АЛГЕБРА, ТРЕТИЙ СЕМЕСТР

Е. Ю. СМИРНОВ

Abstract. Записки лекций по алгебре для второго курса факультета математики ВШЭ, осень 2012/13 учебного года

1. Первая лекция, 3 сентября 2012 г.

1.1. **Симметрические многочлены.** Рассмотрим кольцо многочленов от n переменных $K[x_1, \dots, x_n]$. Это множество конечных линейных комбинаций мономов вида $a_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n}$, где $a_{k_1 \dots k_n} \in K$, которые можно складывать и умножать по обычным правилам. Число $k = k_1 + \dots + k_n$ называется *степенью* монома. Степень многочлена — это максимум по степеням входящих в него мономов.

На кольце $K[x_1, \dots, x_n]$ действует симметрическая группа S_n. Её действие на образующих $x_1, \dots, x_n$ задаётся перестановками переменных: $\sigma(x_i) = x_{\sigma(i)}$, и продолжается на мономы по мультипликативности: $\sigma(a x_1^{k_1} \dots x_n^{k_n}) = x_{\sigma(1)}^{k_1} \dots x_{\sigma(n)}^{k_n}$, и далее на все многочлены по линейности.

Многочлены, инвариантные при этом действии, называются *симметрическими*.

Определение 1.1. Многочлен от n переменных называется симметрическим, если он переходит в себя при любых перестановках переменных.

Группа перестановок порождается транспозициями. Поэтому можно дать следующее определение, эквивалентное предыдущему:

Определение 1.2. Многочлен от n переменных называется симметрическим, если он переходит в себя при перестановке любых двух переменных.

Приведем примеры симметрических многочленов.

Пример 1.3 (многочлены Ньютона)**.** $s_k = x_1^k + x_2^k + \dots + x_n^k$, где $k \geq 1$.

Вы используете эти записки на свой страх и риск. Никто не гарантирует, что их текст полностью соответствует содержанию лекций. Тем более не гарантируется отсутствие в этом тексте ошибок. Впрочем, о найденных ошибках лучше сообщать автору.

Пример 1.4 (элементарные симметрические многочлены)**.** $\sigma_1 = x_1 + \dots + x_n$, $\sigma_2 = \sum_{i<j} x_i x_j$, $\sigma_k = \sum_{i_1<\dots<i_k} x_{i_1} x_{i_2} \dots x_{i_k}$, $\sigma_n = x_1 x_2 \dots x_n$. В отличие от предыдущего примера, здесь k уже не превосходит n.

Элементарные симметрические многочлены возникают в формулах Виета, связывающих коэффициенты многочлена и его корни:

Теорема 1.5 (Виет)**.** *Пусть многочлен* $p(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$ *раскладывается на линейные множители:* $p(x) = a_0 (x - t_1) \dots (x - t_n)$. *Тогда* $a_k = (-1)^k a_0 \sigma_k(t_1, \dots, t_n)$.

Поскольку сумма и произведение симметрических многочленов снова будут симметрическими, множество симметрических многочленов образует подалгебру в $K[x_1, \dots, x_n]$. Она обозначается через $K[x_1, \dots, x_n]^{S_n}$. Кроме того, эта подалгебра градуированная: если многочлен является симметрическим, то каждая его однородная компонента данной степени — снова симметрический многочлен.

Это значит, что если $F(X_1, \dots, X_m)$ — произвольный многочлен, а $f_1, \dots, f_m$ — симметрические многочлены, то многочлен $F(f_1, \dots, f_m)$, полученный в результате подстановки f_i в F, снова будет симметрическим.

Возникает задача о нахождении *системы образующих* этой алгебры: как найти такие симметрические многочлены, через которые всякий симметрический многочлен выражался бы полиномиальным образом? Оказывается, что на эту роль подходят элементарные симметрические многочлены. Кроме того, выражение многочлена через $\sigma_1, \dots, \sigma_n$ оказывается единственным. Это утверждает

1.2. Основная теорема о симметрических многочленах.

Теорема 1.6 (Основная теорема о симметрических многочленах)**.** *Всякий симметрический многочлен единственным образом представляется в виде многочлена от* $\sigma_1, \dots, \sigma_n$. *Иначе говоря, для любого симметрического многочлена* $f(x_1, \dots, x_n)$ *найдётся единственный многочлен* $F(X_1, \dots, X_n)$, *для которого* $f(x_1, \dots, x_n) = F(\sigma_1, \dots, \sigma_n)$.

Пример 1.7. Выразим s_2 через элементарные симметрические. $s_2 = x_1^2 + \dots + x_n^2 = (x_1 + \dots + x_n)^2 - 2\sum_{i<j} x_i x_j = \sigma_1^2 - 2\sigma_2$. То есть в этом случае $F(X_1, X_2) = X_1^2 - X_2$.

Мы приведём два различных доказательства основной теоремы.

Первое доказательство. Определим *лексикографическое упорядочение* на мономах от n переменных. Будем говорить, что моном $x_1^{i_1} \dots x_n^{i_n}$ *старше* монома $x_1^{j_1} \dots x_n^{j_n}$, если для некоторого индекса k имеет место неравенство $i_k > j_k$, и при этом все показатели при

предыдущих переменных равны: $i_1 = j_1$, $i_2 = j_2, \ldots$, $i_{k-1} = j_{k-1}$. Обозначение:

$$x_1^{i_1} \ldots x_n^{i_n} \succ x_1^{j_1} \ldots x_n^{j_n}.$$

Таким образом можно сравнить любые два монома, т.е. это *полный* порядок. Термин "лексикографическое упорядочение" объясняется тем, что наборы $(i_1, \ldots, i_n)$ и $(j_1, \ldots, j_n)$ сравниваются как слова в словаре: сначала сравниваются их первые элементы, потом, в случае их равенства — вторые, и так далее.

Несложно проверить следующие свойства лексикографического упорядочения:

Предложение 1.8. (1) *Если* $u \succ v$ *и* $v \succ w$, *то* $u \succ w$;
(2) *если* $u \succ v$, *то* $uw \succ vw$ *для любого* w;
(3) *если* $u_1 \succ v_1$ *и* $u_2 \succ v_2$, *то* $u_1 v_1 \succ u_2 v_2$.

Упражнение 1.9. Проверьте эти свойства.

Замечание 1.10. Лексикографический порядок не согласован со степенью монома: так, например, $x_1^2 x_2 \succ x_1 x_2^3$, хотя степень второго монома равна четырем, а первого — трем.

Определение 1.11. *Старшим членом* многочлена $P(x_1, \ldots, x_n)$ (обозначение: $\operatorname{ht} P$) называется самый старший при лексикографическом упорядочении из входящих в него мономов.

Пример 1.12. $\operatorname{ht}(2x_1x_3^3 + x_1x_2^2x_3 - x_2x_3^2 + 5x_1^2x_2 - 4x_2) = 5x_1^2x_2$.

Лемма 1.13. *Старший член произведения многочленов равен произведению их старших членов.*

Доказательство. Это следует из свойств лексикографического порядка (предложение 1.8). □

Следующая лемма уже относится к симметрическим многочленам.

Лемма 1.14. *Пусть* f *— симметрический многочлен. Тогда его старший член* $\operatorname{ht} f = u = ax_1^{k_1} \ldots x_n^{k_n}$ *удовлетворяет неравенствам* $k_1 \geq k_2 \geq \cdots \geq k_n$.

Доказательство. Предположим противное: пусть $k_i < k_{i+1}$ для некоторого i. Тогда, по определению симметрического многочлена, f должен содержать и моном $ax_1^{k_1} \ldots x_i^{k_{i+1}} x_{i+1}^{k_i} \ldots x_n^{k_n}$. Но этот моном лексикографически старше, чем u. Противоречие. □

Лемма 1.15. *Пусть* $u = x_1^{k_1} \ldots x_n^{k_n}$. *Тогда существуют и однозначно определены числа* $\ell_1, dots, \ell_n$, *что старший член многочлена* $\sigma_1^{\ell_1} \ldots \sigma_n^{\ell_n}$ *совпадает с* u.

Доказательство. Старший член многочлена σ_k равен $x_1 \dots x_k$. Поэтому старший член многочлена $\sigma_1^{\ell_1} \dots \sigma_n^{\ell_n}$ равен

$$x_1^{\ell_1}(x_1x_2)^{\ell_2} \dots (x_1 \dots x_n)^{\ell_n} = x_1^{\ell_1+\dots+\ell_n} x_2^{\ell_2+\dots+\ell_n} x_n^{\ell_n}.$$

Получаем систему уравнений на ℓ_i:

$$\begin{aligned} \ell_1 + \ell_2 + \dots + \ell_n &= k_1; \\ \ell_2 + \dots + \ell_n &= k_2; \\ &\dots \\ \ell_n &= k_n. \end{aligned}$$

Она имеет единственное решение: $\ell_i = k_i - k_{i+1}$. Лемма доказана.

Перейдём к доказательству теоремы. Пусть $f(x_1, \dots, x_n)$ — симметрический многочлен. Докажем существование такого многочлена $F(X_1, \dots, X_n)$, что $f = F(\sigma_1, \dots, \sigma_n)$. Пусть $\operatorname{ht} f = u = ax_1^{k_1} \dots x_n^{k_n}$. Согласно предыдущей лемме, существует такой многочлен $F_1(X_1, \dots, X_n)$, что $\operatorname{ht} F(\sigma_1, \dots, \sigma_n) = u$. Рассмотрим разность этих многочленов:

$$f_1(x_1, \dots, x_n) = f - F(\sigma_1, \dots, \sigma_n).$$

Если $f_1 = 0$, то всё доказано. Если нет, то пусть $u_2 = \operatorname{ht} f_1$. Ясно, что $u_2 \prec u_1$. Применим к u_2 ту же процедуру: найдём многочлен от $\sigma_1, \dots, \sigma_n$ со старшим членом u_2 и вычтем его из f_1, получим многочлен со старшим членом u_3, и так далее. Мы получим убывающую последовательность мономов

$$u_1 \succ u_2 \succ u_3 \succ \dots$$

Все эти мономы являются старшими членами симметрических многочленов, т.е. удовлетворяют условию леммы 1.14. Значит, все показатели при всех x_i во всех u_j не превосходят показателя при x_1 в мономе u_1, т.е. k_1. Таких мономов имеется конечное число. Поэтому процесс оборвётся: на каком-то шаге $u_N = 0$. Тем самым мы получим выражение многочлена f через элементарные симметрические.

Докажем единственность такого выражения. Предположим противное: пусть найдутся такие многочлены $F(X_1, \dots, X_n)$ и $G(X_1, \dots, X_n)$, что $F(\sigma_1, \dots, \sigma_n) = G(\sigma_1, \dots, \sigma_n)$. Положим $H(X_1, \dots, X_n) = F - G$; получаем, что $H(\sigma_1, \dots, \sigma_n) = 0$.

Покажем, что $H = 0$. Пусть $H_1(X_1, \dots, X_n), \dots, H_s(X_1, \dots, X_n)$ — все ненулевые мономы, входящие в H. Пусть $w_i(x_1, \dots, x_n) = \operatorname{ht} H_i(\sigma_1, \sigma_n)$ — старшие члены многочленов, которые получаются при подстановке σ_k в H_i. Согласно лемме 1.15, среди w_i нет пропорциональных. Выберем среди них старший моном. Пусть это будет w_1. По построению, w_1 старше всех остальных мономов, входящих в $H_1(\sigma_1, \dots, \sigma_n)$,

и всех мономов, входящих в $H_i(\sigma_1, \ldots, \sigma_n)$. Поэтому после приведения подобных слагаемых в сумме

$$H(\sigma_1, \ldots, \sigma_n) = H_1(\sigma_1, \ldots, \sigma_n) + \cdots + H_n(\sigma_1, \ldots, \sigma_n)$$

член w_1 сохранится, т.к. ему не с кем будет сократиться. Противоречие. Значит, $\sigma_1, \ldots, \sigma_n$ *алгебраически независимы.* □

□

2. Вторая лекция, 11 сентября 2012 г.

2.1. **Другое доказательство основной теоремы о симметрических многочленах.** Назовём *весом* монома $u = aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$ число

$$\operatorname{wt} u = k_1 + 2k_2 + 3k_3 + \dots + nk_n.$$

Вес многочлена $F(X_1, \dots, X_n)$ определим как максимальный вес входящего в него монома.

Ясно, что вес многочлена $F(X_1, \dots, X_n)$ равняется степени многочлена $F(\sigma_1, \dots, \sigma_n) \in K[x_1, \dots, x_n]$, получаемого из F подстановкой σ_k в качестве X_k.

Теперь уточним формулировку основной теоремы о симметрических многочленах.

Теорема 2.1 (Основная теорема о симметрических многочленах)**.** *Всякий симметрический многочлен единственным образом представляется в виде многочлена от элементарных симметрических многочленов $\sigma_1, \dots, \sigma_n$. Иначе говоря, для любого симметрического многочлена $f(x_1, \dots, x_n)$ степени d найдётся единственный многочлен $F(X_1, \dots, X_n)$,* вес которого не превосходит d*, для которого $f(x_1, \dots, x_n) = F(\sigma_1, \dots, \sigma_n)$.*

Второе доказательство. Будем доказывать утверждение по индукции по n. При $n = 1$ доказывать нечего. Пусть утверждение доказано для многочленов от $n-1$ переменной.

Заметим, что при подстановке $x_n = 0$ в k-й элементарный симметрический многочлен $\sigma_k(x_1, \dots, x_n)$ мы получаем k-й элементарный симметрический многочлен *от $n-1$ переменной* (обозначим его через $\tilde\sigma_k(x_1, \dots, x_{n-1})$, если $k < n$, и 0, если $k = n$.

Будем вести индукцию по $d = \deg f$. База ($\deg f = 0$) очевидна. Пусть утверждение доказано для многочленов степени меньше d.

Возьмём многочлен $f(x_1, \dots, x_n)$ и подставим в него 0 в качестве последней переменной. Мы получим *симметрический* многочлен от $x_1, \dots, x_{n-1}$. Ясно, что $\deg f(x_1, \dots, x_{n-1}, 0) \le \deg f = d$. По предположению индукции, существует такой многочлен $G(X_1, \dots, X_{n-1})$ веса не выше d, что

$$f(x_1, \dots, x_{n-1}, 0) = G(\tilde\sigma_1, \dots, \tilde\sigma_{n-1}).$$

Теперь подставим в многочлен G не $\tilde\sigma_k$, а σ_k. Полученный многочлен $G(\sigma_1, \dots, \sigma_{n-1})$ будет снова симметрическим многочленом, но уже от $x_1, \dots, x_n$. Вычтем его из $f(x_1, \dots, x_n)$:

$$f_1(x_1, \dots, x_n) = f(x_1, \dots, x_n) - G(\sigma_1, \dots, \sigma_{n-1}).$$

Это тоже симметрический многочлен, степень которого не превосходит d (т.к. оба его слагаемых имеют степень не выше d). При этом $f_1(x_1, \dots, x_{n-1}, 0) = 0$. Это значит, что f_1 делится на x_n. Но

f_1 симметрический, значит, он делится и на произведение $x_1 \dots x_n$, т.е. на σ_n.

Стало быть, $f_1 = \sigma_n \cdot f_2(x_1, \dots, x_n)$, где f_2 снова симметрический. При этом $\deg f_2 = \deg f_1 - n \leq d - n < d$. Значит, для него справедливо предположение индукции: найдется такой многочлен $F_2(X_1, \dots, X_n)$ веса не выше $d - n$, что $f_2(x_1, \dots, x_n) = F_2(\sigma_1, \dots, \sigma_n)$.

Тем самым мы получили выражение и для многочлена f:

$$f = G(\sigma_1, \dots, \sigma_{n-1}) + \sigma_n F_2(\sigma_1, \dots, \sigma_n) = \\ = \left[G(X_1, \dots, X_{n-1}) + X_n F_2(X_1, \dots, X_n)\right]_{X_i = \sigma_i}.$$

Аналогичным образом можно доказать и единственность[1] такого многочлена $F(X_1, \dots, X_n)$. Снова будем вести индукцию по n. Предположим, что единственность нарушается, и рассмотрим такой многочлен наименьшей степени $F(X_1, \dots, X_n)$, отличный от нуля, для которого $F(\sigma_1, \dots, \sigma_n) = 0$.

Запишем F как многочлен от X_n с коэффициентами в кольце $K[X_1, \dots, X_{n-1}]$:

$$F(X_1, \dots, X_n) = F_0(X_1, \dots, X_{n-1}) + \dots + F_d(X_1, \dots, X_{n-1}) X_n^d.$$

Тогда $F_0 \neq 0$, поскольку иначе F делился бы на X_n, из чего следовало бы, что $F(X_1, \dots, X_n) = X_n \Phi(X_1, \dots, X_n)$, причём $\sigma_n \Phi(\sigma_1, \dots, \sigma_n) = 0$, что противоречило бы минимальности степени многочлена F.

