

ЛЕКЦИЯ 19

ТЕОРЕМА ФРОБЕНИУСА

ПРЕДСТАВЛЕНИЯ ГРУПП

ТЕОРЕМА ФРОБЕНИУСА

Напомним предложение, которое мы доказали на прошлой лекции:

ПРЕДЛОЖЕНИЕ 1. *В ассоциативной алгебре A с единицей размерности n над полем K каждый элемент является корнем многочлена $\mu_a \in K[x]$ степени $\leq n$.*

Элемент $a \in A$ обратим тогда и только тогда, когда $\mu_a(0) \neq 0$.

Если в A нет делителей нуля, то A — алгебра с делением. Если при этом поле K алгебраически замкнуто, то $n = 1$ и $A = K$.

А теперь снова сформулируем теорему Фробениуса:

ТЕОРЕМА 1 (ТЕОРЕМА ФРОБЕНИУСА). *Над полем $\mathbb{R}$ существует только три конечномерные ассоциативные алгебры с делением: $\mathbb{R}$, $\mathbb{C}$ и $\mathbb{H}$.*

Прежде, чем доказывать теорему, исследуем аддитивную структуру алгебры с делением A .

Как мы видели, у каждого элемента из A есть некоторый минимальный аннулирующий многочлен $\mu_a(t)$, из рассуждений прошлого предложения видно, что он обязательно неприводим.

Так как многочлены мы рассматриваем над полем $\mathbb{R}$, то неприводимые многочлены имеют вид

$$\mu_a(t) = t - \alpha,$$

либо

$$\mu_a(t) = t^2 - 2\alpha t + \beta,$$

где

$$\alpha^2 < \beta.$$

В первом случае $a \in \mathbb{R}$. Если это не так, то положим $b = a - \alpha$, получим тогда

$$\mu_b(t) = t^2 + (\beta - \alpha^2).$$

Значит, каждый элемент алгебры A имеет вид $\alpha + y$, где $\alpha \in \mathbb{R}$, $y = 0$ или $y^2 = \gamma < 0$, $\gamma \in \mathbb{R}$.

Для дальнейшего доказательства нам понадобится лемма.

ЛЕММА 1. *Подмножество*

$$A' = \{u \in A \mid u^2 \in \mathbb{R}, u^2 \leq 0\}$$

является векторным подпространством в A .

Доказательство. Ясно, что если $u \in A'$, $\alpha \in \mathbb{R}$, то $\alpha u \in A'$, поэтому достаточно убедиться, что из $u, v \in A'$ следует $u + v \in A'$ для двух произвольных непропорциональных векторов u, v .

Сначала проверим, что линейная зависимость

$$u = \alpha v + \beta, \quad \alpha, \beta \in \mathbb{R},$$

невозможна.

В самом деле, по условию $uv \neq 0$, и

$$u^2 = \gamma < 0, \quad v^2 = \delta < 0.$$

Поэтому

$$u = \alpha v + \beta \implies \gamma = u^2 = (\alpha v + \beta)^2 = \alpha^2 \delta + 2\alpha\beta v + \beta^2.$$

Так как $v \notin \mathbb{R}$, то $\alpha\beta = 0$, т.е. или $\alpha = 0$, или $\beta = 0$.

Если $\alpha = 0$, то $u \in \mathbb{R}$, а если $\beta = 0$, то u пропорционально v . Обе возможности были исключены.

Итак, линейная независимость $u, v \in A'$ приводит к линейной независимости $1, u, v$. Оба элемента $u+v$, $u-v$ — корни квадратных уравнений, т.е.

$$(u+v)^2 = p(u+v)+q, \quad (u-v)^2 = r(u-v)+s, \quad p, q, r, s \in \mathbb{R}.$$

Используя соотношения

$$(u \pm v)^2 = u^2 \pm (uv + vu) + v^2, \quad u^2 = \gamma, v^2 = \delta,$$

будем иметь

$$\begin{aligned} \gamma + \delta + (uv + vu) &= p(u + v) + q, \\ \gamma + \delta - (uv + vu) &= r(u - v) + s. \end{aligned}$$

Складывая, находим

$$(p + r)u + (p - r)v + (q + s - 2\gamma - 2\delta) = 0.$$

Но, как мы видели, $u, v, 1$ линейно независимы, поэтому $p = r = 0$.

