ТЕОРИЯ ПРЕДСТАВЛЕНИЙ ГРУПП И АЛГЕБР

§ 104. Постановка задачи

Пусть $\mathfrak{G}$ — произвольная группа. Под *представлением группы* $\mathfrak{G}$ *над полем* K понимается любой гомоморфизм групп, который каждому элементу исходной группы a сопоставляет линейное преобразование A некоторого n-мерного векторного пространства над K (или, что по существу равносильно, некоторую n-строчную матрицу A). Размерность n называется *степенью* представления. Представление называется *точным*, если оно является изоморфизмом.

Точно так же под *представлением произвольного кольца* $\mathfrak{o}$ *над полем* K понимается гомоморфизм колец $a \longmapsto A$, где A — вновь линейное преобразование n-мерного векторного пространства. Это определение совпадает с определением из § 87. Еще тогда было показано, что каждому представлению кольца $\mathfrak{o}$ над полем K соответствует двойной модуль $\mathfrak{M}$ (на который $\mathfrak{o}$ действует слева, а K — справа), названный *модулем представления*, и наоборот; каждый такой модуль представления задает некоторое представление. Изоморфным модулям представления соответствуют эквивалентные представления, и наоборот. Представление называется *приводимым*, если модуль представления обладает собственным ненулевым подмодулем, и *неприводимым*, если соответствующий модуль представления прост.

Если $\mathfrak{o}$ — некоторая алгебра над полем P, то от представления дополнительно требуется, чтобы основное поле P принадлежало полю K и чтобы из соответствия $a \longmapsto A$ для любого β из P следовало соответствие $a\beta \longmapsto A\beta$. Для модуля представления $\mathfrak{M}$ это означает, что

$$(a\beta)\,u = (au)\,\beta \quad \text{для} \quad a \in \mathfrak{o}, \quad \beta \in \mathsf{P}, \quad u \in \mathfrak{M}.$$

Основная задача состоит в отыскании всех представлений заданной группы или алгебры. При этом задача о представлениях для конечных групп немедленно сводится к аналогичной задаче для алгебр: нужно лишь в соответствии с § 93 построить из группы групповое кольцо

$$\mathfrak{o} = a_1\mathsf{K} + \ldots + a_h\mathsf{K},$$

базисными элементами $a_1, \ldots, a_h$ которого будут элементы группы $\mathfrak{G}$. Если $a_i \longmapsto A_i$ — представление группы, то

$$\sum a_i\beta_i \longmapsto \sum A_i\beta_i$$

— представление группового кольца $\mathfrak{o}$, в чем легко убедиться. Обратно, любое представление группового кольца $\mathfrak{o}$ над полем K сопоставляет, в частности, и базисным элементам $a_1, \ldots, a_h$ некоторые линейные преобразования, а они определяют представление самой группы. Мы получили предложение:

Каждое представление конечной группы над полем K *задается некоторым представлением группового кольца.*

В теории представлений алгебр, как правило, предполагается, что поле представления K совпадает с основным полем P. Общий случай можно свести к этому частному, расширив алгебру $\mathfrak{o}$ до алгебры $\mathfrak{o}_{\mathsf{K}}$. Если в исходном представлении базисным элементам $a_1, \ldots, a_h$ алгебры $\mathfrak{o}$ соответствовали матрицы $A_1, \ldots, A_h$, то произвольному элементу $\sum a_i\beta_i$ $(\beta_i \in \mathsf{K})$ алгебры $\mathfrak{o}_{\mathsf{K}}$ можно сопоставить матрицу $\sum A_i\beta_i$ и тем самым продолжить представление алгебры $\mathfrak{o}$ до представления алгебры $\mathfrak{o}_{\mathsf{K}}$. *Тем самым каждое представление алгебры* $\mathfrak{o}$ *над полем* K *задает некоторое представление алгебры* $\mathfrak{o}_{\mathsf{K}}$.

Дальнейшее ограничение постановки задачи получится в случае, когда кольцо $\mathfrak{o}$ обладает единицей. Здесь мы всегда можем считать, что единица 1 является и единичным оператором на модуле представления, т. е. в данном представлении этому элементу соответствует единичная матрица. В противном случае, как на это было указано в § 84, модуль представления является прямой суммой $\mathfrak{M}_0 + \mathfrak{M}_1$, где $\mathfrak{M}_0$ аннулируется кольцом $\mathfrak{o}$, а на $\mathfrak{M}_1$ единица является единичным оператором. Таким образом, представление распадается на две части, первая из которых состоит из нулевых матриц и поэтому неинтересна, а вторая является представлением, в котором единица переходит в единичный оператор.

Особенно важным представлением алгебры является *регулярное представление*, которое получается, когда сама алгебра $\mathfrak{o}$ берется в качестве модуля представления, на который $\mathfrak{o}$ действует слева, а P — справа. Подмодулями здесь служат левые идеалы кольца $\mathfrak{o}$. Регулярное представление вполне приводимо, если вполне приводимым слева является само кольцо.

§ 105. Представления алгебр

В § 100 (теорема 18) мы видели, что радикал $\mathfrak{R}$ алгебры $\mathfrak{o}$ представляется нулем в любом неприводимом представлении этой алгебры. То же самое верно, конечно, и для вполне приводимого представления, потому что оно складывается из неприводимых

представлений. Таким образом, любое вполне приводимое представление алгебры $\mathfrak{o}$ можно считать представлением полупростой алгебры $\mathfrak{o}/\mathfrak{R}$.

Следующая теорема указывает, как получаются представления полупростых алгебр или, более общо, полупростых колец с условием минимальности для левых идеалов. Согласно § 98 каждое такое кольцо $\mathfrak{o}$ обладает единичным элементом и вполне приводимо слева, т. е. является прямой суммой простых левых идеалов. Каждому представлению кольца $\mathfrak{o}$ соответствует некоторый $\mathfrak{o}$-модуль $\mathfrak{M}$. Имеет место следующая

Основная теорема. *Пусть $\mathfrak{o}$ — вполне приводимое слева кольцо с единицей и $\mathfrak{M}$ — некоторый $\mathfrak{o}$-модуль с конечным базисом. Единичный элемент кольца $\mathfrak{o}$ считается единичным оператором на $\mathfrak{M}$. Тогда $\mathfrak{M}$ является прямой суммой простых $\mathfrak{o}$-модулей. Каждый из них изоморфен некоторому простому левому идеалу в $\mathfrak{o}$.*

Доказательство. Согласно предположению кольцо $\mathfrak{o}$ является прямой суммой простых левых идеалов:

$$\mathfrak{o} = \mathfrak{l}_1 + \ldots + \mathfrak{l}_r. \tag{1}$$

Далее, по условию модуль $\mathfrak{M}$ обладает конечным $\mathfrak{o}$-базисом $(u_1, \ldots, u_s)$. Отсюда

$$\mathfrak{M} = (\mathfrak{o}u_1, \ldots, \mathfrak{o}u_s). \tag{2}$$

Подставляя (1) в (2), получим

$$\mathfrak{M} = (\ldots, \mathfrak{l}_i u_k, \ldots). \tag{3}$$

Из суммы в правой части равенства (3) можно удалить модули $\mathfrak{l}_i u_k$, равные нулю. Если же $\mathfrak{l}_i u_k \neq \{0\}$, то сопоставление $x \longmapsto xu_k$ определяет операторный изоморфизм из $\mathfrak{l}_i$ на $\mathfrak{l}_i u_k$. Отличные от нуля модули $\mathfrak{l}_i u_k$ изоморфны, таким образом, модулю $\mathfrak{l}_i$, а потому являются простыми. Если одно из слагаемых $\mathfrak{l}_i u_k$ содержится в сумме остальных, то его можно удалить. Продолжать в таком духе можно до тех пор, пока каждый из оставшихся членов $\mathfrak{l}_i u_k$ не будет иметь нулевое пересечение с суммой остальных. В таком случае сумма будет прямой.

Разумеется, основная теорема остается верной и тогда, когда кольцу $\mathfrak{o}$ и модулю $\mathfrak{M}$ придана область правых мультипликаторов Ω со следующими свойствами:

$$(au)\beta = a(u\beta) = (a\beta)u \qquad (\beta \in \Omega).$$

В применениях к теории представлений алгебр Ω является полем коэффициентов P алгебры $\mathfrak{o}$ и одновременно полем представления. Если $\mathfrak{M}$ — векторное пространство конечной размерности над P, то $\mathfrak{M}$ автоматически имеет конечный $\mathfrak{o}$-базис, что и требуется в основной теореме.

Для полупростых алгебр эта теорема утверждает, что каждое представление любой из них вполне приводимо, и что составляющие неприводимые представления входят в качестве неприводимых составляющих в регулярное представление. Неприводимые составляющие регулярного представления в соответствии с (1) связаны с простыми левыми идеалами $\mathfrak{l}_i$.

Любая полупростая алгебра $\mathfrak{o}$ в соответствии с § 99 является прямой суммой простых алгебр $\mathfrak{a}_\nu$:

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_s. \tag{4}$$

Алгебры $\mathfrak{a}_\nu$ можно разлагать в свою очередь на минимальные левые идеалы $\mathfrak{l}_i$. Входящие в фиксированную алгебру $\mathfrak{a}_\nu$ идеалы $\mathfrak{l}_i$ попарно изоморфны, а потому задают одно и то же представление. Идеалы $\mathfrak{l}_i$, содержащиеся в алгебре $\mathfrak{a}_\nu$, аннулируются каждой из алгебр $\mathfrak{a}_\mu$ при $\mu \neq \nu$:

$$\mathfrak{a}_\mu \mathfrak{l}_i \subseteq \mathfrak{a}_\mu \mathfrak{a}_\nu = \{0\}.$$

Поэтому все эти алгебры $\mathfrak{a}_\mu$ представляются нулем в том представлении, которое соответствует идеалу $\mathfrak{l}_i$. Лишь алгебра $\mathfrak{a}_\nu$ будет представляться этим представлением точно. Действительно, ядро представления алгебры $\mathfrak{a}_\nu$ является двусторонним идеалом в $\mathfrak{a}_\nu$, и так как $\mathfrak{a}_\nu$ — простая алгебра, не вся представляющаяся нулем, ядро может быть только нулевым идеалом.

Мы рассмотрим теперь представление простой алгебры, которое связано с любым простым левым идеалом этой алгебры.

Простая алгебра $\mathfrak{o}$ с единицей согласно § 102 изоморфна полному матричному кольцу над некоторым телом Δ. Если c_{ik} — введенные в § 93 матричные единицы, которые там обозначались через C_{ik}, то

$$\mathfrak{o} = c_{11}\Delta + c_{12}\Delta + \ldots + c_{nn}\Delta.$$

Минимальный левый идеал $\mathfrak{l}$ будет задаваться равенством

$$\mathfrak{l} = c_{11}\Delta + c_{21}\Delta + \ldots + c_{n1}\Delta.$$

Наконец, основное поле P, над которым определено представление, содержится в центре тела Δ, и Δ имеет конечный ранг над P.

Рассмотрим сначала случай $\Delta = \mathsf{P}$. Базис $(c_{11}, c_{21}, \ldots, c_{n1})$ идеала $\mathfrak{l}$ может служить для явного описания матриц представления. Если $a = \sum_{i,\, k=1}^{n} c_{ik}\alpha_{ik}$ — элемент кольца $\mathfrak{o}$, то

$$ac_{k1} = \sum_{i=1}^{n} c_{ik}c_{k1}\alpha_{ik} = \sum_{i=1}^{n} c_{i1}\alpha_{ik},$$

тем самым в представлении, соответствующем идеалу $\mathfrak{l}$, *элементу* a *сопоставляется матрица* $\|\alpha_{ik}\|$. Следовательно, изоморфизм кольца $\mathfrak{o}$

и полного кольца матриц $\|\alpha_{ik}\|$ — это то самое неприводимое представление, которое соответствует минимальному левому идеалу $\mathfrak{l}$.

Примечательно, что в рассматриваемом случае $\Delta = \mathsf{P}$ представляемые матрицы образуют *полное* матричное кольцо n-й степени. Это же обстоятельство можно выразить и такими словами: среди представляемых матриц есть ровно n^2 линейно независимых.

Пусть теперь Δ — собственное расширение конечной степени поля P:

$$\Delta = \lambda_1\mathsf{P} + \ldots + \lambda_r\mathsf{P}.$$

В этом случае мы прежде всего построим регулярное представление алгебры Δ над полем P, при котором каждому элементу β из Δ сопоставляется матрица B с помощью равенства

$$\beta\lambda_j = \sum \lambda_i\beta_{ij}, \qquad B = \|\beta_{ij}\|.$$

Затем мы построим идеал

$$\mathfrak{l} = c_{11}\Delta + \ldots + c_{n1}\Delta = \\ = (c_{11}\lambda_1\mathsf{P} + \ldots + c_{11}\lambda_r\mathsf{P}) + \ldots + (c_{n1}\lambda_1\mathsf{P} + \ldots + c_{n1}\lambda_r\mathsf{P}).$$

Если с помощью этого базиса представить элемент $c_{ik}\beta$ алгебры $\mathfrak{o}$, то получится:

$$c_{ik}\beta \longmapsto \begin{Vmatrix} 0 \ldots 0 \ \ldots 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 0 \ldots B \ldots 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 0 \ldots 0 \ldots 0 \end{Vmatrix},$$

где нули представляют r-строчные нуль-матрицы, а матрица B занимает место на пересечении k-го столбца и i-й строки. Суммируя, получаем отсюда:

$$\sum_{i,\,k=1}^{n} c_{ik}\alpha_{ik} \longmapsto \begin{Vmatrix} A_{11} \ldots A_{1n} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ A_{n1} \ldots A_{nn} \end{Vmatrix}, \tag{5}$$

где A_{ik} — опять-таки матрицы, соответствующие элементам α_{ik} в регулярном представлении алгебры Δ.

Из вида неприводимого представления, соответствующего модулю $\mathfrak{l}$, можно понять, каким образом оно распадается при том или ином расширении основного поля P до какого-то поля Ω. При таком расширении тело Δ переходит в систему $\Delta_\Omega = \Delta \times \Omega$, а левый идеал $\mathfrak{l} = c_{11}\Delta + \ldots + c_{n1}\Delta$ — в

$$\mathfrak{l}_\Omega = c_{11}\Delta_\Omega + \ldots + c_{n1}\Delta_\Omega.$$

Если кольцо Δ_Ω приводимо и содержит собственный левый идеал $\mathfrak{l}'$, то и $\mathfrak{l}_\Omega$ содержит собственный подидеал

$$\mathfrak{L}' = c_{11}\mathfrak{l}' + \ldots + c_{n1}\mathfrak{l}'.$$

Точно так же: если Δ_Ω распадается на левые идеалы $\mathfrak{l}'$, то идеал $\mathfrak{l}_\Omega$ распадается на то же число левых идеалов $\mathfrak{l}'$. Следовательно: *приводимость или разложение неприводимого представления кольца* $\mathfrak{o}$, *соответствующего идеалу* $\mathfrak{l}$ *при расширении поля* P *до поля* Ω, *полностью определяется приводимостью или соответственно разложением алгебры* Δ_Ω *на левые идеалы.*

Если $\Delta \neq \mathsf{P}$, то согласно § 103 поле Ω всегда можно выбрать так, чтобы алгебра Δ_Ω содержала делители нуля и, следовательно, не являлась телом, а содержала по крайней мере один собственный левый идеал. В таком случае неприводимое представление над полем P, соответствующее идеалу $\mathfrak{l}$, будет приводимо над полем Ω. В случае $\Delta = \mathsf{P}$, наоборот, представление, соответствующее идеалу $\mathfrak{l}$, *абсолютно неприводимо*, т. е. остается неприводимым при любом расширении основного поля. *Тем самым условие* $\Delta = \mathsf{P}$ *является необходимым и достаточным для абсолютной неприводимости представления, заданного над* P.

Если алгебра $\mathfrak{o}$ является не простой, а всего лишь полупростой, равной прямой сумме простых алгебр $\mathfrak{a}_1 + \ldots + \mathfrak{a}_s$, и $\mathfrak{l}$ — какой-нибудь левый идеал, скажем, $\mathfrak{a}_\nu$, то для описания представления произвольного элемента a из $\mathfrak{o}$, задаваемого идеалом $\mathfrak{l}$, нужно поступить так: сначала записать a в виде суммы $a_1 + \ldots + a_s$, затем из этой суммы извлечь компоненту a_ν и в соответствии с формулой (5) построить для элемента a_ν матрицу. Остальные же компоненты $a_1, \ldots, a_{\nu-1}, a_{\nu+1}, \ldots, a_s$ аннулируют идеал $\mathfrak{l}$ и поэтому представляются нулем.