Теперь подставим в предыдущее равенство σ_i вместо X_i. Получим, что

$$F(\sigma_1, \dots, \sigma_n) = F_0(\sigma_1, \dots, \sigma_{n-1}) + \dots + F_d(\sigma_1, \dots, \sigma_{n-1}) \sigma_n^d.$$

Это соотношение в кольце $K[x_1, \dots, x_n]$. Если теперь подставить в него $x_n = 0$, мы получим равенство

$$F_0(\tilde{\sigma}_1, \dots, \tilde{\sigma}_{n-1}) = 0.$$

Мы получили нетривиальное соотношение между элементарными симметрическими многочленами σ_k от $n-1$ переменной. Противоречие. □

2.2. **Результант.** Рассмотрим два многочлена от одной переменной (над произвольным полем K), степени n и m соответственно:

$$\begin{aligned} f(x) &= a_n x^n + \dots + a_1 x + a_0; \\ g(x) &= b_m x^m + \dots + b_1 x + b_0. \end{aligned}$$

Наша ближайшая задача — определить, имеют ли эти многочлены общий сомножитель.

Сначала дадим на этот вопрос "малоинформативный" ответ. Предположим, что общий множитель у f и g есть: $f = f_1 h$, $g = g_1 h$,

[1] На лекции этого не рассказывалось.

где $\deg h > 0$. Это значит, что у них имеется общее кратное степени строго меньшей, чем $m+n$. Это кратное есть $f_1 g_1 h$. При этом "дополнительные множители", на которые надо домножить f и g для того, чтобы его получить, равны g_1 и f_1 соответственно, и их степени не превосходят $m-1$ и $n-1$. Напротив, если у f и g нет общих множителей, то их наименьшее общее кратное имеет степень $m+n$, и нельзя найти такие многочлены p и q, где $\deg p < m$, $\deg q < n$, что $fp + gq = 0$.

Тем самым, имеет место следующее предложение:

Предложение 2.2. *Многочлены $f(x)$ и $g(x)$, где $\deg f = n$, $\deg g = n$, имеют общий множитель тогда и только тогда, когда найдутся такие многочлены $p(x)$ и $q(x)$, не равные одновременно нулю, где $\deg p(x) \leq m-1$, $\deg q(x) \leq n-1$, что $f(x)p(x) + g(x)q(x) = 0$.*

Попробуем интерпретировать это условие как-то ещё. Выпишем многочлены $p(x)$ и $q(x)$:

$$\begin{aligned} p(x) &= p_{m-1}x^{m-1} + \cdots + p_1 x + p_0; \\ q(x) &= q_{n-1}x^{n-1} + \cdots + q_1 x + q_0. \end{aligned}$$

Запишем в явном виде условие из предложения 2.2:

$$\begin{aligned} f(x)p(x) + g(x)q(x) = \\ = (a_n p_{m-1} + b_m q_{n-1})x^{m+n-1} + \\ + (a_{n-1}p_{m-1} + a_n p_{m-2} + b_{m-1}q_{n-1} + b_m q_{n-2})x^{m+n-2} + \\ + \ldots + a_0 p_0 + b_0 q_0 = 0. \end{aligned}$$

Условие равенства многочлена степени $m+n-1$ нулю — это система из $m+n$ линейных однородных уравнений на неизвестные $p_{m-1}, \ldots, p_0, q_{n-1}, q_0$. Искомые многочлены $p(x)$ и $q(x)$ существуют тогда и только тогда, когда у этой системы есть ненулевое решение, т.е. когда матрица системы вырождена. Определитель этой матрицы называется *результантом* многочленов $f(x)$ и $g(x)$ и обозначается $\mathrm{Res}(f,g)$. Выпишем его явно:

$$\mathrm{Res}(f,g) = \begin{vmatrix} a_n & & & & b_m & & & \\ a_{n-1} & a_n & & & b_{m-1} & b_m & & \\ \vdots & a_{n-1} & \ddots & & \vdots & b_{m-1} & \ddots & \\ a_0 & \vdots & \ddots & a_n & b_0 & \vdots & \ddots & b_m \\ & a_0 & & a_{n-1} & & b_0 & & b_{m-1} \\ & & \ddots & \vdots & & & \ddots & \vdots \\ & & & a_0 & & & & b_0 \end{vmatrix}$$

Мы доказали следующую теорему.

Теорема 2.3. *Многочлены $f(x)$ и $g(x)$ имеют общий множитель тогда и только тогда, когда их результант $\mathrm{Res}(f,g)$ равен нулю.*

Следствие 2.4. *Пусть многочлены $f(x)$ и $g(x)$ имеют общий корень. Тогда* $\mathrm{Res}(f,g)=0$.

2.3. **Другие формулы для результанта.** Предположим, что многочлены $f(x)$ и $g(x)$ раскладываются на линейные множители:

$$\begin{aligned} f(x) &= a_n(x-t_1)\dots(x-t_n);\\ g(x) &= b_m(x-u_1)\dots(x-u_m). \end{aligned}$$

Коэффициенты a_k и b_k выражаются через корни этих многочленов:

$$(*)a_k = a_n(-1)^{n-k}\sigma_{n-k}(t_1,\dots,t_n),\quad b_k = b_m(-1)^{m-k}\tilde\sigma_{m-k}(u_1,\dots,u_m),$$

где σ и $\tilde\sigma$ — элементарные симметрические многочлены от n и m переменных соответственно. Также полезно заметить, что $\mathrm{Res}(f,g)$ является однородным многочленом от a_i степени m и от b_j степени n.

Предложение 2.5. $\mathrm{Res}(f,g)=a_n^m b_m^n\prod_{i=1}^n\prod_{j=1}^m(t_i-u_j)=a_n^m\prod_{i=1}^n g(t_i)=(-1)^{mn}b_m^n\prod_{j=1}^m f(u_j)$.

Доказательство. Последние два равенства очевидно следуют из вида разложения $f(x)$ и $g(x)$ на линейные множители. Докажем первое равенство.

Во-первых, из равенств $(*)$ следует, что $\mathrm{Res}(f,g)$ как многочлен от a_n, b_m, t_i, u_j делится на $a_n^m b_m^n$. Кроме того, $\mathrm{Res}(f,g)$ обращается в нуль, если многочлены f и g имеют общий корень, т.е. если $t_i=u_j$ при каких-то i,j. Поэтому $\mathrm{Res}(f,g)$ делится на любую из разностей t_i-u_j, а значит, и на их произведение. Мы доказали, что $\mathrm{Res}(f,g)$ делится на $a_n^m b_m^n\prod_{i=1}^n\prod_{j=1}^m(t_i-u_j)$.

Далее, заметим, что оба эти выражения имеют степень m как многочлены от $a_0,\dots,a_n$: про результант это, как было сказано выше, следует из его явного вида, а про правую часть это верно в силу того, что она равна $(-1)^{mn}b_m^n\prod_{j=1}^m f(u_j)$, а каждый из сомножителей $f(u_j)$ линеен как многочлен от a_i. По тем же соображениям они оба имеют степень n как многочлены от $b_0,\dots,b_m$. Следовательно, эти выражения получаются друг от друга домножением на элемент основного поля K.

Для завершения доказательства заметим, что оба эти выражения как многочлены от a_i и b_j содержат одночлен $a_n^m b_m^n$ с коэффициентом 1. Поэтому они равны. □

2.4. **Дискриминант.** Рассмотрим многочлен $f(x)$, раскладывающийся на линейные множители:

$$f(x)=a_n(x-t_1)\dots(x-t_n).$$

Определение 2.6. *Дискриминант* многочлена f — это многочлен

$$D(f) = a_n^{2n-2} \prod_{i<j} (t_i - t_j)^2 = \left[a_n^{n-1} \prod_{i<j} (t_i - t_j) \right]^2 .$$

Из определения ясно, что дискриминант обращается в нуль тогда и только тогда, когда среди корней многочлена $f(x)$ есть совпадающие.

Далее, дискриминант является симметрическим многочленом от $t_1, \ldots, t_n$, поэтому это многочлен от $a_0, \ldots, a_{n-1}, a_n$ и a_n^{-1}. (Контрольный вопрос: зачем здесь a_n^{-1}?) Найдём этот многочлен. Для этого нам потребуется понятие *производной* многочлена.

Определение 2.7. Пусть $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$ — многочлен. Его *производная* — это многочлен $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1 \in K[x]$.

Замечание 2.8. Это определение производной многочлена является чисто алгебраическим (в отличие от того, которое давалось в курсе математического анализа — в последнем участвовало понятие предельного перехода). Поэтому имеет смысл говорить о производной многочлена над произвольным полем, в том числе ненулевой характеристики. В отличие, скажем, от вещественной или комплексной ситуации, в характеристике p бывают многочлены, имеющие нулевую производную, но отличные от констант — например, x^p.

Упражнение 2.9. Докажите, что сумму и произведение многочленов можно дифференцировать по правилам, известным из матанализа: $(f+g)' = f' + g'$ и $(fg)' = f'g + fg'$.

Предложение 2.10. *Дискриминант многочлена пропорционален результанту его самого и его производной:*

$$D(f) = (-1)^{n(n-1)/2} a_n^{-1} \operatorname{Res}(f, f').$$

Доказательство. Продифференцируем производную многочлена по правилу Лейбница:

$$f'(x) = \left(a_n \prod_{i=1}^{n} (x - t_i) \right)' = a_n \sum_{i=1}^{n} \prod_{j \neq i} (x - t_j).$$

Особенно хорошо выглядит выражение для производной f' в корне t_i многочлена f: там все слагаемые в последней сумме, кроме i-го, обращаются в нуль:

$$f'(t_i) = a_n \prod_{j \neq i} (t_i - t_j).$$

Воспользовавшись предложением 2.5, получим:

$$\operatorname{Res}(f, f') = a_n^{2n-1} \prod_{i=1}^{n} \prod_{j \neq i} (t_i - t_j) =$$

$$= a_n (-1)^{n(n-1)/2} a_n^{2n-2} \prod_{i<j} (t_i - t_j)^2 = a_n (-1)^{n(n-1)/2} D(f),$$

что и требовалось доказать.

□

3. Третья лекция, 18 сентября 2012 г.

Следующие несколько лекций будут посвящены различным сюжетам из теории групп.

3.1. **Прямые произведения.** Для начала напомним понятие прямого произведения групп.

Определение 3.1. Группа G раскладывается в *прямое произведение* своих подгрупп $G_1, \dots, G_k$, если:

(1) каждый элемент $g \in G$ единственным образом представляется в виде произведения $g = g_1 \dots g_k$, где $g_i \in G_i$;
(2) $g_i g_j = g_j g_i$ при $g_i \in G_i$, $g_j \in G_j$, $i \neq j$.

Обозначение: $G = G_1 \times \dots \times G_k$.

Во-первых, из условия 1) (точнее, из единственности такого представления) следует, что $G_i \cap G_j = \{e\}$. Далее, если условие 1) выполнено, то условие 2) равносильно требованию нормальности групп G_i. Докажем это.

Лемма 3.2. *Пусть G_1 и G_2 — нормальные подгруппы в G, причем $G_1 \cap G_2 = \{e\}$. Тогда $g_1 g_2 = g_2 g_1$ для любых $g_1 \in G_1$, $g_2 \in G_2$.*

Доказательство. Докажем, что $g_1 g_2 g_1^{-1} g_2^{-1} = e$. Действительно, $g_1 g_2 g_1^{-1} g_2^{-1} = (g_1 g_2 g_1^{-1}) g_2^{-1} \in G_2$, т.к. в силу нормальности группы G_2 имеем $g_1 g_2 g_1^{-1} \in G_2$. По той же причине $g_1 g_2 g_1^{-1} g_2^{-1} = g_1 (g_2 g_1^{-1} g_2^{-1}) \in G_1$. Значит, $g_1 g_2 g_1^{-1} g_2^{-1} \in G_1 \cap G_2$, то есть равняется единице. □

Рассмотрим случай двух множителей отдельно.

Предложение 3.3. *Группа G разлагается в прямое произведение своих подгрупп G_1 и G_2 тогда и только тогда, когда*

(1) *G_1 и G_2 — нормальные подгруппы;*
(2) *$G_1 \cap G_2 = \{e\}$;*
(3) *$G_1 G_2 = G$, т.е. каждый элемент $g \in G$ представляется в виде $g = g_1 g_2$, где $g_1 \in G_1$, $g_2 \in G_2$.*

Доказательство. Часть “только тогда” доказана выше. Пусть теперь выполнены условия 1)–3). Тогда по предыдущей лемме $g_1 g_2 = g_2 g_1$ при $g_1 \in G_1$, $g_2 \in G_2$. Проверим единственность такого представления. Пусть $g_1 g_2 = \tilde{g}_1 \tilde{g}_2$. Тогда $\tilde{g}_1^{-1} g_1 = g_2 \tilde{g}_2^{-1} \in G_1 \cap G_2 = \{e\}$. Поэтому $g_1 = \tilde{g}_1$, $g_2 = \tilde{g}_2$. □

Выше мы предполагали, что группы G_i — подгруппы в одной и той же группе G. В этой ситуации иногда говорят о *внутреннем* прямом произведении. Можно, наоборот, для заданного набора групп G_i (вообще говоря, не вложенных в какую-то бóльшую группу) построить такую группу G, которая будет раскладываться в прямое произведение своих подгрупп, изоморфных G_i.

Определение 3.4. *Прямым произведением* групп $G_1, \ldots, G_k$ называется множество последовательностей $(g_1, \ldots, g_k)$, где $g_i \in G_i$, с покомпонентными операциями умножения и взятия обратного. Обозначение: $G_1 \times \cdots \times G_k$.

Ясно, что такие операции задают на $G_1 \times \cdots \times G_k$ структуру группы, единицей которой является набор $(e, \ldots, e)$. Кроме того, каждая из групп G_i вкладывается в $G_1 \times \cdots \times G_k$ как подгруппа: $g_i \mapsto (e, \ldots, e, g_i, e, \ldots, e)$, где неединичный элемент стоит на i-м месте. Тогда $G_1 \times \cdots \times G_k$ есть прямое произведение своих подгрупп G_i в смысле первого определения.

Пример 3.5. Группа ненулевых комплексных чисел $\mathbb{C}^*$ раскладывается в прямое произведение групп $\mathbb{R}_+ \times U(1)$, где $U(1)$ — группа комплексных чисел единичного модуля. Это не что иное, как представление комплексного числа в тригонометрической форме: $z = re^{i\varphi}$ (для ненулевого числа это представление единственно).

Пример 3.6. Каждое движение плоскости может быть представлено, причем единственным образом, в виде композиции параллельного переноса и ортогонального преобразования (сохраняющего начало координат). Однако это не прямое произведение, т.к., например, подгруппа ортогональных преобразований не является нормальной в группе всех движений (или, иначе говоря, ортогональные преобразования не коммутируют с параллельными переносами). Зато оказывается, что это является разложением в так называемое *полупрямое произведение*, о котором речь пойдёт дальше.

3.2. **Автоморфизмы групп.**

Определение 3.7. *Автоморфизм* группы — это её изоморфизм на себя.

Пример 3.8. Отображение $A \mapsto (A^T)^{-1}$ является автоморфизмом группы матриц.

Все автоморфизмы группы G образуют группу, обозначаемую через $\operatorname{Aut} G$.

Любой элемент $g \in G$ задаёт автоморфизм $a(g) \in \operatorname{Aut} G$ при помощи *сопряжения*: $a(g)x = gxg^{-1}$. Такие автоморфизмы называются *внутренними*, их множество обозначается $\operatorname{Int} G$.

Ясно, что $\operatorname{Int} G$ — подгруппа в $\operatorname{Aut} G$. Эта подгруппа нормальна: для любого автоморфизма $\varphi \in \operatorname{Aut} G$ верно, что $\varphi a(g)\varphi^{-1} = a(\varphi(g))$.

Итак, у нас имеется отображение $G \to \operatorname{Aut} G$ (каждому элементу группы $g \in G$ сопоставляется внутренний автоморфизм $a(g) \in \operatorname{Aut} G$). Несложно проверить, что это отображение является гомоморфизмом:

$$a(gh)x = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = a(g)a(h)x.$$

Его ядро — это центр $Z(G)$ группы G. По теореме о гомоморфизме $\operatorname{Int} G \cong G/Z(G)$.

Пример 3.9. При $n \geq 3$ центр симметрической группы S_n тривиален. Поэтому $\operatorname{Int} S_n \cong S_n$. Можно доказать, что при $n \neq 6$ никаких других автоморфизмов у S_n нет, а при $n = 6$ подгруппа $\operatorname{Int} G \subset \operatorname{Aut} G$ имеет индекс 2.

Пример 3.10. Найдём группу $\operatorname{Aut} \mathbb{Z}_n$. Пусть $\varphi \in \operatorname{Aut} \mathbb{Z}_n$, $\varphi(\overline{1}) = \overline{k}$. Тогда

$$\varphi(\overline{\ell}) = \overline{k\ell} = \overline{k} \cdot \overline{\ell},$$

где умножение понимается в смысле кольца $\mathbb{Z}_n$. Таким образом, всякий автоморфизм группы $\mathbb{Z}_n$ имеет вид $\varphi_k \colon \ell \to k\ell$. Обратно, для любого k отображение $\ell \mapsto k\ell$ является гомоморфизмом группы $\mathbb{Z}_n$ в себя. Значит, гомоморфизм φ_k является автоморфизмом тогда и только тогда, когда k обратимо в кольце $\mathbb{Z}_n$. Поэтому $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^*$.

