группа G является объединением $|H|$ попарно непересекающихся наборов $R_1, \dots, R_{|H|}$ представителей правых смежных классов G по H, ввиду (i) получаем

$$\sum_{x \in G} \varphi^\circ(xgx^{-1}) = \sum_{i=1}^{|H|} \sum_{x \in R_i} \varphi^\circ(xgx^{-1}) = |H|\varphi^G(g).$$

(iii) Любой элемент из класса сопряжённости g^G представи́м в виде ygy^{-1}, где $y \in G$, ровно $|\mathrm{C}_G(g)|$ способами. Поэтому в силу (ii)

$$\text{(Б.5)} \qquad |H|\varphi^G(g) = \sum_{y \in G} \varphi^\circ(ygy^{-1}) = |\mathrm{C}_G(g)| \sum_{x \in g^G} \varphi^\circ(x) = |\mathrm{C}_G(g)| \sum_{x \in g^G \cap H} \varphi(x).$$

Пусть R_g — набор представителей всех классов сопряжённости группы H, содержащихся в классе g^G. Так как $\varphi \in \mathrm{cf}_F(H)$, то правая часть в (Б.5) равна

$$|\mathrm{C}_G(g)| \sum_{x \in R_g} |x^H| \varphi(x).$$

По условию $|H| \neq 0$ в поле F. Поэтому $|x^H|/|H| = 1/|\mathrm{C}_H(x)|$. Разделив обе части на $|H|$, получим требуемое. □

Доказательство (13.1). (i) Выберем произвольный элемент $h^g \in H^g$, где $h \in H$. Тогда

$$(Wg)h^g = Wg(g^{-1}hg) = (Wh)g = Wg,$$

т. е. Wg является FH^g-модулем. Выберем базис $w_1, \ldots, w_n$ подпространства W. Тогда $w_1 g, \ldots, w_n g$ — базис Wg. Пусть $\mathscr{X}$ и $\mathscr{Y}$ — представления, соответствующие FH-модулю W и FH^g-модулю Wg, соответственно, относительно выбранных базисов. Покажем, что $\mathscr{Y} = \mathscr{X}^g$.

Пусть $h \in H$ и $\mathscr{X}(h) = (\alpha_{ij})$. Тогда $\mathscr{X}^g(h^g) = \mathscr{X}(h) = (\alpha_{ij})$ и

$$w_i \mathscr{X}(h) = w_i h = \sum_j \alpha_{ij} w_j.$$

Поэтому

$$w_i g \mathscr{Y}(h^g) = (w_i g) h^g = (w_i h) g = (\sum_j \alpha_{ij} w_j) g = \sum_j \alpha_{ij} w_j g$$

и, значит, $\mathscr{Y}(h^g) = (\alpha_{ij}) = \mathscr{X}^g(h^g)$.

(ii) Пусть $\mathscr{X}$ — представление, соответствующее модулю W. По условию FH^g-модуль M соответствует представлению $\mathscr{X}^t$ для некоторого $t \in G$ такого, что $H^g = H^t$ Однако, мы только что показали, что FH^t-модуль Wt также соответствует представлению $\mathscr{X}^t$. Значит, $M \cong Wt$ и $tg^{-1} \in \mathrm{N}_G(H)$.

(iii) Поскольку модули M и W изоморфны, то в подходящем базисе они соответствуют одному и тому же представлению $\mathscr{X}$. Тогда FH^g-модули Mg и Wg соответствуют представлению $\mathscr{X}^g$ группы H^g и, значит, также изоморфны. □

Доказательство (13.3). Каждый двойной смежный класс HtK является объединением правых смежных классов по H. Пусть K_t — набор элементов из K таких, что $HtK = \cup_{k \in K_t} Htk$. Покажем, что K_t является полным набором представителей правых смежных классов группы K по подгруппе $H^t \cap K$. Заметим, что два элемента $k_1, k_2 \in K_t$ совпадают тогда и только тогда, когда $tk_1k_2^{-1}t^{-1} \in H$, т. е. $k_1k_2^{-1} \in H^t$. С другой стороны $k_1k_2^{-1} \in K$. Значит, $k_1 = k_2$ тогда и только тогда, когда k_1 и k_2 лежат в одном правом смежном классе группы K по $H^t \cap K$. Обратно, для любого $k \in K$ существуют $h \in H$ и $k_0 \in K_t$ такие, что $tk = htk_0$. Поэтому $kk_0^{-1} = h^t \in H^t \cap K$, т. е. K_t — это полная система представителей K по $H^t \cup K$.

Как и в доказательстве предложения (12.2), представим FG-модуль W^G в виде прямой суммы

$$W^G = \bigoplus_{t \in T} \bigoplus_{k \in K_t} W \otimes tk.$$

Легко видеть, что для любого $t \in T$ слагаемое

(Б.6)
$$\bigoplus_{k \in K_t} W \otimes tk$$

является подмодулем FK-модуля $(W^G)_K$.

С другой стороны, в силу (13.1)(i) для любого $t \in T$ подпространство Wt является FH^t-модулем, а поскольку K_t — это полная система представителей K по $H^t \cap K$, то можно записать

(Б.7)
$$((Wt)_{H^t \cap K})^K = \bigoplus_{k \in K_t} Wt \otimes k.$$

Достаточно показать, что отображение φ из FK-модуля (Б.6) в FK-модуль (Б.7), определённое по правилу $(w \otimes tk)\varphi = wt \otimes k$ для всех $w \in W$, $k \in K_t$, является изоморфизмом.

Пусть $x \in K$ и $k \in K_t$. Тогда существуют $h \in H$ и $k_0 \in K_t$ такие, что $kx = h^t k_0$ и, значит,

$$(w \otimes tk)\varphi x = (wt \otimes k)x = wt \otimes h^t k_0 = wht \otimes k_0,$$
$$(w \otimes tk)x\varphi = (w \otimes htk_0)\varphi = (wh \otimes tk_0)\varphi = wht \otimes k_0,$$

откуда следует требуемое. □

Доказательство (15.3). Если $\mathscr{R}$ — регулярное F-представление, то $\mathscr{R}^E$ — регулярное E-представление. Для нахождения неприводимых компонент представления $\mathscr{R}^E$ нужно взять неприводимые компоненты $\mathscr{X}_i$ представления $\mathscr{R}$ и затем найти неприводимые компоненты представлений $\mathscr{X}_i^E$ (это следует из теоремы Жордана-Гёльдера (3.33)). Осталось заметить, что по предложению (9.6) представление $\mathscr{Y}$ является неприводимой компонентой регулярного E-представления $\mathscr{R}^E$. □

Доказательство (16.1). Воспользуемся соотношением

(Б.8)
$$|G| = \sum_{\chi\in\mathrm{Irr}(G)} \chi(1)^2,$$

где число слагаемых совпадает с $|\mathscr{K}(G)|$.

Если G абелева, то $|\mathscr{K}(G)| = |G|$ и, значит, все слагаемые в (Б.8) равны 1. Обратно, пусть $\deg\chi = 1$ для всех $\chi \in \mathrm{Irr}(G)$. Тогда, чтобы правая часть в (Б.8) равнялась $|G|$ необходимо, чтобы число слагаемых было равно $|G|$, откуда следует $|\mathscr{K}(G)| = |G|$ и, значит, G абелева. □

Доказательство (16.3). (i) Ограничение представления $\mathscr{X}$ на циклическую подгруппу $\langle g\rangle$ является вполне приводимым по теореме Машке (7.11) и поэтому эквивалентно блочно-диагональному представлению с неприводимыми компонентами по диагонали. Из (16.1) следует, что неприводимые компоненты одномерны и, в частности, $\mathscr{X}(g)$ подобна диагональной матрице $\mathrm{diag}(\zeta_1,\dots,\zeta_n)$.

(ii) Равенство $\zeta_i^k = 1$ следует из (i) и того, что $g^k = 1$. Значит, $|\zeta_i| = 1$ и $\zeta_i^{-1} = \overline{\zeta_i}$.

(iii) Поскольку следы подобных матриц равны, то из (i) вытекает, что $\chi(g) = \sum\zeta_i$. Поэтому из (ii) следует, что $|\chi(g)| \leqslant \sum|\zeta_i| = n$.

(iv) Так как $\mathscr{X}(g^{-1}) = \mathscr{X}(g)^{-1}$, а $\mathscr{X}(g)$ подобна $\mathrm{diag}(\zeta_1,\dots,\zeta_n)$ в силу (i), то матрица $\mathscr{X}(g^{-1})$ подобна $\mathrm{diag}(\zeta_1^{-1},\dots,\zeta_n^{-1})$. Значит, из (ii) следует, что $\chi(g^{-1}) = \overline{\chi(g)}$. □

Доказательство (16.11). (i) Если g и g^{-1} сопряжены, то $\chi(g) = \chi(g^{-1}) = \overline{\chi(g)}$ в силу (16.3)(iv), т. е. $\chi(g)\in\mathbb{R}$. Обратно, пусть $g\in K$, и $g^{-1}\in K'$ где $K, K' \in \mathscr{K}(G)$. Поскольку для любого $\chi\in\mathrm{Irr}(G)$ по условию $\chi(g) = \overline{\chi(g)} = \chi(g^{-1})$, отсюда следует, что столбцы таблицы характеров группы G, соответствующие классам K и K', совпадают. Из невырожденности таблицы характеров вытекает, что $K = K'$ и, значит, элементы g и g^{-1} сопряжены.

