

Содержание

1 Введение	2
Лекция 1. Теорема Абеля-Руфини	2
2 Полиномиальные уравнения, многозначные функции	2
3 Теорема Абеля	3
4 Топологическая теория Галуа	3
Лекция 2. Группа монодромии накрытия	4
5 Поднятие	4
6 Группа монодромии	5
Лекция 3.	6
7 Разветвленные накрытия	6
Лекция 4. Разрешимость группы монодромии	7
8 Разрешимость группы монодромии накрытия функции, выраженной в радикалах	8
Лекция 5. Системы уравнений I	9
9 Системы уравнений, их носитель, понятие разрешимости в радикалах	9
Лекция 6. Системы уравнений II	10
10 Основные соображения по упрощению	10
11 Смешанный объём Минковского	11
12 Критерий разрешимости системы в радикалах	12

1 Введение

- «Теорема Абеля в задачах и решениях», Алексеев
- По алгебраической геометрии: Харцкорн, Шафаревич.

Лекция 1. Теорема Абеля-Руфини

2 Полиномиальные уравнения, многозначные функции

Задача обращения: $f : \mathbb{C} \rightarrow \mathbb{C}$, найти $g : \mathbb{C} \rightarrow \mathbb{C}$, $f(g(y)) = y$, притом функция многозначная.

Если f — многочлен, то знаем формулу для $\deg f \leq 4$.

Определение 1 (Многозначная функция). Многозначная функция f — неявная функция $\mathbb{C} \rightarrow \mathbb{C}$, заданная полиномиальным уравнением $\{F = 0\}$, $F : \mathbb{C}^2 \rightarrow \mathbb{C}$.

Либо $f = \{x \in \mathbb{C}^2 \mid F(x) = 0\}$, либо $f : \mathbb{C} \rightarrow 2^{\mathbb{C}}$, $f(x) = \{y \in \mathbb{C} \mid F(x, y) = 0\}$.

Если f, g — многозначные, то можно определить композицию $h = g \circ f = \{(x, z) \mid \exists y : F(x, y) = G(y, z) = 0\}$. Определение пока что некорректно, нужно как-то перейти к одному уравнению.

Определение 2 (Аффинное алгебраическое многообразие). Аффинное (в смысле не проективное) алгебраическое многообразие $X \subset \mathbb{C}^n$ — это множество, заданное системой полиномиальных уравнений.

$X = \{x \in \mathbb{C}^n \mid F_j(x) = 0, j = 1, \dots, k\}$, $F_j : \mathbb{C}^n \rightarrow \mathbb{C}$ — многочлены.

Проблема: если взять аффинное алгебраическое многообразие, заданное двумя уравнениями в \mathbb{C}^3 , то его проекция на (x, z) одним уравнением может и не задаваться.

Теорема 1 (О проекции аффинного алгебраического многообразия). Пусть отображение $H : \mathbb{C}^n \rightarrow \mathbb{C}^m$ полиномиальное. Тогда $H(X) \subset \mathbb{C}^m$ — аффинное алгебраическое многообразие.

Пример. Многообразие $X = \{xy = yz = xz = 0\}$ имеет коразмерность 2, хочется задать его двумя уравнениями, но можно показать, что это невозможно.

Теорема 2. Любое алгебраическое многообразие размерности $n - 1$ в \mathbb{C}^n можно задать одним уравнением.

В этом свете наша композиция определена корректна.

Определение 3 (Сумма, произведение многозначных функций). Если $l : \mathbb{C}^2 \rightarrow \mathbb{C}$, то $l(f, g) = \{(x, l(y_1, y_2)) \mid F(x, y_1) = F(x, y_2) = 0\}$. В частности, так можно определить сложение и умножение.

Так как это проекция многообразия $\{(x, y_1, y_2, z) \mid F(x, y_1) = F(x, y_2) = z - l(y_1, y_2) = 0\}$, то полученный объект — это многозначная функция.

3 Теорема Абеля

Определение 4 (Выразимость в радикалах). Функция $f : \mathbb{C} \rightarrow \mathbb{C}$ выражена в радикалах, если:

- $f(x) = c, f(x) = \sqrt[n]{x} (F(x, y) = x^n - y)$.
- Композиция функций, выраженных в радикалах.
- $l(f, g)$, где l — многочлен, f, g выражены в радикалах.

Определение 5 (Разрешимость в радикалах). $f : \mathbb{C} \rightarrow \mathbb{C}$ — разрешима в радикалах, если существует g — многозначная $\mathbb{C} \rightarrow \mathbb{C}$, выраженная в радикалах, такая что $g(y) \supset f^{-1}(y)$.