3.3. **Полупрямое произведение.** Понятие внутреннего автоморфизма позволяет переформулировать определение нормальной подгруппы: подгруппа нормальна тогда и только тогда, когда она инвариантна относительно всех внутренних автоморфизмов.

Пусть N — нормальная подгруппа в G, H — произвольная подгруппа. Тогда произведение $NH = \{nh : n \in N, h \in H\}$ является подгруппой. Действительно,

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2,$$
$$(nh)^{-1} = h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1}.$$

Кроме того, $NH = HN$.

Определение 3.11. Говорят, что группа G разлагается в *полупрямое произведение* своих подгрупп N и H, если

(1) N — нормальная подгруппа;
(2) $N \cap H = \{e\}$;
(3) $NH = G$.

Обозначение: $G = N \ltimes H$ (иногда используется другой значок: $G = N \leftthreetimes H$).

Как и в случае прямого произведения, свойства 2) и 3) эквивалентны тому, что каждый элемент из G единственным образом представляется в виде произведения элементов из N и H.

Пример 3.12. $S_n = A_n \ltimes \langle (12) \rangle$.

Пример 3.13. $S_4 = V_4 \langle S_3$, где V_4 — четверная группа Клейна, а S_3 вложена в S_4 как группа перестановок, оставляющих на месте символ 4.

Пример 3.14. $\operatorname{GL}_n(K) = \operatorname{SL}_n(K) \ltimes \{\operatorname{diag}(\lambda, 1, \ldots, 1) \mid \lambda \in K^*\}$.

4. Четвертая лекция, 24 сентября 2012 г.

4.1. **Снова полупрямое произведение групп.** На прошлой лекции мы определили разложение группы в полупрямое произведение двух своих подгрупп (одна из которых должна быть нормальна). Можно действовать иначе: для двух групп N и H рассмотреть их *внешнее* полупрямое произведение, т.е. построить группу $G = N \ltimes H$ аналогично тому, как это делалось для прямого произведения. Отличие от прямого произведения состоит в том, что для описания полупрямого произведения необходима дополнительная информация — а именно, нужно задать для каждого элемента из H нужно задать автоморфизм $\alpha(h)$ группы N, которым h будет действовать на N. Это соответствие должно быть гомоморфизмом групп $H \to \operatorname{Aut} N$.

Итак, пусть $N \times H$ — прямое произведение N и H *как множеств*, т.е. множество пар (n, h). Пусть также задан гомоморфизм $\alpha\colon H \to \operatorname{Aut} N$. Определим на множестве $N \times H$ умножение следующим образом:

$$(n_1, h_1)(n_2, h_2) = (n_1\alpha(h_1)n_2, h_1h_2).$$

Обратный элемент к (n, h) будет определяться так:

$$(n, h)^{-1} = (\alpha(h^{-1})n^{-1}, h^{-1}).$$

Тем самым на $N \times H$ будет задана структура группы, которая называется *внешним полупрямым произведением N и H* и обозначается через $N \ltimes_\alpha H$. При этой конструкции разным гомоморфизмам α будут соответствовать, вообще говоря, неизоморфные группы! Так, например, если α переводит каждый элемент H в тождественный автоморфизм группы N, то полученная группа будет прямым произведением групп N и H.

Обратно, если группа G раскладывается в полупрямое произведение своих подгрупп: $G = N \ltimes H$, то имеется изоморфизм групп $N \ltimes_\alpha H \to G$. (Как при этом будет действовать на N автоморфизм $\alpha(h)$?)

Пример 4.1. Рассмотрим две циклические группы: $\langle a\rangle_n = \mathbb{Z}_n$ и $\langle b\rangle_m = \mathbb{Z}_m$. Гомоморфизм $\langle b\rangle_m \to \operatorname{Aut}\mathbb{Z}_n$ полностью определяется тем, как действует образующая b. Как обсуждалось на прошлой лекции, $\operatorname{Aut}\mathbb{Z}_n = \mathbb{Z}_n^*$, поэтому всякий автоморфизм $\mathbb{Z}_n$ есть возведение элемента a в некоторую степень k. Таким образом, задать гомоморфизм $\langle b\rangle_m \to \mathbb{Z}_n$ значит задать такое k, что $k^m \equiv 1 \mod n$. Такое полупрямое произведение обозначается через $\langle a\rangle_n \ltimes_k \langle b\rangle_m$. Вообще говоря, при различных k эти группы могут оказаться изоморфными.

В частности, если $(\varphi(n), m) = 1$, то $k = 1$, и всякий такой гомоморфизм α тривиален, т.е. в этом случае не бывает полупрямых произведений $\mathbb{Z}_n$ и $\mathbb{Z}_m$, отличных от прямого произведения.

Пример 4.2. Рассмотрим группу $\langle a\rangle_n \ltimes_{-1} \langle b\rangle_2$. Она задаётся соотношениями соотношениями $a^n = b^2 = 1$ и $bab^{-1} = a^{-1}$. Поэтому это группа самосовмещений n-угольника.

4.2. **Коммутант.** Пусть $x, y \in G$ — два элемента группы. Их *коммутатором* называется элемент $(x, y) = xyx^{-1}y^{-1}$. Очевидны следующие свойства коммутатора:

(1) $(x, y) = e$ тогда и только тогда, когда x и y коммутируют.
(2) $(x, y)^{-1} = (y, x)$ (обратный к коммутатору элемент снова является коммутатором).

Напротив, произведение двух коммутаторов не обязано быть коммутатором.

Все коммутаторы порождают подгруппу в G, которая называется *коммутантом* группы G (или, реже, её *производной группой*) и обозначается через G':

$$G' := \langle (x, y) \mid x, y \in G\rangle.$$

Ясно, что $G' = \{e\}$ тогда и только тогда, когда G абелева.

Пусть $\varphi\colon G \to H$ — гомоморфизм групп. Поскольку $\varphi((x, y)) = (\varphi(x), \varphi(y))$, то $\varphi(G') \subset H'$. Если φ к тому же является эпиморфизмом, то $\varphi(G') = H'$.

Теперь возьмём в качестве H саму G, а в качестве φ — какой-нибудь её внутренний автоморфизм. Получается, что $\varphi(G') = G'$. Это значит, что G' — подгруппа, инвариантная относительно всех внутренних автоморфизмов. Значит, она нормальна в G.

Теорема 4.3. *Всякая подгруппа $H \subset G$, содержащая G', нормальна. При этом факторгруппа G/H абелева (в частности, G/G' тоже абелева). Обратно, если H — такая нормальная подгруппа в G, что G/H абелева, то G' содержится в H. Другими словами, G' — наименьшая нормальная подгруппа в G, факторгруппа по которой абелева.*

Доказательство. Пусть $H \supset G'$. Пусть $h \in H$, $g \in G$. Тогда

$$ghg^{-1} = ghg^{-1}h^{-1} = (g, h) \cdot h \in G' \cdot H \subset H,$$

поэтому $H \lhd G$.

Далее, пусть H — нормальная подгруппа в G, и $g_1, g_2 \in G$. Докажем, что g_1H и g_2H коммутируют, т.е. G/H коммутативна, тогда и только тогда, когда $G' \subset H$.

$$(g_1H, g_2H) = g_1Hg_2Hg_1^{-1}Hg_2^{-1}H = g_1g_2g_1^{-1}g_2^{-1}H = (g_1, g_2)H.$$

Если факторгруппа G/H абелева, то $(g_1, g_2)H = eH$, т.е. $(g_1, g_2) \in H$. Обратно, если $(g_1, g_2) \in H$, то из приведенного равенства получаем, что элементы факторгруппы g_1H и g_2H коммутируют. Теорема доказана. □

4.3. **Коммутанты некоторых групп.** Из курса прошлого семестра вам известно следующее

Предложение 4.4. *Группа чётных перестановок A_n порождается тройными циклами (ijk). При $n \geq 5$ группа A_n порождается парами независимых транспозиций $(ij)(kl)$.*

Пример 4.5. $S_n' = A_n$ при $n \geq 3$. Действительно, $S_n' \subset A_n$, т.к. группа $S_3/A_3 = \mathbb{Z}_2$ абелева. Далее, найдём S_3'. Эта группа содержится в A_3. Но в A_3 нет никакой меньшей подгруппы, кроме единичной, поэтому S_3' совпадает со всей A_3 (он отличен от $\{e\}$, т.к. S_3 некоммутативна). A_3 содержит оба 3-цикла (123) и (132). Поэтому S_n' содержит всевозможные 3-циклы. Поэтому из предложения 4.4 следует, что $S_n' = A_n$.

Пример 4.6. $A_4' = V_4$, где $V_4 = \langle (ij)(kl) \rangle$ — четверная группа Клейна. Действительно, $A_4/V_4 \cong \mathbb{Z}_3$ абелева, т.е. $A_4' \subset V_4$. Но V_4 не содержит никаких нетривиальных подгрупп, нормальных в A_4 (и вообще V_4 — единственная нормальная подгруппа в A_4, отличная от единичной и её самой), поэтому $A_4' = V_4$.

Пример 4.7. Предыдущий пример показывает, что при $n \geq 5$ коммутант A_n' содержит все пары независимых транспозиций. Поэтому он совпадает со всей группой A_n.

Замечание 4.8. Можно показать, что при $n \geq 5$ группа A_n проста, т.е. не содержит нетривиальных нормальных подгрупп (этот результат принадлежит Эвариста Галуа). Разумеется, для всякой неабелевой простой группы G верно, что $G' = G$.

Вычислим коммутанты групп $GL_n(K)$ и $\mathrm{SL}_n(K)$. Для этого нам понадобится следующее утверждение.

Предложение 4.9. *Группа $\mathrm{SL}_n(K)$ порождается трансвекциями $E + cE_{ij}$ при $i \neq j$, т.е. матрицами элементарных преобразований первого рода (здесь E — единичная матрица, E_{ij} — матричная единица, т.е. матрица, все элементы которой равны нулю, кроме (i,j)-го, который равен 1).*

Задача 4.10. Докажите предложение 4.9.

Докажем, что $\mathrm{GL}_n(K)' = \mathrm{SL}_n(K)' = \mathrm{SL}_n(K)$, в предположении, что поле K содержит более трёх элементов. Во-первых, $\mathrm{GL}_n(K)/\mathrm{SL}_n(K)$ есть группа скалярных матриц, которая является абелевой, т.е. $\mathrm{GL}_n(K)' \subset \mathrm{SL}_n(K)$. Далее, можно проверить явно, что

$$\left(\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & (\lambda^2 - 1)c \\ 0 & 1 \end{pmatrix}.$$

Поэтому если в K найдётся элемент λ, отличный от 0 и ± 1, то группа $\mathrm{GL}_n(K)'$ будет содержать все трансвекции. Поэтому она совпадает с $\mathrm{SL}_n(K)$ в силу предыдущего предложения.

4.4. **Разрешимые группы.** Определим *высшие коммутанты* $G^{(i)}$ группы G по следующему правилу: $G^{(1)} = G'$, $G^{(i)} = (G^{(i-1)})'$. Получим ряд подгрупп, каждая из которых нормальна в предыдущей:

$$G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(k)} \rhd \dots$$

Определение 4.11. Группа G *разрешима*, если $G^{(k)} = \{e\}$ для некоторого k.

Пример 4.12. В предыдущем пункте мы видели, что S_4 разрешима (для неё $S_4^{(3)} = \{e\}$, т.к. $S_4^{(2)} = V_4$ абелева), а при $n \geq 5$ группа S_n уже не является разрешимой.

Справедлива следующая несложная

Теорема 4.13. *Пусть $H \lhd G$ — нормальная подгруппа. Группа G разрешима тогда и только тогда, когда H и G/H разрешимы.*

Задача 4.14. Докажите эту теорему.

5. Пятая лекция, 9 октября 2012 г.

5.1. **Действия групп на множествах.** Напомним несколько определений из прошлогоднего курса.

Определение 5.1. Говорят, что группа G действует на множестве X (обозначение: $G \curvearrowright X$, раньше ещё часто писали $G : X$), если задано отображение $G \times X \to X$, $(g, x) \mapsto y = g \circ x$, удовлетворяющее следующим требованиям: $g \circ (g' \circ x) = (gg') \circ x$, и $e \circ x = x$ для любых $g, g' \in G$ и $x \in X$.

Множество $Gx = \{y \in X \mid y = g \circ x\} \subset X$ называется *орбитой* элемента X. Множество элементов группы G, оставляющих x на месте, называется *стабилизатором* элемента x и обозначается $\mathrm{Stab}_G x$ или G_x:

$$\mathrm{Stab}_G x = G_x = \{g \in G | g \circ x = x\} \subset G.$$

Очевидно, что это подгруппа в G.

Теорема Лагранжа утверждает, что если группа G конечна, то $|G| = |Gx| \cdot |\mathrm{Stab}_G x|$ для любого элемента $x \in X$.

Если $X = Gx$, то есть все элементы X образуют одну орбиту, действие называется *транзитивным*.

Вот пример важного *нетранзитивного* действия.

Пример 5.2. Группа действует на себе сопряжениями: $G \curvearrowright G$, $g \circ h = ghg^{-1}$. Это действие не транзитивно, т.к. $Ge = \{e\}$. Орбита элемента h для этого действия называется его *классом сопряжённости* и обозначается через $C(h)$, а стабилизатор — *централизатором* элемента h и обозначается через $Z(h)$. Ясно, что $Z(h) = \{g \in G | gh = hg\}$.

Одноточечные орбиты этого действия суть в точности элементы центра $Z(G)$ (это элементы группы, коммутирующие со всеми элементами).

Для конечных групп теорема Лагранжа утверждает, что $|Z(h)| \cdot |C(h)| = |G|$. В частности, $|C(h)|$ делит $|G|$. Это нам ещё неоднократно пригодится.

5.2. **p-группы.** Пусть G — конечная группа. Её порядок, как известно, делится на порядок любой подгруппы в G. Можно задать обратный вопрос: для всякого ли делителя $|G|$ найдётся подгруппа $H \in G$ соответствующего порядка? Несложно понять, что ответ будет отрицательным: так, например, группа A_5 имеет порядок 60, а подгрупп порядка 30 в ней нет: если бы такая подгруппа была, она была бы нормальной, а группа A_5, как известно, проста.

Однако в некоторых случаях — в частности, для делителей числа $|G|$, имеющих вид p^k — подгруппа соответствующего порядка всегда существует. Чтобы доказать это, подробнее изучим группы порядка p^k.

Определение 5.3. Группа G называется *p-группой*, где p — простое число, если $|G| = p^k$.

Теорема 5.4. *Нетривиальная p-группа имеет нетривиальный центр: если $|G| = p^k$, то $Z = Z(G) \neq \{e\}$.*

Доказательство. $G \backslash Z$ распадается на классы сопряжённости, содержащие более одного элемента (все одноэлементные классы лежат в центре). Порядок каждого из них $|C(x)|$ делит порядок группы, значит, $|C(x)| \vdots p$. Но $|G| \vdots p$. Поэтому и порядок центра кратен p. А значит, Z нетривиален. □

Следствие 5.5. *Всякая p-группа разрешима.*

Доказательство. Индукция по $\log_p |G|$. База очевидна: если $|G| = p$, то $G = \mathbb{Z}/p\mathbb{Z}$. Переход: центр $Z \subset G$ является нормальной абелевой подгруппой в G, в частности, он разрешим. Но G/Z — это p-группа, но уже меньшего порядка (предположение индукции!). Из разрешимости Z и G/Z следует разрешимость G. □

Следствие 5.6. *Всякая группа порядка p^2 абелева.*

Доказательство. Предположим, что $|G| = p^2$ и $Z \neq G$. Тогда $|Z| = p$ и $|G/Z| = p$, то есть G/Z — циклическая группа. Пусть aZ — её порождающий элемент. Тогда любой элемент из G представи́м в виде $a^k z$, где $z \in Z$. Но любые два таких элемента коммутируют — противоречие. □

5.3. **Силовские подгруппы.** Пусть $|G| = p^n m$, причём $(p, m) = 1$.

Определение 5.7. *Силовская p-подгруппа* группы G — это любая её подгруппа порядка p^n.

Теорема 5.8 (первая теорема Силова)**.** *Силовская p-подгруппа существует.*

Доказательство. Если группа G абелева, теорема следует из теоремы о структуре конечных абелевых групп: её силовская подгруппа — это $\mathrm{Tors}_p G$. В общем случае воспользуемся индукцией по $|G|$.

Пусть $|G| > 1$. Рассмотрим разбиение G на классы сопряжённых элементов: $G = \bigcup C(x_i)$.

Случай 1: найдётся такой нетривиальный класс $C(x)$, число элементов в котором *не* делится на p. Тогда $Z(x) \vdots p^n$, и в $Z(x)$ по предположению индукции есть подгруппа порядка p^n — она-то и будет силовской подгруппой в G.