(ii) Пусть g и g^k сопряжены для всех k таких, что $(k,|g|) = 1$. Возьмём $\chi\in\mathrm{Irr}(G)$. По (16.8)(ii) имеем $\chi(g)\in\mathbb{Q}_m$, где $m = \exp G$. В силу (16.9)(ii) существует целое число k взаимно простое с m такое, что для любого $\sigma\in\mathrm{Gal}(\mathbb{Q}_m,\mathbb{Q})$ выполнены равенства $(\chi(g))^\sigma = \chi^\sigma(g) = \chi(g^k)$. Поскольку k также взаимно просто с $|g|$, то предположению отсюда вытекает, что $(\chi(g))^\sigma = \chi(g)$ и, значит, число $\chi(g)$ лежит в неподвижном подполе поля $\mathbb{Q}_m$ относительно группы $\mathrm{Gal}(\mathbb{Q}_m,\mathbb{Q})$. Поэтому это подполе равно $\mathbb{Q}$.

Докажем обратное утверждение. Пусть $k\in\mathbb{Z}$, $(k,|g|) = 1$ и элементы g и g^k лежат в классах сопряжённости K и K', соответственно. В силу (16.2) существует (единственный) автоморфизм $\sigma\in\mathrm{Gal}(\mathbb{Q}_{|g|},\mathbb{Q})$, такой, что $\zeta^\sigma = \zeta^k$, где $\zeta\in\mathbb{Q}_{|g|}$ — примитивный корень степени $|g|$ из 1. Из (16.3) следует, что для любого $\chi\in\mathrm{Irr}(g)$ значение $\chi(g)$ — сумма степеней числа ζ. По условию $\chi(g)\in\mathbb{Q}$, т. е. $\chi(g) = \chi(g)^\sigma = \chi(g^k)$. Как и выше отсюда следует, что столбцы таблицы характеров группы G, соответствующие классам K и K', совпадают и, значит, элементы g и g^k сопряжены.

(iii) Если $g\in S_n$ и $(k,|g|) = 1$, то элементы g и g^k имеют одинаковое цикловое строение и, значит, сопряжены в S_n. Из (ii) вытекает, что значения всех неприводимых характеров рациональны. С другой стороны по (16.8)(i) они являются целыми алгебраическими числами, и поэтому целые рациональные в силу (A.1). □

Доказательство (16.13). В силу (7.11) алгебра $\mathbb{C}G$ полупроста. Из (7.16)(iv) и (7.21) вытекает разложение регулярного модуля

$$\mathbb{C}G^\circ = \bigoplus_{\chi\in\mathrm{Irr}(G)} n_\chi M_\chi,$$

где $n_\chi = \mathrm{n}_{M_\chi}(\mathbb{C}G) = \dim M_\chi = \chi(1)$. Отсюда следует требуемое разложение регулярного характера. □

Доказательство (16.19). (i) – (ii) Утверждения следуют из того, что произведение $(\varphi,\chi)_G$ совпадает с коэффициентом при χ в разложении φ в виде линейной комбинации неприводимых характеров.

(iii) – (iv) Пусть $\varphi = \sum_{\chi\in\mathrm{Irr}(G)} a_\chi\chi$ и $\psi = \sum_{\chi\in\mathrm{Irr}(G)} b_\chi\chi$ для неотрицательных целых чисел a_χ и b_χ. Тогда $(\varphi,\psi)_G = (\psi,\varphi)_G = \sum_\chi a_\chi b_\chi$ — неотрицательное целое число. Поэтому $(\varphi,\varphi)_G = \sum_\chi \alpha_\chi^2 = 1$ тогда и только тогда, когда один из коэффициентов a_χ равен 1, а остальные — 0. □

Доказательство (16.21). В случае поля $\mathbb{C}$ из (12.10)(ii) вытекает, что

$$\varphi^G(g) = \frac{1}{|H|}\sum_{x\in G}\varphi^\circ(xgx^{-1}).$$

Поэтому
$$(\varphi^G,\psi)_{_G}=\frac{1}{|G|}\sum_{g\in G}\varphi^G(g)\overline{\psi(g)}=\frac{1}{|G|}\frac{1}{|H|}\sum_{g\in G}\sum_{x\in G}\varphi^\circ(xgx^{-1})\overline{\psi(g)}.$$
Переобозначив $y=xgx^{-1}$ и заметив, что $\psi(g)=\psi(y)$, получим
$$(\varphi^G,\psi)_{_G}=\frac{1}{|G|}\frac{1}{|H|}\sum_{x\in G}\sum_{y\in G}\varphi^\circ(y)\overline{\psi(y)}=\frac{1}{|H|}\sum_{y\in G}\varphi^\circ(y)\overline{\psi(y)}=\frac{1}{|H|}\sum_{y\in H}\varphi(y)\overline{\psi(y)}=(\varphi,\psi_H)_{_H}.$$
□

Доказательство (16.25). (i) В доказательстве предложения (16.15) мы отмечали, что $\mathscr{X}_\theta(e_\chi)=\mathbf{0}$ при $\chi\neq\theta$ и $\mathscr{X}_\theta(e_\theta)=\mathbf{1}$. Отсюда следует требуемое.

(ii) Пусть $\tau:\mathrm{Z}(\mathbb{C}G)\to\mathbb{C}$ — гомоморфизм $\mathbb{C}$-алгебр. Поскольку центральные идемпотенты e_χ образуют базис алгебры $\mathrm{Z}(\mathbb{C}G)$, гомоморфизм τ однозначно задаётся значениями $e_\chi\tau$, которые являются идемпотентами из $\mathbb{C}$, т. е. равны 0 или 1. В силу (i) достаточно показать, что существует $\chi\in\mathrm{Irr}(G)$ такой, что $e_\chi\tau=1$ и $e_\theta\tau=0$ для всех $\theta\neq\chi$. Так как $1_{\mathrm{Z}(\mathbb{C}G)}\tau=1_{\mathbb{C}}$, то $e_\chi\tau=1$ хотя бы для одного $\chi\in\mathrm{Irr}(G)$. Если существуют различные $\chi_1,\chi_2\in\mathrm{Irr}(G)$ такие, что $e_{\chi_1}\tau=e_{\chi_2}\tau=1$, то $(e_{\chi_1}+e_{\chi_2})\tau=2$, вопреки тому, что образ идемпотента $e_{\chi_1}+e_{\chi_2}$ под действием τ должен быть идемпотентом из $\mathbb{C}$.

(iii) Поскольку $\widehat{K}\in Z(\mathbb{C}G)$ и центральные идемпотенты e_χ образуют базис алгебры $Z(\mathbb{C}G)$, существуют константы $\alpha_{K,\chi}\in\mathbb{C}$ такие, что
$$\widehat{K}=\sum_{\chi\in\mathrm{Irr}(G)}\alpha_{K,\chi}e_\chi.$$
Подействовав гомоморфизмом ω_θ, где $\theta\in\mathrm{Irr}(G)$, на обе части этого равенства, в силу (i) получим требуемое равенство $\omega_\theta(\widehat{K})=\alpha_{K,\theta}$. □

Доказательство (16.31). Пусть $\chi\in\mathrm{Irr}(G)$. Подставим в равенство
$$\omega_\chi(\widehat{K})\omega_\chi(\widehat{L})=\sum_{M\in\mathscr{K}(G)}a_{_{KLM}}\omega_\chi(\widehat{M})$$
выражения для $\omega_\chi(\widehat{K})$, $\omega_\chi(\widehat{L})$, $\omega_\chi(\widehat{M})$ из (16.26). Тогда
$$\frac{|K||L|}{\chi(1)}\chi(x_K)\chi(x_L)=\sum_{M\in\mathscr{K}(G)}a_{_{KLM}}|M|\chi(x_M).$$
Пусть $N\in\mathscr{K}(G)$. Умножим обе части последнего равенства на $\overline{\chi(x_{_N})}$, просуммируем по χ и воспользуемся вторым соотношением ортогональности (16.22). Имеем
$$\begin{aligned}|K||L|\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(x_{_K})\chi(x_{_L})\overline{\chi(x_{_N})}}{\chi(1)}&=\sum_{M\in\mathscr{K}(G)}a_{_{KLM}}|M|\sum_{\chi\in\mathrm{Irr}(G)}\chi(x_{_M})\overline{\chi(x_{_N})}\\&=\sum_{M\in\mathscr{K}(G)}a_{_{KLM}}|M|\cdot\delta_{_{M,N}}|\mathrm{C}_G(x_{_M})|=a_{_{KLN}}|N||\mathrm{C}_G(x_{_N})|.\end{aligned}$$
Учитывая, что $|N||\mathrm{C}_G(x_{_N})|=|G|$ и переобозначая N через M, получаем требуемый результат. □

Доказательство (17.2). Включение $p\mathbb{Z}\subseteq M\cap\mathbb{Z}$ очевидно. Покажем обратное включение. Допустим, напротив, что $m\in M\cap\mathbb{Z}$ и $p\nmid m$. Тогда $ap+bm=1$ для некоторых $a,b\in\mathbb{Z}$. Отсюда следует, что $1\in M$. Противоречие. □

Доказательство (17.8). (i) – (ii) Оба утверждения следуют из того, что для всякого $g\in G_{p'}$ матрица $\mathscr{X}(g)$ имеет тот же набор характеристических корней, что и любая сопряжённая с ней матрица.

(iii) Мы уже отмечали, что матрица $\mathscr{X}(g)$ подобна $\mathrm{diag}(\zeta_1^\star,\ldots,\zeta_n^\star)$, где $\zeta_1,\ldots,\zeta_n\in U$. Поэтому $\mathscr{X}(g^{-1})=\mathscr{X}(g)^{-1}$ подобна $\mathrm{diag}((\zeta_1^{-1})^\star,\ldots,(\zeta_n^{-1})^\star)$. Поскольку $\zeta_i^{-1}=\overline{\zeta_i}$, отсюда следует, что $\varphi(g^{-1})=\sum\overline{\zeta_i}=\overline{\sum\zeta_i}=\overline{\varphi(g)}$.

