§ 7. Полуторалинейная двойственность

Существуют формы „почти“ билинейные, для которых описанные выше результаты остаются верными почти без изменений; их нужно рассмотреть отдельно для сохранения ясности в используемых обозначениях.

Пусть R имеет автоморфизм периода 2. Мы будем записывать этот автоморфизм так: $a \mapsto \bar{a}$ (имея в виду аналогию с комплексным сопряжением).

Следуя Бурбаки, будем говорить, что отображение

$$f\colon E \times F \to R$$

является *полуторалинейной формой*, если оно $\mathbf{Z}$-билинейно и если для $x \in E$, $y \in F$ и $a \in R$ мы имеем

$$f(ax, y) = af(x, y)$$

и

$$f(x, ay) = \bar{a}f(x, y).$$

Пусть E, E' — модули. Отображение $\varphi\colon E \to E'$ называется *антилинейным* (или *полулинейным*), если оно $\mathbf{Z}$-линейно и $\varphi(ax) = \bar{a}\varphi(x)$ для всех $x \in E$. Таким образом, мы можем сказать, что полуторалинейная форма линейна по своему первому аргументу и антилинейна по второму аргументу. Пусть $\overline{\mathrm{Hom}}_R(E, E')$ обозначает модуль антилинейных отображений E в E'.

Теперь мы последовательно повторим все те замечания, которые раньше были сделаны для билинейных форм.

Для полуторалинейной формы f определяем, как и прежде, перпендикулярность, а также ядра справа и слева. Эти ядра являются подмодулями, скажем, E_0 и F_0, и мы получаем индуцированную полуторалинейную форму

$$E/E_0 \times F/F_0 \to R,$$

которая невырождена с обеих сторон.

Пусть F — R-модуль. Назовем его *антимодулем* модуль $\bar{E}$, аддитивная группа которого та же, что и у F, а операция $R \times \bar{F} \to \bar{F}$ задается отображением

$$(a, y) \mapsto \bar{a}y.$$

Имеем естественный изоморфизм R-модулей

$$\mathrm{Hom}_R(\bar{F}, R) \leftrightarrow \overline{\mathrm{Hom}}_R(F, R).$$

Полуторалинейная форма $f\colon E \times F \to R$ индуцирует линейное отображение

$$\varphi_f\colon E \to \mathrm{Hom}_R(\bar{F}, R).$$

Мы говорим, что f — *неособая слева*, если φ_f — изоморфизм. Аналогично имеем соответствующее линейное отображение

$$\varphi'_f\colon \bar{F} \to \mathrm{Hom}_R(E, R)$$

модуля $\bar{F}$ в модуль, дуальный к E, и мы говорим, что f — *неособая справа*, если φ'_f — изоморфизм. Мы говорим, что форма f *неособая*, если она неособая слева и справа.

Заметим, что наша полуторалинейная форма f может рассматриваться как билинейная форма

$$f\colon E \times \bar{F} \to R$$

и наши понятия неособости совместимы с соответствующими понятиями, определенными раньше для билинейных форм.

Имея фиксированную неособую полуторалинейную форму на $E \times F$, мы получаем зависящий от этой формы изоморфизм между модулем полуторалинейных форм на $E \times F$ и модулем эндоморфизмов модуля E. Мы также получаем антиизоморфизм между этими модулями и модулем эндоморфизмов модуля F. В частности, мы можем ввести понятие *сопряженного эндоморфизма*, обозначаемого в случае полуторалинейных форм звездочкой. Именно, пусть $f\colon E \times F \to R$ — неособая полуторалинейная форма, $A\colon E \to E$ — некоторое линейное отображение. Существует однозначно определенное линейное отображение

$$A^*\colon F \to F,$$

такое, что

$$\langle Ax, y\rangle = \langle x, A^*y\rangle$$

для всех $x \in E$ и $y \in F$. Отметим, что A^* линейно, а не антилинейно. Мы называем A^* *сопряженным* с A относительно нашей формы f. Имеют место правила

$$(cA)^* = \bar{c}A^*, \quad (A + B)^* = A^* + B^*, \quad (AB)^* = B^*A^*$$

для линейных отображений A, B модуля E в себя и $c \in R$.