Замечание. $g(y) = f^{-1}(y)$ не получается, например, в случае формулы Кардано 6 корней. Однако, нас в принципе не очень смущает наличие побочных корней.

Если мы можем выразить корни уравнения формулой в радикалах, то можно разрешить в радикалах соответствующий многочлен, просто подставив $c_0 - y$ вместо свободного члена c_0 .

Теорема 3 (Теорема Абеля). *Многочлен f общего положения $\deg f \geq 5$ неразрешим в радикалах.*

Говоря про общее положение подразумеваем, что это неверно лишь на нигде не плотном множестве. Более того, в нашем случае это нигде не плотное множество будет алгебраическим многообразием меньшей размерности.

4 Топологическая теория Галуа

Определение 6 (Накрытие). Накрытие $\pi : E \rightarrow B$ — это непрерывное отображение топологических пространств, такое, что существует F — дискретное топологическое пространство, такое что $\forall x \in B \rightarrow \exists U = U(x) : \exists \varphi_x : \pi^{-1}(U) \rightarrow U \times F$, такое что оно осуществляет гомеоморфизм, а также $p_u(\varphi_x(e)) = \pi(e)$, где $p : F \times U$ — проектор на U .

Замечание. Если просто попросить, что $\pi^{-1}(U) \cong U \times F$, то накрытием будет отображение из интервала в интервал, которое левую треть отображает в левую половину линейно, правую в правую, а середину склеивает в одну точку.

$|f^{-1}(y)| = \deg f$, кроме некоторых точек, а именно тех, где $f(x) = y, f'(x) = 0$, то есть это верно для всех y кроме так называемых критических значений многочлена B' .

Утверждение 1. Пусть $B' = \{y \mid \exists x : f'(x) = 0, y = f(x)\}$. Тогда отображение $f|_{\mathbb{C} \setminus f^{-1}(B')}$ является накрытием над $\mathbb{C} \setminus B'$.

Доказательство. Нужно взять окрестность некоторой точки $x \in \mathbb{C} \setminus B'$, взять все её прообразы, взять у них по окрестности, пересечь их образы, позаботиться о том, чтобы они не пересекались и не содержали плохих точек и применить теорему об обратной функции. \square

Лекция 2. Группа монодромии накрытия

5 Поднятие

Лемма (О поднятии). Для любого пути в базе $\varphi : [0; 1] \rightarrow B$ и $v_0 \in \pi^{-1}(\varphi(0))$ существует единственный путь-поднятие: $\bar{\varphi}_v : [0; 1] \rightarrow E : \bar{\varphi}_v(0) = v$ и $\varphi = \pi \circ \bar{\varphi}_v$.

Доказательство. Для каждой точки отрезка $\forall t \in [0; 1] \exists U_t$ — окрестность точки t с таким свойством, что $\varphi(U_t) \subset U(\varphi(t))$, где $U(\varphi(t))$ — тривиализующая окрестность: $\pi^{-1}(U(\varphi(t))) \xrightarrow{k} U(\varphi(t)) \times F$.

В силу компактности отрезка выберем конечное подпокрытие: $\exists t_0, \dots, t_N : [0; 1] = \bigcup_{j=0}^N U_{t_j}$. Более того, сузим все интервалы до отрезков, граничащих

по концам: $[0; 1] = \bigcup_{j=0}^{N-1} [t_j; t_{j+1}]$.

Для каждого $j \exists U_j \subset B : \varphi([t_j; t_{j+1}]) \subset U_j, k_j : \pi^{-1}(U_j) \rightarrow U_j \times F$ (при этом $\pi = k_j \circ p_1$).

Поднятие тогда определим так: $\bar{\varphi} = k_j^{-1}(\varphi(t), p_2 \circ k(\bar{\varphi}(t_j)))$. Это отображение непрерывно, так как непрерывно на каждом из замкнутых множеств, которые разбивают весь отрезок.

$$\pi \circ \bar{\varphi}(t) = \pi(k^{-1}(\varphi(t), \dots)) = p_1(\varphi(t), \dots) = \varphi(t).$$

Единственность покажем по индукции: если $\bar{\varphi}'$ тоже поднятие и оно совпадает на нескольких первых отрезках, нужно показать, что оно совпадает и на следующем. \square

Определение 1 (Действие фундаментальной группы). Действие группы $\pi_1(B, b_0)$ на множестве $\pi^{-1}(b_0)$ определим формулой $\psi : \pi_1(B, b_0) \rightarrow S(\pi^{-1}(b_0)), \psi([\varphi])(v) = \bar{\varphi}_v(1)$.