(iv) По (10.3), пример 7, мы можем считать, что $\mathscr{X}^*(g)=\mathscr{X}(g)^\iota$ для всякого $g\in G$. Пусть $g\in G_{p'}$ и $\zeta_1^\star,\ldots,\zeta_n^\star\in F$ — характеристические корни матрицы $\mathscr{X}(g)$ для подходящих $\zeta_1,\ldots,\zeta_n\in U$. Тогда характеристические корни для $\mathscr{X}(g)^\iota$ равны $(\zeta_1^{-1})^\star,\ldots,(\zeta_n^{-1})^\star$, откуда следует, что значение брауэрова характера представления $\mathscr{X}^*$ на элементе g равно $\sum\zeta_i^{-1}=\sum\overline{\zeta_i}=\overline{\sum\zeta_i}=\overline{\varphi(g)}=\overline{\varphi}(g)$.

(v) Это следует из того, что $H_{p'}\subseteq G_{p'}$ и ограничение представления $\mathscr{X}$ на H будет F-представлением группы H. □

Доказательство (19.13). Пусть ρ — автоморфизм Фробениуса поля F, действующий по правилу $\alpha^\rho = \alpha^p$ для любого $\alpha \in F$. Пусть σ — автоморфизм группы U, являющийся «поднятием» автоморфизма ρ, т. е. для произвольного $\xi \in U$ выполнено соотношение $(\xi^\star)^\rho = (\xi^\sigma)^\star$. Отсюда следует, что $\xi^\sigma = \xi^p$ и поэтому σ однозначно продолжается до автоморфизма из $\mathrm{Gal}(\mathbb{Q}(\xi), \mathbb{Q})$, который также обозначим через σ. Таким образом σ определён на всех элементах поля $\mathbb{Q}(U)$. В частности, $\alpha_1^\sigma + \alpha_2^\sigma = (\alpha_1+\alpha_2)^\sigma$ для любых $\alpha_1, \alpha_2 \in \mathbb{Q}(U)$.

Дальнейшее рассуждение повторяет идею из доказательства (19.12)(i.1). Пусть $\varphi \in \mathrm{IBr}(G)$ и $\mathscr{X}$ — F-представление с брауэровым характером φ. Если $\zeta_1^\star, \ldots, \zeta_s^\star$ — характеристические значения матрицы $\mathscr{X}(g)$, где $\zeta_i \in U$, то $\varphi(g) = \zeta_1 + \ldots + \zeta_s$. С другой стороны характеристическими значениями матрицы $\mathscr{X}^\rho(g)$ являются $(\zeta_1^\star)^\rho, \ldots, (\zeta_s^\star)^\rho$. По определению автоморфизма σ имеем $(\zeta_i^\star)^\rho = (\zeta_i^\sigma)^\star$, откуда следует, что значение брауэрова характера F-представления $\mathscr{X}^\rho$ равно $\zeta_1^\sigma + \ldots + \zeta_s^\sigma = (\zeta_1 + \ldots + \zeta_s)^\sigma = \varphi(g)^\sigma = \varphi^\sigma(g)$.

Поскольку $\zeta^{\sigma^i} = \zeta^{p^i}$ для любого i, где $\zeta \in U$ — примитивный корень степени $m_{p'}$ из 1, то порядок σ как элемента из $\mathrm{Gal}(\mathbb{Q}_{m_{p'}}, \mathbb{Q})$ равен порядку p по модулю $m_{p'}$. □

Доказательство (20.1). В случае, когда $\eta \in \mathrm{IBr}(G)$, утверждение следует из того факта, что F-представление $\mathscr{X} : FG \to \mathrm{M}_n(F)$ с брауэровым характером η является гомоморфизмом алгебр.

Пусть $\eta \in \mathrm{Irr}(G)$. Поскольку отображение λ_η является гомоморфизмом колец, достаточно показать, что его действие на базисных элементах из $\mathrm{Z}(FG)$ перестановочно с умножением на скаляры из F. Для любых $K \in \mathscr{K}(G)$ и $\alpha^\star \in F$, где $\alpha \in R$, имеем

$$\lambda_\eta(\alpha^\star \widehat{K}) = \omega_\chi(\alpha \widehat{K})^\star = \alpha^\star \omega_\chi(\widehat{K})^\star.$$

□

Доказательство (20.4). Пусть $z \in \mathrm{Z}(\widetilde{\boldsymbol{R}}G)$. Тогда $z = \sum_{K\in\mathscr{K}(G)} \alpha_{K} \widehat{K}$ для некоторых $\alpha_K \in \widetilde{\boldsymbol{R}}$. Из (20.2) получаем

$$(\omega_\chi(z))^\star = \sum_{K\in\mathscr{K}(G)} (\alpha_{K})^\star \omega_\chi(\widehat{K})^\star = \sum_{K\in\mathscr{K}(G)} (\alpha_{K})^\star \lambda_\chi(\widehat{K}) = \lambda_\chi\Big(\sum_{K\in\mathscr{K}(G)} (\alpha_{K})^\star \widehat{K}\Big) = \lambda_\chi(z^\star)$$

в силу того, что $\omega_\chi : \mathrm{Z}(\widetilde{\boldsymbol{R}}G) \to \widetilde{\boldsymbol{R}}$ — гомоморфизм $\widetilde{\boldsymbol{R}}$-алгебр, $\lambda_\chi : \mathrm{Z}(FG) \to F$ — гомоморфизм F-алгебр и * — гомоморфизм колец. □

Доказательство (20.21). (i) Это следует из (2.18)(iii) и (20.20), поскольку

$$\sum_{B\in\mathrm{Bl}(G)} f_{B} = \sum_{x\in\mathrm{Irr}(G)} e_\chi = 1$$

и идемпотенты f_{B} попарно ортогональны.

(ii) Это следует из (2.18)(iv). □

Доказательство (20.23). В силу (19.4)(ii) столбцы матрицы D линейно независимы. Поэтому из равенства (20.22) видно, что линейно независимы столбцы всех матриц разложения D_{B_i}. Так как число столбцов у D_{B_i} совпадает с $|\,\mathrm{IBr}(B_i)|$, а число строк — с $|\,\mathrm{Irr}(B_i)|$, то отсюда следуют оба утверждения. □

Доказательство (22.3). Легко видеть, что для любого $B \in \mathrm{Bl}(G)$ идеал $\mathrm{Z}(W_B)$ содержится в $\mathrm{Z}_P(FG)$ для $P \in \mathrm{Syl}_p(P)$, т. к. в этом случае $\mathrm{Z}_P(FG) = \mathrm{Z}(FG)$. Отсюда следует существование требуемого класса p-подгрупп.

Пусть теперь P и Q минимальные по включению p-подгруппы, удовлетворяющие условиям $\mathrm{Z}(W_B) \subseteq \mathrm{Z}_P(FG)$ и $\mathrm{Z}(W_B) \subseteq \mathrm{Z}_Q(FG)$, соответственно. Тогда в силу (22.2)(ii)

$$e_{B} \in \mathrm{Z}(W_B) \subseteq \mathrm{Z}_P(FG) \cap \mathrm{Z}_Q(FG) = \sum_{x,y\in G} \mathrm{Z}_{P^x\cap Q^y}(FG).$$

Из (21.4)(vii) следует, что найдутся $x, y \in G$ такие, что $e_{B} \in \mathrm{Z}_{P^x\cap Q^y}(FG)$. Значит,

$$\mathrm{Z}(W_B) = e_{B}\mathrm{Z}(FG) \subseteq \mathrm{Z}_{P^x\cap Q^y}(FG) = \mathrm{Z}_{P^{xy^{-1}}\cap Q}(FG) = \mathrm{Z}_{P\cap Q^{yx^{-1}}}(FG).$$

В силу минимальности p-подгрупп P и Q имеем $Q \subseteq P^{xy^{-1}}$ и $P \subseteq Q^{yx^{-1}}$, откуда следует, что P и Q сопряжены. □

Доказательство (24.4). Легко видеть, что $\beta_{P}(\widehat{K}) = 0$ тогда и только тогда, когда $K \cap C = \varnothing$, что эквивалентно существованию в K элемента x, централизующего P, т. е. включению $P \leqslant S$ для некоторой $S \in \mathrm{Syl}_p(\mathrm{C}_G(x)) \subseteq \Delta(K)$, которое означает, что $P \leqslant_G \delta(K)$. □

Доказательство (24.14). По определению отображения $\lambda_{b^N}^G$ для любого $K \in \mathscr{K}(G)$ имеем

$$\lambda_{b^N}^G(\widehat{K}) = \lambda_{b^N}\left(\sum_{x \in K \cap N} x\right) = \lambda_b^N\left(\sum_{x \in K \cap N} x\right) = \lambda_b\left(\sum_{x \in K \cap N \cap H} x\right) = \lambda_b\left(\sum_{x \in K \cap H} x\right) = \lambda_b^G(\widehat{K}).$$

Значит, отображения $\lambda_{b^N}^G$ и λ_b^G совпадают и поэтому либо одновременно являются, либо не являются гомоморфизмами F-алгебр. В первом случае блоки b^G и $(b^N)^G$ определены и совпадают. $\square$

Доказательство (24.19). Пусть $P = \delta(B)$ и $N = \mathrm{N}_G(P)$. Поскольку $B \in \mathrm{Bl}(G|P)$, из теоремы (24.17)(i) следует, что множество $\mathrm{Bl}(N|P)$ непусто. В силу (22.13) получаем $\mathrm{O}_p(\mathrm{N}_G(P)) \leqslant P$. С другой стороны $P \trianglelefteqslant N$ и, значит, $P \leqslant \mathrm{O}_p(\mathrm{N}_G(P))$. Поэтому $\mathrm{O}_p(\mathrm{N}_G(P)) = P$. $\square$

Доказательство (25.1). (i) В силу (3.7)(ii) базис алгебры $\mathrm{Z}(FG)$ состоит из классовых сумм. Поэтому достаточно проверить, что для произвольных $K, L \in \mathscr{K}(K)$ справедливо равенство $\varrho(\widehat{K}\widehat{L}) = \varrho(\widehat{K})\varrho(\widehat{L})$. Это легко установить, используя (3.7)(iv), (21.1)(i), и тот факт, что $\lambda_{_B}$ — гомоморфизм F-алгебр.

