

Алгебра, третий семестр

Е. Ю. Смирнов

АННОТАЦИЯ. Записки лекций по алгебре для второго курса факультета математики ВШЭ, осень 2013/14 учебного года

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.

1. ПЕРВАЯ ЛЕКЦИЯ, 4 СЕНТЯБРЯ 2013 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 $k \geq 1$.

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 $u_1 v_1 \succ u_2 v_2$.

Упражнение 1.9. Проверьте эти свойства.

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

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

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

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

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

Следующая лемма уже относится к симметрическим многочленам.

Лемма 1.14. *Пусть f — симметрический многочлен. Тогда его старший член $\text{ht } f = u = ax_1^{k_1} \dots x_n^{k_n}$ 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. \square

Лемма 1.15. *Пусть $u = x_1^{k_1} \dots x_n^{k_n}$. Тогда существуют и однозначно определены числа ℓ_1, \dots, ℓ_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 $\text{ht } f = u = ax_1^{k_1} \dots x_n^{k_n}$. Согласно предыдущей лемме, существует такой многочлен $F_1(X_1, \dots, X_n)$, что $\text{ht } F(\sigma_1, \dots, \sigma_n) = u$. 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 $u_2 = \text{ht } f_1$. 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 $w_i(x_1, \dots, x_n) = \text{ht } H_i(\sigma_1, \sigma_n)$ — 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 $H_i(\sigma_1, \dots, \sigma_n)$. Поэтому после приведения подобных слагаемых в сумме

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

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

\square

2. ВТОРАЯ ЛЕКЦИЯ, 11 СЕНТЯБРЯ 2013 Г.

2.1. Факториальность кольца многочленов. Лемма Гаусса.

Наша ближайшая цель — доказать теорему о единственности разложения на множители для многочленов от нескольких переменных. Единственность разложения на множители для многочленов от одной переменной нам уже известна; она вытекает из евклидовости кольца $K[x]$.

В этой лекции через A будет обозначаться целостное (т.е. без делителей нуля) коммутативное кольцо с единицей.

Напомним, что необратимый ненулевой элемент a кольца A называется *простым*, если из равенства $a = bc$ вытекает, что либо b , либо c — обратимый элемент кольца A .

Определение 2.1. Кольцо A называется *факториальным*, если каждый его необратимый ненулевой элемент раскладывается на простые множители, причём это разложение единственно с точностью до перестановки сомножителей и умножения их на обратимые элементы кольца A .

Мы уже знаем, что всякое кольцо главных идеалов (в частности, \mathbb{Z} и $K[x]$) факториально. Как мы увидим чуть ниже, обратное неверно: существуют факториальные кольца, не являющиеся кольцами главных идеалов.

В факториальном кольце для любых двух элементов можно рассмотреть их наибольший общий делитель. А именно, пусть

$$a = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}, \quad b = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k},$$

где p_i — простые элементы кольца A , а $n_i, m_i \in \mathbb{Z}_{\geq 0}$. Тогда

$$(a, b) = p_1^{\min(n_1, m_1)} \dots p_k^{\min(n_k, m_k)}.$$

Элементы a и b называются *взаимно простыми*, если $(a, b) = 1$, то есть в разложениях a и b на простые множители нет общих сомножителей.

Упражнение 2.2. Докажите, что кольцо $K[x, y, z, t]/(xy = zt)$ не является факториальным.

Теорема 2.3. Пусть A — факториальное кольцо. Тогда кольцо многочленов $A[x]$ тоже факториально.

Следствие 2.4. Кольца многочленов от нескольких переменных $\mathbb{Z}[x_1, \dots, x_n]$ и $K[x_1, \dots, x_n]$ факториальны.

Доказательство теоремы. Назовём многочлен $f(x) \in A[x]$ *примитивным*, если его коэффициенты взаимно просты в совокупности.