Случай 2: такого класса нет. Тогда $C(x_i) \vdots p$, и поэтому $|Z| \vdots p$ (рассуждение аналогично доказательству теоремы о нетривиальности

центра p-группы). Пускай $|Z| = p^{n_0} m_0$. Выберем в Z силовскую подгруппу Z_1: порядок Z_1 равен p^{n_0}. В G/Z_1 по предположению индукции существует подгруппа порядка p^{n-n_0}. Её полный прообраз при каноническом эпиморфизме $G \to G/Z_1$ и будет искомой силовской p-подгруппой. □

Теорема 5.9 (вторая теорема Силова)**.** *Всякая p-подгруппа содержится в некоторой силовской p-подгруппе. Все силовские p-подгруппы сопряжены.*

Доказательство. Пусть $S \subset G$ — фиксированная силовская p-подгруппа, $S_1 \subset G$ — произвольная p-подгруппа.

Рассмотрим действие $S_1 \curvearrowright G/S$ на левых смежных классах по S. Число элементов любой нетривиальной S_1-орбиты делится на p, а число элементов в G/S равно m и поэтому на p не делится. Значит, S_1 имеет в G/S неподвижные точки. Пусть gS — такая точка. Тогда $S_1 \subset gSg^{-1}$, откуда следует первое утверждение теоремы. Если S_1 силовская подгруппа, то из сравнения порядков групп заключаем, что $S_1 = gSg^{-1}$. □

Теорема 5.10 (третья теорема Силова)**.** *Число силовских подгрупп сравнимо с 1 по модулю p.*

Доказательство. Пусть S — силовская подгруппа, $C(S)$ — класс подгрупп, сопряжённых S. По предыдущей теореме это и есть множество всех силовских подгрупп. При действии G на $C(S)$ сопряжениями стабилизатором каждой подгруппы $S' \in C(S)$ служит её нормализатор $N(S')$. Ограничим это действие на S. Тогда $C(S)$ как-то разобьется на нетривиальные S-орбиты, число элементов в каждой из которых кратно p, и неподвижные точки. Покажем, что неподвижная точка будет ровно одна — сама подгруппа S. Отсюда и будет следовать утверждение теоремы.

Пусть $S' \in C(S)$ — неподвижная точка. Это значит, что $S \subset N(S')$. Тогда S и S' — силовские подгруппы в $N(S')$, а значит, что они в ней сопряжены. Но S' — нормальная подгруппа в $N(S')$. Поэтому $S = S'$. □

5.4. **Применение теорем Силова.**

Пример 5.11. Пусть $|G| = n$, и p — наименьший простой делитель числа n. Покажем, что всякая подгруппа H *индекса* p нормальна. Действительно, рассмотрим действие H на левых смежных классах G/H. Число элементов каждой орбиты делит $|H|$, то есть оно либо равно 1, либо не меньше p. Но, поскольку $|G/H| = p$ и действие имеет неподвижную точку eH, то оно тривиально.

Пример 5.12. Покажем, что всякая группа G порядка pq, где p и q — различные простые числа, является полупрямым произведением циклических групп порядка p и q. Пусть $p > q$. Тогда силовская p-подгруппа G_p нормальна в силу предыдущего примера.

Если G_q — силовская q-подгруппа, то $G_p \cap G_q = \{e\}$, а поэтому $|G_pG_q| = pq = |G|$. Значит, $G = G_p \leftthreetimes G_q$.

Пример 5.13. Докажем, что каждая группа порядка 45 абелева. Действительно, пусть n_3 и n_5 — число её силовских 3-подгрупп и 5-подгрупп соответственно. Тогда $n_3 \equiv 1 \mod 3$ и $n_3|5$, откуда $n_3 = 1$. Значит, имеется единственная силовская 3-подгруппа, которая тем самым нормальна. Аналогично из условий $n_5 \equiv 1 \mod 5$ и $n_5|9$ получаем, что силовская 5-подгруппа нормальна и поэтому единственна. Поэтому вся группа будет прямым произведением этих двух подгрупп, следовательно, будет абелевой.

Пример 5.14. Докажем, что не существует простых групп порядка 30. Для этого покажем, что в каждой группе G порядка 30 есть нормальная подгруппа. Рассмотрим силовские 5-подгруппы в G. Они все суть циклические подгруппы порядка 5. Ясно, что пересекаться они могут только по единице. Их число, по третьей теореме Силова, даёт остаток 1 от деления на 5. Предположим, что оно больше 1. Тогда оно может равняться только шести, что даст нам 24 элемента порядка 5 в G. Теперь посмотрим на силовские 3-подгруппы. В каждой из них два элемента порядка 3. Если силовская подгруппа не одна, то их не менее 4, что даёт ещё 8 элементов порядка 2. Но в группе всего 30 элементов, что меньше, чем 24+8. Противоречие. Значит, в G есть нормальная подгруппа.

6. Шестая лекция, 16 октября 2012 г.

6.1. **Кватернионы.** Рассмотрим четырехмерное вещественное векторное пространство V с базисом $\{1, i, j, k\}$. Введём на этом пространстве некоммутативное умножение, определив его на базисных элементах при помощи следующей таблицы:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Упражнение 6.1. Проверьте, что эту таблицу умножения можно вывести из следующих соотношений: $i^2 = j^2 = k^2 = ijk = -1$.

Мы утверждаем, что определенное таким образом умножение задаёт на V структуру ассоциативной алгебры с единицей, которую мы будем обозначать через $\mathbb{H}$. Она называется алгеброй кватернионов, а её элементы — кватернионами. Элементы 1, i, j, k называются базисными кватернионами. Ассоциативность алгебры $\mathbb{H}$ можно проверить непосредственно, но мы поступим иначе: реализуем ее в качестве подалгебры в алгебре матриц $\mathrm{Mat}_2(\mathbb{C})$.

Рассмотрим следующее отображение $\mathbb{H} \to \mathrm{Mat}_2(\mathbb{C})$:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \qquad i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}; \qquad j \mapsto \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}; \qquad k \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Легко видеть (проверьте это!), что это действительно гомоморфизм алгебр над $\mathbb{R}$. При нём кватернион $a + bi + cj + dk$ соответствует матрице $\begin{pmatrix} a+di & -b-ci \\ b-ci & a-di \end{pmatrix} = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$, где $z, w \in \mathbb{C}$. Кроме того, все такие матрицы, кроме нулевой, невырождены:

$$\det \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} = z\overline{z} + w\overline{w} = |z|^2 + |w|^2 = a^2 + b^2 + c^2 + d^2. \qquad (*)$$

Определение 6.2. *Нормой* кватерниона z называется вещественное неотрицательное число $|z| = (a^2 + b^2 + c^2 + d^2)^{1/2}$. Кватернион $\overline{z} = a - bi - cj - dk$ называется *сопряжённым* к z.

Норма есть положительно определённая квадратичная форма на $\mathbb{H}$, поэтому она задаёт на $\mathbb{H}$ структуру евклидова пространства.

Как и для комплексных чисел, $z\overline{z} = |z|^2$.

Однако, в отличие от $\mathbb{C}$, сопряжение в $\mathbb{H}$ является не автоморфизмом, а *антиавтоморфизмом*: $\overline{zw} = \overline{w} \cdot \overline{z}$.

Упражнение 6.3. Проверьте это.

Кроме того, $|zw| = |z||w|$. Это следует, например, из равенства $(*)$ и мультипликативности определителя, или из равенства $|zw|^2 = zw\overline{zw} = zw\overline{w}\,\overline{z} = |z|^2|w|^2$.

Понятие нормы позволяет найти для каждого ненулевого кватерниона z обратный: такой кватернион z^{-1}, что $zz^{-1} = z^{-1}z = 1$. Он находится по формуле $z^{-1} = \overline{z}/|z|^2$. Поэтому $\mathbb{H}$ является *алгеброй с делением*, или *телом* (т.е. "некоммутативным полем").

6.2. **Кватернионы единичного модуля и чисто мнимые кватернионы.** Множество кватернионов единичного модуля образует группу по умножению, которую мы обозначим через $\mathrm{SU}(2)$. Геометрически $\mathrm{SU}(2)$ является трёхмерной сферой S^3, т.к. оно задаётся уравнением $a^2+b^2+c^2+d^2 = 1$. Следующее предложение объясняет это, на первый взгляд, странное обозначение.

Предложение 6.4. *При описанном выше гомоморфизме* $\mathbb{H} \to \mathrm{Mat}_2(\mathbb{C})$ *кватернионам из* $\mathrm{SU}(2)$ *соответствуют в точности специальные унитарные матрицы* 2×2 *(т.е. унитарные матрицы с определителем 1).*

Доказательство. Определитель матрицы равен квадрату нормы соответствующего кватерниона. Остаётся проверить условие унитарности. Пусть $A = \begin{pmatrix} z & w \\ x & y \end{pmatrix}$, причём $\det A = 1$. Тогда $A^{-1} = \begin{pmatrix} y & -w \\ -x & z \end{pmatrix}$. Условие унитарности $A^{-1} = A^*$ тогда равносильно равенству

$$\begin{pmatrix} y & -w \\ -x & z \end{pmatrix} = \begin{pmatrix} \overline{z} & \overline{x} \\ \overline{w} & \overline{y} \end{pmatrix},$$

т.е. равенствам $x = -\overline{w}$, $y = \overline{z}$. Это и значит, что матрица A соответствует некоторому кватерниону. □

Кстати, отметим, что если $z \in SU(2)$, то $z^{-1} = \overline{z}$.

Рассмотрим теперь множество *чисто мнимых кватернионов* $\mathfrak{I} = \{bi + cj + dk\} = \{z \in \mathbb{H} \mid z + \overline{z} = 0\}$. Оно является трёхмерным евклидовым пространством (скалярное произведение (v, w) строится по норме). Кроме того, на трёхмерном евклидовом пространстве есть антисимметричная операция векторного произведения $[v, w]$.

$\mathfrak{I}$ не замкнуто относительно умножения: произведение двух чисто мнимых кватернионов не обязано быть чисто мнимым. Но оказывается, что кватернионное умножение "знает" и про скалярное, и про векторное произведение на $\mathfrak{I}$. А именно, если $v, w \in \mathfrak{I}$, то их произведение в $\mathbb{H}$ равняется

$$v \cdot w = -(v, w) + [v, w],$$

где первое слагаемое — это вещественное число, а второе — вектор, т.е. элемент $\mathfrak{I}$.

Упражнение 6.5. Проверьте это равенство.

В частности, если $v \in \mathfrak{I}$, то $[v, v] = 0$, а значит, $v^2 = -|v|^2$. Получается, что квадрат всякого чисто мнимого кватерниона есть отрицательное число. В частности, всякий чисто мнимый кватернион единичного модуля является квадратным корнем из -1.

6.3. **Действие** $\mathrm{SU}(2)$ **на** $\mathfrak{I}$. [2] Наша цель — сопоставить каждому кватерниону $z \in \mathrm{SU}(2)$ вращение евклидова трёхмерного пространства $R_z \colon \mathfrak{I} \to \mathfrak{I}$.

Во-первых, заметим, что для фиксированного кватерниона $z \in \mathrm{SU}(2)$ отображения $\mathbb{H} \to \mathbb{H}$, заданные формулами $q \mapsto zq$ и $q \mapsto qz^{-1}$ суть ортогональные преобразования, т.к. они сохраняют норму. Однако ни одно из них не определяет действие на подпространстве $\mathfrak{I}$. Для того, чтобы $\mathfrak{I}$ переходило бы в себя, на нём можно действовать *композицией* этих преобразований, т.е. сопряжениями.

Лемма 6.6. *Пусть* $z \in \mathrm{SU}(2)$. *Отображение* $q \mapsto zqz^{-1}$ *переводит чисто мнимые кватернионы в чисто мнимые.*

Доказательство. Пусть $q \in \mathfrak{I}$. Это значит, что $q + \overline{q} = 0$. Докажем, что $zqz^{-1} + \overline{(zqz^{-1})} = 0$. Действительно,

$$zqz^{-1} + \overline{(zqz^{-1})} = zqz^{-1} + \overline{z^{-1}}\,\overline{qz} = zqz^{-1} + z\overline{q}z^{-1} = z(q + \overline{q})z^{-1} = 0.$$

□

Поскольку левое и правое умножение задают ортогональные преобразования, получаем, что отображение $R_z \colon q \mapsto zqz^{-1}$ есть ортогональное преобразование пространства $\mathbb{R}^3 = \mathfrak{I}$.

Лемма 6.7. *Отображение* $z \mapsto R_z$ *задаёт гомоморфизм групп* $\mathrm{SU}(2) \to \mathrm{O}(3)$.

Доказательство. Мы доказали, что преобразование R_z ортогонально. Необходимо лишь проверить, что это отображение — гомоморфизм. Проверим, что $R_z R_w = R_{zw}$. Это несложно:

$$R_z(R_w(q)) = R_z(wqw^{-1}) = zwqw^{-1}z^{-1} = zwq(zw)^{-1} = R_{zw}(q).$$

□

Далее мы покажем, что образ этого гомоморфизма есть в точности групп *специальных* ортогональных матриц $\mathrm{SO}(3)$. По теореме Эйлера, каждое специальное ортогональное преобразование $\mathbb{R}^3$ есть вращение. Вращение задаётся двумя параметрами: направлением оси и углом вращения. Мы увидим, как узнать эти параметры для преобразования R_z, зная кватернион $z \in \mathrm{SU}(2)$.

Пусть $z = a + bi + cj + dk = a + v' \in \mathrm{SU}(2)$, где a и v' — вещественная и мнимая части кватерниона z. Тогда $|z|^2 = a^2 + |v'|^2 = 1$. Поэтому существует такой угол $\varphi \in [0, \pi]$, что $a = \cos\varphi$, $|v| = \sin\varphi$.

[2] Порядок изложения немного отличается от того, что было на лекции

По причинам, которые станут понятны позже, сделаем замену переменной: положим $\varphi = \theta/2$, где $\theta \in [0, 2\pi]$. Тогда

$$z = \cos\frac{\theta}{2} + \sin\frac{\theta}{2} \cdot v,$$

где $v = v'/\sin(\theta/2)$ — вектор длины 1.

Предложение 6.8. *Пусть* $z = \cos(\theta/2) + \sin(\theta/2) \cdot v \in SU(2)$. *Преобразование* $R_z \colon \mathfrak{I} \to \mathfrak{I}$, $q \mapsto zqz^{-1}$ *есть поворот относительно оси, натянутой на вектор* v, *на угол* θ.

Замечание 6.9. Теперь понятно, зачем надо было полагать $\varphi = \theta/2$!

Доказательство. Сперва докажем, что R_z оставляет вектор v на месте. Это проверяется прямым вычислением. Если $z = \cos(\theta/2) + \sin(\theta/2) \cdot v$, то $z^{-}1 = z = \cos(\theta/2) - \sin(\theta/2) \cdot v$. Тогда

$$\begin{aligned} zvz^{-1} &= (\cos(\theta/2) + \sin(\theta/2) \cdot v)v(\cos(\theta/2) - \sin(\theta/2) \cdot v) = \\ &= (\cos(\theta/2)v - \sin(\theta/2)(v, v))(\cos(\theta/2) - \sin(\theta/2) \cdot v) = \\ &= \cos^2(\theta/2) \cdot v + \sin^2(\theta/2) \cdot v = v. \end{aligned}$$

(мы пользовались тем, что $(v, v) = 1$ и $[v, v] = 0$).

Значит, v остаётся на месте под действием R_z.

Далее, проверим, что R_z задаёт поворот на угол θ в плоскости, ортогональной вектору v. Выберем в этой плоскости ортогональный базис: пусть w — произвольный единичный вектор, ортогональный v, а $u = [v, w]$. Применим R_z к w.

Упражнение 6.10. Проверьте, что $R_z(w) = \cos\theta w + \sin\theta u$.

Таким образом, в плоскости $\langle w, u\rangle$ преобразование R_z действует поворотами на угол θ. Это завершает доказательство предложения. □

Значит, R_z отвечает вращению, и всякое вращение можно получить таким образом. Мы получили следующее предложение:

Предложение 6.11. *Имеется сюръективный гомоморфизм групп* $\mathrm{SU}(2) \to \mathrm{SO}(3)$.

Выясним, чему равно ядро этого гомоморфизма. Кватернион $z = \cos(\theta/2) + \sin(\theta/2) \cdot v$ отвечает тождественному преобразованию, когда угол θ равен $2\pi n$, т.е. $\theta/2 \in \{0, \pi\}$. Значит, $\sin(\theta/2) = 0$, а $\cos(\theta/2) = \pm 1$. Таким образом, $z = \pm 1$.

Поэтому предыдущее предложение можно уточнить:

Предложение 6.12. *Имеется изоморфизм групп* $\mathrm{SU}(2)/\pm 1 \to \mathrm{SO}(3)$.

С топологической точки зрения этот изоморфизм отвечает двулистному накрытию $S^3 \to \mathbb{RP}^3$ трёхмерной проективной плоскости трёхмерной сферой.

7. Седьмая лекция, 30 октября 2012 г.

7.1. **Представления: определение и несколько важных примеров.** Ранее мы изучали действия групп на множествах. Представлением группы называется её действие на векторном пространстве, согласованное со структурой этого векторного пространства.