(ii) Это следует из (21.1)(iii).

(iii) Это следует из (ii).

(iv) В силу линейной независимости идемпотентов $e_{_B}$, элемент $x \in \mathrm{Z}(FG)$ лежит в ядре ϱ тогда и только тогда, когда $\lambda_{_B}(x) = 0$ для всех $B \in \mathrm{Bl}(G)$ и, значит, лежит в $\mathrm{J}(\mathrm{Z}(FG))$ ввиду (21.2). $\square$

Доказательство (27.3). (i) – (iv) следуют из определения p-сечения.

(v) Если $x \in \mathrm{S}_H(g)$, существует элемент $h \in H$ такой, что $(x_p)^h = g_p = g$, т. е. $x^h = (x_p x_{p'})^h = gc$, где $c = (x_{p'})^h \in C$ — p-регулярный элемент. Тогда найдётся элемент $k \in H$ такой, что $c^k = t$ для подходящего $t \in T$. Значит, $x^{hk} = gc^k = gt$, т. е. $x \in (gt)^H$. Обратно, для любого $t \in T$ имеем $gt \in \mathrm{S}_H(g)$, поскольку $(gt)_p = g$. Тогда из (iii) следует, что $(gt)^H \subseteq \mathrm{S}_H(g)$ и, значит, имеет место обратное включение. $\square$

Доказательство (A.2). (i) Пусть алгебраическое число α является корнем многочлена $f(x) = a_0x^n + a_1x^{n-1} + + \ldots + a_n$, где $a_{,0}, a_1, \ldots, a_n \in \mathbb{Q}$ и $a_0 \neq 0$. Умножив, если необходимо, многочлен $f(x)$ на наименьшее общее кратное знаменателей своих коэффициентов, можно считать, что $a_0, a_1, \ldots, a_n \in \mathbb{Z}$. Тогда

$$a_0^{n-1}f(x) = (a_0x)^n + a_1(a_0x)^{n-1} + a_2a_0(a_0x)^{n-2} + \ldots + a_na_0^{n-1}.$$

Поскольку $a_0^{n-1}f(\alpha) = 0$, мы видим, что число $a_0\alpha$ является целым алгебраическим для целого рационального числа a_0, что и требовалось доказать.

(ii) Пусть ω — целое алгебраическое число, являющееся корнем многочлена $f(x) = x^n + b_1x^{n-1} + \ldots + b_n$, где $b_1, b_2, \ldots, b_n \in \mathbb{Z}$, и пусть $0 \neq m \in \mathbb{Z}$. Разделив обе части равенства $f(\omega) = 0$ на m^n легко проверить, что ω/m является корнем многочлена

$$y^n + \frac{b_1}{m}y^{n-1} + \frac{b_2}{m^2}y^{n-2} + \ldots + \frac{b_n}{m^n},$$

и, значит, является алгебраическим. $\square$

Доказательство (A.7). Пусть R — конечная область целостности и $0 \neq r \in R$. Рассмотрим степени $r, r^2, r^3, \ldots$ В силу конечности R существуют $m \leqslant n$ такие, что $r^m = r^n$. Тогда $r^m(1 - r^{n-m}) = 0$. Так как $r^m \neq 0$, отсюда вытекает $r^{n-m} = 1$, т. е. элемент r обратим. $\square$

Доказательство (A.9). Пусть $\alpha \in A$ и $\alpha \neq 0$. Существуют $a_i \in \mathbb{Z}$ такие, что $\alpha^m + a_1\alpha^{m-1} + \ldots + a_m = 0$, причём можно считать, что $a_m \neq 0$. Но тогда a_m — ненулевой элемент из $A \cap \mathbb{Z}$. $\square$

Доказательство (A.12). Пусть $A_1 \subseteq A_2 \subseteq \ldots$ — цепочка идеалов из D. Так как факторкольцо D/A_1 конечно в силу (A.11), то существует лишь конечное число различных идеалов, содержащих A_1. $\square$

Доказательство (A.16). Если P — простой идеал в D, то в силу (A.11) факторкольцо D/P — конечная область целостности. Из (A.7) вытекает, что D/P — поле, а потому идеал P максимален. $\square$

B Таблицы характеров некоторых групп

$G = S_3$

$|G| = 6 = 2 \cdot 3$

$\mathrm{X}(S_3)$

K	$1a$	$2a$	$3a$
$\lvert K\rvert$	1	3	2
$\lvert \mathrm{C}_G(x_K)\rvert$	6	2	3
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	.	-1

$\Phi_2(S_3)$

K	$1a$	$3a$
$\lvert K\rvert$	1	2
$\lvert \mathrm{C}_G(x_K)\rvert$	6	3
φ_1	1	1
φ_2	2	-1

D	φ_1	φ_2
χ_1	1	.
χ_2	1	.
χ_3	.	1

$$C = \begin{pmatrix} 2 & . \\ . & 1 \end{pmatrix}$$

$\Phi_3(S_3)$

K	$1a$	$2a$
$\lvert K\rvert$	1	3
$\lvert \mathrm{C}_G(x_K)\rvert$	6	2
φ_1	1	1
φ_2	1	-1

D	φ_1	φ_2
χ_1	1	.
χ_2	.	1
χ_3	1	1

$$C = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

$G = A_4$

$|G| = 12 = 2^2 \cdot 3$

$\mathrm{X}(A_4)$

K	$1a$	$2a$	$3a$	$3b$
$\lvert K\rvert$	1	3	4	4
$\lvert \mathrm{C}_G(x_K)\rvert$	12	4	3	3
χ_1	1	1	1	1
χ_2	1	1	ζ	ζ^2
χ_3	1	1	ζ^2	ζ
χ_4	3	-1	.	.

Иррациональные величины

$$\zeta = e^{2\pi i/3}$$

$\Phi_2(A_4)$

K	$1a$	$3a$	$3b$
$\lvert K\rvert$	1	4	4
$\lvert \mathrm{C}_G(x_K)\rvert$	12	3	3
φ_1	1	1	1
φ_2	1	ζ	ζ^2
φ_3	1	ζ^2	ζ

D	φ_1	φ_2	φ_3
χ_1	1	.	.
χ_2	.	1	.
χ_3	.	.	1
χ_4	1	1	1

$$C = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$$

$\Phi_3(A_4)$

K	$1a$	$2a$
$\lvert K\rvert$	1	3
$\lvert \mathrm{C}_G(x_K)\rvert$	12	4
φ_1	1	1
φ_2	3	-1

D	φ_1	φ_2
χ_1	1	.
χ_2	1	.
χ_3	1	.
χ_4	.	1

$$C = \begin{pmatrix} 3 & . \\ . & 1 \end{pmatrix}$$

$G = S_4$

$|G| = 24 = 2^3 \cdot 3$

$\mathrm{X}(S_4)$

K	$1a$	$2a$	$2b$	$3a$	$4a$
$\lvert K\rvert$	1	6	3	8	6
$\lvert \mathrm{C}_G(x_K)\rvert$	24	4	8	3	4
χ_1	1	1	1	1	1
χ_2	1	-1	1	1	-1
χ_3	2	.	2	-1	.
χ_4	3	1	-1	.	-1
χ_5	3	-1	-1	.	1

$\Phi_2(S_4)$

K	$1a$	$3a$
$\|K\|$	1	8
$\|C_G(x_K)\|$	24	3
φ_1	1	1
φ_2	2	-1

D	φ_1	φ_2
χ_1	1	.
χ_2	1	.
χ_3	.	1
χ_4	1	1
χ_5	1	1

$$C = \begin{pmatrix} 4 & 2 \\ 2 & 3 \end{pmatrix}$$

$\Phi_3(S_4)$

K	$1a$	$2a$	$2b$	$4a$
$\|K\|$	1	6	3	6
$\|C_G(x_K)\|$	12	4	8	4
φ_1	1	1	1	1
φ_2	1	-1	1	-1
φ_3	3	1	-1	-1
φ_4	3	-1	-1	1

D	φ_1	φ_2	φ_3	φ_4
χ_1	1	.	.	.
χ_2	.	1	.	.
χ_3	1	1	.	.
χ_4	.	.	1	.
χ_5	.	.	.	1

$$C = \begin{pmatrix} 2 & 1 & . & . \\ 1 & 2 & . & . \\ . & . & 1 & . \\ . & . & . & 1 \end{pmatrix}$$

$G = A_5 \cong \mathrm{PSL}_2(5) \cong \mathrm{SL}_2(4)$

$|G| = 60 = 2^2 \cdot 3 \cdot 5$

$\mathrm{X}(A_5)$

K	$1a$	$2a$	$3a$	$5a$	$5b$
$\|K\|$	1	15	20	12	12
$\|C_G(x_K)\|$	60	4	3	5	5
χ_1	1	1	1	1	1
χ_2	3	-1	.	α	α^*
χ_3	3	-1	.	α^*	α
χ_4	4	.	1	-1	-1
χ_5	5	1	-1	.	.

