

Элементарные теории абелевых групп

Н. А. Баженов

Институт математики им. С. Л. Соболева СО РАН (г. Новосибирск)

11–13 апреля 2023 г.

Факты из первой лекции

Абелевы группы рассматриваются в сигнатуре $\sigma_{AG} = \{=; +, -, 0\}$.
Все рассматриваемые группы являются абелевыми.

Если $H_1 \leq H$ и $H_2 \leq H$, то $[H_1 : H_2] = [H_1 : H_1 \cap H_2]$.

Лемма 1

Пусть H — абелева группа; $H_1 \leq H$ и $H_2 \leq H$; $a \in H$.

- (a) $[(H_1 + H_2) : H_2] = [H_1 : H_2]$.
- (b) $[H : H_1] \cdot [H_1 : H_2] \geq [H : H_2]$.
- (c) Число классов смежности по H_2 , которые имеют непустое пересечение с классом $H_1 + a$, равно $[H_1 : H_2]$.

Определение

Позитивно примитивной формулой (п.п.ф.) называем формулу вида

$$\varphi(x_1, \dots, x_n) = \exists y_1 \exists y_2 \dots \exists y_m \theta(\bar{x}, \bar{y}),$$

где θ — это конъюнкция атомарных формул (т.е. формул вида $t = q$ для некоторых термов t и q).

Лемма 2

Пусть $\varphi(\bar{x})$ — позитивно примитивная формула; H — абелева группа; $a_1, \dots, a_k \in H$, где $k < n$.

1. Формула $\varphi(\bar{x})$ определяет подгруппу в декартовой степени H^n .
2. Формула $\varphi(a_1, \dots, a_k, x_{k+1}, \dots, x_n)$ либо не выполняется в H , либо задаёт смежный класс по подгруппе $G \leq H^{n-k}$, такой что G определима формулой $\varphi(0, \dots, 0, x_{k+1}, \dots, x_n)$.

Проблема элементарных индексов

Пусть $\varphi(x), \psi(x)$ — позитивно примитивные формулы, A — абелева группа. Будем обозначать

$$[\varphi : \psi, A] := [\varphi(A) : \psi(A)]$$

(т.е. это индекс подгруппы, определяемой φ в A , по подгруппе, определяемой ψ).

Определение

Говорят, что абелева группа A имеет *разрешимую проблему элементарных индексов*, если существует алгоритм, который по данным позитивно примитивным формулам $\varphi(x), \psi(x)$ и данному $n \geq 1$ определяет, верно ли

$$[\varphi : \psi, A] \geq n.$$

Сведение к проблеме элементарных индексов

Предложение A

Пусть A — абелева группа. Любая формула $\varphi(x_1, \dots, x_n)$ сигнатуры σ_{AG} эквивалентна в $Th(A)$ булевой комбинации $\varphi^*(\bar{x})$ позитивно примитивных формул. Более того, если в A разрешима проблема элементарных индексов, то существует алгоритм, который по данной формуле φ строит φ^* .

Следствие A.1

Элементарная теория $Th(A)$ разрешима в том и только том случае, когда в группе A разрешима проблема элементарных индексов.

Доказательство предложения А (окончание)

Осталось рассмотреть следующий случай:

$$\varphi(x_1, \dots, x_n) = \forall y \left[\varphi_0(\bar{x}, y) \rightarrow \bigvee_{1 \leq i \leq n} \varphi_i(\bar{x}, y) \right], \text{ где } \varphi_i \text{ — п.п.ф.}$$

Группа B_i — это подгруппа в A , определяемая формулой $\varphi_i(\vec{0}, y)$.

Можно считать, что $[B_0 : B_i] \leq n!$.