Если $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ — полные матричные кольца порядков $n_1, \ldots, n_s$ соответственно над телами $\Delta_1, \ldots, \Delta_s$ и если r_ν — ранг тела Δ_ν, а $\mathfrak{D}_\nu$ — неприводимое представление, соответствующее левому идеалу $\mathfrak{a}_\nu$, то ранг h алгебры $\mathfrak{o}$ равен сумме рангов алгебр $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$, т. е.

$$h = \sum_1^s n_\nu^2 r_\nu; \tag{6}$$

далее, степень представления $\mathfrak{D}_\nu$ согласно (5) равна

$$g_\nu = n_\nu r_\nu. \tag{7}$$

Наконец, алгебра $\mathfrak{a}_\nu$ распадается на n_ν эквивалентных левых идеалов $\mathfrak{l}_\nu$, благодаря чему регулярное представление содержит представление $\mathfrak{D}_\nu$ как n_ν-кратную составляющую.

В частности, если все $\mathfrak{D}_\nu$ абсолютно неприводимы, то все $r_\nu = 1$; тем самым (6) и (7) принимают более простой вид:

$$h = \sum_1^s n_\nu^2; \quad g_\nu = n_\nu. \tag{8}$$

§ 106. Представления центра

Центр алгебры $\mathfrak{o}$ при любом неприводимом представлении должен отображаться на такие матрицы, которые перестановочны со всеми матрицами представления. Если основное поле алгебраически замкнуто и кольцо представляющих матриц — полное матричное кольцо, то матрицы центра состоят лишь из кратных единичной матрицы E; следовательно, центр алгебры $\mathfrak{o}$ в этом случае представляется матрицами вида $E\alpha$. То же самое верно и для абсолютно неприводимых представлений, потому что в этом случае можно перейти к алгебраически замкнутому основному полю, не утрачивая неприводимости. Итак: *при любом абсолютно неприводимом представлении алгебры $\mathfrak{o}$ элементы ее центра представляются кратными единичной матрицы.*

Если кольцо $\mathfrak{o}$ коммутативно, и, следовательно, является своим собственным центром, то все матрицы абсолютно неприводимого представления имеют вид $E_n\lambda$. Из неприводимости следует, что представления должны иметь первую степень. Итак: *абсолютно неприводимые представления коммутативной алгебры имеют степень* 1.

Любое представление первой степени алгебры $\mathfrak{o}$ — это гомоморфное отображение из $\mathfrak{o}$ в тело представления K. Если K коммутативно, то два эквивалентных представления первой степени просто равны, потому что если $A = \|\alpha\|$ — матрица представления и λ — элемент поля K, то

$$\lambda^{-1}\|\alpha\|\lambda = \|\lambda^{-1}\alpha\lambda\| = \|\alpha\|.$$

Отсюда следует утверждение: *число неэквивалентных представлений первой степени коммутативной алгебры $\mathfrak{o}$ в поле K равно числу различных гомоморфизмов из $\mathfrak{o}$ в K.*

Вернемся к некоммутативным алгебрам и предположим, что алгебра $\mathfrak{o}$ полупроста. Тогда она является прямой суммой простых алгебр:

$$\mathfrak{o} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_s,$$

и центр $\mathfrak{Z}$ алгебры $\mathfrak{o}$ представляется в виде суммы того же числа полей:

$$\mathfrak{Z} = \mathfrak{Z}_1 + \ldots + \mathfrak{Z}_s \qquad (\mathfrak{Z}_s \text{ — центр в } \mathfrak{a}_s).$$

Число неэквивалентных неприводимых представлений кольца $\mathfrak{o}$ и равным образом его центра $\mathfrak{Z}$ равно числу s двусторонних компонент в $\mathfrak{o}$ или в $\mathfrak{Z}$, потому что каждое такое представление $\mathfrak{D}_\nu$ кольца $\mathfrak{o}$ определяется некоторым левым идеалом в $\mathfrak{a}_\nu$, а каждое неприводимое представление $\mathfrak{D}'_\nu$ центра $\mathfrak{Z}$ определяется полем $\mathfrak{Z}_\nu$. Итак: *существует столько же неэквивалентных неприводимых представлений кольца $\mathfrak{o}$, сколько неприводимых неэквивалентных представлений центра $\mathfrak{Z}$, и каждому неприводимому представлению $\mathfrak{D}_\nu$*

кольца $\mathfrak{o}$, *при котором все* $\mathfrak{a}_1 \ldots, \mathfrak{a}_s$, *кроме* $\mathfrak{a}_\nu$, *переходят в нуль, можно сопоставить представление* $\mathfrak{D}'_\nu$ *центра* $\mathfrak{Z}$, *при котором все* $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$, *кроме* $\mathfrak{Z}_\nu$, *переходят в нуль.*

В частности, если $\mathfrak{o}$ — сумма полных матричных колец над P, то поля $\mathfrak{Z}_\nu$ имеют ранг 1 и изоморфны P; тем самым в данном случае число s неприводимых представлений кольца $\mathfrak{o}$ равно рангу центра $\mathfrak{Z}$. Связь между неприводимыми представлениями $\mathfrak{D}_\nu$ кольца $\mathfrak{o}$ и неприводимыми представлениями (первой степени) центра $\mathfrak{Z}$ в рассматриваемом случае совершенно проста. Именно, представление $\mathfrak{D}_\nu$ переводит каждый элемент центра z в матрицу вида $E\alpha$, где E — единичная матрица n_ν-го порядка. Каждому элементу z таким образом сопоставляется (при фиксированном ν) некоторый элемент α, и можно записать:

$$\alpha = \Theta_\nu(z).$$

Функция Θ_ν определяет гомоморфизм центра, т. е.

$$\Theta_\nu(y+z) = \Theta_\nu(y) + \Theta_\nu(z),$$
$$\Theta_\nu(yz) = \Theta_\nu(y)\,\Theta_\nu(z),$$
$$\Theta_\nu(z\beta) = \Theta_\nu(z)\cdot\beta.$$

При этом гомоморфизме поля $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$, за исключением $\mathfrak{Z}_\nu$, представляются нулем, т. е. гомоморфизм Θ_ν — это не что иное, как обозначавшееся раньше через $\mathfrak{D}'_\nu$ представление первой степени центра.

Представление Θ_ν задано всякий раз, когда задан P-базис модуля $\mathfrak{Z}_\nu$, а в качестве последнего можно взять единичный элемент e_ν поля $\mathfrak{Z}_\nu$. Если каждый элемент z из $\mathfrak{Z}$ записать в виде

$$z = \sum_{\nu=1}^{s} e_\nu \beta_\nu, \tag{1}$$

то получится

$$ze_\nu = e_\nu^2 \beta_\nu = e_\nu \beta_\nu;$$

тем самым $E\beta_\nu$ будет представляющей матрицей, т. е.

$$\Theta_\nu(z) = \beta_\nu.$$

Вместо (1) мы можем теперь писать

$$z = \sum_{\nu=1}^{s} e_\nu \Theta_\nu(z). \tag{2}$$

Иначе говоря: *коэффициенты* $\Theta_\nu(z)$ *разложения элемента* z *центра по идемпотентным элементам* e_ν *того же центра задают гомоморфизмы или представления первой степени этого центра.*

Задача 1. Число представлений первой степени коммутативной алгебры $\mathfrak{o}$ над алгебраически замкнутым расширением Ω поля P равно рангу алгебры $\mathfrak{o}_\Omega/\mathfrak{R}$ над P, где $\mathfrak{R}$ — радикал кольца $\mathfrak{o}_\Omega$.

Задача 2. Если K — поле, являющееся расширением поля P, то число представлений первой степени поля K над Ω равно редуцированной степени поля K над полем P. Равенство $\mathfrak{R}=\{0\}$ имеет место тогда и только тогда, когда поле K сепарабельно над полем P.

§ 107. Следы и характеры

Следом элемента a в представлении $\mathfrak{D}$ — обозначение

$$S_{\mathfrak{D}}(a) \text{ или просто } S(a)$$

— называется след $S(A)$ матрицы A, которую представление $\mathfrak{D}$ сопоставляет элементу a. След $S_{\mathfrak{D}}$ при фиксированном $\mathfrak{D}$, рассматриваемый как функция от a, называется также *следом представления* $\mathfrak{D}$.

В силу соотношения

$$S(P^{-1}AP)=S(A)$$

эквивалентные представления имеют равные следы.

Следы являются *линейными функциями*, т. е. справедливы равенства:

$$S(a+b)=S(a)+S(b),$$
$$S(a\beta)=S(a)\beta.$$

Следы абсолютно неприводимых представлений (или, что то же самое, следы неприводимых представлений над алгебраически замкнутым полем) называются *характерами*[1]). Характер элемента a в ν-м неприводимом представлении $\mathfrak{D}_\nu$ будет обозначаться через

$$\chi_\nu(a).$$

Когда речь идет о фиксированном представлении, индекс ν будет, как правило, опускаться.

При любом абсолютно неприводимом представлении $\mathfrak{D}_\nu$ степени n_ν элементы центра z представляются в соответствии с § 106 диагональными матрицами $E\cdot\Theta_\nu(z)$, где Θ_ν — некоторый гомоморфизм центра в поле Ω. След матрицы $E\cdot\Theta_\nu(z)$ задается равенством

$$\chi_\nu(z)=n_\nu\cdot\Theta_\nu(z). \tag{1}$$

В частности, единичный элемент кольца $\mathfrak{o}$ представляется единичной матрицей E, след которой равен n_ν:

$$\chi_\nu(1)=n_\nu.$$

---

[1]) Многие авторы употребляют слово «характер» и для приводимых представлений и говорят в этом случае о «сложных характерах». Мы избегаем такой терминологии, потому что в частном случае абелевых групп она не совпадает по смыслу с принятым еще в давние времена термином «характер» (ср. § 54); кроме того, слово «след» не менее четко выражает суть дела.

В дальнейшем мы предполагаем, что степень n_ν абсолютно неприводимых представлений не делится на характеристику поля Ω. Тогда (1) можно разделить на n_ν и получить

$$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu}. \tag{2}$$

Так гомоморфизмы центра описываются с помощью характеров.

Теорема. *Любое вполне приводимое представление алгебры $\mathfrak{o}$ над полем Ω характеристики 0 однозначно с точностью до эквивалентности определяется следами представляемых матриц.*

Доказательство. Если $\mathfrak{R}$ — радикал кольца $\mathfrak{o}$, то любое вполне приводимое представление алгебры $\mathfrak{o}$ совпадает с некоторым вполне приводимым представлением факторалгебры $\mathfrak{o}/\mathfrak{R}$. По условию, следы матриц, представляющих элементы алгебры $\mathfrak{o}/\mathfrak{R}$, известны. Пусть

$$\mathfrak{o}/\mathfrak{R} = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n$$

и $e_1, \ldots, e_n$ — единицы в кольцах $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ соответственно. Тогда в неприводимом представлении $\mathfrak{D}_\nu$ элемент a_ν представляется n_ν-строчной единичной матрицей; тем самым соответствующий след равен

$$S_\nu(e_\nu) = n_\nu,$$

и одновременно

$$S_\nu(e_\mu) = 0 \text{ для } \mu \neq \nu.$$

Далее, вполне приводимое представление известно, как только известно, сколько раз в него входит каждое неприводимое представление $\mathfrak{D}_\nu$. Если, скажем, представление $\mathfrak{D}_\nu$ входит q_ν раз, то все рассматриваемое представление состоит из q_1 блоков $\mathfrak{D}_1$, q_2 блоков $\mathfrak{D}_2$ и т. д. След элемента e_ν в этом представлении равен тогда

$$S(e_\nu) = q_\nu n_\nu. \tag{3}$$

Из (3) можно вычислить параметры q_ν, как только известны следы $S(e_\nu)$. Теорема доказана.

Замечание. Следы всех элементов кольца $\mathfrak{o}$ становятся известными, как только известны следы базисных элементов алгебры $\mathfrak{o}$. Таким образом, если, например, $\mathfrak{o}$ — групповое кольцо некоторой конечной группы, то нужно лишь знать следы элементов группы — и тогда представление задано. Если $a_1, \ldots, a_n$ — базисные элементы и $\chi_\nu(a_i)$ — их следы при неприводимых представлениях, то для любого представления имеют место равенства:

$$S(a_i) = \sum_{\nu=1}^{s} q_\nu \chi_\nu(a_i). \tag{4}$$

Согласно доказанной выше теореме этими равенствами числа q_ν определяются однозначно. Равенства (4) дают численный метод

разложения вполне приводимого представления на неприводимые составляющие посредством вычисления следов. При этом должны быть заранее заданы характеры неприводимых представлений.

§ 108. Представления конечных групп

Мы докажем прежде всего следующую теорему:

Теорема Машке. *Любое представление конечной группы* $\mathfrak{G}$ *над полем* P, *характеристика которого не делит порядок* h *группы* $\mathfrak{G}$, *вполне приводимо.*

Доказательство. Пусть модуль представления $\mathfrak{M}$ приводим и $\mathfrak{N}$ — его минимальный подмодуль. Покажем, что $\mathfrak{M}$ является прямой суммой $\mathfrak{N}+\mathfrak{N}''$, где $\mathfrak{N}''$ — вновь некоторый модуль представления.

Как векторное пространство, модуль $\mathfrak{M}$ распадается в прямую сумму $\mathfrak{N}+\mathfrak{N}'$, но пространство $\mathfrak{N}'$ при этом может и не быть инвариантным относительно $\mathfrak{G}$. Если y — произвольный элемент из $\mathfrak{N}'$ и a — произвольный элемент из $\mathfrak{G}$, то ay однозначно представляется в виде суммы некоторого элемента из $\mathfrak{N}$ и некоторого элемента y' из $\mathfrak{N}'$, так что

$$ay \equiv y' \pmod{\mathfrak{N}}.$$

При фиксированном a элемент y' однозначно определяется элементом y и зависит от y линейно: из $ay \equiv y'$ и $az \equiv z'$ следует, что $a(y+z) \equiv y'+z'$ и $ay\beta \equiv y'\beta$ для любого $\beta \in \mathsf{P}$. Поэтому можно записать

$$y' = A'y, \quad A'y \equiv ay \pmod{\mathfrak{N}},$$

где A' — линейное преобразование подпространства $\mathfrak{N}'$, зависящее от a. Таким образом, преобразования A' составляют некоторое представление группы $\mathfrak{G}$, потому что из $a \longmapsto A'$ и $b \longmapsto B$ следует, что $ab \longmapsto A'B'$.

Положим

$$\frac{1}{h}\sum_a a^{-1}A'y = Qy = y'';$$

тогда y'' также линейно зависит от y и элементы y'' образуют некоторое линейное подпространство $\mathfrak{N}'' = Q\mathfrak{N}'$. Но тогда по модулю $\mathfrak{N}$ имеем

$$y'' \equiv \frac{1}{h}\sum_a a^{-1}ay = y.$$

Следовательно, каждый элемент модуля $\mathfrak{M}$ сравним по модулю $\mathfrak{N}$ не только с некоторым элементом y из $\mathfrak{N}'$, но и с некоторым однозначно определенным элементом y'' из $\mathfrak{N}''$. Это означает, что

имеет место разложение в прямую сумму

$$\mathfrak{M} = \mathfrak{N} + \mathfrak{N}''.$$

Наконец, для каждого элемента b из $\mathfrak{G}$ имеем

$$by'' = \frac{1}{h}\sum_a ba^{-1}A'y = \frac{1}{h}\sum_a (ab^{-1})^{-1}(A'B'^{-1})B'y = QB'y \in Q\mathfrak{M}' = \mathfrak{N}'',$$

т. е. подпространство $\mathfrak{N}''$ переводится в себя операторами b из $\mathfrak{G}$, а это и означает, что $\mathfrak{N}''$ — модуль представления.

Если модуль $\mathfrak{N}''$ приводим, то тем же способом можно выделить меньший модуль и т. д. В конце концов будет найдено полное разложение модуля $\mathfrak{M}$ в прямую сумму и, следовательно, требуемое представление. Теорема Машке доказана.

Согласно § 104 каждое представление группы $\mathfrak{G}$ можно продолжить до некоторого представления группового кольца

$$\mathfrak{o} = a_1\mathsf{P} + \ldots + a_h\mathsf{P};$$

наоборот, каждое представление группового кольца $\mathfrak{o}$ естественным образом задает представление группы $\mathfrak{G}$. Из теоремы Машке теперь следует, что каждое представление кольца $\mathfrak{o}$ вполне приводимо. В частности, это верно и для регулярного представления, допускающего в качестве своего модуля само $\mathfrak{o}$. Поэтому кольцо $\mathfrak{o}$ является прямой суммой минимальных левых идеалов и в соответствии с § 98 (теорема 13) *полупросто*. Согласно § 105 минимальные левые идеалы кольца $\mathfrak{o}$ задают все неприводимые представления.