Пусть K — поле частных кольца A . Очевидно, что каждый многочлен можно представить в виде

$$h(x) = \frac{a}{b} h_0(x),$$

где $a, b \in A$ взаимно просты, а $h(x)$ — примитивный многочлен.

Лемма 2.5 (лемма Гаусса). *Если многочлен $f(x)$ делится на примитивный многочлен $g(x)$ в кольце $K[x]$, то он делится на него и в кольце $A[x]$ (т.е. все коэффициенты отношения этих многочленов принадлежат кольцу A).*

Примитивность здесь существенна: скажем, многочлен $x^2 - 1$ делится на многочлен $2x + 2$ (не являющийся примитивным) в кольце $\mathbb{Q}[x]$, однако, очевидно, не делится на него в $\mathbb{Z}[x]$.

Доказательство леммы Гаусса. Пусть $f(x) = g(x)h(x)$, где $h(x)$ примитивен. Представим $h(x)$ как $\frac{a}{b}h_0(x)$ и покажем, что b — обратимый элемент в кольце A .

Для этого используем редукцию по простому модулю. Пусть p — какой-то простой делитель элемента b . Умножим равенство $f(x) = \frac{a}{b}g(x)h_0(x)$ на b и произведем редукцию $A \rightarrow A/(p)$:

$$0 = [a]_p[g(x)]_p[h_0(x)]_p.$$

Все множители в правой части отличны от нуля: если бы $g(x)$ или $h_0(x)$ равнялись бы нулю в $A/(p)$, это значило бы, что все их коэффициенты делятся на p , что противоречит примитивности. Однако факторкольцо по простому идеалу является целостным — противоречие. \square

Следствие 2.6. *Если многочлен $f(x) \in A[x]$ раскладывается в произведение двух многочленов меньшей степени над $K[x]$, то он может быть разложен в произведение двух многочленов меньшей степени и над $A[x]$.*

Упражнение 2.7. Завершите доказательство теоремы 2.3. \square

Замечание 2.8. В кольцах многочленов простые элементы принято называть *неприводимыми*. Поэтому далее мы будем говорить о неприводимых многочленах, а не о «простых многочленах».

Ясно, что всякий многочлен первой степени неприводим.

Докажем следующую полезную лемму.

Лемма 2.9. *Если многочлен $f(x) \in K[x_1, \dots, x_n]$ обращается в нуль во всех точках гиперплоскости $H_\ell = \{(x_1, \dots, x_n) \mid \ell(x) = a_1x_1 + \dots + a_nx_n = 0\}$, то он делится на ℓ .*

Доказательство. Сделав аффинную замену переменных, можем считать, что $\ell = x_1$. Тогда условие леммы означает, что все мономы многочлена $f(x)$ содержат x_1 , а значит, $f(x)$ делится на ℓ . \square

С помощью этой леммы и факториальности кольца многочленов можно, например, вычислить другим способом определитель Вандермонда.

Пример 2.10. Пусть $\Delta(x_1, \dots, x_n) = \det(x_i^{j-1})_{i,j=1}^n$. Это многочлен от x_1, \dots, x_n степени $n(n-1)/2$. Из свойств определителя следует, что он обращается в нуль при $x_i = x_j$, значит, в силу предыдущей леммы, он делится на $x_i - x_j$. Все эти многочлены неприводимы, значит, в силу факториальности, $\Delta(x_1, \dots, x_n)$ делится и на их произведение $\prod_{i>j}(x_i - x_j)$. Сравнивая степени, получаем, что коэффициент пропорциональности — константа. Вычислив коэффициент при каком-нибудь мономе (скажем, $x_2 x_3^2 \dots x_n^{n-1}$, получаем, что эта константа равна единице. Поэтому

$$\Delta(x_1, \dots, x_n) = \prod_{i>j}(x_i - x_j).$$

2.2. Другое доказательство основной теоремы о симметрических многочленах. В качестве ещё одного примера использования теоремы о факториальности кольца многочленов приведём другое, более короткое, доказательство основной теоремы о симметрических многочленах.