Пусть $B^* := \bigcap_{0 \leq i \leq n} B_i$.

$$\varphi(x_1, \dots, x_n) = \forall y \left[\varphi_0(\bar{x}, y) \rightarrow \bigvee_{1 \leq i \leq n} \varphi_i(\bar{x}, y) \right].$$

Для $b_1, \dots, b_n \in A$ и $F \subseteq \{1, \dots, n\}$ формула

$$\varphi_0(\bar{b}, y) \wedge \bigwedge_{i \in F} \varphi_i(\bar{b}, y)$$

определяет в A множество $Z_{F, \bar{b}}$.

Либо $Z_{F, \bar{b}} = \emptyset$, либо $Z_{F, \bar{b}}$ содержит $n(F) = [B_0 \cap \bigcap_{i \in F} B_i : B^*]$ смежных классов по подгруппе B^* .

Для $S \subseteq P(\{1, 2, \dots, n\})$ зададим формулу

$$\psi^S(\bar{x}) = \left(\bigwedge_{F \in S} \exists y \bigwedge_{i \in F \cup \{0\}} \varphi_i(\bar{x}, y) \right) \wedge \left(\bigwedge_{F \in P(\{1, \dots, n\}) \setminus S} \neg \exists y \bigwedge_{i \in F \cup \{0\}} \varphi_i(\bar{x}, y) \right).$$

Другими словами, множество $Z_{F, \bar{x}} \neq \emptyset$ в том и только том случае, когда $F \in S$.

Заметим, что формула вида $\exists y \bigwedge_i \varphi_i$ эквивалентна п.п.ф.

Лемма 4

Пусть $C, A_1, \dots, A_n$ — конечные множества. Тогда

$$C \subseteq \bigcup_{i=1}^n A_i \iff \sum_{F \subseteq \{1, \dots, n\}} (-1)^{|F|} \cdot \left| C \cap \bigcap_{i \in F} A_i \right| = 0. \quad (1)$$

Здесь считаем, что $C \cap \bigcap_{i \in \emptyset} A_i = C$.

Зададим множество

$$V = \left\{ S : S \subseteq P(\{1, 2, \dots, n\}), \sum_{F \in S} (-1)^{|F|} \cdot n(F) = 0 \right\}.$$

(1) Пусть $\mathcal{A} \models \varphi(\bar{b})$. Тогда выберем $S_0 = \{F : Z_{F, \bar{b}} \neq \emptyset\}$. Ясно, что $\mathcal{A} \models \psi^{S_0}(\bar{b})$.

Также рассмотрим:

- ▶ C — (конечное) множество всех смежных классов по B^* во множестве $\{y : \mathcal{A} \models \varphi_0(\bar{b}, y)\}$;
- ▶ A_i , $1 \leq i \leq n$, — это (возможно, пустое) множество всех смежных классов по B^* в $\{y : \mathcal{A} \models \varphi_0(\bar{b}, y) \wedge \varphi_i(\bar{b}, y)\}$.

Из $(1:\Rightarrow)$ следует, что $S_0 \in V$.

(2) Пусть теперь $S \in V$ и $\mathcal{A} \models \psi^S(\bar{b})$. Опять рассмотрим:

- ▶ C — множество всех смежных классов по B^* во множестве $\{y : \mathcal{A} \models \varphi_0(\bar{b}, y)\}$;
- ▶ A_i , $1 \leq i \leq n$, — множество всех смежных классов по B^* в $\{y : \mathcal{A} \models \varphi_0(\bar{b}, y) \wedge \varphi_i(\bar{b}, y)\}$.

Из $(1:\Leftarrow)$ следует, что $\mathcal{A} \models \varphi(\bar{b})$.

$$V = \left\{ S : S \subseteq P(\{1, 2, \dots, n\}), \sum_{F \in S} (-1)^{|F|} \cdot n(F) = 0 \right\}.$$

Итак, получили, что

$$\mathcal{A} \models \varphi(\bar{x}) \leftrightarrow \bigvee_{S \in V} \psi^S(\bar{x}).$$

В свою очередь, формула $\bigvee_S \psi^S$ эквивалентна $\varphi^*(\bar{x})$ — булевой комбинации п.п.ф.