Иррациональные величины

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \alpha^* = \frac{1-\sqrt{5}}{2}$$

$\Phi_2(A_5)$

K	$1a$	$3a$	$5a$	$5b$
$\|K\|$	1	20	12	12
$\|C_G(x_K)\|$	60	3	5	5
φ_1	1	1	1	1
φ_2	2	-1	$-\alpha^*$	$-\alpha$
φ_3	2	-1	$-\alpha$	$-\alpha^*$
φ_4	4	1	-1	-1

D	φ_1	φ_2	φ_3	φ_4
χ_1	1	.	.	.
χ_2	1	1	.	.
χ_3	1	.	1	.
χ_4	.	.	.	1
χ_5	1	1	1	.

$$C = \begin{pmatrix} 4 & 2 & 2 & . \\ 2 & 2 & 1 & . \\ 2 & 1 & 2 & . \\ . & . & . & 1 \end{pmatrix}$$

$\Phi_3(A_5)$

K	$1a$	$2a$	$5a$	$5b$
$\|K\|$	1	15	12	12
$\|C_G(x_K)\|$	60	4	5	5
φ_1	1	1	1	1
φ_2	3	-1	α	α^*
φ_3	3	-1	α^*	α
φ_4	4	.	-1	-1

D	φ_1	φ_2	φ_3	φ_4
χ_1	1	.	.	.
χ_2	.	1	.	.
χ_3	.	.	1	.
χ_4	.	.	.	1
χ_5	1	.	.	1

$$C = \begin{pmatrix} 2 & . & . & 1 \\ . & 1 & . & . \\ . & . & 1 & . \\ 1 & . & . & 2 \end{pmatrix}$$

$\Phi_5(A_5)$

K	$1a$	$2a$	$3a$
$\|K\|$	1	15	20
$\|C_G(x_K)\|$	60	4	3
φ_1	1	1	1
φ_2	3	-1	.
φ_3	5	1	-1

D	φ_1	φ_2	φ_3
χ_1	1	.	.
χ_2	.	1	.
χ_3	.	1	.
χ_4	1	1	.
χ_5	.	.	1

$$C = \begin{pmatrix} 2 & 1 & . \\ 1 & 3 & . \\ . & . & 1 \end{pmatrix}$$

$G = \mathrm{PSL}_2(7) \cong \mathrm{GL}_3(2)$

$|G| = 168 = 2^3 \cdot 3 \cdot 7$

$\mathrm{X}\big(PSL_2(7)\big)$

K	$1a$	$2a$	$3a$	$4a$	$7a$	$7b$
$\lvert K\rvert$	1	21	56	42	24	24
$\lvert \mathrm{C}_G(x_K)\rvert$	168	8	3	4	7	7
χ_1	1	1	1	1	1	1
χ_2	3	-1	.	1	α	$\overline{\alpha}$
χ_3	3	-1	.	1	$\overline{\alpha}$	α
χ_4	6	2	.	.	-1	-1
χ_5	7	-1	1	-1	.	.
χ_6	8	.	-1	.	1	1

Иррациональные величины

$$\alpha = \frac{-1+i\sqrt{7}}{2} = \varepsilon + \varepsilon^2 + \varepsilon^4, \quad \varepsilon = e^{2\pi i/7}$$

$\Phi_2\big(PSL_2(7)\big)$

K	$1a$	$3a$	$7a$	$7b$
$\lvert K\rvert$	1	56	24	24
$\lvert \mathrm{C}_G(x_K)\rvert$	168	3	7	7
φ_1	1	1	1	1
φ_2	3	.	α	$\overline{\alpha}$
φ_3	3	.	$\overline{\alpha}$	α
φ_4	8	-1	1	1

D	φ_1	φ_2	φ_3	φ_4
χ_1	1	.	.	.
χ_2	.	1	.	.
χ_3	.	.	1	.
χ_4	.	1	1	.
χ_5	1	1	1	.
χ_6	.	.	.	1

$$C = \begin{pmatrix} 2 & 1 & 1 & . \\ 1 & 3 & 2 & . \\ 1 & 2 & 3 & . \\ . & . & . & 1 \end{pmatrix}$$

$\Phi_3\big(PSL_2(7)\big)$

K	$1a$	$2a$	$4a$	$7a$	$7b$
$\lvert K\rvert$	1	21	42	24	24
$\lvert \mathrm{C}_G(x_K)\rvert$	168	8	4	7	7
φ_1	1	1	1	1	1
φ_2	3	-1	1	α	$\overline{\alpha}$
φ_3	3	-1	1	$\overline{\alpha}$	α
φ_4	6	2	.	-1	-1
φ_5	7	-1	-1	.	.

D	φ_1	φ_2	φ_3	φ_4	φ_5
χ_1	1	.	.	.	.
χ_2	.	1	.	.	.
χ_3	.	.	1	.	.
χ_4	.	.	.	1	.
χ_5	.	.	.	.	1
χ_6	1	.	.	.	1

$$C = \begin{pmatrix} 2 & . & . & . & 1 \\ . & 1 & . & . & . \\ . & . & 1 & . & . \\ . & . & . & 1 & . \\ 1 & . & . & . & 2 \end{pmatrix}$$

$\Phi_7\big(PSL_2(7)\big)$

K	$1a$	$2a$	$3a$	$4a$
$\lvert K\rvert$	1	21	56	42
$\lvert \mathrm{C}_G(x_K)\rvert$	168	8	3	4
φ_1	1	1	1	1
φ_2	3	-1	.	1
φ_3	5	1	-1	-1
φ_4	7	-1	1	-1

D	φ_1	φ_2	φ_3	φ_4
χ_1	1	.	.	.
χ_2	.	1	.	.
χ_3	.	1	.	.
χ_4	1	.	1	.
χ_5	.	.	.	1
χ_6	.	1	1	.

$$C = \begin{pmatrix} 2 & . & 1 & . \\ . & 3 & 1 & . \\ 1 & 1 & 2 & . \\ . & . & . & 1 \end{pmatrix}$$

$G = D_{2n} = \langle x, y \mid x^n = y^2 = 1,\ x^y = x^{-1}\rangle, \quad n \geqslant 3$

$\lvert G\rvert = 2n$

$\mathrm{X}(D_{2n})$
n нечётно

K	$1a$	$2a$	$(x^r)^G$
$\lvert K\rvert$	1	n	2
$\lvert \mathrm{C}_G(x_K)\rvert$	$2n$	2	n
x_K	1	y	x^r
χ_1	1	1	1
χ_2	1	-1	1
θ_s	2	.	$\zeta^{rs} + \zeta^{-rs}$

Параметры

$r, s \ = \ 1, \ldots, (n-1)/2$

Иррациональные величины

$\zeta = e^{2\pi i/n}$

$\mathrm{X}(D_{2n})$
$n = 2m$

K	$1a$	$2a$	$2b$	$2c$	$(x^r)^G$
$\lvert K\rvert$	1	1	m	m	2
$\lvert \mathrm{C}_G(x_K)\rvert$	$2n$	$2n$	4	4	n
x_K	1	x^m	y	xy	x^r
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	1	$(-1)^m$	1	-1	$(-1)^r$
χ_4	1	$(-1)^m$	-1	1	$(-1)^r$
θ_s	2	$(-1)^s\, 2$	.	.	$\zeta^{rs} + \zeta^{-rs}$

Параметры

$r, s \ = \ 1, \ldots, m-1$

Иррациональные величины

$\zeta = e^{2\pi i/n}$

$G = Q_{2^m} = \langle x, y \mid x^{2^{m-1}} = 1,\ y^2 = x^{2^{m-2}},\ x^y = x^{-1}\rangle, \quad m \geqslant 3$

$|G| = 2^m$

$\mathrm{X}(Q_{2^m})$

K	$1a$	$2a$	$4a$	$4b$	$(x^r)^G$
$\lvert K\rvert$	1	1	2^{m-2}	2^{m-2}	2
$\lvert \mathrm{C}_G(x_K)\rvert$	2^m	2^m	4	4	2^{m-1}
x_K	1	y^2	y	xy	x^r
χ_1	1	1	1	1	1
χ_2	1	1	-1	-1	1
χ_3	1	1	1	-1	$(-1)^r$
χ_4	1	1	-1	1	$(-1)^r$
θ_s	2	-2	.	.	$\zeta^{rs}+\zeta^{-rs}$

Параметры

$r, s \;=\; 1, \ldots, 2^{m-2}-1$

Иррациональные величины

$\zeta = e^{2\pi i/2^{m-1}}$

$G = \mathrm{PSL}_2(q)$

$|G| = \frac{1}{(2,q-1)} q(q^2-1)$

$\mathrm{X}\big(PSL_2(q)\big)$, $q = 2^m$

K	$1a$	$2a$	$(x^r)^G$	$(y^t)^G$
$\lvert K\rvert$	1	q^2-1	$q(q+1)$	$q(q-1)$
$\lvert \mathrm{C}_G(x_K)\rvert$	$q(q^2-1)$	q	$q-1$	$q+1$
x_K	1	z	x^r	y^t
χ_1	1	1	1	1
χ_2	q	.	1	-1
θ_s	$q+1$	1	$\zeta^{rs}+\zeta^{-rs}$	.
τ_h	$q-1$	-1	.	$-\xi^{th}-\xi^{-th}$

Элементы

$|z| = 2,\ |x| = q-1,\ |y| = q+1$

Параметры

$r, s \;=\; 1, \ldots, (q-2)/2;$

$t, h \;=\; 1, \ldots, q/2$

Иррациональные величины

$\zeta = e^{2\pi i/(q-1)},\ \xi = e^{2\pi i/(q+1)}$

$\Phi_p\big(PSL_2(q)\big)$, $q = 2^m$, $p \mid (q-1)$

K	$1a$	$2a$	$(x_0^r)^G$	$(y^t)^G$
$\lvert K\rvert$	1	q^2-1	$q(q+1)$	$q(q-1)$
$\lvert \mathrm{C}_G(x_K)\rvert$	$q(q^2-1)$	q	$q-1$	$q+1$
x_K	1	z	x_0^r	y^t
φ_1	1	1	1	1
φ_2	q	.	1	-1
ψ_j	$q+1$	1	$\zeta_0^{rj}+\zeta_0^{-rj}$	.
η_f	$q-1$	-1	.	$-\xi^{tf}-\xi^{-tf}$

