ЛЕКЦИЯ 21

ГРУППОВЫЕ АЛГЕБРЫ

РАСШИРЕНИЯ ГАЛУА

ГРУППОВЫЕ АЛГЕБРЫ

Пусть $\mathbb{K}$ — поле, G — группа.

Рассмотрим множество $\mathbb{K}[G]$ всевозможных формальных сумм

$$\sum_g \alpha_g g, \qquad \alpha_g \in \mathbb{K}.$$

По определению

$$\sum_g \alpha_g g = \sum_g \beta_g g \Longleftrightarrow \alpha_g = \beta_g \quad \forall g \in G.$$

Введем операции над рассматриваемыми формальными суммами

$$\sum_g \alpha_g g + \sum_g \beta_g g = \sum_g (\alpha_g + \beta_g) g,$$

$$\lambda \left(\sum_g \alpha_g g \right) = \sum_g (\lambda \alpha_g) g,$$

$$\left(\sum_g \alpha_g g \right) \left(\sum_h \beta_h h \right) = \sum_{g,h} \alpha_g \beta_h (gh).$$

Такие операции задают на $\mathbb{K}[G]$ структуру ассоциативной алгебры.

Данную алгебру называют *групповой алгеброй группы G над полем $\mathbb{K}$*.

Базисными элементами пространства $\mathbb{K}[G]$ служат формальные произведения $1 \cdot g$, $g \in G$, то есть данная алгебра имеет размерность

$$\dim_{\mathbb{K}} \mathbb{K}[G] = |G|.$$

Теорема 1. *Существует взаимно однозначное соответствие между $\mathbb{K}[G]$-модулями, являющимися конечномерными векторными пространствами над $\mathbb{K}$, и линейными представлениями группы G.*

Доказательство. Пусть φ — представление группы G в пространстве V. Продолжим φ по линейности на элементы из $\mathbb{K}[G]$, определяя

$$\widetilde{\varphi}\left(\sum \alpha_g g\right) = \sum \alpha_g \varphi(g),$$

и положим

$$\left(\sum \alpha_g g\right) v = \sum \alpha_g \varphi(g) v \text{ для всех } v \in V.$$

Данная операция вводит на V структуру $\mathbb{K}[G]$-модуля в обычном понимании этого слова.

Заметим, что

$$\left(\sum \alpha_g g\right)(\lambda v) = \sum \alpha_g \varphi(g)(\lambda g) = \sum \alpha_g \lambda \varphi(g) v = \\ = \lambda \left(\sum \alpha_g \varphi(g) v\right) = \lambda \left(\left(\sum \alpha_g g\right) v\right),$$

т.е. умножение на скаляры в V и в $\mathbb{K}[G]$ согласованы.

Отображение $\widetilde{\varphi}$ естественно называть линейным представлением алгебры $\mathbb{K}[G]$.

Обратно, если V — векторное пространство над $\mathbb{K}$, являющееся модулем над $\mathbb{K}[G]$ с действием

$$\left(\sum \alpha_g g, v\right) \mapsto \left(\sum \alpha_g g\right) \circ v,$$

то, полагая

$$\widetilde{\varphi}\left(\sum \alpha_g g\right) v = \left(\sum \alpha_g g\right) \circ v,$$

мы определим гомоморфизм

$$\widetilde{\varphi} : \mathbb{K}[G] \to \operatorname{End}_{\mathbb{K}}(V)$$

(т.е. представление алгебры $\mathbb{K}[G]$), ограничение которого φ на G даст нам представление группы G. □

В соответствии с этой теоремой пространство представления V группы G часто называют *модулем представления* группы G или, коротко, G-модулем.

В этих терминах инвариантному подпространству U G-модуля V соответствует подмодуль модуля V.

Значит, неприводимому представлению соответствуют простые G-модули.

Прямым суммам представлений — прямые суммы модулей.

Вполне приводимый модуль — это тот, который раскладывается в прямую сумму простых подмодулей.

Лемма Шура в этой терминологии утверждает, что кольцо эндоморфизмов простого $\mathbb{C}[G]$-модуля изоморфно полю $\mathbb{C}$.

Теорема Машке утверждает, что при определенных условиях любой $\mathbb{K}[G]$-модуль раскладывается в прямую сумму простых подмодулей.

РАСШИРЕНИЯ ГАЛУА

Для того, чтобы ввести основные понятия теории Галуа, нам понадобятся некоторые пройденные знания о группах и о расширениях полей.