Напомним, что B_i — это подгруппа в $\mathcal{A}$, определяемая п.п.ф. $\varphi_i(\vec{0}, y)$.

Для алгоритмического построения формулы φ^* достаточно уметь:

1. проверять, верно ли, что $[B_0 : B_i] > n!$;
2. находить натуральные числа $n(F) = [B_0 \cap \bigcap_{i \in F} B_i : \bigcap_{0 \leq i \leq n} B_i]$.

Это можно делать эффективно, если проблема элементарных индексов разрешима. □

Разрешимость элементарных теорий
для групп $(\mathbb{Z}, +, -, 0)$ и $(\mathbb{Q}, +, -, 0)$.

Как проверять позитивно примитивные формулы

Через T_{AG} обозначаем теорию абелевых групп.

Предложение Б

Любая позитивно примитивная формула $\varphi(x_1, \dots, x_n)$ сигнатуры σ_{AG} эквивалентна относительно T_{AG} конечной конъюнкции формул вида

$$\exists y \left(\sum_{i=1}^n m_i x_i = p^k y \right) \text{ и } \sum_{i=1}^n m_i x_i = 0,$$

где $m_i \in \mathbb{Z}$, $k \in \omega$ и p — простое число. При этом такая конъюнкция находится эффективно.

Следствия предложения Б

Напомним, что в проблеме элементарных индексов нужно проверять формулы вида $[\varphi : \psi] \geq n$, где $\varphi(x), \psi(x)$ — п.п.ф.

В T_{AG} любая п.п.ф. $\varphi(x)$ эквивалентна конъюнкции формул вида:

$$\exists y (tx = p^k y) \text{ и } tx = 0.$$

Следствие Б.1

Теория $Th(\mathbb{Q}, +, -, 0)$ разрешима.

Доказательство. В группе $(\mathbb{Q}, +, -, 0)$ формула вида $\exists y (tx = p^k y)$ выделяет всю группу, а формула вида $tx = 0$ (при $t \neq 0$) выделяет нулевую подгруппу.

Следовательно, в $(\mathbb{Q}, +, -, 0)$ разрешима проблема элементарных индексов. □

Следствия предложения Б

Следствие Б.2

Теория $Th(\mathbb{Z}, +, -, 0)$ разрешима.

Доказательство. Обозначим группу $(\mathbb{Z}, +, -, 0)$ через $\mathcal{Z}$.

Пусть $k, m > 0$. В теории $Th(\mathcal{Z})$ выполнено:

(a) Формула $\exists y(mx = ky)$ эквивалентна

$$\exists y \left(x = \frac{k}{\text{НОД}(k, m)} \cdot y \right).$$

Формула $\exists y_1(x = ky_1) \wedge \exists y_2(x = my_2)$ эквивалентна

$$\exists y(x = \text{НОК}(k, m) \cdot y).$$

(b) Пусть $\theta_k(x) := \exists y(x = ky)$. Тогда θ_k выделяет подгруппу $k\mathcal{Z}$ и

$$[\theta_k : \theta_m, \mathcal{Z}] = \frac{m}{\text{НОД}(k, m)}.$$

Отсюда можно получить, что группа $\mathcal{Z}$ имеет разрешимую проблему элементарных индексов. □

Доказательство предложения Б

$$\text{П.п.ф. } \varphi(x_1, \dots, x_m) = \exists y_1 \dots \exists y_n \theta(x_1, \dots, x_m, y_1, \dots, y_n)$$

можно представить в виде пары целочисленных матриц (N, M) :

- ▶ N имеет размер $r \times n$, M имеет размер $r \times m$, где r — это число конъюнктов в бескванторной формуле θ ;
- ▶ $\varphi \equiv \exists \vec{y} (N \cdot \vec{y} = M \cdot \vec{x})$, где $\vec{y}$ и $\vec{x}$ — это вектор-столбцы переменных.

Будем считать, что (N, M) — это матрица размера $r \times (n + m)$.