Число абсолютно неприводимых представлений согласно § 106 равно рангу центра, а центр группового кольца, как легко проверить, состоит из всех тех сумм

$$\sum_\lambda a_\lambda\beta_\lambda \quad (a_\lambda \in \mathfrak{G},\ \beta_\lambda \in \mathsf{P}), \tag{1}$$

в которых сопряженные элементы имеют одинаковые коэффициенты. Элементы, сопряженные с данным элементом a, составляют некоторый «класс». Если k_a — сумма элементов этого класса, то (1) — сумма таких k_a с коэффициентами из P. Следовательно, имеет место теорема: *центр группового кольца порождается суммами классов k_a*. Ранг центра равен, таким образом, числу классов сопряженных элементов группы. Мы получили теорему:

Число неэквивалентных абсолютно неприводимых представлений группы равно числу классов сопряженных элементов в этой группе.

Согласно § 105 для степеней $n_1, \ldots, n_s$ неприводимых представлений выполняется соотношение:

$$n_1^2 + n_2^2 + \ldots + n_s^2 = h.$$

Среди рассматриваемых представлений первой степени всегда есть «тождественное представление», которое каждый групповой элемент переводит в элемент 1. Если же существуют еще и другие представления первой степени, то в данной группе должны существовать собственные нормальные подгруппы с абелевой факторгруппой, потому что матрицы любого представления первой степени перестановочны между собой и образуют абелеву группу, в которую гомоморфно отображается данная группа. Наоборот, если существует собственная нормальная подгруппа с абелевой факторгруппой, то характеры этой факторгруппы задают представления первой степени. Все остальные представления имеют бо́льшую степень.

Примеры. 1. *Симметрическая группа* $\mathfrak{S}_3$. Число классов равно 3, поэтому есть всего три неэквивалентных неприводимых представления. По знакопеременной подгруппе имеем два смежных класса $\mathfrak{K}_0$, $\mathfrak{K}_1$: четные и нечетные подстановки. Вот два характера факторгруппы $\mathfrak{S}_3/\mathfrak{A}_3$:

$$\chi(\mathfrak{K}_0)=1, \quad \chi(\mathfrak{K}_1)=\pm 1;$$

они определяют представления первой степени. Так как

$$n_1^2+n_2^2+n_3^2=6,$$

третье представление должно иметь степень 2. Возьмем в плоскости три вектора, e_1, e_2, e_3, сумма которых равна нулю; тогда перестановки этих трех векторов дадут точное представление рассматриваемой группы подстановок. Легко установить, что это представление неприводимо. Пусть e_1 и e_2 — базисные векторы; тогда представление выглядит так:

$$\left.\begin{aligned}(1\ 2)\,e_1&=e_2,\\(1\ 2)\,e_2&=e_1,\end{aligned}\right\}\qquad \left.\begin{aligned}(1\ 3)\,e_1&=-e_1-e_2,\\(1\ 3)\,e_2&=e_2,\end{aligned}\right\}\qquad \left.\begin{aligned}(2\ 3)\,e_1&=e_1,\\(2\ 3)\,e_2&=-e_1-e_2,\end{aligned}\right\}$$

$$\left.\begin{aligned}(1\ 2\ 3)\,e_1&=e_2,\\(1\ 2\ 3)\,e_2&=-e_1-e_2,\end{aligned}\right\}\qquad \left.\begin{aligned}(1\ 2\ 3)\,e_2&=-e_1-e_2,\\(1\ 2\ 3)\,e_2&=e_1.\end{aligned}\right\}$$

2. *Группа кватернионов* $\mathfrak{Q}_3$ — это группа восьми кватернионных единиц ± 1, $\pm j$, $\pm k$, $\pm l$. Она имеет две порождающие j и k, удовлетворяющие соотношениям:

$$j^4=1, \quad k^2=j^2, \quad kj=j^3k.$$

Число классов равно 5; поэтому имеется пять представлений. Нормальная подгруппа $\{1, j^2\}$ определяет в качестве факторгруппы четверную группу Клейна, обладающую четырьмя характерами, дающими четыре представления. В силу соотношения

$$n_1^2+n_2^2+n_3^2+n_4^2+n_5^2=8$$

остальные представления должны иметь степень 2. Если групповым элементам $1, j, j^2, j^3, k, jk, j^2k, j^3k$ сопоставить кватернионы $1, j, -1, -j, k, l, -k, -l$, то получится гомоморфное отображение группового кольца $\mathfrak{o}$ на тело кватернионов. Поэтому тело кватернионов должно быть среди двусторонних прямых слагаемых кольца $\mathfrak{o}$ и тем самым получается разложение кольца $\mathfrak{o}$ над полем рациональных чисел $\mathbb{Q}$,

$$\mathfrak{o} = \mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 + \mathfrak{a}_4 + \mathfrak{a}_5,$$

где $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4$ изоморфны полю $\mathbb{Q}$, а $\mathfrak{a}_5$ изоморфно телу кватернионов. Если перейти к алгебраически замкнутому основному полю (в данном случае достаточно присоединить $i = \sqrt{-1}$), то тело кватернионов распадается и получается матричное представление

$$j \longmapsto \begin{Vmatrix} i & 0 \\ 0 & -i \end{Vmatrix}, \quad k \longmapsto \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}, \quad l \longmapsto \begin{Vmatrix} 0 & i \\ i & 0 \end{Vmatrix}.$$

3. *Знакопеременная группа* $\mathfrak{A}_4$ может быть исследована тем же методом, что и симметрическая группа $\mathfrak{S}_3$, — мы предоставляем это читателю. В результате будут найдены четыре представления степеней 1, 1, 1, 3.

4. *Симметрическая группа* $\mathfrak{S}_4$. Число классов равно 5, поэтому должно быть пять представлений. Четверная группа Клейна $\{1, (12)(34), (13)(24), (14)(23)\}$ определяет факторгруппу, изоморфную группе $\mathfrak{S}_3$, для которой мы уже нашли три представления степеней 1, 1, 2. Они задают также представления самой группы $\mathfrak{S}_4$ степеней 1, 1, 2. Если эти степени обозначить через n_1, n_2, n_3, то

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 24,$$

так что

$$n_4^2 + n_5^2 = 18.$$

Такое равенство может иметь место лишь для $n_4 = 3$, $n_5 = 3$. Если мы введем четыре вектора e_1, e_2, e_3, e_4 с нулевой суммой, то подстановки этой четверки векторов дадут точное представление третьей степени группы $\mathfrak{S}_4$. Выберем e_1, e_2, e_3 в качестве базисных векторов; тогда упомянутое представление выглядит так:

$$\left.\begin{aligned} (1\ 2)\,e_1 &= e_2, \\ (1\ 2)\,e_2 &= e_1, \\ (1\ 2)\,e_3 &= e_3, \end{aligned}\right\} \quad \left.\begin{aligned} (1\ 3)\,e_1 &= e_3, \\ (1\ 3)\,e_2 &= e_2, \\ (1\ 3)\,e_3 &= e_1, \end{aligned}\right\} \quad \left.\begin{aligned} (1\ 4)\,e_1 &= -e_1 - e_2 - e_3, \\ (1\ 4)\,e_2 &= e_2, \\ (1\ 4)\,e_3 &= e_3, \end{aligned}\right\}$$

$$\left.\begin{aligned} (1\ 2\ 3)\,e_1 &= e_2, \\ (1\ 2\ 3)\,e_2 &= e_3, \\ (1\ 2\ 3)\,e_3 &= e_1, \end{aligned}\right\}$$

Поскольку представление точное, оно не может сводиться к представлениям первой и второй степени; следовательно, оно неприводимо. Если матрицы, представляющие нечетные подстановки, умножить на —1, то получится новое и тоже точное неприводимое представление третьей степени, заведомо не эквивалентное предыдущему, потому что их следы различны.

Задача 1. Элемент $s=\sum_{a\in\mathfrak{G}} a$ группового кольца $\mathfrak{o}$ удовлетворяет равенствам $bs=s$ для $b\in\mathfrak{G}$. Какой левый идеал порождает s? Какое представление соответствует этому идеалу? Какой идемпотентный элемент содержится в этом идеале?

Задача 2. Если число h элементов группы делится на характеристику поля, то названный в задаче 1 идеал нильпотентен. Это свидетельствует о том, что условие о невозможности деления h на характеристику поля является в теореме Машке необходимым.

§ 109. Групповые характеры

Кронекерово произведение преобразований

Пусть даны два линейных преобразования A', A'', переводящих некоторое векторное пространство $(u_1, \ldots, u_n)$ в другое векторное пространство $(v_1, \ldots, v_m)$:

$$A'u_k=\sum_i u_i\alpha'_{ik},$$

$$A''v_l=\sum_j v_j\alpha''_{jl}.$$

Построим в соответствии с § 94 произведение этих двух векторных пространств — оно будет порождаться произведениями u_kv_l — и положим

$$A(u_kv_l)=(A'u_k)(A''x_l)=\sum_i\sum_j u_iv_j\alpha'_{ik}\alpha''_{jl}. \tag{1}$$

Определенное таким образом линейное преобразование A на произведении векторных пространств называется *кронекеровым произведением преобразований* и обозначается через $A'\times A''$. Элементами матрицы, соответствующей преобразованию A, будут согласно (1) произведения $\alpha'_{ik}\alpha''_{jl}$. След матрицы A равен

$$\sum_i\sum_j \alpha'_{ii}\alpha''_{jj}=\sum_i \alpha'_{ii}\cdot\sum_j \alpha''_{jj}=S(A')\cdot S(A'').$$

Отсюда: *след произведения преобразований $A'\times A''$ является произведением следов преобразований A' и A''.*

Если на векторы u последовательно подействовать преобразованиями B' и A', а на векторы v — преобразованиями B'' и A'', то на произведения u_kv_l последовательно подействуют преобра-

зования $B' \times B''$ и $A' \times A''$, т. е.

$$(A' \times A'') \cdot (B' \times B'') = A'B' \times A''B''. \tag{2}$$

Если матрицы A', B', ... составляют некоторое представление $\mathfrak{D}'$ группы $\mathfrak{G}$, а матрицы A'', B'', ... — другое представление $\mathfrak{D}''$ той же самой группы, то из (2) следует, что произведения преобразований $A = A' \times A''$, $B = B' \times B''$, ... тоже составляют некоторое представление. Это *произведение представлений* $\mathfrak{D}'$ и $\mathfrak{D}''$ обозначается через $\mathfrak{D}' \times \mathfrak{D}''$.

Если символом $\mathfrak{D}' + \mathfrak{D}''$ обозначать приводимое представление, распадающееся на $\mathfrak{D}'$ и $\mathfrak{D}''$, и считать эквивалентные представления одинаковыми, то верны следующие равенства:

$$\mathfrak{D}' + \mathfrak{D}'' = \mathfrak{D}'' + \mathfrak{D}',$$
$$\mathfrak{D}' \times \mathfrak{D}'' = \mathfrak{D}'' \times \mathfrak{D}',$$
$$\mathfrak{D}' + (\mathfrak{D}'' + \mathfrak{D}''') = (\mathfrak{D}' + \mathfrak{D}'') + \mathfrak{D}''',$$
$$\mathfrak{D}' \times (\mathfrak{D}'' \times \mathfrak{D}''') = (\mathfrak{D}' \times \mathfrak{D}'') \times \mathfrak{D}''',$$
$$\mathfrak{D}' \times (\mathfrak{D}'' + \mathfrak{D}''') = \mathfrak{D}' \times \mathfrak{D}'' + \mathfrak{D}' \times \mathfrak{D}''',$$
$$(\mathfrak{D}'' + \mathfrak{D}''') \times \mathfrak{D}' = \mathfrak{D}'' \times \mathfrak{D}' + \mathfrak{D}''' \times \mathfrak{D}'.$$

В частности, если $\mathfrak{G}$ — конечная группа, порядок которой не делится на характеристику поля P, то любое представление полностью распадается на неприводимые представления $\mathfrak{D}_\nu$ и оказывается выполненным равенство

$$\mathfrak{D}_\nu \times \mathfrak{D}_\mu = \sum_\nu c_{\lambda\mu}^\nu \mathfrak{D}_\nu, \tag{3}$$

где $c_{\lambda\mu}^\nu$ — целые неотрицательные числа. В формуле (3) символ ν — не показатель степени, а индекс.

Из (3) для следов следует равенство

$$S_\lambda(a) \cdot S_\mu(a) = \sum_\nu c_{\lambda\mu}^\nu S_\nu(a).$$

Если представления абсолютно неприводимы и, следовательно, следы являются характерами, то отсюда можно заключить, что

$$\chi_\lambda(a) \cdot \chi_\mu(a) = \sum_\nu c_{\lambda\mu}^\nu \chi_\nu(a) \tag{4}$$

(*первое соотношение между характерами*).

Характеры как функции классов

Если a и a' — сопряженные элементы группы, т. е.

$$a' = bab^{-1},$$

то для представляющих матриц имеет место равенство

$$A' = BAB^{-1}.$$

Тем самым A и A' имеют одинаковые следы:

$$S(bab^{-1}) = S(a);$$

в частности,

$$\chi(bab^{-1}) = \chi(a).$$

Если мы соберем все те элементы группы, которые сопряжены с фиксированным элементом a, в один класс $\mathfrak{K}_a$, то каждый характер будет иметь одно и то же значение на всех элементах этого класса.

Пусть h_a — число элементов класса $\mathfrak{K}_a$, а k_a — сумма элементов этого класса (в групповом кольце $\mathfrak{o}$); тогда характер, соответствующий k_a, является суммой характеров, соответствующих элементам рассматриваемого класса; таким образом,

$$\chi(k_a) = h_a \cdot \chi(a).$$

Отныне мы будем предполагать, что ни порядок группы h, ни степень n_ν абсолютно неприводимых представлений $\mathfrak{D}_\nu$ не делятся на характеристику основного поля. Как было показано в § 108, элементы k_a порождают центр $\mathfrak{Z}$ группового кольца $\mathfrak{o}$. Согласно § 107 гомоморфизмы Θ_ν центра $\mathfrak{Z}$ связаны с характерами χ_ν следующими соотношениями:

$$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu};$$

в частности,

$$\Theta_\nu(k_a) = \frac{\chi_\nu(k_a)}{n_\nu} = \frac{h_a}{n_\nu}\chi_\nu(a). \tag{5}$$

Произведение $k_a k_b$ является суммой групповых элементов, вновь принадлежащей центру $\mathfrak{Z}$ и поэтому вновь выражающейся через суммы классов k_a:

$$k_a \cdot k_b = \sum_c g_{ab}^c k_c. \tag{6}$$

Гомоморфность отображения Θ_ν выражается в таком случае равенством

$$\Theta_\nu(k_a) \cdot \Theta_\nu(k_b) = \sum_c g_{ab}^c \Theta_\nu(k_c), \tag{7}$$

которое с помощью (5) переписывается в виде

$$h_a h_b \chi_\nu(a)\chi_\nu(b) = n_\nu \sum_c g_{ab}^c h_c \chi_\nu(c) \tag{8}$$

(*второе соотношение между характерами*).

В суммах (6), (7) и (8) индекс c пробегает произвольно фиксированную систему представителей всех классов. Если же c пробегает все элементы группы, то в (8) следует справа вычерк-

нуть множитель h_c. Так как Θ_ν — единственно возможные гомоморфизмы центра $\mathfrak{Z}$, характеры χ_ν являются единственно возможными решениями уравнения (8).

Сопряженные характеры

Для каждого представления $a \longmapsto A$ существует *«сопряженное* (или *контраградиентное*) *представление»* $a \longmapsto A'^{-1}$, где A' — матрица, транспонированная по отношению к A. Действительно, при таком сопоставлении имеем:

$$ab \longmapsto (AB)'^{-1} = (B'A')^{-1} = A'^{-1}B'^{-1}.$$

Представление, сопряженное к сопряженному представлению, совпадает с исходным. Если представление $a \longmapsto A$ приводимо, то таково же и сопряженное, и наоборот. Таким образом, представление, сопряженное к неприводимому, тоже неприводимо.

Если от данного представления A перейти к эквивалентному представлению $P^{-1}AP$, то сопряженное представление перейдет в

$$(P^{-1}AP)'^{-1} = P'A'^{-1}P'^{-1},$$

т. е. тоже в эквивалентное.