Определение 7.1. Пусть G — группа, V — конечномерное векторное пространство над полем K. *Представление* группы G в пространстве V — это гомоморфизм $\rho\colon G \to GL(V)$. Пространство V называется *пространством представления*, а размерность $\dim V$ называется *размерностью* представления ρ.

Иными словами, представление сопоставляет каждому элементу группы невырожденный линейный оператор $\rho(g)$ на V, причём произведению элементов группы соответствует композиция операторов, а единичному элементу — тождественный оператор.

Приведём несколько примеров представлений групп.

Пример 7.2. Пусть G — произвольная группа, V — произвольное векторное пространство. *Тривиальное* представление G — это гомоморфизм $\rho\colon G \to \mathrm{GL}(V)$, переводящий любой элемент $g \in G$ в единичный оператор Id_V.

Пример 7.3. Пусть $M \subset V = \mathbb{R}^n$ — произвольное подмножество. Тогда имеется представление групп симметрий $\mathrm{Sym}M$ и вращений $\mathrm{Sym}^+ M$ в пространстве V: каждому элементу группы соответствует преобразование пространства V. В частности, так можно получить трёхмерные представления групп A_4, S_4 и A_5 как групп вращений правильных многогранников.

Пример 7.4 (перестановочное представление)**.** Пусть группа G действует на конечном множестве: $G \curvearrowright X$, где X — конечное множество. Рассмотрим векторное пространство V_X размерности $n = |X|$ с фиксированным базисом $e_{x_1}, \ldots, e_{x_n}$, где $x_1, \ldots, x_n$ — элементы из X. Тогда в пространстве V_X определено представление группы G по правилу

$$\rho(g)e_x = e_{g(x)}.$$

Пример 7.5 (леворегулярное представление)**.** Пусть G — конечная группа. Тогда она действует в пространстве $KG = \langle e_{g_1}, \ldots, e_{g_m} \rangle$. Определим представление R так:

$$R(g)e_h = e_{gh}.$$

Это частный случай перестановочного представления, где $X = G$, а группа действует на себе левыми сдвигами.

Пример 7.6 (праворегулярное представление)**.** Оно устроено так же, как и леворегулярное, только вместо левых сдвигов надо взять

правые: $R'(g)e_h = e_{hg^{-1}}$. Контрольный вопрос: зачем там минус первая степень?

Замечание 7.7. Мы будем рассматривать представления групп в *конечномерных* пространствах. Представления в бесконечномерных пространствах (обычно с дополнительной структурой, например, в гильбертовых пространствах) тоже имеет смысл рассматривать, но это совсем другая история. Кроме того, мы довольно скоро предположим, что основное поле K алгебраически замкнуто и имеет характеристику нуль (или что вообще $K = \mathbb{C}$). Теория представлений групп над алгебраически незамкнутыми полями и полями конечной характеристики — это тоже важный сюжет, но там жизнь устроена значительно сложнее, чем над $\mathbb{C}$.

Замечание 7.8 (терминологическое). Мы часто будем допускать различные вольности в словоупотреблении. Так, словом "представление" мы иногда будем называть не гомоморфизм, а само пространство V. Кроме того, оператор $\rho(g)$, действующий на пространстве V, иногда будет обозначаться g_V, а иногда — даже просто g (когда будет ясно, о каком пространстве идёт речь).

7.2. **Операции над представлениями.** На множестве векторных пространств имеются операции прямой суммы, тензорного произведения и взятия двойственного пространства. Кроме того, у векторных пространств бывают подпространства, по которым можно брать фактор. Те же понятия можно перенести и на представления, которые, по сути дела, являются векторными пространствами с дополнительной структурой (т.е. с действием группы).

Определение 7.9. Пусть $\rho_1 : G \to \mathrm{GL}(V)$ и $\rho_2 : G \to \mathrm{GL}(W)$ — два представления группы G (одной и той же!). *Прямая сумма* представлений $\rho_1 \oplus \rho_2 : G \to \mathrm{GL}(V \oplus W)$ — это представление группы G в пространстве $V \oplus W$, действие на котором определено по правилу

$$(\rho_1 \oplus \rho_2)(g)(v, w) = (\rho_1(g)v, \rho_2(g)w).$$

При этом, если выбрать в пространствах V и W базисы, то в соответствующем базисе пространства $V \oplus W$ матрица оператора $(\rho_1 \oplus \rho_2)(g)$ запишется блочной матрицей $\begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix}$.

Определение 7.10. *Тензорное произведение* представлений $\rho_1 \otimes \rho_2 : G \to \mathrm{GL}(V \otimes W)$ — это представление группы G в пространстве $V \otimes W$, действие на котором определено на *разложимых* тензорах из $V \otimes W$ по правилу

$$(\rho_1 \oplus \rho_2)(g)(v \otimes w) = (\rho_1(g)v) \otimes (\rho_2(g)w),$$

и продолжено по линейности на неразложимые тензоры.

Определение 7.11. *Сопряжённое представление* к представлению $\rho\colon G \to \mathrm{GL}(V)$ — это представление ρ' группы G в пространстве линейных функционалов V^*, определённое по правилу

$$\rho'(g)(\xi(v)) = \xi(\rho(g)^{-1}v), \qquad \xi \in V^*.$$

Отметим, что при этом определении каноническое спаривание $V \times V^* \to K$, $(v, \xi) \mapsto \langle \xi, v\rangle = \xi(v)$ окажется G-инвариантным:

$$\langle \xi, v\rangle = \langle \rho'(g)\xi, \rho(g)v\rangle \qquad \forall g \in G.$$

7.3. Морфизмы представлений, подпредставления, неприводимость и неразложимость.

Определение 7.12. Пусть V и W — представления одной и той же группы G. Линейное отображение векторных пространств $\varphi\colon V \to W$ называется *морфизмом представлений*, или *сплетающим оператором*, если оно перестановочно с действием группы G на V и W, т.е. если

$$g_W(\varphi(v)) = \varphi(g_V(v)) \qquad \forall v \in V.$$

Определение 7.13. *Ядро* $\operatorname{Ker}\varphi \subset V$ и *образ* $\operatorname{Im}\varphi \subset W$ — это ядро и образ φ как отображения векторных пространств.

Определение 7.14. *Подпредставление* $U \subset V$ — это подпространство в пространстве V, инвариантное относительно действия G (т.е. такое, что $\rho(g)u \in U$ для любых $g \in G$, $u \in U$).

Упражнение 7.15. Дайте определение факторпредставления.

Упражнение 7.16. Проверьте, что ядро и образ морфизма представлений $\varphi\colon V \to W$ — это подпредставления в V и W соответственно.

У каждого представления всегда есть два тривиальных подпредставления: это 0 и оно само.

Определение 7.17. Представление называется *неприводимым*, если у него нет нетривиальных подпредставлений.

Определение 7.18. Представление называется *неразложимым*, если оно не раскладывается в прямую сумму двух нетривиальных подпредставлений.

Ясно, что из неприводимости следует неразложимость: если у представления вовсе нет подпредставлений, то о разложении в прямую сумму не может быть и речи. Обратное, вообще говоря, неверно.

Пример 7.19. Рассмотрим двумерное представление аддитивной группы $\mathbb{Z} \to \mathrm{GL}_2(K)$, $n \mapsto \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Линейная оболочка первого базисного вектора есть подпредставление, дополнение к которому

не выделяется прямым слагаемым. Таким образом, это представление приводимо, но неразложимо.

К счастью, для достаточно большого класса групп понятия неприводимости и неразложимости совпадают. Как мы сейчас докажем, к этому классу относятся все конечные группы (а в лекции 11 мы увидим, что для компактных групп это тоже верно, причём доказательство практически ничем не отличается).

7.4. **Полная приводимость и теорема Машке.**

Определение 7.20. Представление V группы G называется *вполне приводимым*, если для каждого его подпредставления $W \subset V$ найдётся дополнительное подпредставление (т.е. такое подпредставление $U \subset V$, что $V = U \oplus W$).

Замечание 7.21 (терминологическое). Всякое неприводимое представление является вполне приводимым.

Теорема Машке утверждает, что представления *конечных* групп вполне приводимы, если характеристика поля не делит порядок группы или равна нулю. Сейчас мы докажем эту теорему в случае, когда основное поле — это $\mathbb{R}$ или $\mathbb{C}$. Доказательство для произвольного поля будет приведено в следующей лекции.

Определение 7.22. Скалярное произведение на пространстве представления V называется G-инвариантным, если $(gv, gw) = (v, w)$ для любых $g \in G$ и $v, w \in V$.

Лемма 7.23. *На каждом вещественном или комплексном представлении конечной группы G существует положительно определенное (соотв. эрмитово) G-инвариантное скалярное произведение.*

Доказательство. Пусть $(\ ,\ )$ — произвольное положительно определённое или эрмитово скалярное произведение. Построим по нему G-инвариантное скалярное произведение, усреднив его по группе. А именно, определим новое скалярное произведение $(\ ,\ )_G$ по формуле

$$(v, w)_G = \frac{1}{|G|} \sum_{g \in G} (gu, gw).$$

(без множителя $1/|G|$ при желании можно и обойтись). Ясно, что $(gu, gv)_G = (u, v)_G$, так как левый сдвиг на группе просто будет переставлять слагаемые в правой части формулы, то есть построенное скалярное произведение будет G-инвариантно. □

Теорема 7.24 (Машке). *Пусть V — вещественное или комплексное представление конечной группы G, W — подпредставление в V. Тогда в V найдётся дополнительное подпредставление U, т.е. такое подпредставление, для которого $U \oplus W = V$.*

Доказательство. В качестве U можно взять $U = W^\perp = \{u \in V \mid (u, w)_G = 0 \quad \forall w \in W\}$, где ортогональное дополнение берется относительно G-инвариантного положительно определенного (соотв. эрмитова) скалярного произведения. Тогда $V = W \oplus U$ как векторные пространства. Осталось проверить, что U является подпредставлением группы G. Проверим это: пусть $u \in U$, убедимся, что $gu \in U$. Для этого надо доказать, что $(gu, w)_G = 0$ для любого $w \in W$. Действительно,

$$(gu, w) = (g^{-1}(gu), g^{-1}(w))_G = (u, g^{-1}w)_G = 0,$$

поскольку $g^{-1}w \in W$ (так как W — подпредставление), а $u \in W^\perp$. Поэтому U является дополнительным подпредставлением к W. $\square$

Следствие 7.25. *Всякое представление конечной группы над* $\mathbb{R}$ *или* $\mathbb{C}$ *вполне приводимо.*

8. Восьмая лекция, 6 ноября 2012 г.

8.1. **Другое доказательство теоремы Машке.** Докажем теорему Машке в более общем виде: для произвольного поля, не обязательно для $\mathbb{R}$ или $\mathbb{C}$.

Теорема 8.1 (Машке)**.** *Пусть V — представление конечной группы G над полем K, причём $|G| \not\vdots \operatorname{char} K$. Пусть W — подпредставление в V. Тогда в V найдётся дополнительное подпредставление U, т.е. такое подпредставление, для которого $U \oplus W = V$.*

Доказательство. Основная идея этого доказательства та же, что и предыдущего: каким-то образом выбрать дополнительное к W подпространство, а потом "подправить" этот выбор так, чтобы дополнение было бы G-инвариантным.

Напомним, что оператор $\pi\colon V \to V$ называется *проектором* на подпространство W, если $\pi|_W = Id_W$ и $\operatorname{Im}\pi = W$. Из линейной алгебры известно, что в этом случае $V = W \oplus \operatorname{Ker}\pi$. То есть $\operatorname{Ker}\pi$ — дополнительное к W подпространство. Проблема только в том, что оно может быть не G-инвариантным. Исправить это можно опять-таки с помощью усреднения по группе G.

Возьмём произвольный проектор π на подпространство W. Определим новый оператор π_G по следующей формуле:

$$\pi_G(v) = \frac{1}{|G|}\sum_{g\in G} g_V v).$$

Легко видеть, что π_G снова является проектором на подпространство W. Для этого надо проверить, что для любого $w \in W$ оператор π_G оставляет его на месте: $\pi_G(w) = w$, и что $\operatorname{Im}\pi_G \subset W$. Эта проверка оставляется читателю в качестве лёгкого упражнения.

Кроме того, π_G является морфизмом представлений. Проверим это: действительно, для любого $h \in G$ и для любого $v \in V$

$$h_V(\pi_G(v)) = h_V\left(\frac{1}{|G|}\sum_{g\in G} g_V v\right) = \frac{1}{|G|}\sum_{g\in G} h_V g_V v =$$
$$= \frac{1}{|G|}\sum_{g\in G}(h_V g_V h_V^{-1})h_V v = \frac{1}{|G|}\sum_{g\in G} g_V h_V v = \pi_G(h_V v).$$

(в предпоследнем равенстве мы воспользовались тем, что действие группы на себе сопряжениями — это биекция).

Мы видели в прошлой лекции, что ядро морфизма — это подпредставление. Поэтому $\operatorname{Ker}\pi_G$ и есть искомое дополнительное к W подпредставление. □

8.2. **Лемма Шура.** Это очень простое, но в то же время крайне полезное утверждение о том, как устроены морфизмы между *неприводимыми* представлениями.

Теорема 8.2 (лемма Шура)**.** *Пусть V, W — неприводимые представления группы G, $\varphi\colon V \to W$ — морфизм представлений. Тогда:*

(1) *либо φ — изоморфизм (т.е. $V \cong W$), либо $\varphi = 0$;*
(2) *если основное поле алгебраически замкнуто, то $\varphi = \lambda\mathrm{Id}$ (т.е. всякий изоморфизм неприводимых представлений пропорционален тождественному).*

Доказательство. 1) Поскольку φ — морфизм, $\operatorname{Ker}\varphi$ — подпредставление в V. Но V неприводимо, поэтому либо $\operatorname{Ker}\varphi = V$ (откуда $\varphi = 0$), либо $\operatorname{Ker}\varphi = 0$, и φ — мономорфизм.

Аналогично из того, что $\operatorname{Im}\varphi$ — подпредставление в W, заключаем, что φ — эпиморфизм. Поэтому φ либо нуль, либо изоморфизм.

2) Пусть $\varphi\colon V \to V$ — изоморфизм представлений. Кроме того, $\lambda\mathrm{Id}\colon V \to V$ — тоже морфизм представлений. Значит, их разность $\varphi - \lambda\mathrm{Id}$ опять-таки является морфизмом представлений при любом λ.

Пусть теперь λ равняется какому-нибудь собственному значению оператора φ (над алгебраически замкнутым полем у любого оператора есть собственное значение!). Тогда оператор $\varphi - \lambda\mathrm{Id}$ вырожден, т.е. $\operatorname{Ker}(\varphi - \lambda\mathrm{Id}) \neq 0$. Но ядро морфизма — подпредставление в неприводимом представлении V, поэтому $\operatorname{Ker}(\varphi - \lambda\mathrm{Id}) = V$. Стало быть, $\varphi = \lambda\mathrm{Id}$, что и требовалось. □

8.3. **Представления абелевых групп.** Пусть $\rho\colon G \to \mathrm{GL}(V)$ — представление группы G. Всякий элемент $g \in G$ определяет отображение $g_V\colon V \to V$. Это отображение, вообще говоря, не будет морфизмом: нет никакой причины, по которой оно должно быть перестановочно с действием других элементов группы G. Иначе говоря, для какого-либо другого элемента $h \in G$ может случиться так, что $h_V g_V \neq g_V h_V$. Ясно, что это равенство будет всегда выполнено, если $g \in Z(G)$. Соответственно, для элемента $g \in Z(G)$ центра группы G отображение g_V будет морфизмом.

Упражнение 8.3. Докажите, что это условие не только достаточное, но и необходимое: иначе говоря, для любого элемента $g \notin Z(G)$ *найдётся* такое представление V, для которого $g_V\colon V \to V$ не будет морфизмом.

Пускай теперь у нас выполнены условия леммы Шура, и пусть G — *абелева* группа. Тогда $Z(G) = G$. Пусть V — неприводимое представление группы G. Для всякого элемента $g \in G$ оператор $g_V\colon V \to V$ является морфизмом. Согласно лемме Шура, он скалярен. Получается, что всякий элемент группы G действует на

представлении V скалярной матрицей. Поэтому всякое подпространство в V инвариантно относительно G. Но в силу неприводимости представления V это возможно только в том случае, когда $\dim V = 1$.

Мы доказали следующее

Предложение 8.4. *Все представления абелевой группы над алгебраически замкнутым полем одномерны, т.е. являются гомоморфизмами $G \to K^*$.*

Гомоморфизмы $\mathrm{Hom}(G, K^*)$ сами образуют абелеву группу (относительно композиции). Эта группа называется *двойственной* к G и обозначается $G^\vee$.

Упражнение 8.5. Докажите, что $G^\vee \cong G$. (Этот изоморфизм не является каноническим, он напоминает изоморфизм между пространством и двойственным к нему).

9. Девятая лекция, 13 ноября 2012 г.