(1) Допустимые операции, сохраняющие эквивалентность формул относительно T_{AG} :

- ▶ перестановка строк;
- ▶ умножение i -ой строки на целое $k \neq 0$;
- ▶ перестановка столбцов в матрице N (соответствует перестановке переменных $y_\ell \mapsto y_{\sigma(\ell)}$);
- ▶ прибавление к i -ой строке j -ой строки, умноженной на целое k .

Формула $\varphi \equiv \exists \vec{y}(N \cdot \vec{y} = M \cdot \vec{x})$, при этом (N, M) — это матрица размера $r \times (n + m)$.

Ещё одна допустимая операция: *внутри матрицы* N прибавить к i -ому столбцу j -ый, умноженный на целое k . Почему это так?

Пример:

$$\begin{cases} b_{11}y_1 + b_{12}y_2 = a_{11}x_1, \\ b_{21}y_1 + b_{22}y_2 = a_{22}x_2 \end{cases} \Leftrightarrow \begin{cases} b_{11}(y_1 - ky_2) + (b_{12} + kb_{11})y_2 = a_{11}x_1, \\ b_{21}(y_1 - ky_2) + (b_{22} + kb_{21})y_2 = a_{22}x_2. \end{cases}$$

(2) Используя допустимые операции, можно преобразовать матрицу (N, M) к матрице (N^*, M^*) , где

$$N^* = \begin{pmatrix} D & O_{11} \\ O_{21} & O_{22} \end{pmatrix}, \text{ где } D \text{ — диагональная, а } O_{ij} \text{ — нулевые.}$$

(Возможно, каких-то из блоков D, O_{ij} в матрице N^* нет).

Теперь формула, соответствующая (N^*, M^*) , эквивалентна конъюнкции формул вида

$$\exists y \left(\sum_{i=1}^m a_i x_i = \ell y \right) \text{ и } \sum_{i=1}^m a_i x_i = 0, \text{ где } \ell > 0.$$

(3) Рассмотрим формулу

$$\psi(\bar{x}) = \exists y \left(\sum_{i=1}^m a_i x_i = \ell y \right), \text{ где } \ell > 0.$$

Если $\ell = 1$, то ψ тождественно истинна.

Пусть теперь $\ell = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_t^{k_t}$ — это разложение ℓ на простые множители. Тогда формула ψ будет эквивалентна в T_{AG} конъюнкции формул

$$\exists y \left(\sum_{i=1}^m a_i x_i = p_j^{k_j} y \right), \text{ где } 1 \leq j \leq t. \quad (2)$$

В самом деле, пусть y_j — это решение (2).

Рассмотрим числа $u_j = \ell / p_j^{k_j}$. Так как $\text{НОД}(u_1, \dots, u_t) = 1$, существуют целые числа c_j , такие что $\sum_{j=1}^t c_j u_j = 1$. Тогда для $y = \sum_{j=1}^t c_j y_j$ получаем:

$$\begin{aligned} \ell y &= p_1^{k_1} p_2^{k_2} \dots p_t^{k_t} \cdot \sum_{j=1}^t c_j y_j = \sum_{j=1}^t c_j u_j p_j^{k_j} y_j = \\ &= \left(\sum_{j=1}^t c_j u_j \right) \cdot \left(\sum_{i=1}^m a_i x_i \right) = \sum_{i=1}^m a_i x_i. \quad \square \end{aligned}$$

Инварианты Шмелевой.

Определения инвариантов Шмелевой

Пусть G — абелева группа; $k \geq 1$; $a \in G$. Введём обозначения для следующих подгрупп:

$$kG = \{kx : x \in G\}, \quad G[k] = \{x \in G : kx = 0\}.$$

Через p и q обозначаем простые числа.

Через $\mathbb{Z}(k)$ обозначаем циклическую группу порядка k . Запись $k \mid a$ означает, что $\exists y(ky = a)$.