Утверждение 1. $\overline{(\varphi_1 \varphi_2)} = \bar{\varphi}_{1, v_1} \bar{\varphi}_{2, v_0}$, где $v_1 = \bar{\varphi}_{2, v_0}(1)$.

Доказательство. Отображение является поднятием какого-то пути, если удовлетворяет двум свойствам из определения. Первое свойство очевидно, второе: $\pi \circ (\bar{\varphi}_{1, v_1} \bar{\varphi}_{2, v_0}) = \varphi_2$ при $t \in [0; \frac{1}{2})$ и $\varphi_1(2t + 1)$ иначе. \square

Корректность определения:

- Гомоморфизм: $\psi([\varphi_1][\varphi_2])(v) = \psi([\varphi_1\varphi_2])(v) = \overline{(\varphi_1\varphi_2)}_v(1) = \overline{\varphi_1}_{v_1}\overline{\varphi_2}_{v_1}(1) = \overline{\varphi_1}_{v_1}(1) = \psi([\varphi_1])(\overline{\varphi_2}_{v_1}(1)) = \psi([\varphi_1]) \circ \psi([\varphi_2])(v)$ где, $v_1 = \overline{\varphi_2}_{v_1}$
- Биективность: обратным будет отображение $\psi([\varphi^{-1}])$.
- Если $[\varphi_1] = [\varphi_2]$, то $\overline{\varphi_1}_{v_1}(1) = \overline{\varphi_2}_{v_1}(1)$ (упражнение).

6 Группа монодромии

Определение 2 (Группа монодромии). Группа монодромии G_{b_0} накрытия $\pi : E \rightarrow B \ni b_0$ — это образ $\psi(\pi_1(B, b_0))$.

Пример. У накрытия $\exp : \mathbb{R} \rightarrow S^1$ выполнено $\psi([\varphi])(v) = v + 1$, то есть $G_{b_0} \cong \mathbb{Z} \cong \pi(B, b_0)$.

Пример. У тривиального накрытия группа монодромии тривиальна, в то время, как фундаментальная группа $\pi_1(B, b_0)$ может быть нетривиальна, то есть нельзя сказать, что ψ — изоморфизм.

Пример. У накрытия $P_k : S^1 \rightarrow S^1, P_k(e^{2\pi it}) = e^{2\pi ikt}$ выполнено $\psi([\varphi])(v) = ve^{\frac{2\pi ikt}{k}}$, то есть $G_{b_0} \cong \mathbb{Z}_k$.

Вообще говоря, корректность определения группы монодромии не очевидна.

Утверждение 2. Пусть $\varphi_1 \sim \varphi_2$, $\Theta : [0; 1]^2 \rightarrow B : \Theta(t, 0) = \varphi_1(t), \Theta(t, 1) = \varphi_2(t)$, тогда $\psi(\varphi_1) = \psi(\varphi_2)$.

Доказательство. $\psi([\varphi_j])(x) = \overline{\varphi_{j,x}}(1)$. Нужно показать, что $\overline{\varphi_{1,x}}(1) = \overline{\varphi_{2,x}}(1)$. Мы будем определять отображение $\overline{\Theta} : [0; 1]^2 \rightarrow E$ так, чтобы еще $\Theta(0, t) = x$.

Лемма (О продолжении поднятия). Пусть $f : D^n \rightarrow B, F_0 : D_1 \rightarrow E : f|_{D_1} \equiv p \circ F$, где $D_1 = \{x \in \partial D^n \mid x_n \leq 0\}$. Тогда $\exists F : D^n \rightarrow B, F_0 = F|_{D_1}, f = p \circ F$.

По лемме, такое поднятие $\overline{\Theta}$ существует. Тогда рассмотрим $p \circ \overline{\Theta}|_{\{(1,t)\}} = \Theta(\{1, \tau\}) = \{\varphi_\tau(1)\}$, а значит, что $\overline{\Theta}(\{1, \tau\}) \subset p^{-1}(b)$ — дискретно, то есть $|\overline{\Theta}(\{1, \tau\})| = 1$.

Доказательство леммы. Легко показать, что у каждой точки x_0 , которую мы смогли поднять, есть окрестность, которую можно поднять. В силу компактности квадрата, достаточно взять конечное число открытых множеств, чтобы его покрыть. Более того, можно показать, что можно взять мелкую сетку из маленьких замкнутых квадратиков, каждый из которых лежит в открытом множестве, над которым накрытие тривиально, и продолжать поднятие построчно по этим квадратикам. \square

□

Определение 3 (Изоморфизм накрытий). Накрытия $\pi_i : E_i \rightarrow B_i$, $i \in \{0, 1\}$ изоморфны, если существует гомеоморфизмы $f : E_1 \leftrightarrow E_2, g : B_1 \leftrightarrow B_2$, такие что $\pi_2 \circ f \cong g \circ \pi_1$.