Обозначим через $\mathfrak{D}_{\nu'}$ представление, сопряженное к $\mathfrak{D}_\nu$; тогда, если $\mathfrak{D}_\nu(a) = A$, то

$$\mathfrak{D}_{\nu'}(a^{-1}) = A',$$

и, так как след матрицы A' равен следу матрицы A, справедливо равенство

$$\chi_{\nu'}(a^{-1}) = \chi_\nu(a).$$

Характер $\chi_{\nu'}$, *сопряженный к* χ_ν, обозначается также и через $\bar{\chi}_\nu$.

Каждый характер является суммой корней из единицы. Это объясняется тем, что каждый элемент a группы $\mathfrak{G}$ порождает некоторую циклическую подгруппу $\mathfrak{C}$, порядок m которой является делителем h, а любое неприводимое представление $\mathfrak{D}_\nu$ группы $\mathfrak{G}$ задает некоторое представление группы $\mathfrak{C}$; последнее полностью распадается на представления первой степени, матричные элементы которых являются корнями m-й степени из единицы. След представляющей матрицы равен сумме диагональных элементов, т. е. сумме корней m-й степени из единицы:

$$\chi(a) = \zeta^{\nu_1} + \zeta^{\nu_2} + \ldots + \zeta^{\nu_n}, \tag{9}$$

где ζ — примитивный корень m-й степени из единицы.

Дальнейшие соотношения между характерами

Если $S(c)$ — след группового элемента c в регулярном представлении, то

$$S(c) = \sum_\nu n_\nu \chi_\nu(c),$$

так как регулярное представление содержит неприводимое представление $\mathfrak{D}_\nu$ точно n_ν раз. След $S(c)$, однако, вычисляется непосредственно: групповые элементы $a_1, \ldots, a_h$ составляют базис векторного пространства $\mathfrak{v}$, на котором действует регулярное представление и

$$ca_i = a_k.$$

Элементы с $i = k$ входят сюда лишь тогда, когда c равно единичному элементу группы 1; в этом случае каждое i равно соответствующему k. Таким образом

$$S(1) = h, \quad S(c) = 0 \text{ для } c \neq 1$$

и, следовательно,

$$\sum_\nu n_\nu \chi_\nu(c) = \begin{cases} h \text{ для } c = 1, \\ 0 \text{ для } c \neq 1. \end{cases} \tag{10}$$

Если теперь просуммировать (8) по всем ν и сравнить с (10), то получится

$$h_a h_b \sum_\nu \chi_\nu(a)\, \chi_\nu(b) = g^1_{ab} \cdot h. \tag{11}$$

Число g^1_{ab} показывает, как часто произведение $a'b'$, где a' принадлежит классу $\mathfrak{K}_a$, а b' — классу $\mathfrak{K}_b$, обращается в 1. Следовательно, это число равно нулю, если $\mathfrak{K}_a$ и $\mathfrak{K}_b$ не имеют взаимно обратных элементов. Но если такая пара элементов существует, — допустим, $b = a^{-1}$, — то для каждого элемента $a' = cac^{-1}$ из $\mathfrak{K}_a$ есть обратный элемент $b' = a'^{-1} = cbc^{-1}$ из $\mathfrak{K}_a$ и мы получаем

$$g^1_{ab} = h_a = h_b.$$

Тем самым, деля соотношение (11) на h_b, мы приходим к *третьему соотношению между характерами*:

$$h_a \sum_\nu \chi_\nu(a)\, \chi_\nu(b) = \begin{cases} h \text{ для } \mathfrak{K}_b = \mathfrak{K}_{a^{-1}}, \\ 0 \text{ для } \mathfrak{K}_b \neq \mathfrak{K}_{a^{-1}}. \end{cases} \tag{12}$$

В частном случае $a = 1$ отсюда вновь получается (10).

Пусть теперь $a_1, \ldots, a_s$ — система представителей всех классов сопряженных элементов. Положим

$$\chi_{\nu\mu} = \chi_\nu(a_\mu),$$
$$\eta_{\mu\nu} = \frac{h_\mu}{h} \bar{\chi}_\nu(a_\mu) = \frac{h_\mu}{h} \chi_\nu(a_\mu^{-1}).$$

Соотношение (12) говорит тогда о том, что матрицы $X = \|\chi_{\mu\nu}\|$ и $Y = \|\eta_{\mu\nu}\|$ взаимно обратны:

$$YX = E \text{ или } Y = X^{-1}. \tag{13}$$

Из (13) следует, что

$$XY = E$$

или, более подробно,

$$\frac{1}{h}\sum_{\mathfrak{K}_a} h_a \chi_\nu(a)\,\bar{\chi}_\mu(a) = \begin{cases} 1 & \text{для } \nu = \mu, \\ 0 & \text{для } \nu \neq \mu. \end{cases} \tag{14}$$

Здесь a пробегает всю систему представителей, указанную выше. Если же a пробегает все элементы группы, то нужно убрать множители h_a. Отсюда получается *ортогональность характеров*:

$$\sum_{a \in \mathfrak{G}} \bar{\chi}_\mu(a)\,\chi_\nu(a) = \begin{cases} h & \text{для } \nu = \mu, \\ 0 & \text{для } \nu \neq \mu \end{cases} \tag{15}$$

(*четвертое соотношение между характерами*).

В частности, если $\mu = 0$, т. е. когда χ_μ есть характер χ_0 единичного представления, то из (15) следует

$$\sum_a \chi_\nu(a) = \begin{cases} h & \text{для } \nu = 0, \\ 0 & \text{для } \nu \neq 0. \end{cases} \tag{16}$$

Тот факт, что матрицы X и Y взаимно обратны, можно использовать для вычисления идемпотентных элементов центра $e_1, \ldots, e_s$, порождающих в $\mathfrak{o}$ двусторонние идеалы. Действительно, согласно § 108 для базисных элементов k_a центра $\mathfrak{Z}$ имеют место равенства

$$k_a = \sum_\nu e_\nu \Theta_\nu(k_a) = \sum_\nu e_\nu \frac{h_a}{n_\nu}\chi_\nu(a). \tag{17}$$

Если умножить это на $\bar{\chi}_\mu(a)$ и просуммировать по всем классам $\mathfrak{K}_a$, то получится

$$\sum_{\mathfrak{K}_a} k_a \bar{\chi}_\mu(a) = e_\mu \cdot \frac{h}{n_\mu},$$

или

$$e_\nu = \sum_{\mathfrak{K}_a} k_a \frac{n_\nu}{h}\chi_\nu(a^{-1}).$$

Литература. Не зависящее от теории алгебр обоснование теории представлений конечных групп дано в работе: Шур (Schur I.). Neue Begründung der Theorie der Gruppencharaktere. — Sitzungsber. Berlin, 1905, S. 406—432. Обобщение этой теории на бесконечные группы принадлежит фон Нейману (von Neumann J.). Almost periodic functions in groups. — Trans. Amer. Math. Soc., 1934, 36, p. 445—492. Дальнейшие сведения о литературе можно найти у автора: van der Waerden B. L. Gruppen von linearen Transformationen. — Ergeb. Math., IV/2, Berlin, 1935.

§ 110. Представления симметрических групп [1])

Мы рассматриваем группу $\mathfrak{S}_n$ подстановок n символов 1, 2, .., n; найдем ее абсолютно неприводимые представления, например, над полем Ω всех алгебраических чисел Впрочем, будет показано, что эти представления рациональны, т е осуществляются над полем $\mathbb{Q}$ рациональных чисел.

Будем исходить из группового кольца $\mathfrak{o}=s_1\Omega+ \quad +s_n\Omega$ и рассмотрим его левые идеалы Каждый такой левый идеал является прямой суммой минимальных левых идеалов, последние дают лишь неприводимые представления Так как каждый левый идеал порождается некоторым идемпотентным элементом, мы найдем сначала эти идемпотентные элементы

Запишем цифры 1, 2, ., n в произвольном порядке в h расположенных друг за другом строк (h произвольно) так, чтобы в ν-й строке α_ν цифр удовлетворяло условиям

$$\left.\begin{aligned} &\alpha_1 \geqslant \alpha_2 \geqslant \ldots \geqslant \alpha_h, \\ &\sum_{\nu=1}^{h} \alpha_\nu = n. \end{aligned}\right\} \tag{1}$$

Мы пишем первые элементы всех h строк друг под другом, точно так же и вторые элементы и т д , следующий ниже пример, в котором точки означают цифры, поясняет сказанное

$$\begin{matrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \\ \cdot & \cdot & \end{matrix} \qquad (\alpha_1, \alpha_2, \alpha_3) = (3, 2, 2); \quad n=7.$$

Любое такое расположение цифр 1, 2, .., n мы будем называть *схемой* и обозначать через Σ_α Индекс α обозначает последовательность цифр (α_1, α_2, , α_h) Индексы α, которые могут появиться при этом, упорядочиваются следующим образом. $\alpha > \beta$, если первая ненулевая разность $\alpha_\nu - \beta_\nu$ положительна Например, при $n=5$

$$(5) > (4, 1) > (3, 2) > (3, 1, 1) > (2, 2, 1) > (2, 1, 1 \quad 1) > (1, 1, 1, 1, 1).$$

Пусть дана такая схема Σ_α; обозначим через p все подстановки, которые меняют цифры лишь внутри строк схемы Σ_α, а сами строки оставляют инвариантными; через q обозначим все те подстановки, которые меняют цифры лишь внутри столбцов схемы Σ_α Для каждой фиксированной подстановки q символ σ_q обозначает $+1$ или -1 в зависимости от того, четна q или нет Если s — произвольная подстановка, то через $s\Sigma_\alpha$ мы обозначаем схему, в которую переходит Σ_α при действии подстановки s. Легко заметить, что если подстановка q оставляет инвариантными столбцы схемы Σ_α, то подстановка sqs^{-1} оставляет инвариантными столбцы схемы $s\Sigma_\alpha$, и наоборот Наконец, положим (в групповом кольце $\mathfrak{o}$) для каждой фиксированной схемы Σ_α

$$S_\alpha = \sum_p p,$$

$$A_\alpha = \sum_q q\sigma_q.$$

Легко проверяются правила·

$$pS_\alpha = S_\alpha p = S_\alpha, \tag{2}$$

$$A_\alpha q\sigma_q = qA_\alpha\sigma_q = A_\alpha. \tag{3}$$

---

[1]) Упрощенными доказательствами предложений теории Фробениуса (см. Sitzungsber. Preuss Akad. Berlin, 1903, S. 328—358), помещенными в этом параграфе, я обязан устному сообщению фон Неймана.

Из (2) и (3) легко следует, что S_α и A_α идемпотентны с точностью до некоторого множителя f_α. Дальнейшие алгебраические свойства элементов S_α и A_α вытекают из следующей *комбинаторной леммы*:

Пусть Σ_α и Σ_β — две схемы указанного выше типа; пусть $\alpha \geqslant \beta$. Если в Σ_α ни в одной строке нет двух цифр, входящих в один столбец схемы Σ_β, то $\alpha = \beta$ и схема Σ_α переходит в схему Σ_β с помощью подстановки вида pq:

$$pq\Sigma_\alpha = \Sigma_\beta.$$

(Обозначения p и q относятся к Σ_α, т. е. p оставляет инвариантными строки, а q — столбцы схемы Σ_α.)

Доказательство. Из $\alpha \geqslant \beta$ следует, что $\alpha_1 \geqslant \beta_1$. В первой строке схемы Σ_α стоит α_1 цифр. Так как те же самые цифры должны в Σ_β стоять в различных столбцах, схема Σ_β содержит не менее α_1 строк, откуда $\alpha_1 \leqslant \beta_1$ и, следовательно, $\alpha_1 = \beta_1$. С помощью некоторой подстановки q'_1, оставляющей инвариантными столбцы в Σ_β, указанные цифры переходят в первую строку схемы Σ_β.

Из $\alpha \geqslant \beta$ следует далее, что $\alpha_2 \geqslant \beta_2$. Во второй строке схемы Σ_α стоит α_2 цифр. Так как они должны входить в разные столбцы схемы $q'_1\Sigma_\beta$, в последней вне первой строки, которую мы уже построили, должно быть не менее α_2 столбцов. Отсюда следует, что $\alpha_2 \leqslant \beta_2$, и поэтому $\alpha_2 = \beta_2$. С помощью некоторой подстановки q'_2, оставляющей инвариантными столбцы схемы $q'_1\Sigma_\beta$, а также ее первую строку, названные цифры переводятся во вторую строку схемы Σ_β.

Продолжая таким образом, мы в конце концов получим схему $q'\Sigma_\beta = q'_h \ldots q'_2 q'_1 \Sigma_\beta$, строки которой совпадают со строками схемы Σ_α. Тем самым с помощью некоторой подстановки p схему Σ_α можно перевести в схему $q'\Sigma_\beta$:

$$q'\Sigma_\beta = p\Sigma_\alpha.$$

Подстановка $q' = q'_h \ldots q'_2 q'_1$ оставляет инвариантными столбцы схемы Σ_β, а потому и схемы $q'\Sigma_\beta = p\Sigma_\alpha$. При подходящей подстановке q выполняется, следовательно, равенство

$$q' = pq^{-1}p^{-1},$$

и поэтому

$$pq^{-1}p^{-1}\Sigma_\beta = p\Sigma_\alpha,$$

$$\Sigma_\beta = pq\Sigma_\alpha,$$

что и требовалось доказать.

Из этой комбинаторной леммы всегда следует, что

$$A_\beta S_\alpha = 0 \quad \text{для} \quad \alpha > \beta. \tag{4}$$

Действительно, согласно лемме, в случае $\alpha > \beta$ существует пара цифр, принадлежащая одной строке схемы Σ_α и одному столбцу схемы Σ_β. Если t — транспозиция, меняющая местами эти цифры, то из (2) и (3) следует, что

$$A_\beta S_\alpha = A_\beta t t^{-1} S_\alpha = -A_\beta S_\alpha,$$

откуда и получается (4).

Точно так же доказывается, что

$$S_\alpha A_\beta = 0 \quad \text{для} \quad \alpha > \beta.$$

Кроме того, все выражения, получающиеся из A_β сопряжением, аннулируются суммой S_α:

$$S_\alpha s A_\beta s^{-1} = 0 \quad \text{для} \quad \alpha > \beta,$$

потому что $sA_\beta s^{-1}$ — это снова некоторое A_β, но для преобразованной схемы $s\Sigma_\beta$. Из этого результата с помощью умножения на $s\Omega$ и суммирования по всем s

из $\mathfrak{G}$ следует, что

$$S_\alpha \left(\sum s\Omega\right) A_\beta = (0),$$

или

$$S_\alpha \mathfrak{o} A_\beta = (0) \qquad (\alpha > \beta). \tag{5}$$

Таким образом, левые идеалы $\mathfrak{o}A_\beta$ с $\beta < \alpha$ аннулируются элементом S_α. Иначе говоря, элемент S_α представляется нулем в том представлении, которое определяется идеалом $\mathfrak{o}A_\beta$. Вместе с тем $S_\alpha A_\alpha \neq 0$, потому что коэффициент при единичном элементе в произведении $S_\alpha A_\alpha$ не равен нулю. Следовательно, элемент S_α в представлении, связанном с идеалом $\mathfrak{o}A_\alpha$, представляется отличным от нуля преобразованием. По этой причине упомянутое представление содержит по крайней мере одну неприводимую составляющую, не входящую ни в один из модулей $\mathfrak{o}A_\beta$ при $\beta < \alpha$. Рассмотрим ее подробнее.

Элемент $S_\alpha A_\alpha = \sum_p \sum_q pq\sigma_q$, согласно (2) и (3), удовлетворяет равенству

$$pS_\alpha A_\alpha q\sigma_q = S_\alpha A_\alpha.$$

Докажем теперь, что $S_\alpha A_\alpha$ является единственным с точностью до множителя элементом с таким свойством. Точнее, мы докажем следующее: *если элемент a кольца $\mathfrak{o}$ удовлетворяет равенству*

$$paq\sigma_q = a \tag{6}$$

для всех p и q, то он имеет вид $(S_\alpha A_\alpha)\gamma$.