9.1. **Два следствия из теоремы Машке.**

Следствие 9.1 (об унитаризуемости/ортогонализуемости представлений)**.** *Пусть $\rho\colon G \to \mathrm{GL}(V)$ — комплексное (соотв. вещественное) представление конечной группы G. Тогда на V существует такая невырожденная эрмитова (соотв. положительно определённая симметрическая) форма, для которой все операторы $\rho(g)$ будут являться унитарными (соотв. ортогональными).*

Доказательство. Условие унитарности/ортогональности оператора $\rho(g)$ можно записать так:

$$(\rho(g)v, \rho(g)w) = (v, w) \text{ для любых } v, w \in V.$$

Это условие имеет место для G-инвариантной эрмитовой (соотв. положительно определённой симметрической) формы, построенной в первом доказательстве теоремы Машке. □

Следствие 9.2. *Пусть $\rho\colon G \to \mathrm{GL}(V)$ — комплексное представление конечной группы. Тогда всякий оператор $\rho(g)$ диагонализуем (т.е. для него существует базис из собственных векторов), причём все его собственные значения по модулю равны 1.*

Доказательство. Действительно, это утверждение верно для любого унитарного оператора. □

Замечание 9.3. Вообще говоря, неверно, что все операторы $\rho(g)$ диагонализуемы *одновременно* (т.е. в одном и том же базисе): это значило бы, что представление распадается в прямую сумму одномерных, что имеет место далеко не всегда.

9.2. **Характеры.**

Далее мы будем считать, что основным полем является поле $\mathbb{C}$. Таким образом, для представлений конечных групп имеют место теорема Машке и лемма Шура.

Определение 9.4. Пусть $\rho\colon G \to \mathrm{GL}(V)$ — представление группы G. *Характером* этого представления называется комплекснозначная функция на группе G, значение которой в точке g равняется следу оператора g_V:

$$\chi_V\colon G \to \mathbb{C}, \qquad \chi_V(g) = \operatorname{tr} g_V.$$

Замечание 9.5. Элемент $e \in G$ действует на пространстве V единичным оператором, след которого равен размерности пространства. Поэтому $\chi_V(e) = \dim V$.

Пример 9.6. Характер тривиального представления — функция, равная 1 во всех точках группы G.

Пример 9.7. Пусть $G \to \mathrm{GL}(V)$ — перестановочное представление, происходящее из действия группы G на конечном множестве X. Тогда значение характера $\chi_V(g)$ на элементе g равно количеству точекиз X, неподвижных относительно действия G:

$$\chi_V(g) = \#\{x \in X : g \circ x = x\}.$$

Для доказательства этого следует записать матрицу g_V в базисе $\{e_x\}$ — это будет матрица перестановки, и отметить, что единицы на диагонали этой матрицы соответствуют неподвижным точкам.

Пример 9.8. Пусть R — регулярное представление конечной группы G (т.е. перестановочное представление, отвечающее действию G на себе левыми сдвигами). Тогда

$$\chi_R(g) = \begin{cases} |G|, & g = e; \\ 0 & \text{иначе.} \end{cases}$$

Действительно, левый сдвиг на неединичный элемент g не имеет неподвижных точек на G: они отвечали бы решениям уравнения $gx = x$, а такое уравнение при $g \neq e$ решений в G неразрешимо.

Характеры замечательны тем, что они "хорошо себя ведут" при взятии прямой суммы и тензорного произведения представлений.

Предложение 9.9. *Пусть V и W — представления конечной группы G. Тогда:*

(1) $\chi_{V\oplus W}(g) = \chi_V(g) + \chi_W(g)$;
(2) $\chi_{V\otimes W}(g) = \chi_V(g)\chi_W(g)$;
(3) $\chi_{V^*}(g) = \overline{\chi_V(g)}$.

Доказательство. Пусть $g \in G$ — произвольный элемент группы. Согласно следствию 9.2, для него существуют собственные базисы $v_1, \ldots, v_n$ и $w_1, \ldots, w_m$ пространств V и W соответственно:

$$g_V v_i = \lambda_i v_i, \qquad g_W w_j = \mu_j w_j.$$

Поскольку след оператора равен сумме его собственных значений, $\chi_V(g) = \sum \lambda_i$ и $\chi_W(g) = \sum \mu_j$.

Набор векторов $v_1, \ldots, v_n, w_1, \ldots, w_m$ является базисом пространства $V \oplus W$, собственным для оператора $g_{V\oplus W}$. Поэтому след данного оператора равен $\sum \lambda_i + \sum \mu_j$, т.е. $\chi_V(g) + \chi_W(g)$.

Аналогично доказывается и второе равенство: $v_i \otimes w_j$ является базисом пространства $V \otimes W$, собственным для оператора $g_{V\otimes W}$, поэтому след последнего равняется $\sum_{i,j} \lambda_i\mu_j = \chi_V(g)\chi_W(g)$.

Последнее равенство вытекает из того, что если диагонализуемый оператор A имеет собственные значения $\lambda_1, \ldots, \lambda_n$ на пространстве V, то сопряжённый к нему оператор A^* на пространстве V^* имеет собственные значения $\lambda_1^{-1}, \ldots, \lambda_n^{-1}$. Поскольку собственные значения g_V по модулю равны 1, для них имеется равенство

$\lambda_i^{-1} = \overline{\lambda_i}$. Поэтому след оператора g_{V^*} равняется $\lambda_1^{-1} + \cdots + \lambda_n^{-1} = \overline{\lambda_1} + \cdots + \overline{\lambda_n} = \overline{\chi_V(g)}$. □

9.3. **Первая формула проекции.** Пусть V — произвольное представление группы G. *Подпространством инвариантов* группы G назовём подпространство

$$V^G = \{v \in V \mid g_V v = v \quad \forall g \in G\} \subset V.$$

Ясно, что это подпредставление, являющееся суммой всех тривиальных подпредставлений в V. Оказывается, несложно выписать проектор на это подпредставление:

Предложение 9.10. *Положим*

$$\pi_V = \frac{1}{|G|} \sum_{g \in G} g_V \in \mathrm{End}(V).$$

Тогда π_V есть морфизм представлений, являющийся проектором на V^G.

Доказательство. Сперва проверим, что π_V — морфизм представлений. Для этого надо проверить, что $\pi_V h_V = h_V \pi_V$ для любого $h \in G$.

$$\pi_V h_v = \left(\frac{1}{|G|} \sum_{g \in G} g_V\right) h_V = \frac{1}{|G|} \sum_{g \in G} h_V h_V^{-1} g_V h_V =$$

$$= \frac{1}{|G|} h_V \sum_{g \in G} h_V^{-1} g_V h_V = h_V \left(\frac{1}{|G|} \sum_{g \in G} g_V\right) = h_V \pi_V.$$

(в предпоследнем равенстве мы меняем порядок суммирования, пользуясь тем, что сопряжение есть взаимно-однозначное отображение группы в себя).

Далее, проверим, что π_V есть проектор на V^G. Для этого надо проверить две вещи: что всякий вектор из V^G переходит под действием π_V в себя (т.е. π_V при ограничении на V^G даёт тождественный оператор) и что $\mathrm{Im}\, \pi_V \subset V^G$.

Проверим первое. Пусть $w \in V^G$. Тогда $g_V w = w$ для любого g, и

$$\pi_V w = \frac{1}{|G|} \sum_{g \in G} g_V w = \frac{1}{|G|} \sum_{g \in G} w = \frac{|G|}{|G|} w = w.$$

Наконец, чтобы убедиться, что $\mathrm{Im}\, \pi_V \subset V^G$, покажем, что всякий вектор из $\mathrm{Im}\, \pi_V$ инвариантен относительно любого элемента $h \in G$:

$$h_V(\pi_V v) = h_V \left(\frac{1}{|G|} \sum_{g \in G} g_V v\right) = \frac{1}{|G|} \sum_{g \in G} h_V g_V v = \frac{1}{|G|} \sum_{g \in G} g_V v = \pi_V v.$$

(снова меняем порядок суммирования, но при этом применяем не сопряжение, а левый сдвиг). □

Поскольку след проектора равен размерности его образа, получаем такое следствие:

Следствие 9.11. $\dim V^G = \operatorname{tr} \pi_V$.

9.4. **Соотношение ортогональности для характеров.** Из результатов двух предыдущих параграфов получается следующий результат, который для нас окажется ключевым.

Теорема 9.12. *Пусть V, W — неприводимые представления конечной группы G. Тогда*

$$\frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_W(g) = \begin{cases}1, & V\cong W;\\ 0, & V\ncong W.\end{cases}$$

Доказательство. Как обсуждалось в прошлой лекции, морфизмы из V в W суть G-инварианты в представлении $\operatorname{Hom}(V,W)$. Их пространство одномерно, если V и W изоморфны, и нульмерно в противном случае. Но $\operatorname{Hom}(V,W)\cong V^*\otimes W$. Поэтому

$$\dim \operatorname{Hom}_G(V,W) = \dim(\operatorname{Hom}(V,W))^G = \dim(V^*\otimes W)^G = \begin{cases}1, & V\cong W;\\ 0, & V\ncong W.\end{cases}$$

Вычислим $\dim(V^*\otimes W)^G$ по предыдущему следствию как след соответствующего проектора:

$$\dim(V^*\otimes W)^G = \operatorname{tr}\pi_{V^*\otimes W} = \frac{1}{|G|}\sum_{g\in G}\operatorname{tr} g_{V^*\otimes W} =$$

$$= \frac{1}{|G|}\sum_{g\in G}\chi_{V^*\otimes W}(g) = \frac{1}{|G|}\sum_{g\in G}\chi_{V^*}(g)\chi_W(g) = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\chi_W(g),$$

что и доказывает теорему. □

9.5. **Центральные функции.** Следующее свойство характеров очевидным образом вытекает из инвариантности следа оператора, т.е. равенства $\operatorname{tr} A = \operatorname{tr} C^{-1}AC$:

Предложение 9.13. $\chi_V(g) = \chi_V(h^{-1}gh)$.

Поэтому характер представления принимает одно и то же значение на всех представителях одного и того же класса сопряжённых элементов в группе G.

Можно дать общее определение:

Определение 9.14. Функция на группе $\alpha\colon G\to\mathbb{C}$ называется *центральной*, если она постоянна на классах сопряжённых элементов, т.е. для любых $g, h\in G$

$$\alpha(g) = \alpha(h^{-1}gh).$$

Пространство всех центральных функций мы будем обозначать как $\mathbb{C}^{class}G$. Его размерность равна числу классов сопряжённости в группе G. Характеры являются примерами центральных функций.

Введём на пространстве $\mathbb{C}^{class}G$ эрмитово скалярное произведение по формуле:

$$\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\alpha(g)} \beta(g).$$

Упражнение 9.15. Проверьте, что это действительно эрмитово скалярное произведение.

Это определение позволяет переформулировать теорему 9.12:

Следствие 9.16. *Характеры неприводимых представлений образуют ортонормированную систему векторов в пространстве* $\mathbb{C}^{class}G$*:*

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1, & V \cong W; \\ 0, & V \ncong W. \end{cases}$$

10. Десятая лекция, 20 ноября 2012 г.

Из теоремы 9.12 сразу следует масса замечательных результатов о представлениях группы G.

10.1. Следствия соотношений ортогональности.

Следствие 10.1. *Характеры различных неприводимых представлений линейно независимы как элементы* $\mathbb{C}^{class}G$.

Доказательство. Действительно, ортогональная система векторов является линейно независимой. □

Следствие 10.2. *Число неприводимых представлений группы G не превосходит числа её классов сопряжённости.*

Доказательство. Количество векторов ортогональной системы не превосходит размерности объемлющего пространства $\mathbb{C}^{class}G$, т.е. числа классов сопряжённости. □

Замечание 10.3. Далее мы увидим, что это неравенство на самом деле является равенством.

Следствие 10.4. *Представление V неприводимо тогда и только тогда, когда* $\langle \chi_V, \chi_V \rangle = 1$.

Доказательство. Пусть $V = V_1 \oplus \cdots \oplus V_k$, где V_i неприводимы. Тогда $\chi_V = \chi_{V_1} + \cdots + \chi_{V_n}$, откуда по полуторалинейности скалярного произведения получаем, что

$$\langle \chi_V, \chi_V \rangle = \sum_{i,j} \langle \chi_{V_i}, \chi_{V_j} \rangle = \sum_i \langle \chi_{V_i}, \chi_{V_i} \rangle = n.$$

□

Следствие 10.5. *Пусть V — произвольное представление, W — неприводимое представление группы G. Тогда кратность вхождения W в V равна* $\langle \chi_W, \chi_V \rangle$.

Доказательство. Докажите это сами. □

Следствие 10.6. *Представление полностью определяется своим характером (у различных представлений разные характеры).*

Доказательство. Действительно, предыдущее следствие утверждает, что кратность вхождения всякого неприводимого представления W в данное представление V однозначно определяется по χ_V. □

Следствие 10.7. *Кратность вхождения любого неприводимого представления V в регулярное R равна* $\dim V$.

Доказательство. Вычислим $\langle \chi_V, \chi_R \rangle$:

$$\langle \chi_V, \chi_R \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)} \chi_R(g) = \frac{1}{|G|} \overline{\chi_V(e)} \chi_R(e) = \frac{|G|}{|G|} \overline{\chi_V(e)} = \dim V.$$

(здесь мы пользуемся тем, что характер регулярного представления равен $|G|$ в единице группы и нулю в остальных точках — см. пример 9.8). □

Следствие 10.8 (Формула Бернсайда)**.** *Пусть $d_1, \dots, d_k$ — размерности всех неприводимых представлений группы G. Тогда*

$$|G| = d_1^2 + \dots + d_k^2.$$

Доказательство. Это вытекает из двух предыдущих следствий (напомним, что $|G|$ — это размерность регулярного представления). □

10.2. **Вторая формула проекции.** Наша следующая цель — понять, что неприводимых представлений *столько же*, сколько классов сопряжённости в группе. Это эквивалентно тому, что их характеры образуют *базис* (а не просто ортонормированную систему) в пространстве центральных функций.

Предложение 10.9. *Пусть $\alpha \in \mathbb{C}^{class}G$ — центральная функция, V — произвольное представление группы G (возможно, приводимое). Тогда линейный оператор*

$$\pi_{\alpha,V} = \frac{1}{|G|} \sum_{g \in G} \alpha(g) g_V \colon V \to V$$

является морфизмом представлений.

Замечание 10.10. При $\alpha \equiv 1$ это предложение есть часть предложения 9.10, а $\pi_{\alpha,V}$ — проектор на подпространство инвариантов.

Доказательство. Проверим, что для любого элемента $h \in G$ оператор h_V перестановочен с $\pi_{\alpha,V}$. Действительно,

$$\pi_{\alpha,V} h_V = \frac{1}{|G|} \sum_{g \in G} \alpha(g) g_V h_V = \frac{1}{|G|} \sum_{g \in G} \alpha(g) h_V h_V^{-1} g_V h_V =$$
$$= h_V \frac{1}{|G|} \sum_{g \in G} \alpha(h^{-1}gh)(h_V^{-1} g_V h_V) = h_V \pi_V.$$

□

Задача 10.11. Докажите обратное: если $\alpha \notin \mathbb{C}^{class}G$, то найдётся такое представление, для которого $\pi_{\alpha,V}$ не будет морфизмом представлений.

Теорема 10.12. *Характеры неприводимых представлений χ_V образуют ортонормированный базис в пространстве $\mathbb{C}^{class}V$.*

Доказательство. Предположим противное: пусть существует такая функция $\alpha \in \mathbb{C}^{class}G$, ортогональная характерам *всех* неприводимых представлений. Значит, она ортогональна характерам всех

представлений (каждое представление есть прямая сумма неприводимых). Пусть V — неприводимое представление. Тогда

$$\langle \alpha, \chi_V \rangle = 0.$$

Рассмотрим морфизм $\pi_{\alpha,V}$ и докажем, что он является нулевым (как эндоморфизм пространства V). Действительно, по лемме Шура $\pi_{\alpha,V} = \lambda \cdot Id$. Вычислим константу λ. Для этого заметим, что $\lambda \dim V = \operatorname{tr} \pi_{\alpha,V}$, и вычислим след оператора $\pi_{\alpha,V}$:

$$\operatorname{tr} \pi_{\alpha,V} = \frac{1}{|G|} \sum_{g \in G} \operatorname{tr} \alpha(g) g_V = \frac{1}{|G|} \sum \alpha(g) \chi_V(g) =$$

$$= \overline{\frac{1}{|G|} \sum \overline{\alpha(g)} \cdot \overline{\chi_V(g)}} = \overline{\langle \alpha, \chi_{V^*} \rangle} = 0.$$

Поэтому $\lambda = 0$, и оператор $\pi_{\alpha,V}$ тождественно равен нулю.

Далее мы выведем отсюда, что $\alpha \equiv 0$ как функция на группе.

Определение 10.13. Представление $\rho\colon G \to \mathrm{GL}(V)$ называется *точным*, если оно является мономорфизмом (т.е. $\rho(g) \neq 1_V$ при $g \neq e$).