Значит, $(u + v)^2 = q \in \mathbb{R}$, а так как $u + v \notin \mathbb{R}$, то $q < 0$. Это и значит, что $u + v \in A'$, т.е. A' — подпространство в A . $\square$

Теперь мы можем перейти к доказательству самой теоремы.

Для $u \in A'$ запишем

$$u^2 = -q(u),$$

где $q(u) \in \mathbb{R}_+$.

Кроме того, $q(u) = 0 \Leftrightarrow u = 0$. Очевидно, что

$$q(\alpha u) = \alpha^2 q(u)$$

и

$$f(u, v) := q(u + v) - q(u) - q(v) = -(uv + vu)$$

— симметричная билинейная форма на A , отвечающая положительно определенной квадратичной форме q .

Если $A = \mathbb{R}$, то рассуждения заканчиваются.

Пусть $A \neq \mathbb{R}$. Тогда $A' \neq 0$ и мы можем выбрать вектор $\mathbf{i} \in A$, для которого $q(\mathbf{i}) = 1$, т.е. $\mathbf{i}^2 = -1$.

С точностью до изоморфизма получаем равенство

$$\mathbb{R}[\mathbf{i}] = \mathbb{C} = \mathbb{R} + \mathbb{R}\mathbf{i}.$$

Если $A = \mathbb{C}$, то наши рассуждения заканчиваются.

Теперь предположим, что A — шире, чем комплексные числа (как мы видели, мы можем считать, что $\mathbb{C} \subset A$).

В этом случае A' — шире, чем $\mathbb{R}\mathbf{i}$, поэтому можно выбрать элемент $\mathbf{j} \perp \mathbb{R}\mathbf{i}$, $q(\mathbf{j}) = 1$.

В этом случае $\mathbf{j}^2 = -1$ и $\mathbf{ij} + \mathbf{ji} = -f(\mathbf{i}, \mathbf{j}) = 0$, т.е. $\mathbf{ij} = -\mathbf{ji}$. Полагая $\mathbf{k} = \mathbf{ij}$, получим $\mathbf{k}^2 = -1$, $\mathbf{ik} + \mathbf{ki} = 0 = \mathbf{jk} + \mathbf{kj}$.

Следовательно, $\mathbf{k} \in A'$ и $\mathbf{k} \perp \mathbf{i}, \mathbf{j}$. Значит, $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ линейно независимы и

$$\mathbb{R} + \mathbb{R}\mathbf{i} + \mathbb{R}\mathbf{j} + \mathbb{R}\mathbf{k} = \mathbb{H}$$

— алгебра кватернионов.

Если A шире, чем алгебра кватернионов, то существует $\mathbf{l} \in A'$ такое, что $q(\mathbf{l}) = 1$ и $\mathbf{l} \perp \mathbf{i}, \mathbf{j}, \mathbf{k}$. Другими словами,

$$\mathbf{li} = -\mathbf{il}, \quad \mathbf{lj} = -\mathbf{jl}, \quad \mathbf{lk} = -\mathbf{kl}.$$

Однако в силу ассоциативности умножения в A первые два соотношения дают

$$\mathbf{lk} = \mathbf{l}(\mathbf{ij}) = (\mathbf{li})\mathbf{j} = -(\mathbf{il})\mathbf{j} = -\mathbf{i}(\mathbf{lj}) = \mathbf{i}(\mathbf{j}\mathbf{l}) = (\mathbf{ij})\mathbf{l} = \mathbf{kl}.$$

Получается противоречие. Значит,

$$A = \mathbb{H}.$$

ПРЕДСТАВЛЕНИЯ ГРУПП: ОПРЕДЕЛЕНИЯ И ПРИМЕРЫ

ОПРЕДЕЛЕНИЕ 1. Пусть G — группа, $\mathbb{F}$ — поле. Тогда любой гомоморфизм $\varphi : G \rightarrow \mathrm{GL}_n(\mathbb{F}) = \mathrm{GL}(V)$ называется *n -мерным представлением группы G над полем $\mathbb{F}$* . Если поле $\mathbb{F}$ — это поле комплексных чисел, то представление называется *комплексным*. Если ядро гомоморфизма φ тривиально, то представление называется *точным*.