Если говорить более конкретно, мы будем опираться на два пройденных раньше предложения.

Предложение 1 (повторение). *Любое конечномерное расширение поля K — алгебраическое. Это расширение является цепочкой некоторых простых алгебраических расширений.*

Предложение 2 (повторение). *Пусть $P(\alpha)$ — расширение поля P, полученное присоединением корня α неприводимого многочлена $h \in P[x]$, и φ — гомоморфизм поля P в некоторое поле F.*

Тогда гомоморфизм φ продолжается до гомоморфизма $\psi : P(\alpha) \to F$ ровно столькими способами, сколько различных корней имеет в F многочлен $\varphi(h)$, полученный из h применением к его коэффициентам гомоморфизма φ.

Определение 1. Пусть L — конечномерное расширение поля K, $\dim_K L = n$. Группа автоморфизмов

$$\mathrm{Aut}_K L$$

— это автоморфизмы поля L, действующие на K тождественно.

Если

$$G \subset \mathrm{Aut}_K L,$$

обозначим через L^G подмножество L, состоящее из всех элементов L, инвариантных относительно G (не сдвигающихся при автоморфизмах из G).

Лемма 1. *Множество L^G является полем.*

Доказательство. Очевидная проверка. □

Предложение 3. *Имеет место*

$$|\mathrm{Aut}_K L| \leqslant n.$$

Если $|G| = n$ (то есть $G = \mathrm{Aut}_K L$), то $L^G = K$.

Доказательство. Пусть расширение L поля K есть последовательность l простых расширений $K = L_0 \subset L_1 \cdots \subset L_{l-1} \subset L_l = L$, где $\dim L_i/L_{i-1} = m_i$. Тогда $n = m_1 \dots m_l$. При каждом из расширений автоморфизм (уже продолженный на L_i) может продолжиться на L_{i+1} не более чем m_{i+1} способами. Таким образом, всего способов продолжить тождественный автоморфизм на K на поле L — не более n.

$$|G| \leqslant \dim_{L^G} L \leqslant \dim_K L = n.$$

Если же $|G| = |\operatorname{Aut}_K L| = n$, то поле L является расширением поля $L^G \supset K$, при этом размерность L над L^G не меньше порядка G, т.е. не меньше n. С другой стороны, эта размерность не больше n, так как K содержится в L^G.

Значит,

$$\dim_{L^G} L = \dim_K L,$$

откуда

$$L^G = K.$$

□

Предложение 4. *Если $L^G = K$, то для любых полей P и Q таких, что*

$$K \subset P \subset Q \subset L,$$

всякий гомоморфизм

$$\varphi : P \to L$$

над K продолжается до гомоморфизма

$$\psi : Q \to L$$

ровно $\dim_P Q$ способами.

Доказательство. Пусть $L^G = K$. Для любого элемента $\alpha \in L$ пусть

$$\{\alpha_1, \ldots, \alpha_m\}$$

— его G-орбита.

Тогда

$$f = \prod_{i=1}^{m} (x - \alpha_i) \in L^G[x] = K[x]$$

есть минимальный многочлен элемента α над K.

Действительно, любом автоморфизм $g \in G$ индуцирует перестановку корней этого многочлена, которая не меняет сам многочлен, поэтому коэффициенты многочлена f не меняются ни от одного автоморфизма $g \in G$. Так как $L^G = K$, то $f \in K[x]$.

С другой стороны, если существовал бы многочлен $h(x) \in K[x]$ меньшей степени и содержащий α в качестве корня, то все элементы вида $g\alpha$, $g \in G$ также должны были являться его корнями.

Значит, $f(x)$ — минимальный многочлен элемента α над K.

По построению он разлагается на различные линейные множители в $L[x]$.

Докажем теперь утверждение предложения.

Ясно, что можно доказывать это утверждение для простого расширения от P к Q, $Q = P(\alpha)$.

Пусть h — минимальный многочлен элемента α над P.

Тогда h делит минимальный многочлен f элемента α над K в кольце $P[x]$.

Следовательно, $\varphi(h)|f$ в кольце $\varphi(P[x])$ (так как $\varphi(f) = f$).

Значит, он разлагается на различные линейные множители в $L[x]$.

По предложению 2 гомоморфизм φ продолжается до гомоморфизма $\psi : Q \to L$ ровно $\deg h = \dim_P Q$ способами.

□

Предложение 5. *Если* $L^G = K$, *то* $|\operatorname{Aut}_K L| = n$.