Назовём *весом* монома $u = aX_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$ число

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

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 2.11 (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 $\deg f(x_1, \dots, x_{n-1}, 0) \leq \deg f = d$. 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 :

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

Аналогичным образом можно доказать и единственность¹ 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

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

¹На лекции этого не рассказывалось.

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

3. ТРЕТЬЯ ЛЕКЦИЯ, 18 СЕНТЯБРЯ 2013 Г.

3.1. Результат. 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: $f = f_1 h$, $g = g_1 h$, 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 3.1. *Многочлены $f(x)$ и $g(x)$, где $\deg f = n$, $\deg g = m$, 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 $q(x)$:

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

Запишем в явном виде условие из предложения 3.1:

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

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,

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 $a_0^m b_m^n$ с коэффициентом 1. Поэтому они равны. \square

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

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

Определение 3.5. *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 3.6. Пусть $f(x) = a_n x^n + \dots + a_1 x + a_0 \in K[x]$ — многочлен. Его *производная* — это многочлен $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1 \in K[x]$.

Замечание 3.7. 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 3.8. Докажите, что сумму и произведение многочленов можно дифференцировать по правилам, известным из математического анализа: $(f + g)' = f' + g'$ и $(fg)' = f'g + fg'$.

Предложение 3.9. *Дискриминант многочлена пропорционален результату его самого и его производной:*

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

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 3.4, получим:

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

что и требовалось доказать. □

4. ЧЕТВЕРТАЯ ЛЕКЦИЯ, 25 СЕНТЯБРЯ 2013 Г.

Следующие несколько лекций будут посвящены различным сюжетам из теории групп.²

4.1. Прямые произведения. Для начала напомним понятие прямого произведения групп.

Определение 4.1. 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 4.2. 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. \square

Рассмотрим случай двух множителей отдельно.

Предложение 4.3. 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 $g_1 = \tilde{g}_1, g_2 = \tilde{g}_2$. \square

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 большую

²Лекцию читала Е.Ю.Америк. Соответствие этого текста прочитанной лекции не гарантируется (вернее, гарантируется обратное).

группу) построить такую группу G , которая будет раскладываться в прямое произведение своих подгрупп, изоморфных G_i .

Определение 4.4. *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 4.5. 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 4.6. 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.

4.2. Автоморфизмы групп.

Определение 4.7. *Автоморфизм* группы — это её изоморфизм на себя.

Пример 4.8. Отображение $A \mapsto (A^T)^{-1}$ является автоморфизмом группы матриц.

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

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

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

Итак, у нас имеется отображение $G \rightarrow \text{Aut } G$ (каждому элементу группы $g \in G$ сопоставляется внутренний автоморфизм $a(g) \in$

$\text{Aut } G$). 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 $\text{Int } G \cong G/Z(G)$.

Пример 4.9. При $n \geq 3$ центр симметрической группы S_n тривиален. Поэтому $\text{Int } S_n \cong S_n$. Можно доказать, что при $n \neq 6$ никаких других автоморфизмов у S_n нет, а при $n = 6$ подгруппа $\text{Int } G \subset \text{Aut } G$ имеет индекс 2.

Пример 4.10. Найдём группу $\text{Aut } \mathbb{Z}_n$. Пусть $\varphi \in \text{Aut } \mathbb{Z}_n$, $\varphi(\bar{1}) = \bar{k}$. Тогда

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

где умножение понимается в смысле кольца \mathbb{Z}_n . Таким образом, всякий автоморфизм группы \mathbb{Z}_n имеет вид $\varphi_k: \ell \rightarrow k\ell$. Обратное, 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 $\text{Aut } \mathbb{Z}_n \cong \mathbb{Z}_n^*$.