Замечание (Связь группы монодромии с фундаментальной группой). Если $\varphi : [0; 1] \rightarrow B, \varphi(0) = b_0, \varphi(1) = b_1$, то $G_{b_0} \cong G_{b_1}$.

Замечание (Изоморфизм групп монодромии). Если два накрытия изоморфны, то $G_{b_1} \cong G_{g(b_1)}$.

Доказательство. Рассмотрим два построения.

Рассмотрим $[\varphi] \in \pi_1(b_1, b_0)$ и $[g(\varphi)] \in \pi_1(B_2, b_2)$. Отображение определим как $h : G_{b_1} \rightarrow G_{g(b_1)}, h(\psi([\varphi])) = \psi(g_*([\varphi]))$, где g_* — индуцированное отображением g отображение фундаментальных групп. Нужно показать, что если $[\varphi_1] \neq [\varphi_2]$, то $\psi([\varphi_1]) \neq \psi([\varphi_2])$.

Пусть $\sigma \in G_{b_1} \subset S(\pi^{-1}(b_1))$. Определим отображение $h(\sigma)(v) = f(\sigma(f^{-1}(v)))$. Нужно показать корректность: $h(\sigma) \in G_{b_2}$.

Если покажем, что эти построения это на самом деле одно и то же, то оба будут корректны.

Утверждается, что $\psi([g(\varphi)])(v) = \overline{g(\varphi)}_v(1) = f(\overline{\varphi}_{f^{-1}(v)})(1)$. Для этого надо проверить свойства: 1) $f(\overline{\varphi}_{f^{-1}(v)})(0) = f(f^{-1}(v)) = v$; 2) $\pi_2(f(\overline{\varphi}_{f^{-1}(v)})) = g(\pi_1(\overline{\varphi}_{f^{-1}(v)})) = g(\varphi)$.

Тогда $\psi([g(\varphi)]) = f(\overline{\varphi}_{f^{-1}(v)})(1) = f(\psi([\varphi])(f^{-1}(v))) = f(\sigma(f^{-1}(v)))$, что нам и надо. □

Замечание (Гомоморфизм накрытий). Эти рассуждения работают, если f, g — непрерывные отображения, такие что $\pi_2 \circ f = g \circ \pi_1$, а также, что $f|_{P_i}$ — биекция, где P_i — это i -й слой накрытия. В этом случае не факт, что индуцированное отображение является изоморфизмом.

Такие f, g задают так называемый гомоморфизм накрытий.

Лекция 3.

7 Разветвленные накрытия

Определение 1. Разветвленное накрытие $\pi : E \rightarrow B$ — это накрытие над $B \setminus B'$, где $B' \subset B$ — конечно (варианты: дискретно, нигде не плотно, имеет меньшую размерность. Все они равносильны, если B одномерно).

Минимальное по включению такое B' называется бифуркационным множеством разветвленного накрытия π .

Определение 2. Пусть $f(x)$ — многозначная комплексная функция ($f(x) = \{y \mid F(x, y) = 0\}$). Её разветвленным накрытием назовём $p : X \rightarrow \mathbb{C}, p(x, y) = x(X = \{(x, y) \mid F(x, y) = 0\})$.

Хочется сказать, что бифуркационное множество многочлена содержится в множестве $\{x \mid \exists y : (x, y) \in X, \frac{\partial F}{\partial y} = 0\}$. Однако, многочлен $xy - 1$ имеет бифуркационное множество $\mathbb{C} \setminus \{0\}$, хотя точек указанного вида нет. Проблема в том, что у точки 0 прообраза нет, однако прообраз окрестности не пуст, поэтому повторить доказательство для многочленов вида $g(y) - x$ не выйдет. Поэтому нам нужно, чтобы окрестности прообразов точки A содержали прообраз какой-то окрестности A , тогда все можно сделать по теореме об обратной функции.

То есть верное утверждение будем таким: бифуркационное множество B функции $f(x)$ лежит в объединении $B_1 = \{x_0 \mid F(x_0, \cdot) < \deg_y F\}$ и B' .