Доказательство. Положим

$$a = \sum_s s\gamma_s \qquad (\gamma_s \in \Omega). \tag{7}$$

Подставляя (7) в (6), получим

$$\sum_s s\gamma_s = \sum_s psq\sigma_q\gamma_s. \tag{8}$$

В левую часть последнего равенства входит лишь одно слагаемое с pq, именно $pq\gamma$; аналогично в правую часть входит также одно слагаемое при $s=1$. Сравнение коэффициентов дает

$$\gamma_{pq} = \sigma_q\gamma_1.$$

Выберем теперь любую подстановку s, отличную от подстановок, имеющих вид pq. Тогда схема $s\Sigma_\alpha$ отлична от всех схем $pq\Sigma_\alpha$ и, согласно комбинаторной лемме, существуют две цифры j, k, которые в Σ_α находятся в одной строке, а в $s\Sigma_\alpha$ — в одном столбце. Если t — транспозиция этих цифр: $t=(jk)$, то подстановка $t' = s^{-1}ts$ меняет местами лишь цифры $s^{-1}j$ и $s^{-1}k$, которые стоят в одном столбце таблицы $s^{-1}s\Sigma_\alpha = \Sigma_\alpha$. Следовательно, t — это подстановка вида p, а t' — подстановка вида q, и мы можем в (8) положить $p=t$, $q=t'$; тогда для выбранной выше подстановки s имеем

$$psq = tss^{-1}ts = s,$$
$$\sigma_q = -1,$$

и сравнение слагаемых с s слева и справа в (8) дает нам

$$\gamma_s = -\gamma_s, \qquad \gamma_s = 0.$$

Следовательно, в (7) входят лишь слагаемые с $s = pq$, $\gamma_s = \sigma_q\gamma_1$ и имеет место равенство

$$a = \sum_{p,\,q} pq\sigma_q\gamma_1 = (S_\alpha A_\alpha)\gamma_1,$$

что и требовалось доказать

Из доказанного немедленно следует, что для каждого элемента b кольца $\mathfrak{o}$ элемент $S_\alpha b A_\alpha$ имеет вид $(S_\alpha A_\alpha)\gamma$, потому что для любых p и q справедливо

равенство

$$pS_\alpha bA_\alpha q\sigma_q = S_\alpha bA_\alpha.$$

Следовательно,

$$S_\alpha \mathfrak{v} A_\alpha \subseteq (S_\alpha A_\alpha)\,\Omega.$$

Положим $S_\alpha A_\alpha = I_\alpha$; тогда

$$I_\alpha \mathfrak{v} I_\alpha \subseteq S_\alpha \mathfrak{v} A_\alpha \subseteq I_\alpha \Omega. \tag{9}$$

Мы утверждаем теперь, что $\mathfrak{v} I_\alpha$ — минимальный левый идеал. Действительно, если $\mathfrak{l}$ — подидеал в $\mathfrak{v} I_\alpha$, то из (9) следует, что

$$I_\alpha \mathfrak{l} \subseteq I_\alpha \Omega,$$

следовательно, так как $I_\alpha \Omega$ — одночленный, а потому минимальный Ω-модуль, имеет место одно из равенств

$$I_\alpha \mathfrak{l} = I_\alpha \Omega \quad \text{или} \quad I_\alpha \mathfrak{l} = (0).$$

В первом случае $\mathfrak{v} I_\alpha = \mathfrak{v} I_\alpha \Omega \subseteq \mathfrak{v} I_\alpha \mathfrak{l} \subseteq \mathfrak{l}$, в силу чего $\mathfrak{l} = \mathfrak{v} I_\alpha$. Во втором же случае $\mathfrak{l}^2 = \mathfrak{v} I_\alpha \mathfrak{l} = (0)$ и, так как нет нильпотентных идеалов, отличных от (0), получается равенство $\mathfrak{l} = (0)$.

Минимальные левые идеалы $\mathfrak{v} I_\alpha$ и $\mathfrak{v} I_\beta$ при $\alpha > \beta$ не являются операторно изоморфными. Действительно, в силу (5) при $\alpha > \beta$ выполняются соотношения

$$S_\alpha \mathfrak{v} I_\beta = S_\alpha \mathfrak{v} S_\beta A_\beta \subseteq S_\alpha \mathfrak{v} A_\beta = (0),$$

следовательно, для любого a' из $\mathfrak{v} I_\beta$ имеем

$$S_\alpha a' = 0.$$

Если бы было $\mathfrak{v} I_\alpha \cong \mathfrak{v} I_\beta$, то для каждого a из $\mathfrak{v} I_\alpha$ было бы

$$S_\alpha a = 0;$$

однако для $a = I_\alpha = S_\alpha A_\alpha$ это не так, потому что $S_\alpha^2 A_\alpha = f_\alpha S_\alpha A_\alpha \neq 0$.

Каждому левому идеалу $\mathfrak{v} I_\alpha$ соответствует некоторое неприводимое представление $\mathfrak{D}_\alpha$, а согласно сделанным выше замечаниям, эти представления при различных α неэквивалентны.

Число так отыскиваемых представлений $\mathfrak{D}_\alpha$ равно числу решений задачи (1). Одновременно это число равно и числу классов сопряженных подстановок, потому что каждый такой класс состоит из всех элементов, распадающихся на циклы длины $\alpha_1, \alpha_2, \ldots, \alpha_h$, а все эти длины можно упорядочить в соответствии с условием (1). Так как число всех неэквивалентных неприводимых представлений задается числом классов сопряженных подстановок, то этим показано, что *представлениями $\mathfrak{D}_\alpha$ исчерпываются все неприводимые представления симметрических групп $\mathfrak{S}_n$*.

Введенные выше левые идеалы $\mathfrak{v} I_\alpha$ определены над рациональными числами. Отсюда следует *рациональность неприводимых представлений* (как и характеров).

§ 111. Полугруппы линейных преобразований

Пусть дано основное поле P; мы рассмотрим множество линейных преобразований, матричные элементы которых принадлежат полю P или его расширению Λ. Такое множество называется *полугруппой*, если вместе с любыми двумя своими преобразованиями оно содержит и их произведение. *Линейная оболочка* произвольной системы преобразований над P состоит из всех линейных

комбинаций преобразований этой системы с коэффициентами из P. В последующем мы будем рассматривать лишь такие системы, которые содержат только конечное число линейно независимых преобразований над P и, следовательно, линейная оболочка которых имеет конечный ранг над P. Линейная оболочка полугруппы при этих условиях является некоторой алгеброй $\mathfrak{A}$ конечного ранга над P. Любой элемент такой алгебры — некоторое линейное преобразование. Следовательно, мы имеем над P некоторую алгебру в совершенно определенном точном представлении $\mathfrak{D}$.

Основной вопрос, интересующий нас в данном случае, таков: *как распадается неприводимое представление $\mathfrak{D}$ над расширением Λ?*

Всякий раз мы будем предполагать, что представление $\mathfrak{D}$ не содержит в качестве составляющего нулевое представление.

Для данной теории основными являются следующие две теоремы:

1. *Если представление $\mathfrak{D}$ вполне приводимо, то алгебра $\mathfrak{A}$ полупроста.*

2. *Если представление $\mathfrak{D}$ неприводимо или распадается на эквивалентные неприводимые составляющие, то алгебра $\mathfrak{A}$ проста.*

Доказательство теоремы 1. Если $\mathfrak{R}$ — радикал алгебры $\mathfrak{A}$, то его элементы в любом неприводимом представлении переходят в нуль. Так как $\mathfrak{D}$ — точное представление, радикал $\mathfrak{R}$ равен нулю.

Доказательство теоремы 2. Алгебра $\mathfrak{A}$ обязательно полупроста, а потому является прямой суммой простых алгебр: $\mathfrak{A}=\mathfrak{a}_1+\ldots+\mathfrak{a}_s$. Согласно § 105 в любом неприводимом представлении все алгебры $\mathfrak{a}_\mu$, кроме какой-то одной подалгебры $\mathfrak{a}_\nu$, представляются нулем. Это утверждение остается справедливым и тогда, когда представление складывается с самим собой несколько раз. Если же представление точное, то может существовать лишь одна подалгебра $\mathfrak{a}_1$, т. е. алгебра $\mathfrak{A}$ проста.

Из теоремы 1 немедленно следует одна теорема Бернсайда и ее обобщение, принадлежащее Фробениусу и Шуру:

Теорема Бернсайда. *В любой абсолютно неприводимой полугруппе матриц n-го порядка имеется ровно n^2 линейно независимых матриц.*

Обобщение. *Если полугруппа матриц над полем Λ распадается на абсолютно неприводимые части, среди которых есть ровно s неэквивалентных порядков $n_1, \ldots, n_s$ соответственно, то полугруппа содержит ровно*

$$n_1^2+n_2^2+\ldots+n_s^2$$

линейно независимых матриц над Λ.

Доказательство обобщения. Линейная оболочка данной полугруппы, построенная над Λ, является суммой s полных

матричных колец порядков $n_1, n_2, \ldots, n_s$ над Λ и поэтому имеет ранг $n_1^2+n_2^2+\ldots+n_s^2$.

Над полями характеристики нуль справедлива, кроме того,

Теорема о следе. *Если две полугруппы могут быть переведены друг в друга взаимно однозначно и с сохранением произведения (или, более общо, если обе они являются образами представлений одной и той же абстрактной полугруппы) и если при этом следы соответствующих матриц равны, то полугруппы (соответственно представления) эквивалентны.*

Доказательство. Если соответствующие друг другу матрицы A и B объединить в новую матрицу по схеме

$$\begin{Vmatrix} A & 0 \\ 0 & B \end{Vmatrix}, \tag{1}$$

то получится некоторая новая вполне приводимая полугруппа $\mathfrak{g}$, линейная оболочка которой является некоторой алгеброй $\mathfrak{A}$. Элементы из $\mathfrak{A}$ являются линейными комбинациями матриц (1) и поэтому точно так же распадаются на две составляющие, каждая из которых задает представление алгебры $\mathfrak{A}$. Следы этих двух представлений являются вполне определенными линейными комбинациями следов исходных матриц A и B и поэтому совпадают. Следовательно (§ 107), оба представления алгебры $\mathfrak{A}$ эквивалентны. Отсюда получается требуемое.

Если $\Lambda=\mathsf{P}$, то теоремы 1 и 2 согласно § 105 непосредственно обратимы. Но если Λ — собственное расширение поля P, то можно высказать нечто более глубокое:

1а. *Если $\mathfrak{A}$ — полупростая алгебра и Λ — сепарабельное расширение поля P, то каждое представление $\mathfrak{D}$ алгебры $\mathfrak{A}$ над Λ вполне приводимо.*

2а. *Если алгебра $\mathfrak{A}$ проста и центральна над P, то каждое представление алгебры $\mathfrak{A}$ над Λ распадается на эквивалентные неприводимые части.*

Доказательство. Согласно § 104 каждое представление алгебры $\mathfrak{A}$ над Λ связано с некоторым представлением алгебры $\mathfrak{A}\times\Lambda$. Если алгебра $\mathfrak{A}$ полупроста, а Λ сепарабельно над P, то согласно § 103 алгебра $\mathfrak{A}\times\Lambda$ тоже полупроста и поэтому любое представление алгебры $\mathfrak{A}\times\Lambda$ над Λ вполне приводимо. Если $\mathfrak{A}$ центральна и проста над P, то алгебра $\mathfrak{A}\times\Lambda$ обязательно проста и, снова согласно § 103, каждое представление алгебры $\mathfrak{A}\times\Lambda$ над Λ распадается на эквивалентные неприводимые составляющие. Тем самым доказаны оба утверждения.

Мы называем полугруппу *центральной* над P, если ее линейная оболочка центральна, т. е. центр ее линейной оболочки совпадает с P.

Если принять во внимание утверждения 1 и 2, то 1а и 2а можно сформулировать и так:

1б. *Вполне приводимая полугруппа линейных преобразований над полем* P *остается вполне приводимой при любом сепарабельном расширении основного поля* P.

2б. *Центральная неприводимая полугруппа линейных преобразований над* P *остается неприводимой или распадается на эквивалентные неприводимые составляющие при произвольном расширении основного поля.*

Точно так же, как 1б, можно доказать и

1в. *Вполне приводимая полугруппа остается вполне приводимой при любом расширении основного поля, если центр соответствующей линейной оболочки является прямой суммой сепарабельных расширений поля* P.

§ 112. Двойные модули и произведения алгебр

Уже в § 104 мы отмечали, что любое представление алгебры $\mathfrak{S}$ над полем K, содержащим основное поле P, определяет некоторое представление расширенной алгебры $\mathfrak{S}_{\mathsf{K}}$. На языке модулей представлений это означает, что любой модуль, для которого $\mathfrak{S}$ — область левых, а K — область правых мультипликаторов, является также и левым $\mathfrak{S}_{\mathsf{K}}$-модулем. Доказать это можно так: если $\mathfrak{S} = a_1\mathsf{P} + \ldots + a_n\mathsf{P}$ и, следовательно, $\mathfrak{S}_{\mathsf{K}} = a_1\mathsf{K} + \ldots + a_n\mathsf{K}$, то умножение слева элементов u рассматриваемого модуля на элемент из $\mathfrak{S}_{\mathsf{K}}$ задается равенством

$$(a_1\varkappa_1 + \ldots + a_n\varkappa_n)\, u = a_1 u\varkappa_1 + \ldots + a_n u\varkappa_n;$$

проверка соответствующих аксиом $\mathfrak{S}_{\mathsf{K}}$-модуля не составляет труда; лишь в доказательстве ассоциативности

$$(bc)\, u = b\,(cu)$$

нужна коммутативность: если, скажем, $b = a_1\varkappa_1$, $c = a_2\varkappa_2$ (достаточно, очевидно, рассмотреть лишь этот частный случай), то ассоциативность следует из равенств

$$(a_1\varkappa_1 \cdot a_2\varkappa_2)\, u = (a_1a_2\varkappa_1\varkappa_2)\, u = (a_1a_2)\, u\,(\varkappa_1\varkappa_2),$$
$$a_1\varkappa_1\,(a_2\varkappa_2 \cdot u) = a_1\varkappa_1\,(a_2 u\varkappa_2) = a_1\,(a_2 u\varkappa_2)\,\varkappa_1 = (a_1a_2)\, u\,(\varkappa_2\varkappa_1).$$

Оба выражения равны, так как $\varkappa_1\varkappa_2 = \varkappa_2\varkappa_1$.

Однако, и в том случае, когда K — тело или даже произвольное кольцо, выход из положения дает конструкция *инверсного кольца* K', т. е. кольца, инверсно изоморфного кольцу K. Если K — алгебра над P, то и K' — алгебра над P. Если K — тело, то и K' является телом.

Имеет место следующее утверждение:

Любой модуль, допускающий $\mathfrak{S}$ *в качестве области левых, а* K — *в качестве области правых мультипликаторов, может рассматриваться и как левый* $(\mathfrak{S} \times \mathsf{K}')$*-модуль.*

Доказательство такое же, как и выше. Пусть $\mathfrak{S} = a_1\mathsf{P} + \ldots + a_n\mathsf{P}$ и, следовательно, $\mathfrak{S} \times \mathsf{K}' = a_1\mathsf{K}' + \ldots + a_n\mathsf{K}'$. Тогда мы можем определить

$$(a_1\varkappa_1' + \ldots + a_n\varkappa_n')\, u = a_1 u\varkappa_1 + \ldots + a_n u\varkappa_n. \tag{1}$$

Теперь легко проверить все аксиомы. Ассоциативность $(bc)\, u = b\,(cu)$ следует из равенств

$$(a_1\varkappa_1' \cdot a_2\varkappa_2')\, u = (a_1a_2\varkappa_1'\varkappa_2')\, u = (a_1a_2)\, u\, (\varkappa_2\varkappa_1),$$
$$a_1\varkappa_1'\,(a_2\varkappa_2' \cdot u) = a_1\varkappa_1'\,(a_2 u\varkappa_2) = a_1\,(a_2 u\varkappa_2)\,\varkappa_1 = (a_1a_2)\, u\, (\varkappa_1\varkappa_2).$$

Тем же способом можно и, наоборот, любой левый $(\mathfrak{S} \times \mathsf{K}')$-модуль рассматривать как левый $\mathfrak{S}$-модуль и как правый K-модуль, пользуясь определением $u\varkappa = \varkappa' u$. *Поэтому изоморфные $(\mathfrak{S} \times \mathsf{K}')$-модули дают изоморфные двойные модули, и наоборот.*

Эти наблюдения имеют много приложений. Пусть K обозначает алгебру с делением, а $\mathfrak{S}$ — простую алгебру с единицей над P, причем по крайней мере одна из алгебр $\mathfrak{S}$ или K центральна над P. Тогда согласно § 103 произведение $\mathfrak{S} \times \mathsf{K}'$ простое. В силу § 105 все простые левые $(\mathfrak{S} \times \mathsf{K}')$-модули изоморфны друг другу и простым левым идеалам в $\mathfrak{S} \times \mathsf{K}'$. Следовательно, изоморфны все простые (левые над $\mathfrak{S}$ и правые над K) двойные модули. Мы получили предложение:

Все неприводимые представления алгебры $\mathfrak{S}$ над K эквивалентны.