4.3. Полупрямое произведение групп. 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,

$$\begin{aligned} (n_1h_1)(n_2h_2) &= n_1(h_1n_2h_1^{-1})h_1h_2, \\ (nh)^{-1} &= h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1}. \end{aligned}$$

Кроме того, $NH = HN$.

Определение 4.11. 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: $G = N \rtimes H$ (иногда используется другой значок: $G = N \ltimes H$).

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 4.12. $S_n = A_n \rtimes \langle (12) \rangle$.

Пример 4.13. $S_4 = V_4 \times S_3$, где V_4 — четверная группа Клейна, а S_3 вложена в S_4 как группа перестановок, оставляющих на месте символ 4.

Пример 4.14. $GL_n(K) = SL_n(K) \times \{\text{diag}(\lambda, 1, \dots, 1) \mid \lambda \in K^*\}$.

4.4. Внешнее полупрямое произведение групп. Мы определили разложение группы в полупрямое произведение двух своих подгрупп (одна из которых должна быть нормальной). Можно действовать иначе: для двух групп N и H рассмотреть их *внешнее* полупрямое произведение, т.е. построить группу $G = N \rtimes H$ 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 $H \rightarrow \text{Aut } N$.

Итак, пусть $N \times H$ — прямое произведение N и H как множеств, т.е. множество пар (n, h) . Пусть также задан гомоморфизм $\alpha: H \rightarrow \text{Aut } N$. 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 $N \rtimes_\alpha H$. 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: $G = N \rtimes H$, то имеется изоморфизм групп $N \rtimes_\alpha H \rightarrow G$. (Как при этом будет действовать на N автоморфизм $\alpha(h)$?)

Пример 4.15. Рассмотрим две циклические группы: $\langle a \rangle_n = \mathbb{Z}_n$ и $\langle b \rangle_m = \mathbb{Z}_m$. Гомоморфизм $\langle b \rangle_m \rightarrow \text{Aut } \mathbb{Z}_n$ полностью определяется тем, как действует образующая b . Как обсуждалось на прошлой лекции, $\text{Aut } \mathbb{Z}_n = \mathbb{Z}_n^*$, поэтому всякий автоморфизм \mathbb{Z}_n есть возведение элемента a в некоторую степень k . Таким образом, задать гомоморфизм $\langle b \rangle_m \rightarrow \mathbb{Z}_n$ значит задать такое k , что $k^m \equiv 1 \pmod n$. Такое полупрямое произведение обозначается через $\langle a \rangle_n \rtimes_k \langle b \rangle_m$. 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 4.16. Рассмотрим группу $\langle a \rangle_n \rtimes_{-1} \langle b \rangle_2$. Она задаётся соотношениями $a^n = b^2 = 1$ и $bab^{-1} = a^{-1}$. Поэтому это группа самосовмещений n -угольника.

5. ПЯТАЯ ЛЕКЦИЯ, 2 ОКТЯБРЯ 2013 Г.

5.1. 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 $\varphi: G \rightarrow H$ — 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 5.1. *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

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

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

5.2. Коммутанты некоторых групп. Из курса прошлого семестра вам известно следующее

Предложение 5.2. *Группа чётных перестановок A_n порождается тройными циклами (ijk) . При $n \geq 5$ группа A_n порождается парами независимых транспозиций $(ij)(kl)$.*

Пример 5.3. $S'_n = A_n$ 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 5.2 следует, что $S'_n = A_n$.

Пример 5.4. $A'_4 = V_4$, 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 5.5. 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 5.6. 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 $G' = G$.

Вычислим³ коммутанты групп $GL_n(K)$ и $SL_n(K)$. Для этого нам понадобится следующее утверждение.

Предложение 5.7. *Группа $SL_n(K)$ 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 5.8. Докажите предложение 5.7.

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

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

³На лекции этого не было, зато было на семинарах

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.