Определение 3. Пара отображений $f : E_1 \rightarrow E_2, g : B_1 \rightarrow B_2$ называется гомоморфизмом накрытий $p_1 : E_1 \rightarrow B_1$ и $p_2 : E_2 \rightarrow B_2$, если $p_2 \circ f = g \circ p_1$, то есть коммутует диаграмма:

$$\begin{array}{ccc} E_1 & \xrightarrow{f} & E_2 \\ \downarrow p_1 & & \downarrow p_2 \\ B_1 & \xrightarrow{g} & B_2 \end{array}$$

Пример.

$$\begin{aligned} p_1 : X &\rightarrow \mathbb{C}, X = \{G = 0\} \subset \mathbb{C}^2 \\ p_2 : X' &\rightarrow \mathbb{C}, X' = \{f(y) = x\} \subset \mathbb{C}^2 \end{aligned}$$

Пусть $p : E \rightarrow \mathbb{C}$ — разветвленное накрытие, $B_1 \supset B$, где B — бифуркационное множество. Тогда:

- $\pi_1(\mathbb{C} \setminus B) \xleftarrow{i_*} \pi_1(\mathbb{C} \setminus B_1)$, где $i : \mathbb{C} \setminus B_1 \hookrightarrow \mathbb{C} \setminus B$, так как локальная связность не нарушается от выкидывания дискретного набора точек. i_* является вместе с тем эпиморфизмом.
- Пусть есть две группы монодромии $G_1 = G_{p|_{\mathbb{C} \setminus B}}, G_2 = G_{p|_{\mathbb{C} \setminus B_1}}$.

$$G_1 = \psi_p(\pi_1(\mathbb{C} \setminus B)) = \psi_p(i_*(\pi_1(\mathbb{C} \setminus B_1))), G_2 = \psi_p(\pi_1(\mathbb{C} \setminus B_1))$$

Поскольку i_* ничего не делает с петлями с точки зрения монодромии, хотя петель могло стать больше, то $G_1 = G_2$.

Таким образом группу монодромии разветвленного накрытия можно корректно определить как группу монодромии накрытия на $\mathbb{C} \setminus B$, где B — любое дискретное множество, содержащее бифуркационное.

Лекция 4. Разрешимость группы монодромии

Список фактов с подсказками:

- Если группа транзитивна и порождена транспозициями, то она есть S_n (комбинаторный факт)
- Группа монодромии транзитивна (нужно, чтобы $\mathbb{C} \setminus p^{-1}(B')$ было линейно связно, что верно, так как второе множество конечно, тогда все пути можно опустить, чтобы они стали петлями в фундаментальной группе).
- Группа монодромии порождена транспозициями (нужно понять, как устроены петли в $\mathbb{C} \setminus p^{-1}(B')$).
- Если E_1 вложено в E_2 (то есть поднакрытие), то можно индуцировать эпиморфизм i^* из группы монодромии $G_2 \rightarrow G_1$.
- Неразрешимая группа не может быть образом разрешимой при эпиморфизме.
- Группа монодромии накрытия, заданного функцией, выраженной в радикалах, разрешима (ближайшая цель).

8 Разрешимость группы монодромии накрытия функции, выраженной в радикалах

Так или иначе, доказывать придется по индукции. База:

- $g(x) = c, G = S_1$.
- $g(x) = \sqrt[n]{x}, X = \{(x, y) \mid x = y^n\}, p : X \rightarrow \mathbb{C}, p(x, y) = x, B' = \{0\}, x = f(y) = y^n$.

$$S_{\{\sqrt[n]{1}\}} \supset G_{p,1} = \psi(\underbrace{\pi_1(\mathbb{C} \setminus \{0\})}_{\cong \mathbb{Z}}).$$

$$G_{p,1} = \langle \psi([\varphi]) \rangle, \varphi(t) = \exp(2\pi i t), \psi([\varphi])(z) = \tilde{\varphi}_z(1).$$

$$\text{Пусть } \tilde{\varphi}(t) = z \exp(2\pi i \frac{t}{n}), p \circ \tilde{\varphi}(t) = (z \exp(2\pi i \frac{t}{n}))^n = z^n \exp(2\pi i t) = \exp(2\pi i t) = \varphi(t).$$

Тогда $\tilde{\varphi}$ — действительно поднятие φ . Таким образом $\psi([\varphi])(z) = \tilde{\varphi}_z(1) = z \exp(\frac{2\pi i}{n})$. Стало быть группа монодромии \mathbb{Z}_n — разрешима.

Для шага нужно две вещи: любой полином от двух разрешенных функций и их композиция.

