Лекция 15.

Гайфуллин Сергей Александрович

МГУ

11 ноября, 2020

Теорема. Пусть $G \triangleright H$ и G/H – не простая группа. Тогда существует нормальная подгруппа N в G такая, что $H \subsetneq N \subsetneq G$. При этом $G \triangleright N \triangleright H$.

Доказательство. Раз G/H – не простая группа, то существует собственная нормальная подгруппа L в ней. Рассмотрим канонический гомоморфизм $\pi_H \colon G \to G/H$. Положим $N = \pi_H^{-1}(L)$. Так как подгруппа L собственная, N не совпадает ни с G, ни с H. Подгруппа N нормальна в G. В самом деле, пусть $g \in G, n \in N$. Тогда $\pi_H(gng^{-1}) = \pi_H(g)\pi_H(n)\pi_H(g)^{-1}$. При этом $\pi_H(n) \in L$, а подгруппа L нормальна в G/H. Значит, $\pi_H(gng^{-1}) \in L$, то есть $gng^{-1} \in N$, что доказывает нормальность N.

Следствие. Любая конечная группа G может быть включена в композиционный ряд, то есть ряд подгрупп $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \ldots G_n = \{e\}$ такой, что G_{i-1}/G_i простая.

Теорема (Жордан-Гельдер). Факторы G_i/G_{i+1} композиционного ряда определены однозначно с точностью до перестановки.

Пусть V – векторное пространство над некоторым полем F. Обозначим через $\mathrm{GL}(V)$ группу обратимых операторов $V \to V$.

Определение. Линейным представлением группы G называется гомоморфизм $G \to \mathrm{GL}(V)$.

Если в V выбрать базис из n векторов, то каждому оператору сопоставляется матрица $n \times n$. Это устанавливает изоморфизм между $\mathrm{GL}(V)$ и $\mathrm{GL}_n(F)$.

Определение. Матричным представлением группы G называется гомоморфизм $G \to \mathrm{GL}_n(F)$.

Выбор базиса в V устанавливает биекцию между линейными и матричными представлениями. Если выбрать другой базис, то все операторы представления сопрягутся матрицей перехода. Размерностью представления называется размерность пространства V. Мы ограничимся рассмотрением конечномерных представлений.

Пример

Отображение $\sigma \mapsto \mathrm{sgn}(\sigma)$ дает одномерное представление группы S_n.

Замечание. Одномерные представления отождествляются с гомоморфизмами $G \to F^\times$.

Пример

Пусть ε_1 и ε_2 – корни из 1 степени n. Отображение $k \mapsto \begin{pmatrix} \varepsilon_1^k & 0 \\ 0 & \varepsilon_2^k \end{pmatrix}$ дает двумерное представление группы $\mathbb{Z}_n$.

Пример

Группа $\mathrm{GL}_n(F)$ имеет естественное n-мерное представление, при котором каждая матрица переходит в себя. Такое представление называется <u>тавтологическим</u>. Аналогичное представление можно рассмотреть для любой матричной группы: $\mathrm{SL}_n(F)$, $\mathrm{O}_n(F)$ и др.

Замечание. Линейное представление задает действие группы G на V.

Определение.

Представление $G \to \mathrm{GL}(V)$ называется <u>точным</u>, если его ядро состоит только из нейтрального элемента.

Определение.

Пусть задан гомоморфизм групп $\varphi\colon G \to H$. Тогда по представлению $\rho\colon H \to \mathrm{GL}(V)$ можно построить представление $\rho \circ \varphi\colon G \to \mathrm{GL}(V)$.
Такая ситуация имеет место, например, если G – это подгруппа в H. В этом случае в качестве φ берем вложение $G \subset H$.
Полученное представление $\rho \circ \varphi\colon G \to \mathrm{GL}(V)$ называется <u>индуцированным</u> представлением.