5.3. 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:

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

Определение 5.9. Группа G *разрешима*, если $G^{(k)} = \{e\}$ для некоторого k .

Пример 5.10. 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 5.11. Пусть $H \triangleleft G$ — нормальная подгруппа. Группа G разрешима тогда и только тогда, когда H и G/H разрешимы.

Задача 5.12. Докажите эту теорему.

6. ШЕСТАЯ ЛЕКЦИЯ, 9 ОКТЯБРЯ 2013 Г.

6.1. **Действия групп на множествах.** Напомним несколько определений из прошлого года курса.

Определение 6.1. Говорят, что группа G действует на множестве X (обозначение: $G \curvearrowright X$, раньше ещё часто писали $G : X$), если задано отображение $G \times X \rightarrow X$, $(g, x) \mapsto y = g \circ x$, 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 $\text{Stab}_G x$ или G_x :

$$\text{Stab}_G x = G_x = \{g \in G \mid g \circ x = x\} \subset G.$$

Очевидно, что это подгруппа в G .

Теорема Лагранжа утверждает, что если группа G конечна, то $|G| = |Gx| \cdot |\text{Stab}_G x|$ 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 6.2. 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 — *центральным стабилизатором* элемента h и обозначается через $Z(h)$. Ясно, что $Z(h) = \{g \in G \mid gh = hg\}$.

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.

6.2. **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 6.3. Группа G называется p -группой, где p — простое число, если $|G| = p^k$.

Теорема 6.4. *Нетривиальная p -группа имеет нетривиальный центр: если $|G| = p^k$, то $Z = Z(G) \neq \{e\}$.*

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

Следствие 6.5. *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 . \square

Следствие 6.6. *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 представляется в виде $a^k z$, где $z \in Z$. Но любые два таких элемента коммутируют — противоречие. \square

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

Определение 6.7. *Силовская p -подгруппа* группы G — это любая её подгруппа порядка p^n .

Теорема 6.8 (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 $\text{Tor}_{p, G}$. 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 $|Z(x):p^n$, 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 $|C(x_i):p$, и поэтому $|Z|:p$ (рассуждение аналогично доказательству теоремы о нетривиальности центра p -группы). Пусть $|Z| = p^{n_0} m_0$. 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 $G \rightarrow G/Z_1$ и будет искомым силовской p -подгруппой. \square

Теорема 6.9 (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 6.10 (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 разобьётся 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

6.4. Применение теорем Силова.

Пример 6.11. 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 6.12. 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, $G = G_p \times G_q$.

Пример 6.13. Докажем, что каждая группа порядка 45 абелева. Действительно, пусть n_3 и n_5 — число её силовских 3-подгрупп и 5-подгрупп соответственно. Тогда $n_3 \equiv 1 \pmod{3}$ и $n_3 | 5$, откуда $n_3 = 1$. Значит, имеется единственная силовская 3-подгруппа, которая тем самым нормальна. Аналогично из условий $n_5 \equiv 1 \pmod{5}$ 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 6.14. 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 пересекаются 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.

7. СЕДЬМАЯ ЛЕКЦИЯ, 16 ОКТЯБРЯ 2013 Г.

7.1. Простые группы.

Определение 7.1. Группа G называется простой, если она не имеет нетривиальных (т.е. отличных от G и $\{e\}$) нормальных подгрупп.

Всякая разрешимая простая группа есть циклическая группа простого порядка. Действительно, так как $G' \neq G$, получаем, что $G' = \{e\}$, то есть G абелева, а в абелевой группе все подгруппы нормальны. Значит, $G = \mathbb{Z}/p\mathbb{Z}$.

Примером неабелевой простой группы может служить группа A_n при $n \geq 5$.

Упражнение 7.2. Докажите, что при $n \geq 5$ группа A_n проста.

Упражнение 7.3. Докажите, что при $n \geq 5$ единственная нормальная подгруппа в S_n — это A_n .