Определение 1. Пусть $p_1, p_2 : E_1, E_2 \rightarrow B$ — два разветвлённых накрытия. Тогда $p_1 \oplus p_2 : E_3 \rightarrow B, E_3 = \{z_1, z_2 \mid p_1(z_1) = p_2(z_2)\} \subset E_1 \times E_2, p(z_1, z_2) = p_1(z_1) = p_2(z_2)$ называется прямой суммой разветвлённых накрытий.

Прямая сумма разветвлённых накрытий есть разветвлённое накрытие: нужно выяснить, в чём содержится бифуркационное множество.

Утверждение 1. $B \subset B_1 \cup B_2$.

Доказательство. Пусть $b \in B \setminus (B_1 \cup B_2)$. Дано: $\exists U_1 \ni b, U_2 \ni b, \xi_1, \xi_2, \xi_j : p_j^{-1}(U_j) \rightarrow U_j \times F_j$.

Рассмотрим тогда $U_3 = U_1 \cap U_2$. $(p_1 \oplus p_2)^{-1}(U_3) = \{(z_1, z_2) \in E_1 \times E_2 \mid p_1(z_1) = p_2(z_2) \in U_3\} \subset p_1^{-1}(U_3) \times p_2^{-1}(U_3) = V_3$.

Нам нужно найти $\xi_3 : V_3 \rightarrow U_3 \times F_1 \times F_2$. Определим её как $\xi_3(z_1, z_2) = (p_1(z_1) = p_2(z_2), \xi_1(z_1)_2, \xi_2(z_2)_2)$. $z_j = \xi_j^{-1}(p_j(z_j), \xi_j(z_j)_2)$, значит это гомеоморфизм.

Проекция ξ_3 на первый сомножитель и есть $p_1 \oplus p_2$, поэтому корректность разветвлённого накрытия доказана. \square

Утверждение 2. $G_{p_1 \oplus p_2} \cong G < G_{p_1} \oplus G_{p_2}$.

Доказательство. Идея: сопоставить $\sigma = \psi_{p_1 \oplus p_2}([\varphi]) \mapsto (\psi_{p_1}([\varphi]), \psi_{p_2}([\varphi])) = (\sigma_1, \sigma_2)$. Нужно показать, что отображение определено корректно.

Утверждение: $\psi_{p_1 \oplus p_2}([\varphi])(z_1, z_2) = (\sigma_1(z_1), \sigma_2(z_2))$, где $\sigma_j = \psi_{p_j}([\varphi])$. То есть, $\sigma_3(z_1, z_2) = (\sigma_1(z_1), \sigma_2(z_2))$.

В самом деле $\tilde{\varphi}_{z_1, z_2}(t) = (\tilde{\varphi}_{z_1}(t), \tilde{\varphi}_{z_2}(t)) \in E_3$, так как $p_1(\tilde{\varphi}_{z_1}(t)) = \varphi(t) = p_2(\tilde{\varphi}_{z_2}(t))$.

$\psi_{p_1 \oplus p_2}([\varphi])(z_1, z_2) = \tilde{\varphi}_{z_1, z_2}(1) = (\psi_{p_1}([\varphi])(z_1), \psi_{p_2}([\varphi])(z_2))$.

Зная это, определим $\chi : G_{p_1 \oplus p_2} \rightarrow G_{p_1} \oplus G_{p_2}$ по формуле $\chi(\sigma_3) = \sigma_{3,1} \oplus \sigma_{3,2}$.

Из доказанного, это корректный гомоморфизм. Докажем, что это мономорфизм. В самом деле, если образ какого-то элемента тривиален, то и сам элемент есть тривиальная перестановка (обе компоненты тривиальны). \square

Лемма. Пусть p_j — накрытие многочлена f_j , $p_j : X_j \rightarrow \mathbb{C}$, $p_3 : X_3 \rightarrow \mathbb{C}$ — накрытие $f_1 + f_2$. Тогда существует эпиморфизм накрытий $h : E_3 \rightarrow X_3$, где $p_1 \oplus p_2 : E_3 \rightarrow \mathbb{C}$, $E_3 \subset X_1 \times X_2$.

Доказательство. Положим $((b, x_1), b(b, x_2)) = (b, x_1 + x_2)$. Легко видеть, что $p_3 \circ h = p_1 \oplus p_2$, а также, что h — непрерывна. Более того, h — сюръекция. Значит h — эпиморфизм. \square

Замечание. Аналогичная лемма дословно верна для произведения.

Лемма. Пусть $h : E_1 \rightarrow E_2$ эпиморфизм накрытий $p_j : E_j \rightarrow B$. Тогда существует индуцированный эпиморфизм $h_* : G_{p_1} \rightarrow G_{p_2}$.