D	φ_1	φ_2	ψ_j	η_f
χ_1	1	.	.	.
χ_2	.	1	.	.
θ_{s_0}	1	1	.	.
θ_{s_i}	.	.	δ_{ij}	.
τ_h	.	.	.	δ_{hf}

$$C = \begin{pmatrix} \frac{p^d+1}{2} & \frac{p^d-1}{2} & . & . \\ \frac{p^d-1}{2} & \frac{p^d+1}{2} & . & . \\ . & . & p^d\mathbf{1}_{(n-1)/2} & . \\ . & . & . & \mathbf{1}_{q/2} \end{pmatrix}$$

Обозначения

$p^d = (q-1)_p,\ n = (q-1)_{p'},$

$x_0 = x^{p^d},\ \zeta_0 = \zeta^{p^d} = e^{2\pi i/n}$

Параметры

$r, i, j \;=\; 1, \ldots, \frac{n-1}{2};$

$f, h, t \;=\; 1, \ldots, \frac{q}{2};$

$s_0 = n, 2n, \ldots, \frac{p^d-1}{2}n;$

$s_i = i, n \pm i, 2n \pm i, \ldots, \frac{p^d-1}{2}n \pm i$

$\Phi_p\big(PSL_2(q)\big)$, $q = 2^m$, $p \mid (q+1)$

K	$1a$	$2a$	$(x^r)^G$	$(y_0^t)^G$
$\lvert K\rvert$	1	q^2-1	$q(q+1)$	$q(q-1)$
$\lvert \mathrm{C}_G(x_K)\rvert$	$q(q^2-1)$	q	$q-1$	$q+1$
x_K	1	z	x^r	y_0^t
φ_1	1	1	1	1
φ_2	$q-1$	-1	.	-2
ψ_j	$q+1$	1	$\zeta^{rj}+\zeta^{-rj}$	.
η_f	$q-1$	-1	.	$-\xi_0^{tf}-\xi_0^{-tf}$

D	φ_1	φ_2	ψ_j	η_f
χ_1	1	.	.	.
χ_2	1	1	.	.
θ_s	.	.	δ_{sj}	.
τ_{h_0}	.	1	.	.
τ_{h_i}	.	.	.	δ_{if}

$$C = \begin{pmatrix} 2 & 1 & \cdot & \cdot \\ 1 & \frac{p^d+1}{2} & \cdot & \cdot \\ \cdot & \cdot & \mathbf{1}_{(q/2)-1} & \cdot \\ \cdot & \cdot & \cdot & p^d\mathbf{1}_{(n-1)/2} \end{pmatrix}$$

Обозначения

$p^d = (q+1)_p,\ n = (q+1)_{p'},$
$y_0 = y^{p^d},\ \xi_0 = \xi^{p^d} = e^{2\pi i/n}$

Параметры

$r, s, j \ = \ 1, \dots, \frac{q}{2} - 1;$
$i, f, t \ = \ 1, \dots, \frac{n-1}{2};$
$h_0 = n, 2n, \dots, \frac{p^d-1}{2}n;$
$h_i = i, n \pm i, 2n \pm i, \dots, \frac{p^d-1}{2}n \pm i$

$\mathrm{X}\big(PSL_2(q)\big)$
$q \equiv 1 \pmod 4$

K	$1a$	$2a$	la	lb	$(x^r)^G$	$(y^t)^G$
$\lvert K\rvert$	1	$\frac12 q(q+1)$	$\frac12(q^2-1)$	$\frac12(q^2-1)$	$q(q+1)$	$q(q-1)$
$\lvert \mathrm{C}_G(x_K)\rvert$	$\frac12 q(q^2-1)$	$q-1$	q	q	$\frac12(q-1)$	$\frac12(q+1)$
x_K	1	z	u	v	x^r	y^t
χ_1	1	1	1	1	1	1
χ_2	q	1	$\cdot$	$\cdot$	1	-1
χ_3	$\frac12(q+1)$	$(-1)^{(q-1)/4}$	$\frac12(1+\sqrt{q})$	$\frac12(1-\sqrt{q})$	$(-1)^r$	$\cdot$
χ_4	$\frac12(q+1)$	$(-1)^{(q-1)/4}$	$\frac12(1-\sqrt{q})$	$\frac12(1+\sqrt{q})$	$(-1)^r$	$\cdot$
θ_s	$q+1$	$2\cdot(-1)^s$	1	1	$\zeta^{rs}+\zeta^{-rs}$	$\cdot$
τ_h	$q-1$	$\cdot$	-1	-1	$\cdot$	$-\xi^{th}-\xi^{-th}$

Обозначения

$q = l^m, \quad l$ простое

Параметры

$r, s \ = \ 1, \dots, \frac{q-5}{4};$
$t, h \ = \ 1, \dots, \frac{q-1}{4}$

Элементы

$\lvert u\rvert = \lvert v\rvert = l,$
$\lvert x\rvert = \frac{q-1}{2},\ \lvert y\rvert = \frac{q+1}{2},$
$z = x^{(q-1)/4}$

Иррациональные величины

$\zeta = e^{4\pi i/(q-1)},\ \xi = e^{4\pi i/(q+1)}$

$\Phi_p\big(PSL_2(q)\big)$
$q \equiv 1 \pmod 4),$
$2 \neq p \mid (q-1)$

K	$1a$	$2a$	la	lb	$(x_0^r)^G$	$(y^t)^G$
$\lvert K\rvert$	1	$\frac12 q(q+1)$	$\frac12(q^2-1)$	$\frac12(q^2-1)$	$q(q+1)$	$q(q-1)$
$\lvert \mathrm{C}_G(x_K)\rvert$	$\frac12 q(q^2-1)$	$q-1$	q	q	$\frac12(q-1)$	$\frac12(q+1)$
x_K	1	z	u	v	x_0^r	y^t
φ_1	1	1	1	1	1	1
φ_2	q	1	$\cdot$	$\cdot$	1	-1
φ_3	$\frac12(q+1)$	$(-1)^{(q-1)/4}$	$\frac12(1+\sqrt{q})$	$\frac12(1-\sqrt{q})$	$(-1)^r$	$\cdot$
φ_4	$\frac12(q+1)$	$(-1)^{(q-1)/4}$	$\frac12(1-\sqrt{q})$	$\frac12(1+\sqrt{q})$	$(-1)^r$	$\cdot$
ψ_j	$q+1$	$2\cdot(-1)^j$	1	1	$\zeta_0^{rj}+\zeta_0^{-rj}$	$\cdot$
η_f	$q-1$	$\cdot$	-1	-1	$\cdot$	$-\xi^{tf}-\xi^{-tf}$

D	φ_1	φ_2	φ_3	φ_4	ψ_j	η_f
χ_1	1	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
χ_2	$\cdot$	1	$\cdot$	$\cdot$	$\cdot$	$\cdot$
χ_3	$\cdot$	$\cdot$	1	$\cdot$	$\cdot$	$\cdot$
χ_4	$\cdot$	$\cdot$	$\cdot$	1	$\cdot$	$\cdot$
θ_{s_+}	1	1	$\cdot$	$\cdot$	$\cdot$	$\cdot$
θ_{s_-}	$\cdot$	$\cdot$	1	1	$\cdot$	$\cdot$
θ_{s_i}	$\cdot$	$\cdot$	$\cdot$	$\cdot$	δ_{ij}	$\cdot$
τ_h	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	δ_{hf}

$$C = \begin{pmatrix} \frac{p^d+1}{2} & \frac{p^d-1}{2} & \cdot & \cdot & \cdot & \cdot \\ \frac{p^d-1}{2} & \frac{p^d+1}{2} & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \frac{p^d+1}{2} & \frac{p^d-1}{2} & \cdot & \cdot \\ \cdot & \cdot & \frac{p^d-1}{2} & \frac{p^d+1}{2} & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & p^d\mathbf{1}_{(n/2)-1} & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \mathbf{1}_{(q-1)/4} \end{pmatrix}$$

Обозначения

$p^d = (q-1)_p,\ n = (\frac{q-1}{2})_{p'},$
$x_0 = x^{p^d},\ \zeta_0 = \zeta^{p^d} = e^{2\pi i/n}$

Параметры

$r, i, j \ = \ 1, \dots, \frac{n}{2} - 1;$
$f, h, t \ = \ 1, \dots, \frac{q-1}{4};$
$s_+ = n, 2n, \dots, \frac{p^d-1}{2}n;$
$s_- = \frac{n}{2}, n + \frac{n}{2}, \dots, \frac{p^d-3}{2}n + \frac{n}{2};$
$s_i = i, n \pm i, 2n \pm i, \dots, \frac{p^d-1}{2}n \pm i$

$\Phi_p\big(PSL_2(q)\big)$
$q \equiv 1 \pmod 4$,
$2 \neq p \mid (q+1)$

K	$1a$	$2a$	la	lb	$(x^r)^G$	$(y_0^t)^G$
$\lvert K\rvert$	1	$\frac{1}{2}q(q{+}1)$	$\frac{1}{2}(q^2{-}1)$	$\frac{1}{2}(q^2{-}1)$	$q(q{+}1)$	$q(q{-}1)$
$\lvert \mathrm{C}_G(x_{\scriptscriptstyle K})\rvert$	$\frac{1}{2}q(q^2{-}1)$	$q-1$	q	q	$\frac{1}{2}(q{-}1)$	$\frac{1}{2}(q{+}1)$
$x_{\scriptscriptstyle K}$	1	z	u	v	x^r	y_0^t
φ_1	1	1	1	1	1	1
φ_2	$q-1$	.	-1	-1	.	-2
φ_3	$\frac{1}{2}(q+1)$	$(-1)^{(q-1)/4}$	$\frac{1}{2}(1+\sqrt{q})$	$\frac{1}{2}(1-\sqrt{q})$	$(-1)^r$	.
φ_4	$\frac{1}{2}(q+1)$	$(-1)^{(q-1)/4}$	$\frac{1}{2}(1-\sqrt{q})$	$\frac{1}{2}(1+\sqrt{q})$	$(-1)^r$	.
ψ_j	$q+1$	$2\cdot(-1)^j$	1	1	$\zeta^{rj}{+}\zeta^{-rj}$	.
η_f	$q-1$	.	-1	-1	.	$-\xi_0^{tf}-\xi_0^{-tf}$