Предложение 10.14. *Регулярное представление R является точным; соответствующие элементы $g_R \in \operatorname{End} R$ линейно независимы (как эндоморфизмы пространства R).*

Доказательство. Рассмотрим базисные векторы $e_g \in R$. Возьмём среди них отвечающий единичному элементу группы e_{id}. Поскольку $g_R(e_{id}) = e_g$, а все e_g, будучи базисными векторами, линейно независимы, то и g_R тоже линейно независимы. □

Вернёмся к доказательству того, что $\alpha = 0$. Мы знаем, что $\pi_{\alpha,V}$ есть нулевой оператор для любого представления V. Рассмотрим этот оператор для регулярного представления, получим, что

$$\sum \alpha(g) g_R = 0$$

как элемент $\operatorname{End} R$. Но, с другой стороны, предыдущее предложение утверждает, что g_R линейно независимы. Следовательно, $\alpha(g) = 0$ при любом g. Получаем, что всякая функция на группе, ортогональная всем характерам неприводимых представлений, тождественно равна нулю. Что и требовалось доказать. □

Следствие 10.15. *Пусть k — количество классов сопряжённости в группе G. Существует ровно k неприводимых представлений группы G, назовём их $V_1, \ldots, V_k$. При этом регулярное представление изоморфно сумме*

$$R = V_1^{\dim V_1} \oplus \cdots \oplus V_k^{\dim V_k}.$$

Задача 10.16. Докажите, что $\pi_{\chi_{V_i^*},R}$ есть проектор на компоненту $V_i^{\dim V_i}$.

10.3. **Групповая алгебра.** Пусть R — регулярное представление группы G. На пространстве R можно ввести умножение, определив его на базисных векторах по правилу

$$e_g e_h = e_{gh}.$$

Мы получим ассоциативную некоммутативную алгебру над $\mathbb{C}$ с единицей, называемую *групповой алгеброй* группы G. Она обозначается через $\mathbb{C}G$.

Определение 10.17. *Представление* групповой алгебры в векторном пространстве V — это гомоморфизм алгебр $\mathbb{C}G \to \operatorname{End} V$.

Ясно, что такой гомоморфизм задаёт на V структуру левого $\mathbb{C}G$-модуля.

Кроме того, всякое представление

$$\rho\colon G \to \mathrm{GL}(V)$$

можно однозначно продолжить по линейности до гомоморфизма *алгебр*

$$\tilde{\rho}\colon \mathbb{C}G \to \operatorname{End}(V).$$

Выше мы видели, что $R = V_1^{\dim V_1} \oplus \cdots \oplus V_k^{\dim V_k}$. Оказывается, имеет место более сильное утверждение.

Теорема 10.18. *Имеется изоморфизм алгебр*

$$\mathbb{C}G \cong \operatorname{End}(V_1) \oplus \cdots \oplus \operatorname{End}(V_k).$$

(иными словами, $\mathbb{C}G$ изоморфна прямой сумме матричных алгебр, каждая из которых есть алгебра эндоморфизмов одного из её неприводимых представлений).

Доказательство. Поскольку V_i — это (неприводимые) представления, у нас имеются гомоморфизмы алгебр

$$\mathbb{C}G \to \operatorname{End}(V_i).$$

Можно рассмотреть диагональное отображение в прямую сумму:

$$\mathbb{C}G \cong \operatorname{End}(V_1) \oplus \cdots \oplus \operatorname{End}(V_k).$$

Оно инъективно, поскольку регулярное представление точно. С другой стороны, левая и правая часть имеют одинаковые размерности (это формула Бернсайда). Значит, это отображение есть изоморфизм. □

11. Одиннадцатая лекция, 27 ноября 2012 г.

Ближайшие три лекции будут посвящены группам Ли и классификации представлений группы Ли SU_2.

Группой Ли называется абстрактная группа, которая снабжена структурой гладкого многообразия (вещественного или комплексного). Иначе говоря, группа Ли — это многообразие, на котором введена структура группы.

11.1. **Напоминание о многообразиях.** Пусть K — это $\mathbb{R}$ или $\mathbb{C}$. Для простоты мы будем работать только с многообразиями, вложенными в K^n.

Определение 11.1. Подмножество $M \subset K^n$ называется *d-мерным гладким многообразием*, если в некоторой окрестности любой своей точки $p \in M$ его можно задать при помощи системы уравнений

$$f_i(x_1, \dots, x_n) = 0, \qquad i = 1, \dots, m$$

где $m = n - d$, причём матрица частных производных этой системы имеет полный ранг: $\operatorname{rk}\left(\frac{\partial f_i}{\partial x_j}\right)(p) = m$.

Замечание 11.2. Всякое *открытое* подмножество в K^n локально задаётся пустой системой уравнений, следовательно, является n-мерным многообразием. Всякое *дискретное* подмножество в K^n локально задаётся системой уравнений $x_i = p_i$ и поэтому является нульмерным подмногообразием.

Равенство $\operatorname{rk}\left(\frac{\partial f_i}{\partial x_j}\right)(p) = m$ означает, что некоторый минор порядка m матрицы частных производных отличен от нуля. Будем считать, что это минор, образованный первыми m столбцами матрицы. Тогда по теореме о неявной функции переменные $x_1, \dots, x_m$ выражаются при помощи гладких функций через свободные переменные, в качестве которых можно взять $x_{m+1}, \dots, x_n$:

$$\begin{aligned} x_1 &= \varphi_1(x_{m+1}, \dots, x_n); \\ &\dots \\ x_m &= \varphi_m(x_{m+1}, \dots, x_n). \end{aligned}$$

Касательное пространство T_pM в точке $p \in M$ состоит из векторов $(dx_1, \dots, dx_n)$, удовлетворяющих системе уравнений

$$df_i(p) = \sum_{j=1}^{n} \frac{\partial f_i}{\partial x_j} dx_j = 0 \qquad (i = 1, \dots, m)$$

Размерность касательного пространства есть пространства решений этой системы, то есть $d = n - m$.

11.2. **Группы Ли: определение и примеры.** Перейдём к определению группы Ли. Мы будем рассматривать только *линейные*, или *матричные* группы Ли — т.е. такие, которые являются подгруппами в $GL_n(K)$.

Определение 11.3. *Линейная группа Ли* — это подгруппа в $\mathrm{GL}_n(K)$, являющаяся гладким многообразием в пространстве $\mathrm{Mat}_n(K)$.

Условие линейности не является очень ограничительным — неформально говоря, все важные группы Ли являются линейными. Бывают такие группы Ли, которые не вкладываются в группу матриц, однако это некоторая экзотика.

Размерность группы Ли — это её размерность как многообразия.

Группа G инвариантна относительно левых сдвигов. Из этого следует, что в окрестности каждой своей точки она (как многообразие) устроена "одинаково". Так, например, если мы хотим доказать, что матричная группа есть группа Ли, то проверять условие гладкости можно только в одной точке — обычно удобнее всего делать это в единице.

Пример 11.4. $\mathrm{GL}_n(K)$ выделяется в $\mathrm{Mat}_n(K)$ условием $\det g \neq 0$. Это условие задаёт открытое множество, поэтому $\mathrm{GL}_n(K)$ — группа Ли размерности n^2.

Пример 11.5. $\mathrm{SL}_n(K) = \{g \in \mathrm{Mat}_n(K) \mid \det g = 1\}$. Проверим, что $\mathrm{SL}_n(K)$ есть многообразие. Для этого найдём размерность его касательного пространства в единице. Несложно проверить (проделайте это!), что $d_E(\det g - 1) = \operatorname{tr} dg$. Поэтому $T_E \mathrm{SL}_n(K)$ задаётся условием $\operatorname{tr} dg = 0$, то есть состоит из матриц со следом нуль. Это (n^2-1)-мерное векторное пространство, поэтому $\mathrm{SL}_n(K)$ является группой Ли размерности $n^2 - 1$.

Далее докажем, что $\mathrm{O}_n(K)$ есть группа Ли. Для этого можно было бы выписать систему из $n(n+1)/2$ уравнений, задающих группу $\mathrm{O}_n(K)$, вычислить матрицу частных производных к этой системе и доказать, что она имеет полный ранг. Однако можно сделать это иначе, если работать с матричнозначными функциями многих переменных.

Пусть $\Phi = \Phi(x_1, \ldots, x_n)$ — гладкая матричнозначная функция n переменных (гладкость означает то, что матричные элементы являются гладкими функциями от x_i. Тогда имеет смысл понятие частных производных $\partial\Phi/\partial x_i$. Определим полный дифференциал функции Φ по формуле

$$d\Phi = \sum \frac{\partial \Phi}{\partial x_i} dx_i.$$

Упражнение 11.6. Докажите, что полный дифференциал линеен и удовлетворяет тождеству Лейбница (некоммутативному!):

$$d(\Phi + \Psi) = d\Phi + d\Psi; \qquad d(\Phi\Psi) = (d\Phi)\Psi + \Phi(d\Psi).$$

Пример 11.7. Докажем, что $\mathrm{O}_n(K)$ — группа Ли. Она задаётся матричным уравнением $gg^t - E = 0$. Продифференцируем это уравнение, получим: $g \cdot dg^t + dg \cdot g^t = 0$. Подставив $g = E$, получаем линейное матричное уравнение $dg + dg^t = 0$. Пространство его решений $T_E\,\mathrm{O}_n$— это пространство кососимметрических матриц, которое имеет размерность $n(n-1)/2$.

Пример 11.8. Аналогичным образом группа U_n задаётся уравнением $gg^* = E$. Её касательное пространство есть пространство *косоэрмитовых* матриц, т.е. матриц, удовлетворяющих условию $dg = -dg^*$. Это *вещественное* (но не комплексное!) подпространство размерности n^2 в ($2n^2$-мерном вещественном) пространстве $\mathrm{Mat}_n(\mathbb{C})$. Итак, группа U_n является *вещественным* (но не комплексным) подмногообразием в $\mathrm{Mat}_n(\mathbb{C}) \cong \mathbb{R}^{2n^2}$.

Пример 11.9. Группа U_1 — это единичная окружность, т.е. подгруппа комплексных чисел модуля 1 в $\mathbb{C}^*$.

Пример 11.10. $\mathrm{SU}_n = \mathrm{U}_n \cap \mathrm{SL}_n(\mathbb{C})$ есть $n^2 - 1$-мерная вещественная группа Ли; её касательное пространство есть пространство косоэрмитовых матриц со следом 0.

Упражнение 11.11. Докажите, что группа $B_n(K)$ невырожденных верхнетреугольных матриц является группой Ли, и опишите касательное пространство $T_E B_n(K)$

Определение 11.12. *Представление* группы Ли G в пространстве V — это гомоморфизм групп $\rho\colon G \to \mathrm{GL}_n(V)$, одновременно являющийся гладким отображением многообразий.

11.3. **Компактные группы.**

Определение 11.13. Группа Ли называется *компактной*, если она компактна как гладкое многообразие.

Замечание 11.14. Всякая группа Ли замкнута в $\mathrm{GL}_n(K)$ (докажите это!), поэтому компактность группы эквивалентна её ограниченности (в какой-либо норме в пространстве $\mathrm{Mat}_n(K)$).

Пример 11.15. Всякая конечная подгруппа в $\mathrm{GL}_n(K)$ является компактной группой Ли.

Упражнение 11.16. Докажите, что группы $\mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}_n(\mathbb{R})$, U_n, SU_n компактны, а $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ — нет.

Компактные группы во многих отношениях очень похожи на конечные. В частности, их конечномерные представления вполне приводимы — а для некомпактных групп это бывает неверно.

Упражнение 11.17. Придумайте представление группы $B_n(K)$, не являющееся вполне приводимым.

Доказать полную приводимость легко, если уметь интегрировать по группе, т.е. если на группе существует *вероятностная мера* μ_G, инвариантная относительно левых сдвигов. Слово "вероятностная" значит, что объём всей группы относительно этой меры равен единице: $\int_G d\mu_G = 1$.

Можно доказать, что такая мера (она называется *мерой Хаара*) существует и единственна на любой компактной группе.

Пример 11.18. Меры Хаара на группах $\mathrm{U}_1 \cong S^1$ и $\mathrm{SU}_2 \cong S^3$ индуцируются обычной лебеговской мерой на плоскости и в четырехмерном пространстве соответственно. Они инвариантны относительно действия этих групп на себе левыми сдвигами (т.е. вращений окружности и трёхмерной сферы).

Предложение 11.19. *Пусть G — компактная группа Ли, на которой задана мера Хаара μ_G. Тогда на каждом вещественном/комплексном представлении V группы Ли G имеется G-инвариантное положительно определённое/эрмитово скалярное произведение.*

Доказательство. Оно ничем не отличается от случая конечных групп.

Пусть $(\ ,\ )$ — произвольное положительно определённое/эрмитово скалярное произведение на V. Построим новое скалярное произведение $(\ ,\ )_G$, усреднив по группе:

$$(v, w)_G = \int_G (gv, gw) d\mu_G.$$

Оно, очевидно, будет G-инвариантно. □

Следствие 11.20 (Теорема Машке)**.** *Всякое конечномерное представление компактной группы Ли G вполне приводимо.*

Доказательство. Дословно повторяет первое доказательство теоремы Машке для конечных групп. □

В следующей лекции мы получим другое доказательство теоремы Машке для компактных групп Ли, не предполагающее известным наличие меры Хаара. В нём вместо этого будут использоваться методы выпуклой геометрии.

12. Двенадцатая лекция, 4 декабря 2012 г.

Мы начнём с того, что изложим доказательство полной приводимости представлений компактных групп Ли, не использующее наличие на группе меры Хаара. Для этого нам придётся вспомнить некоторые понятия выпуклой геометрии.

12.1. **Центр масс.** Предположим, что $M \subset \mathbb{A}^n$ — ограниченное множество ненулевой лебеговской меры в n-мерном аффинном пространстве $\mathbb{A}^n$. Из школьного курса физики известно определение его центра масс:

$$\operatorname{cent} M = \frac{1}{\mu(M)} \int_M x d\mu.$$

(оно получается переходом к пределу из определения центра масс системы k материальных точек: $\operatorname{cent}(p_1, \dots, p_n) = (\sum r_i)/n$, где r_i — радиус-векторы этих материальных точек).

Из определения центра масс следует, что для любого аффинного преобразования $\alpha\colon \mathbb{A}^n \to \mathbb{A}^n$

$$\operatorname{cent} \alpha M = \alpha(\operatorname{cent} M)$$

В частности, если преобразование α переводит множество M в себя ($\alpha(M) = M$), то оно сохраняет и его центр масс: $\alpha(\operatorname{cent} M) = \operatorname{cent} \alpha(M)$.

12.2. **Выпуклые множества.** Напомним, что подмножество $M \subset \mathbb{A}^n$ называется *выпуклым*, если для любых его точек $x, y \in M$ и для любого числа $\lambda \in [0, 1]$ точка $\lambda x + (1 - \lambda)y$ также принадлежит M. Иначе говоря, если выпуклое множество содержит концы отрезка, то оно содержит и весь отрезок.

Предположим, что M — ограниченное выпуклое множество, не лежащее ни в каком собственном аффинном подпространстве $\mathbb{A}^n$. Тогда M имеет ненулевую меру (почему?), и мы можем найти его центр масс. Ясно, что $\operatorname{cent} M \subset \overline{M}$.

Несложно доказать более сильное утверждение: $\operatorname{cent} M$ принадлежит *внутренности* множества M. Действительно, пусть f — некоторый аффинный линейный функционал. Предположим, что $f(x) \geq 0$ для любого $x \in M$, то есть M лежит в замкнутом полупространстве, в котором $f \geq 0$. При этом найдётся такая точка из M, в которой функционал f строго положителен. Докажем, что $\operatorname{cent} M$ лежит в соответствующем открытом полупространстве, т.е. $f(\operatorname{cent} M) > 0$. Действительно,

$$f(\operatorname{cent} M) = \mu(M)^{-1} \int_M f(x) d\mu(x) > 0,$$

поскольку интеграл от неотрицательной непрерывной функции, принимающей в какой-то точке строго положительное значение, также строго положителен.

Лемма 12.1 (о неподвижной точке)**.** *Пусть G — компактная группа аффинных преобразований пространства $\mathbb{A}^n$, $M \subset \mathbb{A}^n$ — непустое выпуклое множество, инвариантное относительно G. Тогда G имеет в M неподвижную точку (т.е. найдётся такая точка $x \in M$, что $gx = x$ для любого $g \in G$).*

Доказательство. Пусть $p \in M$ — произвольная точка. Рассмотрим её орбиту Gp и возьмём её выпуклую оболочку $M' = \mathrm{Conv}(Gp)$. Это выпуклое множество, которое будет ограниченным, т.к. Gp ограничено (образ компакта при непрерывном отображении — компакт, поэтому всякая орбита компактной группы компактна, а следовательно, ограничена). Оно также инвариантно относительно действия группы G. Рассмотрим центр масс множества M' (как подмножества своей аффинной оболочки). В силу предыдущего обсуждения, он будет инвариантен относительно G. Поэтому он и будет искомой неподвижной точкой. □

Лемма о неподвижной точке позволяет дать другое доказательство предложения 11.19.