Определение

Пусть даны представления $\rho\colon G \to \mathrm{GL}(V)$ и $\zeta\colon G \to \mathrm{GL}(W)$. Морфизмом представлений называется линейное отображение $\varphi\colon V \to W$ такое, что для каждого $g \in G$ и для каждого $v \in V$ выполнено $\varphi(\rho(g)(v)) = \zeta(g)(\varphi(v))$.
Если φ – изоморфизм векторных пространств, то мы называем его изоморфизмом представлений.

Замечание. Если ρ и ζ – изоморфные линейные представления, то пространства V и W можно отождествить по изоморфизму φ. ПРи этом базис V перейдет в базис W. Если взять эти соответствующие друг другу базисы и получить матричные представления, то получим одинаковые матричные представления.
Таким образом, матричные представления $\rho\colon G \to \mathrm{GL}_n(F)$ и $\zeta\colon G \to \mathrm{GL}_n(F)$ изоморфны тогда и только тогда, когда существует невырожденная матрица C такая, что для каждого $g \in G$ выполнено $C\rho(g)C^{-1} = \zeta(g)$.

Теорема. Существует n различных (неизоморфных) комплексных одномерных представлений группы $\mathbb{Z}_n$

Доказательство. Пусть $\rho\colon \mathbb{Z}_n \to F^\times$ – одномерное представление. Тогда $\rho(1)^n = \rho(n) = \rho(0) = 1$. То есть $\varepsilon = \rho(1)$ – корень n-ой степени из 1. При этом $\rho(k) = \varepsilon^k$, то есть образом единицы задается ρ. Получаем, что одномерных представлений группы $\mathbb{Z}_n$ столько же, сколько корней из 1 степени n, то есть n. И все они имеют вид $\rho(k) = \varepsilon^k$.

Следствие. Пусть G – абелева группа порядка n. Существует n различных (неизоморфных) комплексных одномерных представлений группы G.

Доказательство. Группа G изоморфна прямой сумме циклических групп $\mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$. Аналогично теореме элемент $(0, \ldots, 0, 1, 0, \ldots 0)$, где 1 стоит на i-м месте может переходить в любой корень n_i степени из 1. Если же $\rho((0, \ldots, 0, 1, 0, \ldots 0)) = \varepsilon_i$, то $\rho((a_1, \ldots, a_k)) = \varepsilon_1^{a_1} \ldots \varepsilon_k^{a_k}$. Число способов выбрать $\varepsilon_1, \ldots, \varepsilon_k$ равно n.

Пример

Рассмотрим следующее n-мерное представление группы S_n: перестановка σ переходит в матрицу A, где
$a_{ij} = \begin{cases} 1, & \text{если } \sigma(j) = i, \\ 0 & \text{иначе.} \end{cases}$ Такое представление называется <u>мономиальным</u>.

Например, при $n = 3$ получаем

$$\mathrm{id} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, (1,2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, (1,3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$(2,3) \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, (1,2,3) \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, (1,3,2) \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Пример

Пусть G – конечная группа порядка n. Рассмотрим n-мерное пространство FG, базисные векторы которого мы индексируем элементами группы: $e_{g_1}, \ldots, e_{g_n}$, где $G = \{g_1, \ldots, g_n\}$. Зададим представление $\rho\colon G \to \mathrm{GL}(FG)$ по правилу $\rho(g)(e_{g_i}) = e_{g \cdot g_i}$. Такое представление называется регулярным представлением группы G.

На самом деле данное представление есть композиция вложения $G \hookrightarrow S_n$, которое строится в теореме Кэли, и мономиального представления $S_n \to \mathrm{GL}_n(F)$.

На самом деле FG имеет более богатую структуру, чем просто векторное пространство. Элементы FG можно умножать друг на друга по правилу

$$(\textstyle\sum_i \lambda_i e_{g_i})(\sum_j \mu_j e_{g_j}) = \sum_{i,j} \lambda_i \mu_j e_{g_i g_j}.$$

Определение.

Множество R с двумя бинарными операциями $+$ и $\cdot$ называется <u>кольцом</u>, если выполнено

1) $(a+b)+c = a+(b+c)$,
2) существует 0 такой, что $a+0=0+a=a$,
3) для каждого a существует $(-a)$ такой, что $a+(-a)=(-a)+a=0$,
4) $a+b=b+a$,
5) $a(b+c)=ab+ac$,
6) $(a+b)c=ac+bc$.