Предположим, что $E = F$. Пусть $f\colon E \times E \to R$ — полуторалинейная форма. Под *автоморфизмом* формы f мы будем понимать линейное отображение $A\colon E \to E$, для которого

$$\langle Ax, Ay\rangle = \langle x, y\rangle,$$

в полной аналогии с автоморфизмами для билинейных форм.

Предложение 11П. *Пусть $f\colon E \times E \to R$ — неособая полуторалинейная форма, $A\colon E \to E$ — некоторое линейное отображение. Тогда A является автоморфизмом f в том и только в том случае, если $A^*A = \mathrm{id}$ и A обратимо.*

Доказательства этого, а также всех последующих предложений, полностью аналогичные соответствующим доказательствам из билинейного случая, опускаются.

Полуторалинейная форма $g\colon E \times E \to R$ называется *эрмитовой*, если

$$g(x, y) = \overline{g(y, x)}$$

для всех $x, y \in E$. Множество эрмитовых форм на E будет обозначаться через $L_h^2(E)$. Пусть R_0 — подкольцо в R, состоящее из всех элементов, неподвижных относительно нашего автоморфизма $a \mapsto \bar{a}$ (т. е. состоящее из всех элементов $a \in R$, таких, что $a = \bar{a}$). Тогда $L_h^2(E)$ есть R_0-модуль.

Фиксируем некоторую эрмитову неособую форму $f\colon (x, y) \mapsto \langle x, y\rangle$ на E. Эндоморфизм $A\colon E \to E$ называется *эрмитовым* относительно f, если $A^* = A$. Ясно, что множество эрмитовых эндоморфизмов является R_0-модулем, который мы будем обозначать символом $\operatorname{Herm}(E)$. *Имеет место R_0-изоморфизм, зависящий от нашей фиксированной эрмитовой неособой формы f,*

$$\boxed{L_h^2(E) \longleftrightarrow \operatorname{Herm}(E)}\,.$$

Этот изоморфизм описывается следующим образом. Эрмитова форма g тогда и только тогда соответствует эрмитову отображению A, когда

$$g(x, y) = \langle Ax, y\rangle$$

для всех $x, y \in E$.

Опишем теперь связи между нашими понятиями и матрицами, так же как это мы сделали для билинейных форм.

Начнем с полуторалинейной формы $f\colon E \times F \to R$.

Если E, F — свободные модули и мы, как и прежде, выбрали в них базисы, то снова можно сопоставить нашей форме матрицу G, и в терминах координатных векторов X, Y эта полуторалинейная форма будет задаваться отображением

$$(X, Y) \mapsto {}^tXG\overline{Y},$$

где $\overline{Y}$ — вектор, полученный из Y применением нашего автоморфизма к каждой компоненте Y.

Если $E = F$ и мы используем один и тот же базис и справа, и слева, то в тех же обозначениях, которые использованы в формуле (1), последняя для полуторалинейных форм f принимает вид

$$M_{\mathscr{C}}^{\mathscr{C}}(f) = {}^tCM_{\mathscr{B}}^{\mathscr{B}}(f)\,\overline{C}. \qquad (1\ \Pi)$$

Таким образом, в формуле *появляется автоморфизм сопряжения.*

Предложение 12 П. *Пусть E, F — свободные модули размерности n над R и f: $E \times F \to R$ — полуторалинейная форма. Тогда следующие условия эквивалентны:*

Форма f — неособая слева.

Форма f — неособая справа.

Форма f — неособая.

Определитель матрицы f относительно любых базисов обратим в R.

Предложение 13 П. *Пусть E, F — свободные модули размерности n над R, f: $E \times F \to R$ — полуторалинейная форма. Пусть $\mathscr{B}$, $\mathscr{B}'$ — базисы над R для E и F соответственно и G — матрица f относительно этих базисов. Пусть, наконец, A: $E \to E$ — линейное отображение и M — его матрица относительно $\mathscr{B}$. Тогда матрицей относительно $\mathscr{B}'$ сопряженного к A отображения A^* будет*

$$(\overline{G}^{-1})^t\, \overline{M}\overline{G}.$$

Следствие 1. *Если G — единичная матрица, то матрица отображения A^* равна ${}^t\overline{M}$.*

Следствие 2. *Сохраняя обозначения предложения, положим $E = F$ и $\mathscr{B} = \mathscr{B}'$. Матрица M размера $n \times n$ тогда и только тогда является матрицей автоморфизма формы f (относительно нашего базиса), когда*

$${}^tMG\overline{M} = G.$$

Матрица M называется *эрмитовой*, если ${}^tM = \overline{M}$.