Так как алгебра $\mathfrak{S}$ проста, все эти представления точные. Каждое из них отображает алгебру $\mathfrak{S}$ и на некоторое подкольцо Σ полного матричного кольца K_r. Любые два таких представления $s \longmapsto S_1$ и $s \longmapsto S_2$, переводящие $\mathfrak{S}$ на Σ_1 и на Σ_2, эквивалентны. Согласно § 87 это означает, что существует некоторая не зависящая от s матрица Q, переводящая S_1 в S_2 по правилу

$$S_2 = Q^{-1}S_1Q. \tag{2}$$

Отсюда совсем легко получается

Теорема об автоморфизмах. *Если Σ_1 и Σ_2 — две изоморфные простые подалгебры центральной простой алгебры K_r, то любой изоморфизм между Σ_1 и Σ_2, оставляющий неподвижными элементы основного поля, определяется некоторым внутренним автоморфизмом алгебры K_r с помощью равенства* (2).

Действительно, любые две такие алгебры Σ_1 и Σ_2 всегда можно рассматривать как представления одной алгебры $\mathfrak{S}$. Если эти представления приводимы, то они распадаются на одно и то же число неприводимых представлений, потому что степени обоих рассматриваемых представлений равны одному и тому же числу r. Так как эти неприводимые представления эквивалентны, то и исходные представления тоже эквивалентны.

В качестве частного случая отсюда мы получаем:

Любой автоморфизм кольца K_r, *оставляющий неподвижными элементы центра* P, *является внутренним.*

Когда в последующем речь зайдет об изоморфизмах или автоморфизмах алгебр с единицей, всегда будет предполагаться, что эти отображения оставляют неподвижными элементы основного поля P. К таковым относятся во всяком случае внутренние автоморфизмы.

Пусть опять $\mathfrak{S}$ — некоторая простая алгебра и K — некоторая алгебра с делением над P. Одна из алгебр $\mathfrak{S}$ или K предполагается центральной. Тогда алгебра $\mathfrak{S}\times\mathsf{K}'$ проста, а потому изоморфна полному матричному кольцу Δ_t над некоторым телом Δ. Выясним, что можно сказать об этом теле Δ.

В общем случае Δ является кольцом правых эндоморфизмов некоторого простого $(\mathfrak{S}\times\mathsf{K}')$-модуля, который согласно сказанному в начале может рассматриваться и как двойной модуль (левый над $\mathfrak{S}$ и правый над K). Каждый эндоморфизм $(\mathfrak{S}\times\mathsf{K}')$-модуля взаимно однозначным образом определяет эндоморфизм упомянутого двойного модуля $\mathfrak{M}$; поэтому кольцо Δ изоморфно кольцу правых эндоморфизмов двойного модуля $\mathfrak{M}$. Следовательно, инверсное тело Δ' изоморфно кольцу левых эндоморфизмов двойного модуля $\mathfrak{M}$. Можно, конечно, отождествить Δ' с этим кольцом левых эндоморфизмов.

Если двойной модуль $\mathfrak{M}$ рассматривается как векторное пространство над K, то элементы a кольца $\mathfrak{S}$ индуцируют линейные преобразования A этого векторного пространства:

$$au = Au.$$

Как мы видели, с помощью представления $a \longmapsto A$ кольцо $\mathfrak{S}$ отображается на подкольцо Σ матричного кольца K_r. Левые эндоморфизмы модуля $\mathfrak{M}$, а потому и элементы кольца Δ', являются согласно § 100 линейными преобразованиями L этого векторного пространства, коммутирующими с преобразованиями A:

$$LA = AL \text{ для всех } A \in \Sigma.$$

Таким образом, кольцо Δ' является *централизатором кольца* Σ *в кольце* K_r, т. е. кольцом тех матриц L из K_r, которые перестановочны со всеми матрицами A из Σ.

Тем самым мы получили структурную теорему о произведениях:

Пусть $\mathfrak{S}$ — *простая алгебра (с единицей) и* K — *алгебра с делением над полем* P. *Одна из данных алгебр предполагается центральной над* P *и через* K' *обозначается тело, инверсно изоморфное телу* K. *Тогда алгебра* $\mathfrak{S}\times\mathsf{K}'$ *изоморфна полному матричному кольцу* Δ_t *над некоторым телом* Δ. *Единственное неприводимое представление алгебры* $\mathfrak{S}$ *над* K *точным образом переводит* $\mathfrak{S}$ *на*

некоторое подкольцо Σ в полной матричной алгебре K_r. Централизатор Δ' алгебры Σ в K_r инверсно изоморфен алгебре Δ.

Степень r представления $\mathfrak{S} \to \Sigma$ является рангом двойного модуля $\mathfrak{M}$ над K. Если $\mathfrak{M}$ рассматривать как $(\mathfrak{S} \times \mathsf{K}')$-модуль, то и над K' его ранг будет равен r. Теперь $\mathfrak{M}$ можно выбрать как простой левый идеал I алгебры $\mathfrak{S} \times \mathsf{K}'$; ранг этого левого идеала равен, таким образом,

$$(\mathsf{I} : \mathsf{K}') = r.$$

Простое кольцо $\mathfrak{S} \times \mathsf{K}' \cong \Delta_t$ является прямой суммой t таких левых идеалов; следовательно, ранг этого кольца над K' равен tr. Отсюда вытекает важное соотношение между рангами:

$$(\Sigma : \mathsf{P}) = (\mathfrak{S} : \mathsf{P}) = (\mathfrak{S} \times \mathsf{K}' : \mathsf{K}') = tr. \tag{3}$$

Формулировка структурной теоремы несколько упростится, если исходить не из $\mathfrak{S}$, а из Σ и вместо $\mathfrak{S} \times \mathsf{K}'$ рассматривать изоморфную алгебру $\Sigma \times \mathsf{K}'$. Таким образом, в полном матричном кольце K_r выбирается подкольцо Σ, о котором предполагается, что его матрицы образуют неприводимую систему. Далее, пусть K или Σ (или обе эти алгебры) — центральная алгебра над P. Тогда структурная теорема утверждает следующее:

Произведение $\Sigma \times \mathsf{K}'$ изоморфно полному матричному кольцу над некоторым телом Δ. Централизатор Δ' алгебры Σ в алгебре K_r инверсно изоморфен телу Δ. Ранг алгебры Σ над полем P равен tr.

Предположение о том, что Σ является неприводимой системой линейных преобразований, тоже можно опустить. Так как алгебра $\Sigma \times \mathsf{K}'$ проста, каждое матричное представление алгебры Σ над K вполне приводимо и его неприводимые составляющие эквивалентны. Следовательно, матрицы системы Σ могут при подходящем выборе базиса привестись к виду

$$A = \begin{Vmatrix} A_1 & & & & \\ & \cdot & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & A_1 \end{Vmatrix} \tag{4}$$

с s одинаковыми клетками A_1, расположенными вдоль диагонали. Матрицы A_1 образуют неприводимую систему Σ_1, к которой можно применить доказанную выше структурную теорему. Централизатор системы Σ_1, включая в себя лишь матрицы L_1, перестановочные со всеми матрицами A_1 из Σ_1, вновь является алгеброй Δ', инверсно изоморфной алгебре с делением Δ. Централизатор T алгебры Σ состоит из матриц

$$L = \begin{Vmatrix} L_{11} & \dots & L_{1s} \\ \cdot & \cdot & \cdot \\ L_{s1} & \dots & L_{ss} \end{Vmatrix}, \tag{5}$$

где L_{ik} выбираются из Δ'. Следовательно, $\mathsf{T} \cong \Delta'_s$.

Как легко проверить, между рангами поэлементно перестановочных колец Σ и T имеет место соотношение

$$(\Sigma : \mathsf{P})(\mathsf{T} : \mathsf{P}) = (\mathsf{K}_r : \mathsf{P}). \tag{6}$$

Из (6) легко получается, что централизатор кольца T — это опять-таки Σ.

Рассмотренное здесь симметричное соотношение между системами Σ и T находится в тесной связи с теорией Галуа, в большой общности рассмотренной в книге: Джекобсон Н. Строение колец, гл. VI и VII.

Обратимся теперь к приложениям основной теоремы.

1. *Строение кольца* $\mathsf{K}\times\mathsf{K}'$. Пусть K — центральная алгебра с делением над полем P. Тогда можно выбрать в качестве Σ само тело K и применить структурную теорему. Порядок r матриц в этом случае равен 1; система Σ тривиальным образом неприводима. Централизатор Δ' алгебры K в K является центром P тела K. Следовательно, $\Delta=\mathsf{P}$. Соотношение (3) между рангами дает равенство

$$(\mathsf{K}:\mathsf{P})=t.$$

Мы получили, таким образом, следующий результат:

Произведение $\mathsf{K}\times\mathsf{K}'$ *является полным матричным кольцом над основным полем* P. *Порядок* t *соответствующих матриц равен рангу линейного пространства* K *над полем* P.

2. *Максимальные поля в алгебре с делением.* Пусть K — произвольная алгебра с делением над полем P. Если K не является с самого начала центральной алгеброй над P, то выберем в качестве нового основного поля P центр Z тела K. Пусть Σ — произвольное максимальное подполе в K. Централизатором поля Σ в теле K является само Σ, потому что если элемент θ перестановочен со всеми элементами из Σ, то тело $\Sigma(\theta)$ является полем, а так как поле Σ должно быть максимальным, элемент θ должен принадлежать Σ.

В соответствии с этим $\Delta=\Sigma$ и, следовательно, $\Sigma\times\mathsf{K}'$ — полное матричное кольцо над Σ. Инверсное к $\Sigma\times\mathsf{K}$ кольцо

$$\mathsf{K}\times\Sigma'=\mathsf{K}\times\Sigma=\mathsf{K}_\Sigma$$

является, таким образом, полным матричным кольцом над Σ, т. е. Σ — поле разложения алгебры K. Представление алгебры K_Σ полным матричным кольцом Σ_t абсолютно неприводимо. В § 103 мы назвали число t *индексом* m алгебры с делением K, если оно равно степени абсолютно неприводимого матричного представления алгебры K над подходящим расширением Σ основного поля P. Таким образом, в данном случае $t=m$ и $r=1$. Соотношение (3) между рангами дает теперь

$$(\Sigma:\mathsf{P})=t=m,$$

и мы получаем следующее предложение:

Максимальные подполя алгебры с делением K, *центр которой равен* P, *являются полями разложения алгебры* K *и их степень* $(\Sigma:\mathsf{P})$ *равна индексу* m *данного тела.*

В качестве приложения этой теоремы мы опишем теперь все *алгебры с делением над полем* $\mathbb{R}$ *вещественных чисел.*

В этом случае коммутативными алгебрами с делением над P являются лишь P и $\mathsf{P}(i)$, т. е. поля вещественных и комплексных чисел. Предположим теперь, что K — некоммутативная алгебра с делением над P. Если Z — ее центр и Σ — какое-нибудь максимальное подполе в K, то

$$\mathsf{P} \subseteq \mathsf{Z} \subseteq \Sigma \subset \mathsf{K}; \quad (\Sigma : \mathsf{Z}) = m; \quad (\mathsf{K} : \mathsf{Z}) = m^2.$$

Так как K — некоммутативная алгебра, должно быть выполнено неравенство $m > 1$. Полями Z и Σ могут быть лишь P и $\mathsf{P}(i)$. Так как $m > 1$, поле Σ не равно Z. Следовательно,

$$\Sigma = \mathsf{P}(i), \quad \mathsf{Z} = \mathsf{P}, \quad m = 2.$$

Искомая алгебра K может, следовательно, иметь ранг лишь $m^2 = 4$.

Автоморфизм поля $\mathsf{P}(i)$, переводящий i в $-i$, согласно теореме об автоморфизмах определяется некоторым внутренним автоморфизмом тела K, т. е. существует элемент k со свойством

$$kik^{-1} = -i. \tag{7}$$

Так как k не содержится в $\Sigma = \mathsf{P}(i)$, то должно иметь место равенство $\Sigma(k) = \mathsf{K}$; следовательно, $\mathsf{K} = \mathsf{P}(i, k)$. Из (7) следует, что

$$k^2ik^{-2} = i,$$

т. е. элемент k^2 перестановочен с элементом i. Так как k^2 перестановочен с k, элемент k^2 принадлежит центру: $k^2 = a \in \mathsf{P}$.

Если бы было $a \geqslant 0$, то мы имели бы $a = b^2$ и

$$k^2 - b^2 = (k - b)(k + b) = 0,$$
$$k - b = 0 \quad \text{или} \quad k + b = 0;$$

следовательно, $k \in \mathsf{P}$, что невозможно. Поэтому должно иметь место неравенство $a < 0$, т. е. $a = -b^2$ $(b \neq 0)$. Умножая k на вещественное число b^{-1}, можно добиться, чтобы было $k^2 = -1$, и при этом не потерять ни одного из отмеченных выше свойств элемента k Для i и k имеем:

$$ki = -ik, \quad i^2 = k^2 = -1.$$

Эти соотношения характеризуют алгебру кватернионов. *Следовательно, алгебра кватернионов — единственная некоммутативная алгебра с делением над полем вещественных чисел.*

Точно так же доказывается, что любая центральная алгебра с делением индекса 2 над полем $\mathbb{Q}$ рациональных чисел является алгеброй обобщенных кватернионов.

4. *Описание всех конечных тел* (тел с конечным числом элементов).

Если K — произвольное конечное тело, Z — его центр, а m — его индекс над Z, то каждый элемент из K обязательно содержится в каком-либо подполе Σ степени m над Z. Однако все

коммутативные расширения m-й степени Σ поля Галуа Z, состоящие из p^n элементов, попарно эквивалентны (действительно, они получаются присоединением всех корней уравнения $x^q = x$, $q = p^{nm}$). Следовательно, все эти поля получаются трансформированием с помощью элементов из K из одного произвольно взятого среди них поля Σ_0:

$$\Sigma = \varkappa \Sigma_0 \varkappa^{-1}.$$

Если удалить из тела K нуль, то K превратится в некоторую группу $\mathfrak{G}$, Σ_0 — в ее подгруппу $\mathfrak{H}$, Σ — в сопряженную подгруппу $\varkappa\mathfrak{H}\varkappa^{-1}$ и эти сопряженные подгруппы все вместе будут составлять всю группу $\mathfrak{G}$ (потому что каждый элемент из K содержится в одном из полей Σ). Докажем следующую теоретико-групповую лемму:

Лемма. *Собственная подгруппа $\mathfrak{H}$ конечной группы $\mathfrak{G}$ не может вместе со всеми своими сопряженными подгруппами $s\mathfrak{H}s^{-1}$ составлять всю группу $\mathfrak{G}$.*

Доказательство. Пусть n и N — порядки $\mathfrak{H}$ и $\mathfrak{G}$ соответственно, и пусть j — индекс подгруппы $\mathfrak{H}$, так что $N = j \cdot n$. Если s и s' принадлежат одному и тому же смежному классу $s\mathfrak{H}$, т. е. $s' = sh$, то

$$s'\mathfrak{H}s'^{-1} = sh\mathfrak{H}h^{-1}s^{-1} = s\mathfrak{H}s^{-1}.$$

Следовательно, различных подгрупп $s\mathfrak{H}s^{-1}$ существует не больше, чем есть смежных классов, т. е. не больше j. Если бы различные подгруппы $s\mathfrak{H}s^{-1}$ (к числу которых относится и сама группа $\mathfrak{H}$) составляли всю группу $\mathfrak{G}$, то у них не было бы общих элементов, потому что иначе нельзя было бы получить все $N = j \cdot n$ элементов группы $\mathfrak{G}$. Но так как любые две подгруппы $s\mathfrak{H}s^{-1}$ обладают общим элементом — единицей, то они должны совпадать. Отсюда $\mathfrak{H} = \mathfrak{G}$, и мы получили противоречие.

Для нашего случая из этой леммы следует, что $\mathfrak{H}$ не может быть *собственной* подгруппой в $\mathfrak{G}$ и, таким образом, $\mathfrak{H} = \mathfrak{G}$ и $\mathsf{K} = \Sigma_0$. Следовательно, тело K коммутативно. Мы доказали теорему:

Любое тело с конечным числом элементов коммутативно, т. е. является полем.