Определение. Подгруппа $H \leq G$ называется p -сервантной подгруппой в G , если для любых $a \in H$ и $k \in \omega$ выполнено:

$$H \models (p^k \mid a) \Leftrightarrow G \models (p^k \mid a).$$

Определение Sz.1

Для $n, k \in \omega$ предложение $A_{p,n,k}$ говорит о том, что «группа G имеет p -сервантную подгруппу вида $\bigoplus_{1 \leq i \leq k} \mathbb{Z}(p^n)$ »: другими словами, существует подгруппа $H \leq G$, изоморфная $\bigoplus_{1 \leq i \leq k} \mathbb{Z}(p^n)$ и такая что её элементы порядка p^ℓ (где $1 \leq \ell \leq n$) не делятся на $p^{n-\ell+1}$ в группе G .

$$\alpha_{p,n}(G) = \sup\{k \in \omega : G \models A_{p,n,k}\}.$$

[Условие « $\alpha_{p,n}(G) \geq k$ » определимо предложением сигнатуры σ_{AG} .]

Определения инвариантов Шмелевой

Определение Sz.2

Для $n, k \in \omega$ предложение $B_{p,n,k}$ говорит о том, что «группа G имеет подгруппу, изоморфную $\bigoplus_{1 \leq i \leq k} \mathbb{Z}(p^n)$ ».

$$\beta_p(G) = \inf\{\sup\{k \in \omega : G \models B_{p,n,k}\} : n \in \omega\}.$$

Замечание. Если $\beta_p(G) < \beta_p(H)$, то $G \neq H$.

(1) Для $\beta_p(H) = \omega$ замечание очевидно.

(2) Пусть $\beta_p(H) < \omega$ и $\beta_p(G)$ достигается на n_G .

Из-за выбора $\beta_p(H)$ группа H содержит копию $\bigoplus_{1 \leq i \leq \beta_p(H)} \mathbb{Z}(p^n)$ для каждого $n \geq 1$. В частности, в H есть подгруппа вида $\bigoplus_{1 \leq i \leq \beta_p(G)+1} \mathbb{Z}(p^{n_G})$, которой нет в G .

Формула $C'_{n,p,k}(x_1, \dots, x_k)$ говорит следующее: «если рассмотреть соответствующие образы $x'_1, \dots, x'_k$ в фактор-группе $\overline{G} = G/G[p^n]$, то смежные классы $p\overline{G} + x'_1, \dots, p\overline{G} + x'_k$ линейно независимы в фактор-группе $\overline{G}/p\overline{G}$ ». Другими словами, не существует нетривиальной линейной комбинации

$$v = \sum_{i=1}^k a_i x_i \text{ с коэффициентами } a_i \in \mathbb{Z}(p),$$

такой что для некоторого y порядок элемента $(v - py)$ делит p^n .

$$C_{n,p,0} = \exists x(x = x).$$

Определение Sz.3

Для $n, k \in \omega$ зададим $C_{n,p,k} = \exists x_1 \dots \exists x_k C'_{n,p,k}(x_1, \dots, x_k)$.

$$\gamma_p(G) = \inf\{\sup\{k \in \omega : G \models C_{p,n,k}\} : n \in \omega\}.$$

Замечание. Если $\gamma_p(G) < \gamma_p(H)$, то $G \not\equiv H$.

Определение Sz.4

Пусть $\varepsilon(G) \in \{0, 1\}$ и

$$\varepsilon(G) = 0 \Leftrightarrow kG = 0 \text{ для некоторого } k \geq 1,$$

т.е. порядок всех элементов группы G ограничен.

Элементарная классификация абелевых групп

Через $Sz(G) = Sz(H)$ будем обозначать, что группы G и H имеют одинаковые инварианты Шмелевой.

Теорема С

Для абелевых групп G и H следующие условия эквивалентны:

- (i) G и H имеют одинаковые проблемы элементарных индексов, т.е. для любых позитивно примитивных формул $\varphi(x), \psi(x)$ выполнено $[\varphi : \psi, G] = [\varphi : \psi, H]$;
- (ii) G и H элементарно эквивалентны;
- (iii) $Sz(G) = Sz(H)$.