Пусть, как и прежде, R_0 — подкольцо в R, состоящее из всех элементов, неподвижных относительно нашего автоморфизма $a \mapsto \overline{a}$ (т. е. состоящее из всех элементов $a \in R$, таких, что $a = \overline{a}$).

Предложение 14 П. *Пусть E — свободный модуль размерности n над R и $\mathscr{B}$ — его базис. Отображение*

$$f \mapsto M^{\mathscr{B}}_{\mathscr{B}}(f)$$

индуцирует R_0-изоморфизм между R_0-модулем эрмитовых форм на E и R_0-модулем эрмитовых матриц размера $n \times n$ над R.

Замечание. Если бы мы предположили с самого начала, что наш автоморфизм $a \mapsto \overline{a}$ имеет период 2 или 1 (т. е. если бы мы позволили ему быть тождественным), то результаты о билинейных и симметрических формах стали бы частными случаями результатов этого параграфа. Однако неудобства, которые причинила бы путаница в обозначениях, вполне оправдывают сделанное нами повторение.

Терминология

По некоторой странной причине группа автоморфизмов симметрической (соответственно знакопеременной или эрмитовой) формы на векторном пространстве называется *ортогональной* (соответственно *симплектической* или *унитарной*) группой этой формы. Слово „ортогональный“ особенно неудачно, так как ортогональное отображение сохраняет не только ортогональность — оно сохраняет также скалярное произведение, т. е. длину. Далее, слово „симплектический“ также неудачно. Дело в том, что часто рассматривают эрмитовы формы над некоторыми телами (обладающими автоморфизмами порядка 2), и их группы автоморфизмов также были названы симплектическими, что создает настоящую путаницу с использованием этого слова применительно к знакопеременным формам.

Я обсуждал с несколькими лицами вопрос, как унифицировать и улучшить терминологию, и нам кажется, что можно было бы принять следующие соглашения.

Как сказано в тексте, группа автоморфизмов любой формы f обозначается символом $\mathrm{Aut}(f)$.

С другой стороны, имеется стандартная форма, которая над полем вещественных чисел выражается через координаты в виде

$$f(x, x) = x_1^2 + \ldots + x_n^2,$$

над полем комплексных чисел

$$f(x, x) = x_1\bar{x}_1 + \ldots + x_n\bar{x}_n$$

и над телом кватернионов — посредством той же формулы, что и в комплексном случае. Группу автоморфизмов этой формы следовало бы называть *унитарной группой* и обозначать через U_n. Группы точек из U_n в поле вещественных чисел (соответственно в поле комплексных чисел или в теле кватернионов) тогда обозначались бы через

$$U_n(\mathbf{R}), \quad U_n(\mathbf{C}), \quad U_n(\mathbf{K}),$$

и эти три группы назывались бы *вещественной унитарной группой* (соответственно *комплексной унитарной группой* или *кватернионной унитарной группой*). Аналогично группа точек из U_n в любом подполе или подкольце k тела кватернионов обозначалась бы через $U_n(k)$.

Наконец, если f — стандартная знакопеременная форма, задаваемая матрицей

$$\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix},$$

то ее группу автоморфизмов можно было бы обозначать через A_{2n} и называть *группой знакопеременной формы* или просто *знакопере-*

менной группой, если нет опасности спутать ее со знакопеременной группой перестановок. Группа точек группы знакопеременной формы в поле k обозначалась бы тогда через $A_{2n}(k)$.

Как обычно, подгруппа в $\mathrm{Aut}(f)$, состоящая из тех элементов, определитель которых равен 1, обозначалась бы добавлением впереди буквы S и называлась бы по-прежнему *специальной группой*. В четырех стандартных случаях это дает $SU_n(\mathbf{R})$, $SU_n(\mathbf{C})$, $SU_n(\mathbf{K})$, $SA_{2n}(k)$.