Другое доказательство этой теоремы, принадлежащее Веддерберну, см. в работе: Витт (Witt E.). — Abh. Math. Sem. Hamburg, 1931, 8, S. 413.

§ 113. Поля разложения простых алгебр

Любая простая алгебра $\mathfrak{A}$ может рассматриваться как полное матричное кольцо над некоторой алгеброй с делением K:

$$\mathfrak{A} = \mathsf{K}_r.$$

Согласно § 103 поля разложения тела K являются в то же время полями разложения и для $\mathfrak{A}$, и наоборот. Поэтому при

изучении полей разложения можно ограничиться лишь полями разложения тел K. Далее, центр тела K можно рассматривать как основное поле P; тогда K — центральная алгебра над P.

Согласно § 112 максимальные подполя в K являются полями разложения для K. Следовательно, существует поле разложения Σ конечной степени над P. Мы ограничимся поэтому рассмотрением лишь конечных расширений Σ основного поля P.

Согласно § 112 каждое такое поле Σ неприводимым образом погружается в алгебру K_r. Поэтому можно рассматривать Σ как неприводимую систему матриц из K_r. Если Σ — поле разложения алгебры K, то это означает, что $\Sigma \times \mathsf{K}'$ является полным матричным кольцом над Σ:

$$\Sigma \times \mathsf{K}' = \Sigma_t, \quad \text{так что} \quad \Delta = \Sigma.$$

Инверсное кольцо Δ' в таком случае тоже равно Σ. Следовательно, централизатор поля Σ равен Σ, т. е. любой элемент из K_r, перестановочный со всеми элементами из Σ, принадлежит самому полю Σ. Отсюда следует, что Σ — максимальное подполе (даже максимальное коммутативное подкольцо) в K_r.

Обратно, пусть Σ — максимальное подполе матричного кольца K_r. Если бы система Σ была приводимой, то согласно (4) из § 112 матрицы A системы Σ можно было бы получить из частей A_1. Эти части образуют некоторую систему Σ_1, изоморфную системе Σ, которая тоже максимальна как подполе в K_{r_1}. Следовательно, без ограничения общности мы можем рассматривать Σ как неприводимую систему.

Централизатор Δ' поля Σ является телом, элементы θ которого перестановочны со всеми элементами из Σ. Если бы один из таких элементов θ не содержался в Σ, то расширение $\Sigma(\theta)$ собственным образом содержало бы поле Σ, а это противоречит максимальности поля K_r. Следовательно, должно иметь место равенство $\Delta' = \Sigma$. Но тогда $\Delta = \Sigma$, т. е. Σ — поле разложения алгебры K.

Тем самым мы получили следующее описание полей разложения:

Каждое максимальное подполе полного матричного кольца K_r является полем разложения тела K; обратно, каждое поле разложения можно представить как максимальное подполе в алгебре K_r (даже неприводимым образом).

В случае неприводимого вложения поля Σ в алгебру K_r, согласно (3) § 112, имеет место соотношение между рангами:

$$(\Sigma : \mathsf{P}) = tr.$$

Здесь t является степенью абсолютно неприводимого представления тела K над полем Σ, т. е. число t равно индексу m тела K.

Следовательно,

$$(\Sigma : \mathsf{P}) = mr.$$

Отсюда получается: *степень поля разложения* Σ *алгебры* K *делится на индекс* m *тела* K. *Максимальное подполе в* K *является полем разложения наименьшей возможной степени* m.

В заключение мы докажем следующую теорему:

Любая центральная алгебра с делением K *над полем* P *обладает по крайней мере одним сепарабельным полем разложения.*

Для доказательства потребуется

Лемма. *Любая* p^f*-строчная матрица* A *над полем характеристики* p, *удовлетворяющая уравнению вида*

$$A^{p^e} = E\zeta \quad (E \text{ — единичная матрица}), \tag{1}$$

имеет характеристический многочлен (см. § 89) *вида*

$$\chi(x) = x^{p^f} - \beta$$

и, следовательно, если $p^f > 1$, *то след такой матрицы равен нулю.*

Доказательство леммы. Мы можем присоединить к основному полю корни p^e-й степени из элемента ζ и считать, что $\zeta = \eta^{p^e}$. Если матрицу A рассматривать как матрицу линейного преобразования некоторого векторного пространства, то для каждого вектора v будут выполнены соотношения

$$0 = (A^{p^e} - \zeta)\, v = (A^{p^e} - \eta^{p^e})\, v = (A - \eta)^{p^e} v.$$

Элементарные делители $f_\nu(x)$ матрицы A согласно их определению (§ 88) являются делителями многочлена $(x-\eta)^{p^e}$, т. е. степенями двучлена $(x-\eta)$. В свою очередь характеристический многочлен $\chi(x)$ является произведением элементарных делителей и поэтому обязательно равен некоторой степени двучлена $(x-\eta)$. Но так как $\chi(x)$ — многочлен степени p^f, выполняются равенства

$$\chi(x) = (x-\eta)^{p^f} = x^{p^f} - \eta^{p^f} = x^{p^f} - \beta.$$

Доказательство существования сепарабельного поля разложения. Пусть Z — максимальное сепарабельное подполе в K и Δ' — централизатор поля Z в K. Согласно структурной теореме из § 112 произведение $\mathsf{Z} \times \mathsf{K}'$ изоморфно полному матричному кольцу Δ_t, где Δ инверсно изоморфно по отношению к Δ'. Центр алгебры $\mathsf{Z} \times \mathsf{K}'$ равен $\mathsf{Z} \times \mathsf{P} = \mathsf{Z}$, так как P — центр тела K'. Следовательно, и центр алгебры Δ_t равен Z. Но центр полного матричного кольца Δ_t равен центру алгебры Δ, так что центр алгебры Δ' равен Z.

Если теперь θ — произвольный элемент из Δ, не принадлежащий центру Z, то поле $\mathsf{Z}(\theta)$ несепарабельно: оно имеет редуцированную степень 1, так как иначе $\mathsf{Z}(\theta)$ содержало бы некоторое

сепарабельное подполе, содержащее центр Z. Элемент θ удовлетворяет, следовательно, неразложимому уравнению вида

$$\theta^{p^e} = \zeta, \quad \zeta \in \mathsf{Z}. \tag{2}$$

То же самое верно (при $p^e = 1$) и тогда, когда θ принадлежит самому центру Z.

Если Σ — максимальное подполе в Δ', то его редуцированная степень над Z как над основным полем равна 1, т. е. его степень как расширения равна p^f. Поле Σ является полем разложения для Δ', т. е. $\Delta' \times \Sigma$ — полное матричное кольцо над Σ порядка p^f. В этом матричном представлении все элементы из Δ' имеют согласно лемме нулевой след, если $p^f > 1$. Объясняется это так: из (2) следует, что если A — матрица, представляющая элемент θ, то имеет место матричное равенство (1); все матрицы из $\Delta' \times \Sigma$ являются линейными комбинациями матриц из Δ' с коэффициентами из Σ — основного поля матричного кольца; следовательно, все эти матрицы имеют нулевой след при $p^f > 1$; противоречие теперь состоит в том, что сказанное относится к полному матричному кольцу. Следовательно, $p^f = 1$, $\mathsf{Z} = \Sigma$ — единственная оставшаяся возможность. Центр Z является теперь максимальным подполем в K, а потому полем разложения.

§ 114. Группа Брауэра. Системы факторов

Распределим центральные простые алгебры над фиксированным основным полем P на классы так, чтобы к одному классу $[\mathsf{K}]$ относились все те алгебры, которые изоморфны полным матричным кольцам над одним и тем же телом K.

Если K и Λ — тела над P, то $\mathsf{K} \times \Lambda$ — вновь центральная и простая алгебра (§ 103) и, следовательно,

$$\mathsf{K} \times \Lambda \cong \Delta_t. \tag{1}$$

Из (1) следует, что

$$\mathsf{K}_r \times \Lambda_s = \mathsf{K} \times \mathsf{P}_r \times \Lambda \times \mathsf{P}_s \cong \Delta_t \times \mathsf{P}_{rs} = \Delta \times \mathsf{P}_t \times \mathsf{P}_{rs} = \Delta \times \mathsf{P}_{trs} = \Delta_{trs};$$

тем самым произведения $\mathsf{K}_r \times \Lambda_s$ алгебр из классов $[\mathsf{K}]$ и $[\Lambda]$ принадлежат одному и тому же клсссу $[\Delta]$. Этот последний назовем *произведением* классов $[\mathsf{K}]$ и $[\Lambda]$. Так как

$$\mathsf{K} \times \Lambda \cong \Lambda \times \mathsf{K},$$
$$\mathsf{K} \times (\Lambda \times \Gamma) = (\mathsf{K} \times \Lambda) \times \Gamma,$$

то операция умножения коммутативна и ассоциативна. Существует также и единичный класс: это класс $[\mathsf{P}]$ основного поля. Наконец, для каждого класса $[\mathsf{K}]$ существует обратный класс, а именно, класс $[\mathsf{K}']$ тела K', инверсно изоморфного телу K.

Следовательно: *классы центральных простых алгебр над* P *образуют абелеву группу*. Первым ее исследовал Р. Брауэр и поэтому ее называют *группой Брауэра классов алгебр*.

Любую подгруппу группы Брауэра всегда составляют те классы алгебр, которые в качестве поля разложения имеют одно и то же расширение Σ поля P. Действительно, любое поле разложения тела K согласно § 103 является полем разложения всего класса $[\mathsf{K}]$, а также и класса $[\mathsf{K}']$, потому что K' инверсно изоморфно K и, следовательно $\mathsf{K}'\times\Sigma$ инверсно изоморфно $\mathsf{K}\times\Sigma$. Если K и Λ обладают одним и тем же полем разложения Σ, т. е. если

$$\mathsf{K}\times\Sigma\cong\Sigma_s,\quad \Lambda\times\Sigma\cong\Sigma_t,$$

то

$$(\mathsf{K}\times\Lambda)\times\Sigma\cong\mathsf{K}\times\Sigma_t\cong\mathsf{K}\times\Sigma\times\mathsf{P}_t\cong\Sigma_s\times\mathsf{P}_t=\Sigma\times\mathsf{P}_s\times\mathsf{P}_t\cong\Sigma_{st},$$

а потому Σ является полем разложения и произведения $\mathsf{K}\times\Lambda$, а, следовательно, и всего класса $[\mathsf{K}\times\Lambda]$.

Каждый брауэров класс алгебр $[\mathsf{K}]$ согласно § 113 обладает сепарабельным полем разложения, скажем, полем $\mathsf{P}(\theta)$. Если вместе с θ присоединить и сопряженные с ним элементы, то получится некоторое нормальное сепарабельное поле разложения Σ. Согласно § 113, это подполе неприводимым образом представляется максимальным коммутативным подполем в простой алгебре $\mathfrak{A}=\mathsf{K}_r$, принадлежащей классу $[\mathsf{K}]$.

Докажем теперь следующее: *алгебра* $\mathfrak{A}$ *является скрещенным произведением поля* Σ *с его группой Галуа* $\mathfrak{G}$ *в смысле* § 94.

Прежде всего, из § 94 следует, что Σ является своим собственным централизатором в $\mathfrak{A}=\mathsf{K}_r$, т. е. каждый элемент из $\mathfrak{A}$, перестановочный со всеми элементами из Σ, принадлежит Σ.

Как и в § 94, мы обозначаем через S, T, ... элементы группы Галуа $\mathfrak{G}$, а через β^S — элемент из Σ, который получился применением к элементу β автоморфизма S. Произведение ST вновь определяется равенством

$$\beta^{ST}=(\beta^S)^T.$$

Согласно теореме об автоморфизмах из § 112 автоморфизмы S порождаются внутренними автоморфизмами алгебры $\mathfrak{A}$. Следовательно, для каждого S существует такой элемент u_S из $\mathfrak{A}$, обладающий обратным u_S^{-1}, что для всех β из Σ имеет место равенство

$$u_S^{-1}\beta u_S=\beta^S,$$

или

$$\beta u_S=u_S\beta^S. \tag{2}$$

Согласно (2) элемент $u_{ST}^{-1}u_Su_T$ перестановочен со всеми элементами из Σ, а потому он является элементом поля Σ. Следовательно, если положить

$$u_{S,T}=u_{ST}^{-1}u_Su_T=\delta_{S,T},$$

то получится правило умножения

$$u_S u_T = u_{ST}\delta_{S,T}. \tag{3}$$

Так как элемент $\delta_{S,T}$ обладает обратным — таковым служит элемент $u_T^{-1}u_S^{-1}u_{ST}$, — то $\delta_{S,T} \neq 0$.

Правила (2) и (3) совпадают с правилами (4) и (5), с помощью которых в § 94 было введено скрещенное произведение. Из этих правил следует, как было тогда доказано, что элементы u_S линейно независимы над полем Σ. Линейные комбинации элементов u_S с коэффициентами из Σ

$$a = \sum_S u_S \beta_S$$

образуют в $\mathfrak{A}$ некоторое кольцо $\mathfrak{A}_1$, ранг которого над Σ равен n, а над P, следовательно, равен n^2, где $n = (\Sigma : \mathsf{P})$ — ранг Σ над P. Согласно § 113 имеет место равенство

$$n = (\Sigma : \mathsf{P}) = rm.$$

Ранг алгебры $\mathfrak{A} = \mathsf{K}_r$ над P равен

$$r^2(\mathsf{K} : \mathsf{P}) = r^2m^2 = n^2.$$

Так как $\mathfrak{A}_1$ и $\mathfrak{A}$ имеют один и тот же ранг n^2 и $\mathfrak{A}_1$ содержится в $\mathfrak{A}$, то $\mathfrak{A}_1 = \mathfrak{A}$, т. е. $\mathfrak{A}$ является скрещенным произведением поля Σ с его группой Галуа $\mathfrak{G}$.

Возможность представления алгебр $\mathfrak{A} = \mathsf{K}_r$ в виде скрещенных произведений впервые обнаружила Эмми Нётер. Поэтому систему $\{\delta_{S,T}\}$ элементов $\delta_{S,T}$ называют *нётеровой системой факторов* алгебры $\mathfrak{A}$ или класса алгебр $[\mathsf{K}]$. Очевидно, что

Алгебра $\mathfrak{A}$ полностью определяется заданием поля Σ и системы факторов $\{\delta_{S,T}\}$.

Обратное неверно. Если заданы $\mathfrak{A}$ и Σ, то вложение поля Σ в алгебру $\mathfrak{A}$ определено однозначно с точностью до внутренних автоморфизмов алгебры $\mathfrak{A}$ и с помощью такого вложения элементы u_S определяются неоднозначно — согласно (14) из § 94 можно заменить элементы u_S на

$$v_S = u_S\gamma_S \quad \gamma_S \neq 0. \tag{4}$$

Это, однако, единственная возможность менять упомянутые u_S, потому что v_S, как и u_S, обладают свойством (2):

$$\beta v_S = v_S \beta^S,$$

так что элемент $v_S u_S^{-1}$ перестановочен со всеми β и Σ:

$$\beta v_S u_S^{-1} = v_S \beta^S u_S^{-1} = v_S u_S^{-1}\beta.$$

Если положить $v_S u_S^{-1} = \gamma_S$, то элементы γ_S будут элементами из Σ и получится, что

$$v_S = \gamma_S u_S.$$

Замена элементов u_S на элементы v_S, как мы видели в § 94, имеет своим следствием замену системы факторов $\{\delta_{S,T}\}$ на *ассоциированную систему факторов* $\{\varepsilon_{S,T}\}$:

$$\varepsilon_{S,T}=\frac{\gamma_S^T\gamma_T}{\gamma_{ST}}\,\delta_{S,T}. \tag{5}$$

Таким образом, брауэровы классы алгебр [K] *с фиксированным полем разложения* Σ *взаимно однозначно соответствуют классам ассоциированных систем факторов* $\{\delta_{S,T}\}$ *из поля* Σ, *подчиняющихся условиям ассоциативности* (13) *из* § 94.

До сих пор мы исходили из некоторого заданного нормального поля разложения Σ. Но, следуя Р. Брауэру, можно определить систему факторов простой алгебры K_r и над полем разложения, не являющимся нормальным.

Пусть Δ — конечное поле разложения, о котором не предполагается, что оно нормально. Пусть $\theta=\theta_1$ — примитивный элемент поля Δ, так что $\Delta=\mathsf{P}(\theta)$, и пусть θ_α $(\alpha=1, 2, \ldots, n)$ — элементы, сопряженные с θ в некотором подходяще выбранном нормальном расширении Σ.

