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: $\sigma(ax_1^{k_1} \dots x_n^{k_n}) = x_{\sigma(1)}^{k_1} \dots x_{\sigma(n)}^{k_n}$, 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: $i_1 = j_1$, $i_2 = j_2, \dots, i_{k-1} = j_{k-1}$. Обозначение:

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

Таким образом можно сравнить любые два монома, т.е. это *полный* порядок. Термин “лексикографическое упорядочение” объясняется тем, что наборы $(i_1, \dots, i_n)$ и $(j_1, \dots, j_n)$ 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 $u_1v_1 \succ u_2v_2$.*

Упражнение 1.9. Проверьте эти свойства.

Замечание 1.10. Лексикографический порядок не согласован со степенью монома: так, например, $x_1^2x_2 \succ x_1x_2^3$, хотя степень второго монома равна четырем, а первого — трем.

Определение 1.11. *Старшим членом* многочлена $P(x_1, \dots, x_n)$ (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 $\operatorname{ht} f = u = ax_1^{k_1} \dots x_n^{k_n}$ удовлетворяет неравенствам $k_1 \geq k_2 \geq \dots \geq k_n$.*

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

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

$\square$

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 $\deg f_2 = \deg f_1 - n \le d - n < d$. 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 $F_0 \ne 0$, 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. $\square$

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 $\deg p(x) \le m-1$, $\deg q(x) \le n-1$, что $f(x)p(x) + g(x)q(x) = 0$.*

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

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

Запишем в явном виде условие из предложения 2.2:

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

Условие равенства многочлена степени $m+n-1$ нулю — это система из $m+n$ линейных однородных уравнений на неизвестные $p_{m-1}, \dots, p_0, q_{n-1}, q_0$. 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 $\operatorname{Res}(f, g)$. Выпишем его явно:

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

Мы доказали следующую теорему.

Теорема 2.3. *Многочлены $f(x)$ и $g(x)$ имеют общий множитель тогда и только тогда, когда их результант $\operatorname{Res}(f,g)$ 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 $t_1,\dots,t_n$, поэтому это многочлен от $a_0,\dots,a_{n-1},a_n$ 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 $f(x) = a_nx^n+\dots+a_1x+a_0 \in K[x]$ — многочлен. Его *производная* — это многочлен $f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2}+\dots+2a_2x+a_1 \in K[x]$.

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:

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

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 $G_1, \ldots, G_k$, если:

(1) каждый элемент $g \in G$ единственным образом представляется в виде произведения $g = g_1 \ldots g_k$, 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: $G = G_1 \times \cdots \times G_k$.

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 $G_1, \dots, G_k$ называется множество последовательностей $(g_1, \dots, g_k)$, где $g_i \in G_i$, с покомпонентными операциями умножения и взятия обратного. Обозначение: $G_1 \times \dots \times G_k$.

Ясно, что такие операции задают на $G_1 \times \dots \times G_k$ структуру группы, единицей которой является набор $(e, \dots, e)$. Кроме того, каждая из групп G_i вкладывается в $G_1 \times \dots \times G_k$ как подгруппа: $g_i \mapsto (e, \dots, e, g_i, e, \dots, e)$, где неединичный элемент стоит на i-м месте. Тогда $G_1 \times \dots \times G_k$ 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. $\mathrm{GL}_n(K) = \mathrm{SL}_n(K) \ltimes \{\operatorname{diag}(\lambda, 1, \dots, 1) \mid \lambda \in K^*\}$.

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 $H \triangleleft G$.

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. $\square$

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 Эваристу 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:

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

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. $\square$

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 $S_1 = gSg^{-1}$. $\square$

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 $S = S'$. $\square$

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 $|G_p G_q| = pq = |G|$. Значит, $G = G_p \ltimes G_q$.

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. $\square$

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. $\square$

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.