Из всего этого, G_{p_1}, G_{p_2} — разрешимы $\Rightarrow G_{f_1+f_2}, G_{f_1 \cdot f_2}$ разрешимы.

Лекция 5. Системы уравнений I

9 Системы уравнений, их носитель, понятие разрешимости в радикалах

У нас теперь есть система полиномиальных уравнений: $P_1 = \dots = P_k = 0$, притом $P_j \in \mathbb{C}[x_1, \dots, x_k]$.

Для начала нужно понять, что вообще может играть роль степени многочлена для системы. Подходы могут быть разные, мы рассмотрим только один из них.

Носитель многочлена P от k переменных x_1, \dots, x_k есть точки $A(P) \subset \mathbb{Z}^k$. В общем случае $P = \sum_{k \in \mathbb{Z}^k} c_k x^k$, где $x^k = \prod x_j^{k_j}$, а носитель это $A(P) = \{k \in \mathbb{Z}^k \mid c_k \neq 0\}$. Положим также, что $|A(P)| < \infty$, чтобы у нас был многочлен, а не ряд Лорана.

Определение 2. Решением общей системы уравнений с носителем A называется функция $F = F_{A_1, \dots, A_k} : \mathbb{C}^{A_1} \times \dots \times \mathbb{C}^{A_k} \rightarrow 2^{\mathbb{C}^{*k}}$.

Для простоты, чтобы облегчить замены переменных, будем рассматривать решения только ненулевые.

$$F(c^1, \dots, c^k) = \{x \in \mathbb{C}^k \mid P_{c^1}(x) = \dots = P_{c^k}(x) = 0\}, c^j \in \mathbb{C}^{A_j}.$$

Определение 3. Нужно теперь как минимум определить многозначную вектор-функцию, выраженную в радикалах. g является таковой, если каждая её компонента является функцией, выраженной в радикалах, то есть либо константа, либо корень из какой-то компоненты, либо сумма, произведение или композиция других выражений в радикалах (частное подразумеваем как корень минус первой степени).

Общая система с носителями A_1, \dots, A_k разрешима в радикалах, если $\forall c_0 \in \mathbb{C}^A, |F(c_0)| < \infty \exists U(c_0) \subset \mathbb{C}^A, U(c_0)$ — открытая по-Зариски, такая что существует разрешимая в радикалах функция $g : \mathbb{C}^{U(c_0)}$, такая, что $G \supset F$.

Замечание. Топология Зарисского на множестве \mathbb{F}^k это $\Omega = \{\mathbb{F}^k \setminus A \mid \exists l \in \mathbb{N}, P_1, \dots, P_l \in \mathbb{F}[x_1, \dots, x_k] \mid A = \{P_1 = \dots = P_l = 0\}\}$.

Лекция 6. Системы уравнений II

10 Основные соображения по упрощению

Самый общий вопрос: при каких A общая система разрешима в радикалах. Первые мысли:

- Удобно рассматривать мономиальные замены переменных на комплексном торе \mathbb{C}^{*k} . $x^k = u^{Mk}$, где $M \in GL_k(\mathbb{Z})$.
- Случаи, которые можно свести к более простым:

$$- A \text{ называется невырожденной, если } \forall i \rightarrow A_i \ni 0 \in \mathbb{Z}^k, \left\langle \bigcup_{j=1}^k A_j \right\rangle_{\mathbb{Z}} =$$

\mathbb{Z}^k . Вырожденные сводятся к невырожденным.

Если $\exists i : 0 \notin A_i$. \mathbb{C}^{A_j} заменяется на $\mathbb{C}^{A_j - \{k_0\}}$.

Если же $\left\langle \bigcup_{j=1}^k A_j \right\rangle_{\mathbb{Z}} \neq \mathbb{Z}^k$, то сведение делается (почти) мономиальной заменой $M : M^{-1}e_j = v_j \Rightarrow M^{-1} = (v_1 \dots v_k)$. Почти потому что замена может быть необратимой.

- Пусть $\exists j_1 < \dots < j_l : \dim \sum_{p=1}^l A_{j_p} \leq l < n$ (сумма Минковского).

Тогда набор A_1, \dots, A_n называется *приводимым*.

Рассмотрим набор векторов $\alpha_1, \dots, \alpha_l \in \mathbb{Z}^n$, которые порождают $\mathbb{Z}^n \cap \left\langle \sum_{p=1}^l A_{j_p} \right\rangle$. Чтобы сделать замену нам хочется достроить

этот набор до базиса \mathbb{Z}^n (это возможно не всегда, но можно достроить хотя бы просто до базиса подрешётки размерности n).