Пусть G — конечная группа, и имеется цепочка вложенных групп

$$G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = \{e\},$$

где $G_{k+1} \triangleleft G_k$. Если факторгруппа $F_k = G_k/G_{k+1}$ содержит нетривиальную нормальную подгруппу N , то между G_k и G_{k+1} можно вставить ещё одну подгруппу, являющуюся полным прообразом N при гомоморфизме $G_k \rightarrow G_k/G_{k+1}$. Поэтому, «уплотнив» такую цепочку, можно считать, что все факторы G_k/G_{k+1} просты. Такая цепочка называется *композиционным рядом*, или *рядом Жордана–Гёльдера*, группы G . Имеет место следующая теорема, которую мы приведем без доказательства.

Теорема 7.4 (Жордан–Гёльдер). *Для данной группы G набор факторов G_k/G_{k+1} её композиционного ряда определён однозначно с точностью до перестановки (т.е. не зависит от выбора композиционного ряда).*

Упражнение 7.5. Докажите, что группа разрешима тогда и только тогда, когда все факторы её композиционного ряда абелевы.

Так, с каждой группой, обладающей композиционным рядом, канонически связывается набор простых групп. Поэтому классификация конечных простых групп играет ключевую роль в описании строения произвольных конечных групп.

Классификация конечных простых групп чрезвычайно сложна. Она изложена в нескольких сотнях журнальных статей общим объёмом более 10 тысяч страниц, принадлежащих примерно ста авторам. В основном эта классификация была завершена в 1983 году, но с тех пор в ней было обнаружено несколько ошибок, которые впоследствии были исправлены.

7.2. Изоморфизмы малых размерностей. Напомним, что через $\mathrm{GL}_n(K)$ и $\mathrm{SL}_n(K)$ обозначаются соответственно группа всех невырожденных матриц размера $n \times n$ над полем K и группа матриц $n \times n$ с единичным определителем.

Центр $\mathrm{GL}_n(K)$ состоит из скалярных матриц: $Z(\mathrm{GL}_n(K)) = \{\lambda E \mid \lambda \in K^*\}$. Нетрудно видеть (убедитесь в этом!), что центр SL_n состоит из скалярных матриц с единичным определителем: $Z(\mathrm{SL}_n(K)) = \{\lambda E \mid \lambda^n = 1\}$.

Отфакторизовав эти группы по их центрам, получим *проективную полную линейную группу* и *проективную специальную линейную группу*:

$$\mathrm{PGL}_n(K) = \mathrm{GL}_n(K)/\{\lambda E\}; \quad \mathrm{PSL}_n(K) = \mathrm{SL}_n(K)/\{\lambda E \mid \lambda^n = 1\}.$$

Пусть $K = \mathbb{F}_q$. Нетрудно найти порядки этих групп:

Предложение 7.6.

$$\begin{aligned} |\mathrm{GL}_n(\mathbb{F}_q)| &= (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}); \\ |\mathrm{SL}_n(\mathbb{F}_q)| &= \frac{1}{q-1}(q^n - 1)(q^n - q) \dots (q^n - q^{n-1}); \\ |\mathrm{PGL}_n(\mathbb{F}_q)| &= \frac{1}{q-1}(q^n - 1)(q^n - q) \dots (q^n - q^{n-1}); \\ |\mathrm{PSL}_n(\mathbb{F}_q)| &= \frac{1}{(q-1)(n, q-1)}(q^n - 1)(q^n - q) \dots (q^n - q^{n-1}). \end{aligned}$$

Упражнение 7.7. Докажите это предложение.

Замечание 7.8. Отметим, что, хотя порядки групп $\mathrm{SL}_n(\mathbb{F}_q)$ и $\mathrm{PGL}_n(\mathbb{F}_q)$ совпадают, при $q > 2$ сами эти группы не изоморфны (почему?).

Приведём без доказательства следующую теорему.