Доказательство. (i) $\Rightarrow$ (ii). Следствие предложения А.

(ii) $\Rightarrow$ (iii). Следует из определений инвариантов Шмелевой.

Скетч доказательства (iii) $\Rightarrow$ (i)

По теореме Лёвенгейма–Скулема можно считать, что рассматриваемые группы G и H не более чем счётны.

Предварительный этап. Если $\varepsilon(G) = 0$, то порядки всех элементов G ограничены. Тогда по теореме Прюфера группа G изоморфна не более чем счётной сумме конечных циклических групп вида $\mathbb{Z}(p^n)$ для конечного числа вариантов p и n .

Инвариант $\alpha_{p,n}(G)$ “давал” максимальное k , для которого группа G имеет p -сервантную подгруппу вида $\bigoplus_{1 \leq i \leq k} \mathbb{Z}(p^n)$.

Из того, что $Sz(G) = Sz(H)$, получаем, что $G \cong H$.

Значит, далее можно считать, что $\varepsilon(G) = 1$.

По предложению В каждая п.п.ф. $\varphi(x)$ эквивалентна конъюнкции формул вида $\exists y(tx = p^k y)$ и $tx = 0$.

«Упростим» формулу $\xi(x) = \exists y(tx = p^k y)$. Пусть $m = p^\ell \cdot m'$, где m' не делится на p . Если $\ell \geq k$, то формула ξ тождественно истинна.

Пусть $\ell < k$. Выберем целые числа u, v , такие что $um + vp^k = p^\ell$. Тогда

$$tx = p^k y \Rightarrow p^\ell x = (um)x + (vp^k)x = p^k(uy + vx).$$

Значит, формула $\xi(x)$ эквивалентна формуле

$$\exists y(p^\ell x = p^k y), \text{ где } \ell < k. \quad (3)$$

Определение

Формулы (3) будем называть *p-базисными формулами второго рода*, а формулы $tx = 0$ — *базисными формулами первого рода*.

Пусть $\varphi(x), \psi(x)$ — п.п.ф. Нужно доказать, что $[\varphi : \psi, G] = [\varphi : \psi, H]$.

- ▶ Так как для произвольных $A_1, A_2, A_3 \leq G$ выполнено $[A_1 : (A_2 \cap A_3)] = [A_1 : A_2] \cdot [(A_1 \cap A_2) : A_3]$, можно считать, что формула $\psi(x)$ уже является базисной.
- ▶ Так как $[(\varphi(G) + \psi(G)) : \psi(G)] = [\varphi(G) : \psi(G)]$ и группу $\varphi(G) + \psi(G)$ можно определить п.п.ф. $\theta(x)$ (при этом формула θ не зависит от выбора группы G), можно считать, что $\psi(G) \subseteq \varphi(G)$.

Приведём доказательство только для случая, когда $\psi(x)$ является p -базисной формулой второго рода: $\exists y(p^\ell x = p^k y)$, $\ell < k$.

p -базисные подгруппы

Определение

Говорят, что подгруппа A группы G является p -базисной для G , если:

- ▶ A есть прямая сумма циклических p -групп и групп, изоморфных $(\mathbb{Z}, +, -, 0)$;
- ▶ A есть p -сервантная подгруппа G ;
- ▶ фактор-группа G/A p -делима, т.е. $(p \mid x)$ для каждого $x \in G/A$.

Для любой G и любого p существует p -базисная подгруппа для G .

Лемма 5

Пусть A — это p -базисная подгруппа группы G .

(а) $\alpha_{p,n}(A) = \alpha_{p,n}(G)$ и $\gamma_p(A) = \gamma_p(G)$.

(б) Пусть $\varphi(x)$ — п.п.ф., $\psi(x)$ — p -базисная формула второго рода. Тогда $[\varphi : \psi, A] = [\varphi : \psi, G]$.