Предложение 12.2. *Пусть G — компактная группа Ли. Тогда на каждом вещественном/комплексном представлении V группы Ли G имеется G-инвариантное положительно определённое/эрмитово скалярное произведение.*

Доказательство. Приведём доказательство для вещественного случая. Рассмотрим пространство $\mathrm{Sym}^2 V^*$ симметрических билинейных форм на V. Это векторное пространство, размерность которого равна $\dim V(\dim V + 1)/2$. В нём есть подмножество положительно определённых форм, которое мы обозначим через P. Это выпуклый конус: действительно, линейная комбинация любых двух положительно определённых форм с положительными коэффициентами снова будет положительно определённой формой. В частности, это верно для выпуклых комбинаций (с коэффициентами λ и $1 - \lambda$, где $\lambda \in [0, 1]$.

Группа G действует на пространстве всех симметрических билинейных форм (как на симметрическом квадрате сопряжённого пространства). Это действие есть не что иное, как действие на аргументе: $g(\beta(v, w)) = \beta(gv, gw)$. При этом действии положительно определённые формы переходят в положительно определённые, поэтому множество P будет G-инвариантно. Стало быть, согласно лемме о неподвижной точке, в P найдётся форма, инвариантная относительно G. □

12.3. **Характеры представлений компактных групп Ли и теорема Петера–Вейля.** В этом разделе мы снова предполагаем, что на нашей компактной группе G определена мера Хаара μ_G.

Пусть $\rho\colon G \to \mathrm{GL}(V)$ — комплексное представление компактной группы Ли G, размерность которого равна n. Выберем в V базис; тогда элемент $\rho(g)$ будет записываться матрицей $(\rho_{ij}^V(g))$. Матричные элементы $\rho_{ij}^V(g)$ — это гладкие функции на группе G. Как и в случае конечной группы, можно определить *характер* представления V:

$$\chi_V(g) = \sum_{i=1}^{n} \rho_{ii}^V(g) = \operatorname{tr} \rho(g) \in C^\infty(G),$$

где $C^{infty}(G)$ — пространство всех гладких комплекснозначных функций на G.

Предложение 12.3 (об ортогональности характеров)**.** *Пусть V и W — неприводимые конечномерные представления компактной группы Ли G. Тогда*

$$\langle \chi_V, \chi_W \rangle := \int_{g\in G} \overline{\chi_V(g)} \chi_W(g) d\mu_G = \begin{cases} 1, & V \cong W; \\ 0, & V \ncong W \end{cases}$$

Доказательство. Это следует из теоремы Машке и леммы Шура аналогично случаю конечной группы. □

В пространстве функций на группе $C^\infty(G)$ можно ввести метрику (и индуцированную ей топологию) — например, C^1-метрику. Расстояние между двумя функциями $f_1(g)$ и $f_2(g)$ в этой метрике будет определяться так:

$$||f_1(g) - f_2(g)|| = \max_{g\in G} |f_1(g) - f_2(g)|.$$

(поскольку группа компактна, супремум всегда является максимумом).

Пространство $C^\infty(G)$ само является представлением группы Ли G (группа умеет действовать на функциях на себе при помощи замен аргумента). О нём можно думать как о регулярном представлении группы. Однако, в отличие от случая конечной группы, это представление бесконечномерно, и для работы с ним приходится привлекать аналитические методы. Имеет место следующий фундаментальный результат, который является аналогом теоремы о разложении представления в прямую сумму неприводимых. Он принадлежит немецкому математику Герману Вейлю и его ученику Фрицу Петеру.

Теорема 12.4 (Петер–Вейль)**.** *Линейная оболочка пространства матричных элементов неприводимых представлений $\rho_{ij}^V(g)$ плотна в пространстве функций на группе $C^\infty(G)$ относительно C^1-метрики.*

Иногда удобно вместо пространства $C^\infty(G)$ рассматривать пространство $L^2(G)$ функций, интегрируемых с квадратом, с L_2-метрикой.

12.4. **Представления одномерного тора и ряды Фурье.** Пусть $T = \{z \in \mathbb{C} \mid |z| = 1\}$ — группа комплексных чисел единичного модуля. Это вещественная одномерная компактная группа Ли. Опишем все её неприводимые представления.

Во-первых, эта группа абелева, поэтому всякое её неприводимое представление одномерно.

Далее, ясно, что всякий гомоморфизм групп $T \to \mathrm{GL}(1) = \mathbb{C}^*$ является просто возведением в некоторую степень:

$$\rho_n \colon z \to z^n, \qquad n \in \mathbb{Z}.$$

Выясним, что в данном случае утверждает теорема Петера–Вейля. Во-первых, пространство $C^\infty(T)$ есть пространство комплекснозначных бесконечно дифференцируемых функций на окружности от переменной z, т.е. 2π-периодических функций на прямой $f(z) = f(e^{it})$.

Далее, все неприводимые представления T одномерны, поэтому каждому представлению соответствует единственный матричный элемент, который одновременно является его характером:

$$\chi_n(t) = e^{int}.$$

Условие ортогональности характеров — это равенство

$$\frac{1}{2\pi}\int_0^{2\pi} \overline{e^{int}} e^{imt} dt = \frac{1}{2\pi}\int_0^{2\pi} e^{i(m-n)t} dt = \delta_{n,m}.$$

($\delta_{n,m}$ — это символ Кронекера; множитель $1/2\pi$ появляется оттого, что мера всей окружности равна единице).

Теорема Петера–Вейля утверждает, что линейная оболочка функций вида e^{int} плотна в пространстве всех гладких функций на окружности. Иначе говоря, каждая 2π-периодическая гладкая функция $f(t)$ является суммой некоторого ряда вида

$$f(t) = \sum_{n=-\infty}^{+\infty} c_n e^{int}.$$

Поскольку система $\{e^{int}\}$ является ортонормированной, коэффициенты разложения функции f по векторам системы равны скалярным произведениям $\langle f, \chi_n \rangle$:

$$c_n = \frac{1}{2\pi}\int_0^{2\pi} f(t) e^{int} dt.$$

Мы получили хорошо известное утверждение из курса анализа: каждая гладкая (и даже непрерывная) функция сходится к своему *ряду Фурье*. Коэффициенты c_n называются *коэффициентами Фурье* функции $f(t)$.

13. Последняя, тринадцатая лекция, 11 декабря 2012 г.

В этой лекции мы изучим представления группы $\mathrm{SU}(2)$.

Напомним, что $\mathrm{SU}(2)$ — это группа унитарных матриц 2×2 с определителем 1, которую также можно отождествить с группой (мультипликативной) кватернионов единичного модуля:

$$\mathrm{SU}(2)\cong\{z\in\mathbb{H}\mid |z|=1\}=\{A\in \mathrm{Mat}_2(\mathbb{C})\mid AA^*=E,\det A=1\}.$$

Топологически $\mathrm{SU}(2)$ — это трёхмерная сфера в $\mathbb{R}^4$.

13.1. **Максимальный тор.** Рассмотрим в $\mathrm{SU}(2)$ *максимальный тор* — подгруппу диагональных матриц $T=\begin{pmatrix} z & 0\\ 0 & z^{-1}\end{pmatrix}$, где $z\in\mathbb{C}$, $|z|=1$. На кватернионном языке $T=\{\cos t+i\sin t\}$.

Предложение 13.1. (1) *Всякий элемент из* $\mathrm{SU}(2)$ *сопряжён некоторому элементу из* T*;*

(2) *Два элемента из* T *сопряжены при помощи некоторого элемента из* $\mathrm{SU}(2)$ *тогда и только тогда, когда они взаимно обратны.*

Доказательство. 1. Любой кватернион единичного модуля представим в виде $q=\cos\theta+v\sin\theta$, где $v\in\mathrm{Im}$, $|v|=1$ — чисто мнимый кватернион. Существует такое сопряжение, которое переводит v в i. Оно и переводит элемент q в $\cos\theta+v\sin\theta\in T$.

2. Сопряжение, переводящее $q=\cos t+i\sin t$ в элемент из T, обязано переводить i либо в i, либо в $-i$. В первом случае оно тривиально, во втором — переводит q в $\overline{q}=q^{-1}$. □

13.2. **Серия представлений** $\mathrm{SU}(2)$**.** В этом разделе мы построим серию неприводимых конечномерных комплексных представлений группы $\mathrm{SU}(2)$, которые будут нумероваться целыми положительными числами. Впоследствии мы докажем, что все неприводимые представления исчерпываются этим списком.

$\mathrm{SU}(2)$ естественным образом действует на линейных формах от двух переменных x,y:

$$g(x,y)=(ax+cy,bx+dy),\qquad g=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$$

Это действие индуцирует действие $\mathrm{SU}(2)$ на однородных формах степени n от двух переменных.

$$g\circ f(x,y)=f(ax+cy,bx+dy).$$

Обозначим пространство однородных форм степени n через V_n. Ясно, что $\dim V_n=n+1$, т.к. $V_n=\langle x^n,x^{n-1}y,x^{n-2}y^2,\dots,xy^{n-1},y^n\rangle$.

Определение 13.2. Вектор $v\in V_n$ называется *весовым*, если он является собственным для всех элементов $h(z)=\begin{pmatrix} z & 0\\ 0 & z^{-1}\end{pmatrix}\in T$.

Его собственное значение называется *весом* вектора v. Число n называется *старшим весом* представления V_n.

Проверим, что вектор $x^{n-m}y^m$ является весовым, и его вес равен z^{n-2m}. Действительно,

$$h(z)(x^{n-m}y^m) = z^{n-m}x^{n-m}z^{-m}y^m = z^{n-2m}(x^{n-m}y^m).$$

Таким образом, если ограничить представление V_n на тор T, то V_n распадётся в прямую сумму $n+1$ попарно неизоморфного одномерного представления, которые будут натянуты на векторы $x^{n-m}y^m$. Веса этих векторов равны $z^n, z^{n-2}, \ldots, z^{-n}$.

Предложение 13.3. *Представление V_n неприводимо.*

Доказательство. Пусть $U \subset V_n$ — ненулевое подпредставление. Тогда U, в частности, является T-инвариантным подпространством. Значит, U натянуто на какие-то из весовых векторов $x^{n-m}y^m$. Рассмотрим какой-нибудь весовой вектор $x^{n-m}y^m$ и подействуем на него элементом "общего положения" из $\mathrm{SU}(2)$ (не диагональным и не антидиагональным). Получим элемент $(ax+cy)^{n-m}(bx+dy)^m$. В частности, в эту сумму входит x^n с каким-то ненулевым коэффициентом. Поэтому $x^n \in U$. Теперь подействуем на x^n тем же элементом — получим $(ax+cy)^n$. В эту сумму уже входят с ненулевыми коэффициентами все весовые векторы. Значит, U совпадает со всем V_n. □

Нашей следующей целью будет доказательство того, что других неприводимых представлений у $\mathrm{SU}(2)$ нет.

13.3. **Снова характеры.** Пусть $\rho\colon \mathrm{SU}(2) \to \mathrm{GL}(V)$ — представление $\mathrm{SU}(2)$, $\chi_V(g) = \operatorname{tr}\rho(g)$ — его характер. Это функция на $\mathrm{SU}(2)$.

Определение 13.4. Характером $\mathrm{ch}_V(z)$ представления V называется ограничение $\chi_V(g)$ на максимальный тор:

$$\mathrm{ch}_V(z) = \chi_V(h(z)).$$

Выберем в V базис из весовых векторов. Из определения следует, что $\mathrm{ch}_V(z)$ является суммой их весов (как мономов от z и z^{-1}).

Пример 13.5. Вычислим $\mathrm{ch}_{V_n}(z)$. В представлении V_n можно выбрать базис из весовых векторов с весами $z^n, z^{n-2}, \ldots, z^{-n}$. Поэтому

$$\mathrm{ch}_{V_n}(z) = z^n + z^{n-2} + \cdots + z^{-n+2} + z^{-n} = \frac{z^{n+1} - z^{-n-1}}{z - z^{-1}}.$$

(последнее равенство — это формула для суммы геометрической прогрессии).

Предложение 13.6. *Для любого представления V группы* $\mathrm{SU}(2)$

(1) $\mathrm{ch}_V(z) \in \mathbb{Z}_{\geq 0}[z, z^{-1}]$;
(2) $\mathrm{ch}_V(z) = \mathrm{ch}_V(z^{-1})$ *(характер является* возвратным *многочленом, т.е. симметричным относительно замены z на z^{-1})*;
(3) *По* $\mathrm{ch}_V(z)$ *однозначно восстанавливается* $\chi_V(g)$ *(а значит, характер* $\mathrm{ch}_V(z)$ *однозначно определяет представление).*

Доказательство. 1. Коэффициент при z^k в $\mathrm{ch}_V(z)$ есть кратность собственного значения z^k элемента $h(z)$, т.е. целое неотрицательное число.

2. Это следует из того, что характер $\chi_V(g)$ постоянен на классах сопряжённости. Элементы $h(z)$ и $h(z^{-1})$ из T сопряжены в $\mathrm{SU}(2)$, поэтому характер χ_V принимает в них равные значения: $\chi_V(h(z)) = \chi_V(h(z^{-1}))$. А это и значит, что $\mathrm{ch}_V(z) = \mathrm{ch}_V(z^{-1})$.

3. Всякий элемент $g \in \mathrm{SU}(2)$ сопряжён некоторому элементу из максимального тора $h(z) \in T$, поэтому $\chi_V(g)$ полностью восстанавливается по значениям $\chi_V(h(z)) = \mathrm{ch}_V(z)$. □

Полезно отметить, что ch_V обладает теми же свойствами, что и "обычный" характер $\chi_V(g)$:

Предложение 13.7. *Пусть V и W — представления* $\mathrm{SU}(2)$. *Тогда* $\mathrm{ch}_{V\oplus W}(z) = \mathrm{ch}_V(z) + \mathrm{ch}_W(z)$, $\mathrm{ch}_{V\otimes W}(z) = \mathrm{ch}_V(z)\,\mathrm{ch}_W(z)$.

Доказательство. ch_V есть ограничение характера $\chi_V(g)$, для которого эти свойства имеют место. □

Теорема 13.8. *Представления V_n, $n \geq 0$, составляют полный список неприводимых представлений* $\mathrm{SU}(2)$.

Доказательство. Характеры $\mathrm{ch}_{V_n}(z)$ образуют *базис* в пространстве возвратных лорановских многочленов от z (над каким-нибудь полем — например, с рациональными коэффициентами). Поскольку характер $\chi_V(g)$ однозначно восстанавливается по $\mathrm{ch}_V(z)$, то функции $\chi_{V_n}(g)$ тоже образуют базис, т.е. полную линейно независимую систему векторов, в пространстве *центральных* функций на $\mathrm{SU}(2)$ (т.е. функций, постоянных на классах сопряжённости). Кроме того, мы знаем, что характеры неизоморфных представлений ортогональны, поэтому этот базис ещё и ортонормированный (а для базиса из $\mathrm{ch}_{V_n}(z)$ это, кстати, неверно — подумайте, почему).

Поэтому для характера произвольного представления W имеет место равенство (в пространстве центральных функций на $\mathrm{SU}(2)$)

$$\chi_W(g) = \sum_{n=0}^{\infty} \langle \chi_W, \chi_{V_n} \rangle \chi_{V_n}(g).$$

Если W конечномерно, то и эта сумма тоже конечна (почти все слагаемые в ней равны нулю), и поэтому $W = a_0 V_0 \oplus a_1 V_1 \oplus \cdots \oplus$

$a_n V_n$. Получается, что всякое конечномерное представление является суммой представлений вида V_n, что и требовалось. □

13.4. **Теорема Клебша–Гордана.** Теория характеров SU(2) позволяет разложить на неприводимые тензорное произведение двух неприводимых представлений V_n и V_m группы SU(2). Пусть $n \leq m$. Запишем характеры этих представлений так:

$$\operatorname{ch}_{V_n}(z) = z^n + z^{n-2} + \cdots + z^{-n}; \qquad \operatorname{ch}_{V_m}(z) = \frac{z^{m+1} - z^{-m-1}}{z - z^{-1}}.$$

Перемножим эти два многочлена Лорана:

$$\operatorname{ch}_{V_n}(z) \operatorname{ch}_{V_m}(z) = (z^n + z^{n-2} + \cdots + z^{-n}) \frac{z^{m+1} - z^{-m-1}}{z - z^{-1}} =$$

$$= \frac{1}{z - z^{-1}} \left(z^{n+m+1} + z^{n+m-1} + \cdots + + z^{-n+m+1} + z^{n-m-1} + \cdots + \right.$$

$$\left. + z^{-n-m+1} + z^{-n-m-1} \right) =$$

$$= \frac{z^{n+m+1} - z^{-n-m-1}}{z - z^{-1}} + \frac{z^{n+m-1} - z^{-n-m+1}}{z - z^{-1}} + \cdots + \frac{z^{m-n+1} - z^{-m+n-1}}{z - z^{-1}} =$$

$$= \operatorname{ch}_{V_{n+m}}(z) + \operatorname{ch}_{V_{n+m-2}}(z) + \cdots + \operatorname{ch}_{V_{m-n}}(z).$$

Мы получили следующий результат.

Теорема 13.9 (Клебш–Гордан)**.**

$$V_n \otimes V_m \cong V_{n+m} \oplus V_{n+m-2} \oplus \cdots \oplus V_{|n-m|}.$$

E-mail address: evgeny.smirnov@gmail.com