Теорема 7.9. *Группа $\mathrm{PSL}_n(\mathbb{F}_q)$ проста при $n \geq 3$ и при $n = 2$, $q \geq 4$.*

Из курса геометрии известно, что группа $\mathrm{PGL}_2(\mathbb{F}_q)$ действует на проективной прямой $\mathbb{P}^1(\mathbb{F}_q)$ (т.е. на $q+1$ -элементном множестве), причём это действие точно, т.е. не имеет ядра неэффективности. Таким образом, имеется вложение

$$\mathrm{PGL}_2(\mathbb{F}_q) \hookrightarrow S_{q+1} = \mathrm{Perm}(\mathbb{P}^1(\mathbb{F}_q)).$$

Также известно, что это действие 3-транзитивно (любую тройку точек можно перевести в любую). Это нам также пригодится.

Теорема 7.10.

$$\begin{aligned} \mathrm{GL}_2(\mathbb{F}_2) = \mathrm{SL}_2(\mathbb{F}_2) = \mathrm{PGL}_2(\mathbb{F}_2) = \mathrm{PSL}_2(\mathbb{F}_2) &\cong S_3; \\ \mathrm{PGL}_2(\mathbb{F}_3) &\cong S_4; \\ \mathrm{PSL}_2(\mathbb{F}_3) &\cong A_4; \\ \mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4) &\cong A_5. \end{aligned}$$

Доказательство. Равенства из первой строки очевидны: во всех этих группах по 6 элементов, и они вкладываются в шестиэлементную группу S_3 , значит, это изоморфизм. Также ясно, что три точки $\mathbb{P}^1(\mathbb{F}_2)$ как раз и соответствуют трём элементам, которые переставляет группа S_3 .

Второй изоморфизм получается аналогично, также из соображений подсчёта числа элементов в левой и правой частях. Третий вытекает из того, что A_4 — единственная подгруппа в S_4 индекса 2.

Порядок группы $\mathrm{PGL}_2(\mathbb{F}_4) = \mathrm{PSL}_2(\mathbb{F}_4)$ равен 60, поэтому её образ при вложении в S_5 является подгруппой индекса 2. А единственная подгруппа в S_5 индекса 2 (и вообще единственная нормальная подгруппа — это A_5). \square

Следующее рассуждение несколько более сложно.

Теорема 7.11. $\mathrm{PGL}_2(\mathbb{F}_5) \cong S_5$; $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.

Доказательство. Порядок группы $\mathrm{PGL}_2(\mathbb{F}_5)$ равен 120. Её действие на $\mathbb{P}^1(\mathbb{F}_5)$ определяет гомоморфизм $\mathrm{PGL}_2(\mathbb{F}_5) \rightarrow S_6$. Докажем, что всякая подгруппа из 120 элементов $H \subset S_6$ изоморфна S_5 .

Действительно, S_6 действует на множестве левых смежных классов S_6/H . Этих классов тоже 6, поэтому имеется гомоморфизм $\alpha: S_6 \rightarrow S_6$. Ядро гомоморфизма α — нормальная подгруппа. Значит, это либо $\{e\}$, либо A_6 , либо S_6 . Последние два случая невозможны, так как тогда на S_6/H транзитивно действовала бы группа из 1 или 2 элементов. Значит, α — изоморфизм.

Осталось заметить, что при этом действии стабилизатор точки eH изоморфен H . Однако стабилизатор одного элемента для обычного действия S_6 на 6-элементном множестве есть S_5 . Значит, $H \cong S_5$.

Заметим, что это эта подгруппа не сопряжена стандартному вложению $S_5 \subset S_6$, так как её действие транзитивно. Мы получили так называемое *экзотическое вложение* $S_5 \hookrightarrow S_6$.

Утверждение о группе $\mathrm{PSL}_2(\mathbb{F}_5)$ следует из того, что в S_5 есть только одна подгруппа индекса 2. \square

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