Кольцо ассоциативно, если
7) $(ab)c=a(bc)$.

Кольцо с единицей, если
8) существует 1 такой, что $1a=a1=a$.

Кольцо коммутативно, если 9) $ab=ba$.

Коммутативное ассоциативное кольцо с единицей называется <u>полем</u>, если 10) для каждого $a \neq 0$ найдется a^{-1} такой, что $aa^{-1}=a^{-1}a=1$.

Определение.

Пусть фиксировано поле F. Множество A называется <u>алгеброй</u> (над F), если на нем определены три операции: сложение, умножение и умножение на скаляр (элемент поля F) такие, что
1) A с операциями сложения и умножения – это кольцо,
2) A с операциями сложения и умножения на скаляр – это векторное пространство над F,
3) $(\lambda a)b = \lambda(ab)$.

Пример.

Матрицы $n \times n$ образуют ассоциативную алгебру с единицей.

Упражнение.

Проверьте, что FG – это ассоциативная алгебра с единицей.
Она называется <u>групповой алгеброй</u> группы G.
В каком случае алгебра FG коммутативна?

Определение.

Пусть $\rho\colon G \to \mathrm{GL}(V)$ – линейное представление. Подпространство $U \subset V$ называется <u>инвариантным</u>, если для любого $g \in G$ выполнено $\rho(g)(U) \subset U$.

Если U – инвариантное подпространство и мы выберем базис $e_1, \ldots, e_k$ в U, а затем дополним его до базиса $e_1, \ldots, e_n$ в V, то матрицы $\rho(g)$ в базисе $e_1, \ldots, e_n$ будут иметь блочно-верхнетреугольный вид

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

Определение.

Представление $\rho\colon G \to \mathrm{GL}(V)$ называется <u>неприводимым</u> если не существует инвариантных подпространств $U \subset V$ кроме $\{0\}$ и V.

Определение.

Пусть $\rho\colon G \to \mathrm{GL}(V)$ и $\zeta\colon G \to \mathrm{GL}(W)$ – два представления одной и той же группы G. Прямой суммой представлений ρ и ζ называется представление $\rho \oplus \zeta\colon G \to \mathrm{GL}(V \oplus W)$, определенное по правилу:

$$\rho \oplus \zeta(g)(v + w) = \rho(g)(v) + \zeta(g)(w).$$

Если выбрать базис в $V \oplus W$, являющийся объединением базисов V и W, то матрица оператора $\rho \oplus \zeta(g)$ имеет в этом базисе блочно-диагональный вид

$$\begin{pmatrix} \rho(g) & 0 \\ 0 & \zeta(g) \end{pmatrix}.$$

Пример

Следующее отображение дает двумерное представление группы $\mathbb{Z}_2$:

$$\rho(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \rho(1) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Оно является прямой суммой двух одномерных.

Определение.

Представление называется <u>вполне приводимым</u>, если оно изоморфно прямой сумме неприводимых.

Замечание.

В частности любое неприводимое представление вполне приводимо.

Пусть U – инвариантное пространство представления $\rho\colon G \to \mathrm{GL}(V)$. Назовем U' <u>дополнительным</u> инвариантным пространством, если U' инвариантно и $V = U \oplus U'$.

Предложение. Если для любого инвариантного подпространства найдется дополнительное инвариантное подпространство, то представление вполне приводимо.

Доказательство. Докажем по индукции по размерности представления n. База при $n = 1$ очевидна.
Шаг индукции. Если ρ неприводимо, то оно вполне приводимо. Пусть это не так. Тогда есть инвариантное подпространство $U \subset V$. Тогда $V = U \oplus U'$. И значит, $\rho = \rho\,|_U \oplus \rho\,|_{U'}$. По предположению индукции представления $\rho\,|_U$ и $\rho\,|_{U'}$ вполне приводимы. Тогда ρ также вполне приводимо.