Доказательство. Применяя предыдущее утверждение к случаю $P = K$, $Q = L$, получим $|\operatorname{Aut}_K L| = n$. □

Далее нам понадобиться следующая вспомогательная лемма.

Лемма 2. *Конечномерное векторное пространство над бесконечным полем не может быть покрыто конечным числом собственных подпространств.*

Доказательство. Пусть утверждение неверно, и некоторое конечномерное векторное пространство над бесконечным полем покрыто конечным числом подпространств, отличных от самого этого пространства.

Сначала последовательно ислючим все подпространства, которые содержатся в объединении остальных. Таким образом, у нас останется конечное число собственных подпространств, в каждом из которых есть вектор, не содержащийся ни в одном из остальных.

Далее выберем по вектору v_i в каждом пространстве, который не лежит в остальных.

Рассмотрим линейные комбинации

$$\alpha v_1 + v_2.$$

Какие-то две из них лежат в одном и том же подпространстве, так как поле бесконечно.

Это не может быть никакое подпространство, кроме первого, так как в ином случае вектор v_1 (как разность двух таких векторов, умноженная на число) содержался бы в каком-то пространстве, отличном от первого.

Но первое тоже не может быть — тогда с нем лежит второй вектор.

Получаем противоречие. □

Теорема 2. *Пусть G — подгруппа группы $\mathrm{Aut}_K L$, $n = \dim_K L$.*

При этих условиях $L^G = K$ тогда и только тогда, когда $|G| = n$ (то есть $G = \mathrm{Aut}_K L$).

Кроме того, если это условие выполнено, то для любых полей P и Q таких, что

$$K \subset P \subset Q \subset L,$$

всякий гомоморфизм

$$\varphi : P \to L$$

над K продолжается до гомоморфизма

$$\psi : Q \to L$$

ровно $\dim_P Q$ способами.

Доказательство. В предложении 3 было доказано, что если $|G| = n$, то $L^G = K$.

В предложении 5 было доказано, что если $L^G = K$, то $|\mathrm{Aut}_K L| = n$.

Получается, что нам достаточно доказать, что если $L^G = K$, то $G = \mathrm{Aut}_K L$.

Пусть $\varphi \in \mathrm{Aut}_K L$.

Тогда для любого $\alpha \in L$ элемент $\varphi(\alpha)$, как и α, является корнем многочлена

$$f = \prod_{i=1}^{m} (x - \alpha_i) \in L^G[x] = K[x]$$

т. е. существует такой элемент $g = g_\alpha \in G$ (быть может, зависящий от α), что $\varphi(a) = ga$.

Если поле L конечно, то в качестве α возьмем элемент, порождающий группу L^* (которая, как мы знаем, является циклической), и тогда мы получим, что

$$\varphi = g \in G.$$

Если же L (и, стало быть, K) бесконечно, то для каждого $g \in G$ положим

$$L_g = \{\alpha \in L : \varphi(\alpha) = g\alpha\} \subset L.$$

Очевидно, что L_g — подпространство над K (и даже подполе в L). Из доказанного следует, что

$$L = \bigcup_{g \in G} L_g.$$

Отсюда мы получаем, что на самом деле $L = L_g$ для некоторого $g \in G$. □

Определение 2. Если $\dim_K L = |\operatorname{Aut}_K L|$, то L называется *расширением Галуа поля* K, группа $\operatorname{Aut}_K L$ в этом случае называется *группой Галуа* $\operatorname{Gal} L/K$.

Предложение 6. *Пусть L — расширение Галуа поля K, $K \subset P \subset L$.*

Тогда L — расширение Галуа поля P.

Доказательство. Если L — расширение Галуа поля K.

Тогда по теореме 1 для поля P такого, что

$$K \subset P \subset L$$

(полагаем в этой теореме $Q = L$), всякий гомоморфизм

$$\varphi : P \to L$$

над K продолжается до гомоморфизма

$$\psi : L \to L$$

ровно $\dim_P L$ способами.

В том числе, тождественный автоморфизм $P \to P$ продолжается $\dim_P L$ способами до эндоморфизма $L \to L$, тождественного на P. Так

как иделов в поле нет, то ядро каждого такого эндоморфизма должно быть нулевым, то есть он является автоморфизмом.

Значит, мы получили не менее $\dim_P L$ различных автоморфизмов поля L, тождественных на P, что означает, что L — расширение Галуа поля P.

□