D	φ_1	φ_2	φ_3	φ_4	ψ_j	η_f
χ_1	1	.	.	.	.	.
χ_2	1	1	.	.	.	.
χ_3	.	.	1	.	.	.
χ_4	.	.	.	1	.	.
θ_s	.	.	.	.	δ_{sj}	.
τ_{h_0}	.	1	.	.	.	.
τ_{h_i}	.	.	.	.	.	δ_{if}

$$C=\begin{pmatrix} 2 & 1 & . & . & . & . \\ 1 & \frac{p^d+1}{2} & . & . & . & . \\ . & . & 1 & . & . & . \\ . & . & . & 1 & . & . \\ . & . & . & . & \mathbf{1}_{(q-5)/4} & . \\ . & . & . & . & . & p^d\mathbf{1}_{(n-1)/2} \end{pmatrix}$$

Обозначения

$p^d=(q+1)_p,\ n=(\frac{q+1}{2})_{p'}$,
$y_0=y^{p^d},\ \xi_0=\xi^{p^d}=e^{2\pi i/n}$

Параметры

$r,s,j \ = \ 1,\ldots,\frac{q-5}{4}$;
$i,f,t \ = \ 1,\ldots,\frac{n-1}{2}$;
$h_0=n,2n,\ldots,\frac{p^d-1}{2}n$;
$h_i=i,n\pm i,2n\pm i,\ldots,\frac{p^d-1}{2}n\pm i$

$\Phi_2\big(PSL_2(q)\big)$
$q \equiv 1 \pmod 4$

K	$1a$	la	lb	$(x_0^r)^G$	$(y^t)^G$
$\lvert K\rvert$	1	$\frac{1}{2}(q^2{-}1)$	$\frac{1}{2}(q^2{-}1)$	$q(q{+}1)$	$q(q{-}1)$
$\lvert \mathrm{C}_G(x_{\scriptscriptstyle K})\rvert$	$\frac{1}{2}q(q^2{-}1)$	q	q	$\frac{1}{2}(q{-}1)$	$\frac{1}{2}(q{+}1)$
$x_{\scriptscriptstyle K}$	1	u	v	x_0^r	y^t
φ_1	1	1	1	1	1
φ_2	$\frac{1}{2}(q-1)$	$\frac{1}{2}(-1+\sqrt{q})$	$\frac{1}{2}(-1-\sqrt{q})$	.	-1
φ_3	$\frac{1}{2}(q-1)$	$\frac{1}{2}(-1-\sqrt{q})$	$\frac{1}{2}(-1+\sqrt{q})$	.	-1
ψ_j	$q+1$	1	1	$\zeta_0^{rj}{+}\zeta_0^{-rj}$	.
η_f	$q-1$	-1	-1	.	$-\xi^{tf}-\xi^{-tf}$

D	φ_1	φ_2	φ_3	ψ_j	η_f
χ_1	1	.	.	.	.
χ_2	1	1	1	.	.
χ_3	1	1	.	.	.
χ_4	1	.	1	.	.
θ_{s_0}	2	1	1	.	.
θ_{s_i}	.	.	.	δ_{ij}	.
τ_h	.	.	.	.	δ_{hf}

$$C=\begin{pmatrix} 2^d & 2^{d-1} & 2^{d-1} & . & . \\ 2^{d-1} & 2^{d-2}+1 & 2^{d-2} & . & . \\ 2^{d-1} & 2^{d-2} & 2^{d-2}+1 & . & . \\ . & . & . & 2^{d-1}\mathbf{1}_{(n-1)/2} & . \\ . & . & . & . & \mathbf{1}_{(q-1)/4} \end{pmatrix}$$

Обозначения

$2^d=(q-1)_2,\ n=(q-1)_{2'}$,
$x_0=x^{2^{d-1}},\ \zeta_0=\zeta^{2^{d-1}}=e^{2\pi i/n}$

Параметры

$r,i,j \ = \ 1,\ldots,\frac{n-1}{2}$;
$f,h,t \ = \ 1,\ldots,\frac{q-1}{4}$;
$s_0=n,2n,\ldots,(2^{d-2}-1)n$;
$s_i=i,n\pm i,2n\pm i,\ldots,(2^{d-2}-1)n\pm i,2^{d-2}n-i$

$\mathrm{X}\big(PSL_2(q)\big)$
$q \equiv -1 \pmod 4$

K	$1a$	$2a$	la	lb	$(x^r)^G$	$(y^t)^G$
$\lvert K\rvert$	1	$\frac{1}{2}q(q-1)$	$\frac{1}{2}(q^2-1)$	$\frac{1}{2}(q^2-1)$	$q(q+1)$	$q(q-1)$
$\lvert \mathrm{C}_G(x_{\scriptscriptstyle K})\rvert$	$\frac{1}{2}q(q^2-1)$	$q+1$	q	q	$\frac{1}{2}(q-1)$	$\frac{1}{2}(q+1)$
$x_{\scriptscriptstyle K}$	1	z	u	v	x^r	y^t
χ_1	1	1	1	1	1	1
χ_2	q	-1	.	.	1	-1
χ_3	$\frac{1}{2}(q-1)$	$-(-1)^{(q+1)/4}$	$\frac{1}{2}(-1+i\sqrt{q})$	$\frac{1}{2}(-1-i\sqrt{q})$	.	$-(-1)^t$
χ_4	$\frac{1}{2}(q-1)$	$-(-1)^{(q+1)/4}$	$\frac{1}{2}(-1-i\sqrt{q})$	$\frac{1}{2}(-1+i\sqrt{q})$	.	$-(-1)^t$
θ_s	$q+1$	.	1	1	$\zeta^{rs}+\zeta^{-rs}$	.
τ_h	$q-1$	$-2\cdot(-1)^h$	-1	-1	.	$-\xi^{th}-\xi^{-th}$

Обозначения

$q = l^m, \quad l$ простое

Параметры

$r,s,t,h \;=\; 1,\dots,(q-3)/4$

Элементы

$|u| = |v| = l,$
$|x| = \frac{1}{2}(q-1),\ |y| = \frac{1}{2}(q+1),$
$z = x^{(q+1)/4}$

Иррациональные величины

$\zeta = e^{4\pi i/(q-1)},\ \xi = e^{4\pi i/(q+1)}$

$\Phi_p\big(PSL_2(q)\big)$
$q \equiv -1 \pmod 4,$
$2 \neq p \mid (q-1)$

K	$1a$	$2a$	la	lb	$(x_0^r)^G$	$(y^t)^G$
$\lvert K\rvert$	1	$\frac{1}{2}q(q-1)$	$\frac{1}{2}(q^2-1)$	$\frac{1}{2}(q^2-1)$	$q(q+1)$	$q(q-1)$
$\lvert \mathrm{C}_G(x_{\scriptscriptstyle K})\rvert$	$\frac{1}{2}q(q^2-1)$	$q+1$	q	q	$\frac{1}{2}(q-1)$	$\frac{1}{2}(q+1)$
$x_{\scriptscriptstyle K}$	1	z	u	v	x_0^r	y^t
φ_1	1	1	1	1	1	1
φ_2	q	-1	.	.	1	-1
φ_3	$\frac{1}{2}(q-1)$	$-(-1)^{(q+1)/4}$	$\frac{1}{2}(-1+i\sqrt{q})$	$\frac{1}{2}(-1-i\sqrt{q})$	.	$-(-1)^t$
φ_4	$\frac{1}{2}(q-1)$	$-(-1)^{(q+1)/4}$	$\frac{1}{2}(-1-i\sqrt{q})$	$\frac{1}{2}(-1+i\sqrt{q})$	.	$-(-1)^t$
ψ_j	$q+1$	.	1	1	$\zeta_0^{rj}+\zeta_0^{-rj}$	.
η_f	$q-1$	$-2\cdot(-1)^f$	-1	-1	.	$-\xi^{tf}-\xi^{-tf}$

D	φ_1	φ_2	φ_3	φ_4	ψ_j	η_f
χ_1	1	.	.	.	.	.
χ_2	.	1	.	.	.	.
χ_3	.	.	1	.	.	.
χ_4	.	.	.	1	.	.
θ_{s_0}	1	1	.	.	.	.
θ_{s_i}	.	.	.	.	δ_{ij}	.
τ_h	.	.	.	.	.	δ_{hf}

$$C = \begin{pmatrix} \frac{p^d+1}{2} & \frac{p^d-1}{2} & . & . & . & . \\ \frac{p^d-1}{2} & \frac{p^d+1}{2} & . & . & . & . \\ . & . & 1 & . & . & . \\ . & . & . & 1 & . & . \\ . & . & . & . & p^d\mathbf{1}_{(n-1)/2} & . \\ . & . & . & . & . & \mathbf{1}_{(q-3)/4} \end{pmatrix}$$

Обозначения

$p^d = (q-1)_p,\ n = (\frac{q-1}{2})_{p'},$
$x_0 = x^{p^d},\ \zeta_0 = \zeta^{p^d} = e^{2\pi i/n}$

Параметры

$r,i,j \;=\; 1,\dots,\frac{n-1}{2};$
$f,h,t \;=\; 1,\dots,\frac{q-3}{4};$
$s_0 = n, 2n, \dots, \frac{p^d-1}{2}n;$
$s_i = i, n\pm i, 2n\pm i, \dots, \frac{p^d-1}{2}n \pm i$

