1 Рациональная параметризация квадрик

В этом разделе и далее задачи, помеченные Симпсонами представляют первостепенную важность, т. е. их нужно решать в первую очередь.

 Выпишите все пифагоровы тройки (a, b, c), такие, что $0 < a < b < c < 100$.

 Решите следующие уравнения в целых числах:

a. $x^2 + 2y^2 = 3z^2$,

b. $x^2 - 15y^2 = z^2$,

c. $x^2 - yz = 9z^2$,

d. $x^2 + 3y^2 = 5z^2$.

2 Группы (продолжение)

Группой G называется множество G с заданной на нём операцией «умножения» $: G \times G \to G$, удовлетворяющей следующим аксиомам:

I. Существует нейтральный элемент 1, такой, что

$$1 \cdot g = g \cdot 1 = g, \ \forall g \in G,$$

II. Для любого элемента группы существует обратный, т. е.

$$\forall g \in G \ \exists g^{-1} \in G \ : \ g \cdot g^{-1} = g^{-1} \cdot g = 1,$$

III. Справедлива ассоциатоивность:

$$a(bc) = (ab)c.$$

1. Докажите, что в группе единичный элемент единственен. Докажите, что в любой группе обратный к данному элемент единственен.

2. Докажите, что $(ab)^{-1} = b^{-1}a^{-1}$, а также обобщение данного равенства.

Рассмотрим множество перестановок S_n, состоящее из наборов (перестановок) $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma_1 & \sigma_2 & \sigma_3 & \dots & \sigma_n \end{pmatrix}$, в которых σ_i — попарно различные целые числа от 1 до n. Перестановка показывает, как переставлены числа от 1 до n, в верхнем ряду указаны порядковые номера, а в нижнем — соответствующие числа на этих позициях.

Две перестановки $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$ и $\tau = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \tau(1) & \tau(2) & \tau(3) & \dots & \tau(n) \end{pmatrix}$ можно перемножить и получить новую $\omega = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \omega(1) & \omega(2) & \omega(3) & \dots & \omega(n) \end{pmatrix}$. Делается это так. Смотрим, что стоит на первом месте у первой перестановки σ — это, ясное дело, число $\sigma(1)$, теперь находим столбик под номером $\sigma(1)$ у второй перестановки и смотрим, какое число внизу — это $\tau(\sigma(1))$ и записываем в перестановке ω под числом 1 этот элемент $\tau(\sigma(1))$. Теперь смотрим, что стоит на втором месте у первой подстановки и т. д. На k-ом шаге смотрим число под номером k у первой подстановки, находим столбик номер $\sigma(k)$ и берём нижнее число $\tau(\sigma(k))$ и записываем в ω на k-ой позиции число $\tau(\sigma(k))$ и т. д.

Рассмотрим пример перемножения подстановок:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

В данном примере 1 перешла в 2 под действием первой перестановки, затем под действием второй 2 перешла в 2, значит, 1 перешла в 2. Дальше $2 \to 3 \to 3 \Rightarrow 2 \to 3$, $3 \to 5 \to 1 \Rightarrow 3 \to 1$, $4 \to 1 \to 5 \Rightarrow 4 \to 5$ и, наконец, $5 \to 4 \to 4 \Rightarrow 5 \to 4$. И мы получили то, что написано справа.


Докажите, что так введённая операция превращает множество S_n в группу, т. е. проверьте выполнение аксиом группы: что является нейтральным элементом, обоснуйте ассоциативность и покажите, как обращать подстановки.

Группа называется *абелевой* (или *коммутативной*), если в ней для любых двух элементов $ab = ba$, т. е. a и b *коммутируют*.

Пример. Все известные вам из школы числовые группы $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ абелевы относительно операции сложения и операции умножения (в этом случае из данных множеств нужно выкинуть 0).


Абелева ли группа S_1? а S_2? а S_3? Что можно сказать про остальные S_n?

Т. е. группа перестановок доставляет первый пример неабелевой группы.

3. Какие из данных групп являются абелевыми: группа симметрий кдварата (она порождена отражениями относительно диагоналей квадрата и отрожениями относительно прямых, проходящих через середины противоположных сторон), группа симметрий прямоугольника, группа симметрий ромба?


Пусть в группе G для любого элемента g выполнено: $g^2 = e$. Докажите, что G — абелева.

4. Докажите, что $a^m = a^{-m}$ для любого целого m и любого $g \in G$. Проверьте остальные свойства целой степени.

Циклическая группа — это группа, порождённая одним элементом, т. е. $G = \{..., g^{-2}, g^{-1}, g^0 = e, g, g^2, g^3, ...\}$.

Примеры: группа вычетов по модулю n: $\mathbb{Z}_n$ с операцией «$+$» — там образующей будет 1, группа целых чисел $\mathbb{Z}$ — там тоже образующая это 1. Первая группа конечная, а вторая — бесконечная.

5. Пусть G — конечная циклическая группа. Наименьшее неотрицательное n, для которого $a^n = e$ называется порядком элемента a. Докажите, что среди элементов $e, a, a^2, \ldots$ нет двух одинаковых. Докажите, что для любого целого m элемент $a^m = a^k$ для $0 \leqslant k < n$.

Очевидно, любая конечная циклическая группа — это $\mathbb{Z}_n$ для некоторого n. (Слово «это» заменяют в алгебре на «изоморфно»).

6. Докажите, что группа вращений правильного n–угольника — это $\mathbb{Z}_n$.

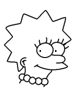
7. Пусть порядок элемента g равен n. Чему равен порядок элемента g^m, $m \in \mathbb{Z}$?

Пример. Рассмотрим множество числовых таблиц (*матриц*) 2×2:

$$\mathrm{GL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{R},\ ad - bc \neq 0 \right\}.$$

Введём на $\mathrm{GL}_2(\mathbb{R})$ умножение так:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$


Докажите, что относительно введённой операции $\mathrm{GL}_2(\mathbb{R})$ является группой.

P. S. Почему матрицы перемножаются таким странным образом? В этом есть глубокий смысл! Дело в том, что если вы захотите записать в базисе матрицу композиции двух линейных операторов, действующих в плоскости $\mathbb{R}^2$, то вам нужно будет по такому правилу перемножить соответствующие матрицы этих операторов.

P. P. S. Условие $ad - bc \neq 0$ означает, что соответствующий линейный оператор невырожден (для этого нужно необходимо и достаточно, чтобы определитель его матрицы был отличен от нуля).

P. P. P. S. На самом деле, можно рассматривать матрицы размера $n \times n$, им в этом случае будут отвечать некоторые операторы, действующие в n-мерном векторном пространстве $\mathbb{R}^n$.