Рассмотрим мономиальную замену $u^k = x^{M^k}$, где $M = (\alpha_1, \dots, \alpha_n)$, переходя к системе $P'_{j_s}(u) = P_{j_s}(x)$ с носителем $A'_{j_s} = A(P'_{j_s}) = M^{-1}(A_{j_s})$. В частности $M^{-1}(\alpha_j) = e_j$. Значит $A'_{j_s} \subset \mathbb{Z}^l \subset \langle e_1, \dots, e_l \rangle$.

Тогда разрешимость системы сводится к двум вопросам: разрешимость системы l уравнений с носителями $A'_{j_s}, s = 1, \dots, l$ (кроме некоторых случаев, если она неразрешима, то и большая тоже) и разрешимость системы с носителями $\{A'_{j_s}/\mathbb{Z}^l \mid s > l\}$.

Теперь можно сформулировать гипотезу.

Утверждение 3. Если система невырождена и неприводима, а ожидаемое количество решений больше 4, то она не разрешима в радикалах.

11 Смешанный объём Минковского

Нужно только уточнить, что понимается под «ожидаемым числом решений».

Теорема 1 (Бернштейн, Хованский). Для системы общего положения с носителями A_1, \dots, A_n (невырожденной) количество решений в $(\mathbb{C}^*)^n$ совпадает со смешанным объёмом Минковского $MV_n(\langle A_1 \rangle, \dots, \langle A_n \rangle)$.

Смешанный объём Минковского можно определить многими способами:

- Конструктивно. Пусть выпуклые тела $A_1, \dots, A_n \subset \mathbb{R}^n$, $F_A : (\mathbb{R}_+)^n \rightarrow \mathbb{R}$, $F(\lambda_1, \dots, \lambda_n) = V_n(\sum_{j=1}^n \lambda_j A_j)$. Можно показать, что F — гладкая,

что даёт нам право рассмотреть $\frac{\partial^n F_A}{\partial \lambda_1 \dots \partial \lambda_n}(0)$ и объявить это *смешанным объёмом Минковского* $MV_n(A_1, \dots, A_n)$.

- Некоторые свойства:

$$- MV(A, \dots, A) = n!V_n(A). \text{ В самом деле } F_A = V_n((\sum \lambda_j)A) = V_n(A)(\sum \lambda_j)^n \Rightarrow \frac{\partial^n F_A}{\partial \lambda_1 \dots \partial \lambda_n} = n!.$$

– MV — симметрична:

$$MV_n(A_1, \dots, A_n) = MV_n(A_{\sigma(1)}, \dots, A_{\sigma(n)}), \sigma \in S_n.$$

– MV — полилинейна:

$$\begin{aligned} MV_n(\lambda_1 A'_1 + \lambda_2 A''_1, A_2, \dots, A_n) = \\ \lambda_1 MV_n(A'_1, A_2, \dots, A_n) + \lambda_2 MV_n(A''_1, A_2, \dots, A_n). \end{aligned}$$

- Предыдущих трёх свойств достаточно, чтобы определить функцию на множестве $(\Omega_n)^n$ (Ω_n — множество выпуклых тел в \mathbb{R}^n) однозначно. В частности:

$$MV_2(A_1, A_2) = V(A_1 + A_2) - V(A_1) - V(A_2).$$

- Предыдущая формула ведёт нас к явному определению:

$$\begin{aligned} MV_n(A_1, \dots, A_n) = \\ V_n\left(\sum A_j\right) - \sum_{k=1}^n V_n\left(\sum_{j \neq k} A_j\right) + \dots + (-1)^{n-1} \sum_k V_n(A_k). \end{aligned}$$

Пример. Найдём ожидаемое число решений системы $P_1(x, y) = ax^3 + bxy + c = P_2(x, y) = dx + ey^2 + f$. Выпуклые оболочки носителей — два треугольника, посчитав площадь суммы и суммы площадей, получаем 6.

12 Критерий разрешимости системы в радикалах

Теорема 2. Утверждение гипотезы верно для наборов A_1, \dots, A_n , для которых $\exists j \exists k_1, k_2 \in A_j : [k_1; k_2] \not\subset \partial \langle A_j \rangle$.

Частный случай такого препятствия — линейные уравнения (A_j — маленький симплекс, который мономиальной заменой приводится к стандартному), которые, казалось бы, отмечаются ограничением на невырожденность и неприводимость, однако, оказываются, бывают более сложные примеры таких многогранников.