$\Phi_p\big(PSL_2(q)\big)$
$q \equiv -1 \pmod 4,$
$2 \neq p \mid (q+1)$

K	$1a$	$2a$	la	lb	$(x^r)^G$	$(y_0^t)^G$
$\lvert K\rvert$	1	$\frac{1}{2}q(q-1)$	$\frac{1}{2}(q^2-1)$	$\frac{1}{2}(q^2-1)$	$q(q+1)$	$q(q-1)$
$\lvert \mathrm{C}_G(x_{\scriptscriptstyle K})\rvert$	$\frac{1}{2}q(q^2-1)$	$q+1$	q	q	$\frac{1}{2}(q-1)$	$\frac{1}{2}(q+1)$
$x_{\scriptscriptstyle K}$	1	z	u	v	x^r	y_0^t
φ_1	1	1	1	1	1	1
φ_2	$q-1$	-2	-1	-1	.	-2
φ_3	$\frac{1}{2}(q-1)$	$-(-1)^{(q+1)/4}$	$\frac{1}{2}(-1+i\sqrt{q})$	$\frac{1}{2}(-1-i\sqrt{q})$	.	$-(-1)^t$
φ_4	$\frac{1}{2}(q-1)$	$-(-1)^{(q+1)/4}$	$\frac{1}{2}(-1-i\sqrt{q})$	$\frac{1}{2}(-1+i\sqrt{q})$	.	$-(-1)^t$
ψ_j	$q+1$	.	1	1	$\zeta^{rj}+\zeta^{-rj}$	.
η_f	$q-1$	$-2\cdot(-1)^f$	-1	-1	.	$-\xi_0^{tf}-\xi_0^{-tf}$

D	φ_1	φ_2	φ_3	φ_4	ψ_j	η_f
χ_1	1	.	.	.	.	.
χ_2	1	1	.	.	.	.
χ_3	.	.	1	.	.	.
χ_4	.	.	.	1	.	.
θ_s	.	.	.	.	δ_{sj}	.
τ_{h_+}	.	1	.	.	.	.
τ_{h_-}	.	.	1	1	.	.
τ_{h_i}	.	.	.	.	.	δ_{if}

$$C = \begin{pmatrix} 2 & 1 & . & . & . & . \\ 1 & \frac{p^d+1}{2} & . & . & . & . \\ . & . & \frac{p^d+1}{2} & \frac{p^d-1}{2} & . & . \\ . & . & \frac{p^d-1}{2} & \frac{p^d+1}{2} & . & . \\ . & . & . & . & \mathbf{1}_{(q-3)/4} & . \\ . & . & . & . & . & p^d\mathbf{1}_{(n/2)-1} \end{pmatrix}$$

Обозначения

$p^d = (q+1)_p,\ n = (\frac{q+1}{2})_{p'},$
$y_0 = y^{p^d},\ \xi_0 = \xi^{p^d} = e^{2\pi i/n}$

Параметры

$r,s,j\ =\ 1,\ldots,\frac{q-3}{4};$
$i,f,t\ =\ 1,\ldots,\frac{n}{2}-1;$
$h_+ = n, 2n, \ldots, \frac{p^d-1}{2}n;$
$h_- = \frac{n}{2}, n+\frac{n}{2}, \ldots, \frac{p^d-3}{2}n+\frac{n}{2};$
$h_i = i, n\pm i, 2n\pm i, \ldots, \frac{p^d-1}{2}n\pm i$

$\Phi_2\big(PSL_2(q)\big)$
$q \equiv -1 \pmod 4$

K	$1a$	la	lb	$(x^r)^G$	$(y_0^t)^G$
$\lvert K\rvert$	1	$\frac12(q^2-1)$	$\frac12(q^2-1)$	$q(q+1)$	$q(q-1)$
$\lvert \mathrm{C}_G(x_K)\rvert$	$\frac12 q(q^2-1)$	q	q	$\frac12(q-1)$	$\frac12(q+1)$
x_K	1	u	v	x^r	y_0^t
φ_1	1	1	1	1	1
φ_2	$\frac12(q-1)$	$\frac12(-1+i\sqrt{q})$	$\frac12(-1-i\sqrt{q})$	.	-1
φ_3	$\frac12(q-1)$	$\frac12(-1-i\sqrt{q})$	$\frac12(-1+i\sqrt{q})$	.	-1
ψ_j	$q+1$	1	1	$\zeta^{rj}+\zeta^{-rj}$	.
η_f	$q-1$	-1	-1	.	$-\xi_0^{tf}-\xi_0^{-tf}$

D	φ_1	φ_2	φ_3	ψ_j	η_f
χ_1	1	.	.	.	.
χ_2	1	1	1	.	.
χ_3	.	1	.	.	.
χ_4	.	.	1	.	.
θ_s	.	.	.	δ_{sj}	.
τ_{h_0}	.	1	1	.	.
τ_{h_i}	.	.	.	.	δ_{if}

$$C = \begin{pmatrix} 2 & 1 & 1 & . & . \\ 1 & 2^{d-2}+1 & 2^{d-2} & . & . \\ 1 & 2^{d-2} & 2^{d-2}+1 & . & . \\ . & . & . & \mathbf{1}_{(q-3)/4} & . \\ . & . & . & . & 2^{d-1}\mathbf{1}_{(n-1)/2} \end{pmatrix}$$

Обозначения

$2^d = (q+1)_2,\ n = (q+1)_{2'},$
$y_0 = y^{2^{d-1}},\ \xi_0 = \xi^{2^{d-1}} = e^{2\pi i/n}$

Параметры

$r,s,j\ =\ 1,\ldots,\frac{q-3}{4};$
$i,f,t\ =\ 1,\ldots,\frac{n-1}{2};$
$h_0 = n, 2n, \ldots, (2^{d-2}-1)n;$
$h_i = i, n\pm i, 2n\pm i, \ldots, (2^{d-2}-1)n\pm i, 2^{d-2}n-i$

Предметный указатель

Список обозначений

$\mathbb{Z}[\mathrm{Irr}_F(G)]$ кольцо обобщённых F-характеров, 34

$(\varphi, \psi)_{G_{p'}}$ скалярное произведение ограничения на $G_{p'}$ классовых функций $\varphi, \psi \in \mathrm{cf}(G) \cup \mathrm{cf}(G_{p'})$, 58

$(\varphi, \psi)_G$ скалярное произведение классовых функций $\varphi, \psi \in \mathrm{cf}(G)$, 43

th_φ главный неразложимый характер, соответствующий брауэрову характеру φ , 58

0_R ноль кольца R, 5

1_G главный F-характер, 31

$1_{G_{p'}}$ главный брауэров характер, 50

1_R единица кольца R, 5

$A(D)$, 82

A° регулярный A-модуль R-алгебры A, 15

$\alpha_{\mathscr{A}}(K)$ коэффициент при $\widehat{K}$ в разложении $f_{\mathscr{A}}$, 64

$\star$ Естественный эпиморфизм $\boldsymbol{R} \to \boldsymbol{R}/M$, 48

$\mathscr{A}_{K,L}$, 81

$\mathrm{Ann}(V)$ аннулятор A-модуля V, 18

$\mathrm{Ann}(v)$ аннулятор v из A-модуля V, 18

$A \otimes B$ кронекерово произведение матриц A и B, 33

$\overline{A}$ матрица $(\overline{\alpha_{ij}})$, где $(\alpha_{ij}) = A$, 44

$A^\star$ матрица $(\alpha_{ij}^\star)$, где $A = (\alpha_{ij})$, 52

$M^\top$ транспонированная к матрице M, 5

$A \triangle B$ симметрическая разность множеств A и B, 6

A_V образ F-алгебры A при отображении $a \mapsto a_V$, 25

a_V отображение $v \mapsto va$ из A-модуля V в себя для элемента $a \in A$, 25

b^G индуцированный p-блок, 77

β_P гомоморфизмом Брауэра, 76

$\mathrm{Bl}(G)$ множество p-блоков группы G, 62

$\mathrm{Bl}(G|P)$ множество p-блоков с дефектной группой P, 79

$\mathrm{Bl}_p(G)$ множество p-блоков группы G, 62

C матрица Картана, 57

$\mathbb{C}$ поле комплексных чисел, 26

C_B матрица Картана p-блока B, 66

$\mathrm{cf}^\circ(G)$ множество функций из $\mathrm{cf}(G)$, тождественно равных нулю вне $G_{p'}$, 58

$\mathrm{cf}_F(G)$ F-алгебра классовых функций на группе G со значениями в поле F, 32

$\mathrm{cf}(G)$ $\mathrm{cf}_{\mathbb{C}}(G)$, 43

$\mathrm{cf}(G_{p'})$ пространство классовых функций на p'-элементах, 50

χ^G характер, индуцированный F-характером χ, 35

Рекомендуемая литература

[1] М. И. Каргаполов, Ю. И. Мерзляков, Основы теории групп, 4-е изд. М.: Наука. 1996.

[2] Ч. Кэртис, И. Райнер, Теория представлений конечных групп и ассоциативных алгебр. М.: Наука. 1969.

[3] С. Ленг, Алгебра. М.: Мир. 1968.

[4] Л. А. Скорняков, Элементы общей алгебры, М.: Наука. 1983.

[5] У. Фейт, Теория представлений конечных групп. М.: Наука. 1990.

[6] I. M. Isaacs, Character theory of finite groups. Pure and Applied Mathematics. N 69. N.Y.: Acad. Press. 1976.

[7] G. Navarro, Characters and blocks of finite groups. London Mathematical Society Lecture Note Series, 250. Camb. Univ. Press, Cambridge. 1998.

[8] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups, Oxford: Clarendon Press. 1985.

[9] E. C. Dade, Counting characters in blocks. II.9. Representation theory of finite groups (Columbus, OH, 1995), 45–59, Ohio State Univ. Math. Res. Inst. Publ., 6, de Gruyter, Berlin. 1997.

[10] D. Gorenstein, Finite groups, 2nd ed. N.Y.: Chelsea Publishing Company. XVII. 1980.