УПРАЖНЕНИЯ

1. Интерпретировать ранг матрицы A в терминах размерности образа и ядра линейного отображения L_A.

2. Пусть $\mathfrak{g}$ — модуль над коммутативным кольцом R. Говоря, что билинейное отображение $\mathfrak{g}\times\mathfrak{g}\to\mathfrak{g}$, записываемое в виде $(x, y)\mapsto[x, y]$, наделяет $\mathfrak{g}$ структурой *алгебры Ли*, если $[x, x]=0$ и

$$[[x, y], z]+[[y, z], x]+[[z, x], y]=0$$

для всех $x, y, z\in\mathfrak{g}$.

(а) Пусть $M_n(R)$ — кольцо матриц над R. Показать, что если $x, y\in M_n(R)$, то произведение

$$(x, y)\mapsto[x, y]=xy-yx$$

превращает $M_n(R)$ в алгебру Ли.

(б) Пусть $\mathfrak{g}$ — алгебра Ли. Сопоставим всякому элементу $x\in\mathfrak{g}$ линейное отображение $\mathrm{ad}x$, задаваемое формулой $(\mathrm{ad}x)(y)=[x, y]$. Показать, что $\mathrm{ad}x$ — дифференцирование $\mathfrak{g}$ в себя (т. е. удовлетворяет правилу $D([x, y])=$ $=[Dx, y]+[x, Dy]$).

(в) Показать, что отображение $x\mapsto\mathrm{ad}\,x$ является гомоморфизмом алгебры Ли $\mathfrak{g}$ в модуль дифференцирований $\mathfrak{g}$ в себя [1]).

3. Если задано некоторое множество многочленов $\{P_\nu(X_{ij})\}$ в кольце многочленов $R[X_{ij}]$ $(1\leqslant i, j\leqslant n)$, то нуль этого множества в R — это всякая матрица $x=(x_{ij})$, такая, что $x_{ij}\in R$ и $P_\nu(x_{ij})=0$ для всех ν. Используя векторные обозначения, пишем $(X)=(X_{ij})$. Пусть $G(R)$ обозначает множество нулей нашего множества многочленов $\{P_\nu\}$. Таким образом, $G(R)\subset$ $\subset M_n(R)$, и если R' — произвольная коммутативная ассоциативная R-алгебра, то $G(R')\subset M_n(R')$. Мы будем говорить, что множество $\{P_\nu\}$ определяет *алгебраическую группу* над R, если $G(R')$ есть подгруппа группы $GL_n(R')$ для всех R' (где $GL_n(R')$ — мультипликативная группа обратимых матриц в R').

Например, группа матриц, удовлетворяющих уравнению ${}^tXX=I_n$, является алгебраической группой.

Пусть $R'=R[t]$ — R-алгебра, которая свободна как R-модуль с базисом $\{1, t\}$, где $t^2=0$. Обозначим через $\mathfrak{g}$ множество матриц $x\in M_n(R)$, таких, что $I_n+tx\in G(R[t])$. Показать, что $\mathfrak{g}$ — алгебра Ли. [*Указание*: заметить, что

$$P_\nu(I_n+tX)=P_\nu(I_n)+\mathrm{grad}\,P_\nu(I_n)\,tX.$$

[1]) Дифференцирования образуют алгебру Ли относительно операции $[D_1, D_2]=D_1D_2-D_2D_1$. — *Прим. ред.*

Использовать алгебру $R[t, u]$, где $t^2 = u^2 = 0$, чтобы показать, что если $I_n + tx \in G(R[t])$ и $I_n + uy \in G(R[u])$, то $[x, y] \in \mathfrak{g}$.]

(Я взял предыдущее из первых четырех страниц записок Серра по группам и алгебрам Ли (Serre J.-P., Lie algebras and Lie groups, New York — Amsterdam, 1965 (готовится русский перевод в изд-ве „Мир")). За дальнейшей информацией, помимо записок Серра, можно обращаться к книгам Джекобсона, Бурбаки и др.)

4. Пусть E — конечное расширение поля k. Возьмем элемент $\alpha \in E$ и рассмотрим k-линейное отображение $f_\alpha: E \to E$, для которого $f_\alpha(x) = \alpha x$. Показать, что след этого линейного отображения совпадает со следом $\mathrm{Tr}_k^E(\alpha)$, определенным в теории полей. [*Указание*: сначала предположить, что $E = k(\alpha)$, взять в качестве базиса степени α и вычислить след f_α относительно этого базиса. Какова будет матрица f_α относительно этого базиса?]