ПРИМЕР 1. Для группы $G = \mathbf{S}_n$ и любого поля $\mathbb{F}$ можно рассмотреть точное n -мерное представление этой группы, при котором подстановка σ переходит в матрицу

$$(\delta_{i\sigma(i)}).$$

ПРИМЕР 2. Группа $\mathrm{SL}_n(\mathbb{F})$ имеет n -мерное точное представление над полем $\mathbb{F}$, при котором каждая матрица переходит тождественно в себя.

ПРИМЕР 3. Произвольная конечная циклическая группа $\mathbf{Z}_n$ имеет ровно n разных комплексных одномерных представлений: образующий переходит в корень n -й степени из единицы.

ПРИМЕР 4. Построим двухмерное точное представление группы кватернионов $\mathbb{Q}_8$:

$$\pm 1 \mapsto \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix};$$

$$\pm \mathbf{i} \mapsto \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix};$$

$$\pm \mathbf{j} \mapsto \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix};$$

$$\pm \mathbf{k} \mapsto \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

НЕПРИВОДИМЫЕ ПРЕДСТАВЛЕНИЯ

ОПРЕДЕЛЕНИЕ 2. Пусть $\varphi : G \rightarrow \text{GL}(V)$ — некоторое конечномерное представление группы G . Подпространство U пространства V называется *инвариантным для представления φ* , если для любого $g \in G$ подпространство U является инвариантным для оператора $\varphi(g)$.

ПРИМЕР 5. Если рассматривать представление их первого примера (представление группы $\mathbf{S}_n$ мономиальными матрицами), то инвариантным подпространством является прямая, натянутая на вектор $e_1 + e_2 + \cdots + e_n$. Действительно, так образ любой подстановки $\sigma \in \mathbf{S}_n$ переставляет базисные векторы соответственно данной подстановке, то

$$\begin{aligned}\varphi(\sigma)(e_1 + \cdots + e_n) &= e_{\sigma(1)} + \cdots + e_{\sigma(n)} = \\ &= e_1 + e_2 + \cdots + e_n.\end{aligned}$$

ПРИМЕР 6. Рассмотрим теперь представление группы $\mathbb{Q}_8$ из четвертого примера.

Предположим, что у этого представления есть нетривиальное (не равное 0 и всему пространству V) представление. Так как все представление двумерно, то данное инвариантное пространство должно быть одномерно, то есть его векторы — собственные для всех образов $\varphi(g)$, $g \in \mathbb{Q}_8$.

У оператора $\varphi(i) = \text{diag}[i, -i]$ собственные прямые — это только $\langle e_1 \rangle$ и $\langle e_2 \rangle$. Однако обе эти прямые не являются инвариантными для оператора

$$\varphi(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Значит, у данного представления есть только тривиальные инвариантные подпространства.

ОПРЕДЕЛЕНИЕ 3. Если у представления $\varphi : G \rightarrow \text{GL}(V)$ есть нетривиальное инвариантное подпространство, то оно называется *приводимым*. В противном случае представление φ называется *неприводимым*. Представление называется *вполне приводимым*, если пространство V раскладывается в прямую сумму инвариантных относительно φ подпространств, на которых φ является неприводимым (т. е. представление φ является прямой суммой неприводимых представлений).

ПРИМЕР 7. Любое одномерное представление группы неприводимо. Как мы видели выше, приведенное двухмерное представление группы $\mathbb{Q}_8$ неприводимо.