Существует лишь одно, с точностью до эквивалентности, абсолютно неприводимое представление алгебры K_r матрицами над Δ. Пусть $a\longmapsto A$ — это представление и пусть $a\longmapsto A_\alpha$ — представления, которые получаются из только что названного применением изоморфизма полей $\theta\longmapsto\theta_\alpha$ к матрицам. Так как все эти представления эквивалентны друг другу (над полем Σ также существует лишь одно неприводимое представление), то имеются матрицы $P_{\alpha\beta}$, переводящие представление A_α в представление A_β:

$$A_\alpha=P_{\alpha\beta}A_\beta P_{\alpha\beta}^{-1}. \tag{6}$$

Матрицы $P_{\alpha\beta}$ могут быть взяты уже над полем $\mathsf{P}(\theta_\alpha, \theta_\beta)$, потому что над этим полем эквивалентны оба представления. Далее, матрицу $P_{\alpha\beta}$ можно выбрать так, чтобы каждый изоморфизм поля $\mathsf{P}(\theta_\alpha, \theta_\beta)$, переводящий θ_α, θ_β в сопряженные θ_γ, θ_δ, переводил матрицу $P_{\alpha\beta}$ в матрицу $P_{\gamma\delta}$. Для достижения этой цели нужно лишь в каждом классе сопряженных пар выбрать одну пару α, β, определить для нее матрицу $P_{\alpha\beta}$, а остальные $P_{\gamma\delta}$ получить из $P_{\alpha\beta}$ применением соответствующих изоморфизмов.

Имеют место соотношения

$$A_\alpha=P_{\alpha\beta}A_\beta P_{\alpha\beta}^{-1}=P_{\alpha\beta}P_{\beta\gamma}A_\gamma P_{\beta\gamma}^{-1}P_{\alpha\beta}^{-1}=P_{\alpha\beta}P_{\beta\gamma}P_{\alpha\gamma}^{-1}A_\alpha P_{\alpha\gamma}P_{\beta\gamma}^{-1}P_{\alpha\beta}^{-1}.$$

Тем самым матрица $P_{\alpha\beta}P_{\beta\gamma}P_{\alpha\gamma}^{-1}$ перестановочна со всеми матрицами A_α любого абсолютно неприводимого представления и, следовательно, является кратным единичной матрицы E:

$$\begin{gathered}P_{\alpha\beta}P_{\beta\gamma}P_{\alpha\gamma}^{-1}=c_{\alpha\beta\gamma}E,\\ P_{\alpha\beta}P_{\beta\gamma}=c_{\alpha\beta\gamma}P_{\alpha\gamma}.\end{gathered} \tag{7}$$

С помощью соотношений (7) оказывается определенной *брауэрова система факторов* $\{c_{\alpha\beta\gamma}\}$. Справедливы следующие свойства:

а) элементы $c_{\alpha\beta\gamma}$ принадлежат полю $\mathsf{P}(\theta_\alpha, \theta_\beta, \theta_\gamma)$;

б) $c_{\alpha\beta\gamma}c_{\alpha\gamma\delta} = c_{\alpha\beta\delta}c_{\beta\gamma\delta}$;

в) $c^S_{\alpha\beta\gamma} = c_{\alpha'\beta'\gamma'}$, если S — изоморфизм поля $\mathsf{P}(\theta_\alpha, \theta_\beta, \theta_\gamma)$, переводящий θ_α, θ_β, θ_γ в $\theta_{\alpha'}$, $\theta_{\beta'}$, $\theta_{\gamma'}$.

Свойство а) немедленно следует из определения элементов $c_{\alpha\beta\gamma}$, свойство б) — из ассоциативности, имеющей место для матриц $P_{\alpha\beta}$, и, наконец, свойство в) вытекает из поведения матриц $P_{\alpha\beta}$ при изоморфизмах S.

Если $P_{\alpha\beta}$ заменить на $k_{\alpha\beta}P_{\alpha\beta}$, где элементы поля $k_{\alpha\beta}$ удовлетворяют тем же условиям сопряженности, что и матрицы $P_{\alpha\beta}$, то система $c_{\alpha\beta\gamma}$ перейдет в *ассоциированную систему факторов*

$$c'_{\alpha\beta\gamma} = \frac{k_{\alpha\beta}k_{\beta\gamma}}{k_{\alpha\gamma}}\, c_{\alpha\beta\gamma}. \tag{8}$$

Если, с другой стороны, заменить представление $a \longmapsto A$ на эквивалентное представление $a \longmapsto QAQ^{-1}$, то матрицы P_α перейдут в матрицы $Q_\alpha P_\alpha Q_\alpha^{-1}$; непосредственно проверяется, что при этом система факторов $c_{\alpha\beta\gamma}$ не меняется. Следовательно, система факторов определена однозначно с точностью до ассоциированности заданием алгебры K_r и поля Δ.

Всю теорию можно построить, рассматривая только нётеровы или только брауэровы системы факторов. Но доказательства получаются проще и нагляднее, если использовать оба вида систем факторов, доказав их равносильность. Действительно, одни свойства легче доказывать для нётеровых, а другие — для брауэровых систем факторов. Мы начнем с основных свойств брауэровых систем факторов.

Если K_r — полное матричное кольцо над основным полем P, т. е. $\mathsf{K}_r = \mathsf{P}_r$, то можно взять $P_{\alpha\beta}$ равным единичной матрице E. Тогда все $c_{\alpha\beta\gamma}$ равны единице и *система факторов алгебры, распадающейся уже над основным полем, ассоциирована с единичной системой факторов* $c_{\alpha\beta\gamma} = 1$.

Найдем систему факторов для прямого произведения $\mathsf{K}_r \times \Lambda_S$. Если $a \longmapsto A$ — неприводимое представление алгебры K над телом Λ и $b \longmapsto B$ — неприводимое представление алгебры Λ_S над тем же телом, то получается представление произведения систем $\mathsf{K}_r \times \Lambda_S$, при котором ab переходит в кронекерово произведение $A \times B$ (§ 109). То, что это представление абсолютно неприводимо, легко увидеть, вычислив его степень. Действительно, если абсолютно неприводимое представление алгебры K_r имеет степень n, а алгебры Λ_S — степень m, то K_r (согласно, например, теореме Бернсайда) имеет ранг n^2, а Λ_S — ранг m^2, так что $\mathsf{K}_r \times \Lambda_S$ имеет ранг n^2m^2, в то время как степень произведения представлений равна mn, т. е. совпадает со степенью абсолютно неприводимого представления алгебры $\mathsf{K}_r \times \Lambda_S$.

Теперь мы можем вычислить систему факторов произведения представлений. Из $A_\alpha = P_{\alpha\beta}^{-1} A_\beta P_{\alpha\beta}$ и $B_\alpha = Q_{\alpha\beta}^{-1} B_\beta Q_{\alpha\beta}$ следует, что

$$A_\alpha \times B_\alpha = (P_{\alpha\beta} \times Q_{\alpha\beta})^{-1} (A_\beta \times B_\beta) (P_{\alpha\beta} \times Q_{\alpha\beta}),$$

поэтому $P_{\alpha\beta} \times Q_{\alpha\beta}$ — трансформирующие матрицы произведения представлений. Точно так же из

$$P_{\alpha\beta} P_{\beta\gamma} = c_{\alpha\beta\gamma} P_{\alpha\gamma} \text{ и } Q_{\alpha\beta} Q_{\beta\gamma} = d_{\alpha\beta\gamma} Q_{\alpha\gamma}$$

следует, что

$$(P_{\alpha\beta} \times Q_{\alpha\beta}) (P_{\beta\gamma} \times Q_{\beta\gamma}) = c_{\alpha\beta\gamma} d_{\alpha\beta\gamma} (P_{\alpha\gamma} \times Q_{\alpha\gamma}).$$

Итак, $\{c_{\alpha\beta\gamma} d_{\alpha\beta\gamma}\}$ — *система факторов произведения алгебр* $\mathsf{K}_r \times \Lambda_s$.

В случае $\mathsf{K} \times \mathsf{P}_r = \mathsf{K}_r$ факторы $d_{\alpha\beta\gamma}$ равны единице, поэтому *матричное кольцо* K_r *имеет ту же систему факторов, что и тело* K. Тем самым каждому брауэрову классу алгебр соответствует однозначно (с точностью до ассоциированной) определенная система факторов.

Объединяя все это, получаем следующее предложение: *каждому элементу группы Брауэра классов алгебр с полем разложения* Δ *соответствует система факторов* $\{c_{\alpha\beta\gamma}\}$, *определенная однозначно с точностью до ассоциированности, причем единичному элементу группы соответствует единичная система факторов, а произведению элементов — произведение систем.*

Выясним теперь, как меняется при расширении поля разложения брауэрова система факторов. Пусть $\Delta' = \mathsf{P}(\theta')$ — конечное сепарабельное расширение поля $\Delta = \mathsf{P}(\theta)$. Каждый изоморфизм $\theta' \longmapsto \theta'_{\alpha'}$ поля Δ' индуцирует и некоторый изоморфизм $\theta \longmapsto \theta_\alpha$ поля Δ, так что каждому индексу α' сопоставляется некоторый индекс α. При переходе к полю Δ' рассматриваемое представление $a \longmapsto A$ алгебры K_r над Δ остается неизменным. Но тогда сопряженные представления A_α также остаются неизменными, т. е. $A'_{\alpha'} = A_\alpha$, если номеру α' соответствует номер α. Соответственно, для трансформирующих матриц $P_{\alpha\beta}$ это дает следующее правило: если номерам α', β' сопоставлены номера α, β, то $P'_{\alpha'\beta'} = P_{\alpha,\beta}$. Наконец, для системы факторов получается следующее: $c'_{\alpha'\beta'\gamma'} = c_{\alpha\beta\gamma}$, *если номерам* α', β', γ' *сопоставлены номера* α, β, γ, *т. е. если изоморфизмы* $\theta' \longmapsto \theta'_{\alpha'}$, $\theta' \longmapsto \theta'_{\beta'}$, $\theta' \longmapsto \theta'_{\gamma'}$ *поля* Δ' *индуцируют изоморфизмы* $\theta \longmapsto \theta_\alpha$, $\theta \longmapsto \theta_\beta$, $\theta \longmapsto \theta_\gamma$ *поля* Δ.

На основании этого правила можно совершенно определенным образом перейти от произвольного сепарабельного поля разложения Δ к содержащему его нормальному полю Σ. Изоморфизмы $\theta \longmapsto \theta_\alpha$ поля Σ являются тогда элементами S, T, ... группы Галуа: $\theta_\alpha = \theta^S$, $\theta_\beta = \theta^T$ и т. д. Следовательно, в этом случае можно использовать элементы S, T, R в качестве индексов вместо использовавшихся до сих пор α, β, γ и писать $c_{S,T,R}$ вместо $c_{\alpha\beta\gamma}$. Свойство в) в этих новых обозначениях выглядит так:

$$c_{S,T,R}^{Q} = c_{SQ,\,TQ,\,RQ}. \tag{9}$$

Теперь можно осуществить переход к нётеровым системам факторов. Для заданного с самого начала скрещенного произведения K_r вычислим брауэрову систему факторов и покажем, что она совпадает с точностью до обозначений с нётеровой системой.

Мы получим неприводимое представление алгебры K_r над полем Σ, если рассмотрим K_r как модуль представления. Базисными элементами алгебры K_r как правого Σ-модуля являются в точности элементы u_S. Матрица, представляющая элемент $a = u_S\beta$ (достаточно рассмотреть лишь эти элементы, потому что остальные являются их суммами), получается так: этот элемент умножается на все базисные элементы u_T, а потом произведения разлагаются по элементам u_T:

$$(u_S\beta)\, u_T = u_S u_T \beta^T = u_{ST}\delta_{S,T}\beta^T.$$

Следовательно, представляющая матрица A имеет в столбце T и строке ST элемент $\delta_{S,T}\beta^T$, а на всех прочих местах этого столбца нули. Тем самым, сопряженная матрица A^R имеет в столбце T и строке ST элемент

$$(\delta_{S,T}\beta^T)^R = \delta^R_{S,T}\beta^{TR}.$$

Найдем теперь матрицу $P_{1,R}$, трансформирующую A в A^R:

$$AP_{1,R} = P_{1,R}A^R. \tag{10}$$

В качестве $P_{1,R}$ мы возьмем матрицу, которая в столбце Y и строке YR имеет элемент $\delta_{Y,R}$, а на всех остальных местах этого столбца нули. Тогда соотношение (10) выполняется, потому что в левой части в столбце T и строке STR стоит элемент $\delta_{S,TR}\beta^{TR}\delta_{T,R}$, а в правой части на том же месте стоит $\delta_{ST,R}\delta^R_{S,T}\beta^{TR}$, что, согласно (13) из § 94, то же самое. Следовательно, матрица $P_{1,R}$ найдена. Остальные $P_{S,T}$ получаются (в соответствии с принятым при определении матриц $P_{\alpha\beta}$ соглашением) применением автоморфизмов S к $P_{1,R}$:

$$P^S_{1,R} = P_{S,RS}.$$

Соотношение $P_{S,T}P_{T,R} = c_{S,T,R}P_{S,R}$ нужно установить лишь для случая $S = 1$, потому что применением автоморфизма S индекс 1 всегда можно превратить в индекс S; ср. (9). Следовательно, мы должны рассмотреть лишь вопрос о равенстве

$$P_{1,R}P_{R,TR} = c_{1,R,TR}P_{1,TR}$$

или о равенстве

$$P_{1,R}P^R_{1,T} = c_{1,R,TR}P_{1,TR}.$$

Матрица, стоящая слева, имеет на пересечении столбца S и строки STR элемент

$$\delta_{ST,R}\delta^R_{S,T} = \delta_{S,TR}\delta_{T,R},$$

а матрица, стоящая справа, — элемент $c_{1,R,TR}\delta_{S,TR}$. Следовательно, нужно положить

$$c_{1,R,TR} = \delta_{T,R}. \tag{11}$$

На основании формулы (11) нётерова система факторов оказывается известной, как только задана брауэрова система. Но нётеровой системой факторов структура алгебры K_r вполне определяется. Мы получили следующее утверждение:

Полем разложения Δ и системой факторов $\{c_{\alpha\beta\gamma}\}$ брауэров класс алгебр определяется однозначно.

На основе проведенных выше рассуждений о системе факторов произведения алгебр мы построили некоторый гомоморфизм из группы Брауэра классов алгебр с фиксированным полем разложения Δ в группу классов ассоциированных с ними систем факторов. В силу доказанной однозначности этот гомоморфизм является *изоморфизмом*.

Легко понять, что соотношение ассоциативности (13) из § 94 является следствием требований а), б), в), наложенных на элементы $c_{\alpha\beta\gamma}$. *Следовательно, каждой системе элементов $c_{\alpha\beta\gamma}$ данного поля, подчиненных требованиям* а), б), в), *соответствует некоторый класс алгебр, представляемый скрещенным произведением с системой факторов $\delta_{S,T}$, определенной равенством* (11).

С помощью равенства (11) основные свойства брауэровых систем факторов переносятся на нётеровы. В частности, именно так получается изоморфизм группы классов алгебр с фиксированным нормальным полем разложения и группы классов ассоциированных с этими алгебрами (нётеровых) систем факторов. Отметим специально следующее утверждение:

Скрещенное произведение K_r является полным матричным кольцом над основным полем P тогда и только тогда, когда система факторов $\delta_{S,T}$ этой алгебры ассоциирована с единичной системой:

$$\delta_{S,T} = \frac{c_S^T c_T}{c_{ST}}.$$

Задача 1. При любом расширении основного поля P до поля Λ тело K переходит в простую алгебру K_Λ. Доказать, что при этом брауэрова система факторов следующим образом «укорачивается»: вложим поля Δ и Λ в какое-нибудь общее для них расширение и найдем элементы θ_α, сопряженные с θ относительно нового основного поля Λ; факторы $c_{\alpha\beta\gamma}$, соответствующие этим элементам θ_α, сохранятся, а остальные окажутся отброшенными. На языке нётеровых систем факторов это означает, что сохраняются лишь те $\delta_{S,T}$, для которых S и T принадлежат определенной (какой именно?) подгруппе группы Галуа

Задача 2. С помощью задачи 1 ответить на следующий вопрос: какие подполя поля Σ являются полями разложения алгебры с системой факторов $\delta_{S,T}$?

Задача 3. Две циклические алгебры (δ, Σ, S) и (ε, Σ, S) изоморфны тогда и только тогда, когда δ и ε отличаются лишь множителем, являющимся нормой. В частности, (δ, Σ, S) тогда и только тогда является полным матричным кольцом над P, когда δ является нормой некоторого элемента из Σ.