5. Пусть E — конечное расширение поля k. Показать, что норма $N_k^E(\alpha)$ равна определителю $\det(f_\alpha)$ (обозначения из предыдущего упражнения).

6. Пусть A — обратимая матрица над коммутативным кольцом R. Показать, что $({}^tA)^{-1} = {}^t(A^{-1})$.

7. Пусть f — неособая билинейная форма на модуле E над R. Пусть A — R-автоморфизм модуля E. Показать, что $({}^tA)^{-1} = {}^t(A^{-1})$. Доказать то же самое в эрмитовом случае, т. е. что $(A^*)^{-1} = (A^{-1})^*$.

8. Пусть $A_1, \ldots, A_r$ — строки размерности n над полем k. Пусть $X = (x_1, \ldots, x_n)$ и $b_1, \ldots, b_r \in k$. Под системой линейных уравнений над k понимают систему типа

$$A_1 \cdot X = b_1, \ \ldots, \ A_r \cdot X = b_r.$$

Если $b_1 = \ldots = b_r = 0$, то говорят, что система *однородная*. Мы называем n числом неизвестных, а r — числом уравнений. Решение X однородной системы называется *тривиальным*, если $x_i = 0$, $i = 1, \ldots, n$.

(а) Показать, что однородная система из r линейных уравнений с n неизвестными при $n > r$ всегда имеет нетривиальное решение.

(б) Пусть L — система однородных линейных уравнений над полем k, причем k — подполе в k'. Показать, что если L имеет нетривиальное решение в k', то она имеет нетривиальное решение также в k.

9. Пусть M — матрица размера $n \times n$ над полем k. Предположим, что $\mathrm{tr}(MX) = 0$ для всех матриц X размера $n \times n$ над k. Показать, что $M = 0$.

10. Пусть S — некоторое множество матриц размера $n \times n$ над полем k. Показать, что столбец $X \neq 0$ размерности n над k такой, что $MX = X$ для всех $M \in S$ существует в том и только в том случае, если такой столбец существует над некоторым расширением k' поля k.

11. Пусть $\mathbf{K}$ — тело над полем вещественных чисел, порожденное элементами i, j, k, такими, что $i^2 = j^2 = k^2 = -1$ и

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Тогда $\mathbf{K}$ обладает антиавтоморфизмом порядка 2, задаваемым отображением

$$a_0 + a_1 i + a_2 j + a_3 k \longmapsto a_0 - a_1 i - a_2 j - a_3 k.$$

Обозначим этот антиавтоморфизм так: $\alpha \mapsto \bar{\alpha}$. Чему равно $\alpha\bar{\alpha}$? Показать, что теория эрмитовых форм может быть построена над телом **K**, которое называется телом *кватернионов*.

12. Пусть $f_{11}, \ldots, f_{1n}$ — многочлены от n переменных над полем k, которое можно считать алгебраически замкнутым. Предположим, что эти многочлены порождают единичный идеал в кольце многочленов $k[X_1, \ldots, X_n]$. Выяснить, существуют ли многочлены f_{ij}, такие, что определитель

$$\begin{vmatrix} f_{11} & f_{12} & \ldots & f_{1n} \\ f_{21} & f_{22} & \ldots & f_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ f_{n1} & f_{2n2} & \ldots & f_{nn} \end{vmatrix}$$

равен 1. (Это очень интересная проблема, которая впервые возникла, когда Серр пытался узнать, является ли всякий конечно порожденный проективный модуль над кольцом многочленов свободным. Ответ на нее до сих пор неизвестен (при $n \geqslant 3$). Однако если $f_{11}, \ldots, f_{1n}$ берутся из целостного кольца главных идеалов, то аналогичная задача является легким упражнением.)

13. Пусть A, B — квадратные матрицы одного и того же размера над полем k. Предположим, что B неособая (т. е. обратимая). Показать, что если t — переменная, то $\det(A+tB)$ является многочленом от t, старший коэффициент которого есть $\det(B)$, а свободный член равен $\det(A)$.