Примером приводимого представления может служить двухмерное представление группы целых чисел $\mathbb{Z}$, при котором

$$n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Вполне приводимое представление группы $\mathbb{Z}_4$:

$$k \mapsto \begin{pmatrix} i^k & 0 \\ 0 & -i^k \end{pmatrix}.$$

ОПРЕДЕЛЕНИЕ 4. Два линейных представления

$$\varphi : G \rightarrow \mathrm{GL}_n(K) \text{ и } \psi : G \rightarrow \mathrm{GL}_n(K)$$

называются *эквивалентными* (изоморфными, подобными), если существует невырожденное линейное отображение $C \in \mathrm{GL}_n(K)$ такое, что

$$\varphi \circ A = A \circ \psi.$$

ПРЕДЛОЖЕНИЕ 2. *Отношение эквивалентности представлений действительно является отношением эквивалентности.*

ПРЕДСТАВЛЕНИЯ АБЕЛЕВЫХ ГРУПП

ПРЕДЛОЖЕНИЕ 3. *Если группа G абелева, а поле $\mathbb{F}$ алгебраически замкнуто, то неприводимыми над $\mathbb{F}$ представлениями группы G являются только одномерные представления.*

Доказательство. Так как группа G абелева, то все операторы $\varphi(g)$, $g \in G$ коммутируют.

Однако множество коммутирующих операторов всегда имеет общий собственный вектор, то есть у данного представления (если оно не одномерно) есть собственная инвариантная прямая.

Таким образом, лишь одномерные представления могут быть неприводимы.

На всякий случай напомним, как доказывается, что у множества коммутирующих операторов есть общий собственный вектор.

Если два оператора A и B коммутируют, поле $\mathbb{F}$ алгебраически замкнуто, рассмотрим некоторое собственное подпространство V_λ^A оператора A с собственным значением λ .

Рассмотрим некоторый вектор $v \in V_\lambda^A$.

Тогда

$$BA(v) = B(\lambda \cdot v) = \lambda B(v) = A(B(v)).$$

Таким образом,

$$B(v) \in V_\lambda^A,$$

то есть подпространство V_λ^A — инвариантно и для оператора B .

Значит, у оператора B на этом подпространстве есть собственный вектор u , который автоматически окажется собственным и для A .

Для произвольного множества векторов доказательство аналогично. $\square$

ПРИМЕР 8. Над полем $\mathbb{R}$ действительных чисел утверждение предыдущего предложения не будет выполняться: у абелевой группы $\mathbb{Z}_n$ ($n > 2$) можно рассмотреть двухмерное представление, при котором

$$k \mapsto \begin{pmatrix} \cos 2\pi/n & \sin 2\pi/n \\ -\sin 2\pi/n & \cos 2\pi/n \end{pmatrix}.$$

Это представление, очевидно, будет неприводимо.

Опишем теперь все неэквивалентные неприводимые представления конечно порожденной абелевой группы A над полем комплексных чисел.

Как мы уже знаем, все они одномерны.

При этом группа A раскладывается в прямую сумму конечных и бесконечных циклических групп.

Пусть, для определенности,

$$A = \oplus_k \mathbb{Z} \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_m}.$$

Обозначим образующие бесконечных циклических групп через $a_1, \dots, a_k$, а образующие групп $\mathbb{Z}_{n_1}, \dots, \mathbb{Z}_{n_m}$ — через $b_1, \dots, b_m$.

Понятно, что нам требуется построить все различные гомоморфизмы из группы A в группу $\mathbb{C}^*$.

Для этого нужно задать гомоморфизм на образующих.

Образующие $a_1, \dots, a_k$ переводятся в произвольные элементы группы $\mathbb{C}^*$, а элементы $b_1, \dots, b_m$ должны при гомоморфизме переходить в корни их единицы степеней $n_1, \dots, n_m$, соответственно (n_i вариантов для каждого b_i).

Далее отображение однозначно продолжается до гомоморфизма.

Заметим в скобках, что если группа A была конечна, то у нее будет ровно $|A|$ различных комплексных неприводимых представлений.

ЛЕММА 2. Для любого одномерного представления φ группы G (над произвольным полем) коммутант группы G содержится в ядре φ .

Доказательство. Так как группа $\mathbb{C}^*$ абелева, то одномерное представление группы G — это гомоморфизм из некоторой группы в абелеву группу. Как мы знаем, в этом случае ядро гомоморфизма содержит коммутант. $\square$

Таким образом, чтобы построить все одномерные представления группы G , нужно рассмотреть группу A — фактор группы G по ее коммутанту и построить все одномерные представления этой абелевой группы, что мы уже умеем делать.