АЛГЕБРЫ ИНВАРИАНТОВ И 14-Я ПРОБЛЕМА ГИЛЬБЕРТА

Летняя школа "Современная математика", Дубна, 19-25 июля 2007 года

Занятие 1. Проблемы конечности в алгебре

На этом занятии мы кратко напомним определения основных алгебраических структур (группа, коммутативная группа, поле, алгебра, а также идеал), и обсудим понятие конечной порожденности для каждой из них.

I. Группы. Множество G с бинарной операцией $\circ$, $(g_1, g_2) \to g_1 \circ g_2$ называется *группой*, если выполнены следующие условия:

• *ассоциативность*: $(g_1 \circ g_2) \circ g_3 = g_1 \cdot (g_2 \circ g_3)$ для любых $g_1, g_2, g_3 \in G$;

• *нейтральный элемент*: существует элемент $e \in G$ такой, что $e \circ g = g \circ e = g$ для любого $g \in G$;

• *обратный элемент*: для любого $g \in G$ существует $g^{-1} \in G$ такой, что $g \circ g^{-1} = g^{-1} \circ g = e$.

Примеры. 1) $(\mathbb{R}, +) \Rightarrow e = 0$; если $g = a$, то $g^{-1} = -a$.

2) $\mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \times) \Rightarrow e = 1$; если $g = a$, то $g^{-1} = \frac{1}{a}$.

3) Группа перестановок $S_n = \left\{ \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix} \right\}$. Это конечная группа, состоящая из $n!$ элементов. Нейтральным элементом здесь является перестановка $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$, а обратным к элементу $\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}$ – элемент $\tau^{-1} = \begin{pmatrix} \tau(1) & \tau(2) & \dots & \tau(n) \\ 1 & 2 & \dots & n \end{pmatrix}$ с переупорядоченными столбцами.

4) Группа матриц $\mathrm{GL}_n(\mathbb{R})$ размера $n \times n$ с вещественными элементами и отличным от нуля определителем относительно операции умножения матриц.

Определение 1. Группа G называется *конечнопорожденной*, если в ней найдутся элементы $g_1, \dots, g_k$ такие, что каждый элемент $g \in G$ можно представить в виде $g = g_{i_1}^{\pm 1} g_{i_2}^{\pm 1} \dots g_{i_s}^{\pm 1}$. Элементы $g_1, \dots, g_k$ называются *порождающими* элементами группы G, и сам факт порождения обозначается как $G = \langle g_1, \dots, g_k \rangle$.

Замечание 1. 1) Любая конечная группа конечно порождена.

2) Каждая конечнопорожденная группа не более чем счетна. В частности, группы $(\mathbb{R}, +)$, $\mathbb{R}^\times$ и $\mathrm{GL}_n(\mathbb{R})$ конечнопорожденными не являются.

Вопрос. Пусть H – подгруппа конечнопорожденной группы G. Верно ли, что H является конечнопорожденной группой ?

Ответ. Нет, см. задачу 1.

Определение 2. Группа G называется *коммутативной*, если $g_1 \circ g_2 = g_2 \circ g_1$ для любых $g_1, g_2 \in G$.

Теорема 1. *Подгруппа конечнопорожденной коммутативной группы конечно порождена.*

Пример 1. Рассмотрим группу $\mathbb{Z}^2 = \{(a_1, a_2)\}$ пар целых чисел с операцией покомпонентного сложения. Эта группа порождается элементами $(1,0)$ и $(0,1)$, поскольку $(a_1, a_2) = a_1(1,0) + a_2(0,1)$. Подгруппа H этой группы, состоящая из пар (a_1, a_2), для которых $a_1 + a_2$ делится на 3, порождается парами $(3,0), (2,1), (1,2), (0,3)$. Более того, уже элементы $(2,1)$ и $(1,2)$ порождают H, поскольку $(3,0) = 2(2,1) - (1,2)$, $(0,3) = 2(1,2) - (2,1)$.

II. Поля. Напомним, что множество $\mathbb{K}$ с двумя бинарными операциями $+$ и $\cdot$ называется *полем*, если $(\mathbb{K}, +)$ – коммутативная группа с нейтральным элементом $e = 0$, $\mathbb{K}^\times := (\mathbb{K}\setminus\{0\}, \cdot)$ – коммутативная группа с нейтральным элементом $e = 1$, и две операции связаны законом дистрибутивности: $a(b + c) = ab + ac$ для любых $a, b, c \in \mathbb{K}$.

Пример 2. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.

Определение 3. Поле $\mathbb{K}$ называется *конечно порожденным*, если найдутся $a_1, \dots, a_k \in \mathbb{K}$ такие, что любой элемент поля $\mathbb{K}$ выражается через $a_1, \dots, a_k$ посредством операций $\pm, \cdot$ и $a \to a^{-1}$.

Пример 3. Поле $\mathbb{Q}$ порождается элементом 1.

Пример 4. Пусть $x_1, \dots, x_n$ – формальные переменные. Тогда поле, порожденное числом 1 и переменными $x_1, \dots, x_n$, называется полем *рациональных дробей*, и состоит из дробей

$$\frac{f(x_1, \dots, x_n)}{h(x_1, \dots, x_n)},$$

где $f(x_1, \dots, x_n)$ и $h(x_1, \dots, x_n)$ – многочлены с рациональными коэффициентами, и многочлен h отличен от нулевого многочлена.

Теорема 2. *Подполе конечнопорожденного поля конечно порождено.*

III. Алгебра многочленов $\mathbb{K}[x_1, \dots, x_n]$. Пусть $\mathbb{K}$ – некоторое поле (можно считать, что $\mathbb{K} = \mathbb{Q}$ или $\mathbb{R}$), и $f(x_1, \dots, x_n) = \sum \alpha_{i_1,\dots,i_n} x_1^{i_1} \dots x_n^{i_n}$, $\alpha_{i_1,\dots,i_n} \in \mathbb{K}$ – многочлен от переменных $x_1, \dots, x_n$. Многочлены можно

- складывать и вычитать;
- умножать;
- умножать на элементы поля $\mathbb{K}$.

В этом случае говорят, что $\mathbb{K}[x_1, \dots, x_n]$ – алгебра над полем $\mathbb{K}$. Ясно, что эта алгебра порождена элементами $x_1, \dots, x_n$.

Вопрос. Верно ли, что любая подалгебра в $\mathbb{K}[x_1, \dots, x_n]$ конечно порождена ?

Пример 5. Пусть $n = 2$ и A – множество многочленов, не содержащих членов, зависящих только от x_2. Несложно проверить, что A – подалгебра в $\mathbb{K}[x_1, \dots, x_n]$. Предположим, что она порождается многочленами $f_1, \dots, f_k$. Каждый f_l имеет вид $f_l(x_1, x_2) = \sum \alpha_{ij} x_1^i x_2^j$. Вычислим $M := \max_{l,i,j} \frac{j}{i}$ (если положить, что для члена $1 = x_1^0 x_2^0$ отношение $\frac{j}{i}$ равно 1, указанная величина будет корректно определена). Покажем, что одночлен $x_1 x_2^{[M]+1} \in A$, где $[M]$ – целая часть числа M, нельзя выразить через элементы $f_1, \dots, f_k$. В самом деле, $(x_1^{i_1} x_2^{j_1})(x_1^{i_2} x_2^{j_2}) = x_1^{i_1+i_2} x_2^{j_1+j_2}$, и если $\frac{j_1}{i_1} \le \frac{j_2}{i_2}$, то $\frac{j_1}{i_1} \le \frac{j_1+j_2}{i_1+i_2} \le \frac{j_2}{i_2}$, откуда для любого члена $x_1^i x_2^j$ многочлена, выражаемого через $f_1, \dots, f_k$, имеем $\frac{j}{i} \le M$. Итак, мы показали, что подалгебра A не является конечнопорожденной.

Пример 6. Рассмотрим подалгебру $B \subset \mathbb{K}[x_1, x_2]$, состоящую из многочленов, каждый член $x_1^i x_2^j$ которых удовлетворяет условию $j < \sqrt{2}i$. Рассуждения, приведенные в предыдущем примере, позволяют показать, что B также не конечно порождена.

IV. Идеалы. Подмножество $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ называется *идеалом*, если

- $f_1 + f_2 \in I$ для всех $f_1, f_2 \in I$;
- $ff_1 \in I$ для всех $f \in \mathbb{K}[x_1, \ldots, x_n]$ и $f_1 \in I$.

Пример 7. Пусть $C \subseteq \mathbb{K}[x_1, \ldots, x_n]$ – произвольное подмножество. Тогда $I(C) := \{h_1 c_1 + \cdots + h_s c_s : h_i \in \mathbb{K}[x_1, \ldots, x_n], c_i \in C, s \in \mathbb{N}\}$ является наименьшим идеалом в $\mathbb{K}[x_1, \ldots, x_n]$, содержащим подмножество C. Он называется идеалом, *порожденным* подмножеством C. В частности, идеал $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ называется *конечнопорожденным*, если он может быть порожден конечным подмножеством.

Пример 8. Множество многочленов $\{f(x_1, \ldots, x_n) : f(0, \ldots, 0) = 0\}$ является идеалом, порожденным элементами $x_1, \ldots, x_n$.

Теорема Гильберта о базисе. Каждые идеал $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ конечно порожден.

Стоит отметить, что в отличие от случаев $I-III$, идеал не является самостоятельной алгебраической структурой, это подструктура в алгебре $\mathbb{K}[x_1, \ldots, x_n]$.