ЛЕКЦИЯ 13

ПОЛУГРУППЫ
МОНОИДЫ
ГРУППЫ

ЦИКЛИЧЕСКИЕ ГРУППЫ

ИЗОМОРФИЗМЫ

ПОЛУГРУППЫ И МОНОИДЫ

Бинарная операция $*$ на множестве X называется *ассоциативной*, если

$$(a * b) * c = a * (b * c)$$

для всех $a, b, c \in X$; она называется *коммутативной*, если

$$a * b = b * a.$$

Те же названия присваиваются и соответствующей алгебраической структуре $(X, *)$.

Требования ассоциативности и коммутативности независимы.

В самом деле, операция $*$ на $\mathbb{Z}$, заданная правилом

$$n * m = -n - m,$$

очевидно, коммутативна, но

$$(1 * 2) * 3 = (-1 - 2) * 3 = -(-1 - 2) - 3 = 0 \neq 4 = 1 * (2 * 3),$$

так что условие ассоциативности не выполняется. Далее, на множестве $M_n(\mathbb{R})$ всех квадратных матриц порядка $n > 1$ определена операция умножения — ассоциативная, но некоммутативная.

Элемент $e \in X$ называется *единичным* (или нейтральным), относительно рассматриваемой бинарной операции $*$, если

$$e * x = x * e = x$$

для всех $x \in X$.

Если e' — еще один единичный элемент, то, как следует из определения,

$$e' = e' * e = e.$$

Значит, в алгебраической структуре $(X, *)$ может существовать не более одного единичного элемента.

Множество X с заданной на нем бинарной ассоциативной операцией называется *полугруппой*.

Полугруппу с единичным (нейтральным) элементом принято называть еще *моноидом*.

Как и для всякого множества, мощность моноида $M = (M, *)$ обозначается символом $|M|$.

В случае конечности числа содержащихся в нем элементов говорят о конечном моноиде порядка $|M|$.

Пример 1. Пусть X — множество, $M(X)$ — множество всех его преобразований (отображений в себя) с операцией композиции (суперпозиции).

Ясно, что $M(X)$ — моноид.

СТЕПЕНЬ ЭЛЕМЕНТА

Благодаря тому, что от расстановки скобок в произведении результат вычислений не меняется, в полугруппе можно ввести понятие степени элемента.

Именно, для любого натурального числа $n \in \mathbb{N}$ и любого элемента $x \in X$ полугруппы n-ая степень этого элемента — это произведение n экземпляров x.

Если мы имеем дело с моноидом, то можно ввести нулевую степень любого элемента: $x^0 = e$.

Так введеная степени удовлетворяет двум самым основным обычным свойствам степени:

(1) для любого $x \in X$ и любых $n, m \in \mathbb{N}$ выполнено

$$(x^n)^m = x^{nm}.$$

(2) для любого $x \in X$ и любых $n, m \in \mathbb{N}$ выполнено

$$x^{n+m} = x^n x^m.$$

При этом привычное для нас свойство

$$x^n y^n = (xy)^n$$

выполняется тогда и только тогда, когда x и y коммутируют в полугруппе.

Если моноид коммутативен, то его принято записывать в аддитивной записи: вместо $\cdot$ пишут $+$, вместо e — 0.

В аддитивной записи выражение x^n записывают иначе — как $x + x + \cdots + x = nx$.

ОБРАТИМЫЕ ЭЛЕМЕНТЫ

Элемент x моноида $(X, \cdot)$ называется *обратимым*, если существует элемент $y \in X$ такой, что $xy = yx = e$.

Элемент y называется *обратным* к x и обозначается x^{-1}.

Понятно, что $(x^{-1})^{-1} = x$. Понятие обратимого элемента моноида служит, очевидно, естественным обобщением понятия обратимой матрицы в моноиде $(M_n(\mathbb{R}), \cdot, E)$.

Так как

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = e$$

и, аналогично,

$$(y^{-1}x^{-1})(xy) = e,$$

то

$$(xy)^{-1} = y^{-1}x^{-1},$$

то есть множество всех обратимых элементов моноида замкнуто относительно умножения, то есть само является моноидом.

Мы можем говорить о подмоноиде обратимых элементов моноида $(X, \cdot)$.

ГРУППЫ

Группой называется моноид, все элементы которого обратимы.

Иначе говоря, группа — это множество X с бинарной операцией $\cdot$, для которой выполнены свойства ассоциативности, наличия нейтрального элемента e и для каждого элемента x существует обратный x^{-1}.

Если умножение в группе коммутативно, то она называется *абелевой группой*.

Приведем несколько самых основных примеров групп.

Пример 2. Множество $\mathbb{Z}$ целых чисел по сложению является абелевой группой.

Действительно, операция сложения целых чисел ассоциативна и коммутативна, при этом нейтральным элементом выступает ноль, а обратным к числу x — противоположное число $-x$.

Пример 3. Также группами являются множества всех рациональных $\mathbb{Q}$ и всех действительных $\mathbb{R}$ чисел по сложению.

Нейтральный элемент — также ноль.

Если вместо операции сложения рассматривать умножение, то надо брать не все рациональные или действительные числа, а их же без нуля: $\mathbb{Q}^* = (\mathbb{Q} \setminus \{0\}, \cdot)$ и $\mathbb{R}^* = (\mathbb{R} \setminus \{0\}, \cdot)$.

Тогда нейтральным элементом в обеих группах будет сложить единица 1, а обратными — обычные обратные элементы.

Пример 4. Предыдущие группы были абелевыми, но пример неабелевой группы нам всем тоже уже известен — это группа S_n всех перестановок порядка n.

Заметим, что внутри нее живет еще одна группа — группа A_n четных перестановок порядка n.

Пример 5. Еще очень хороший пример группы — это группа вычетов по модулю n.

Рассмотрим числа $\{0, 1, 2, \ldots, n-1\}$, а на них введем операцию сложения по модулю n:

$$a \oplus b := a + b \mod n.$$

Очевидно, что сложение по модулю ассоциативно и коммутативно. Нейтральным элементов является ноль, а обратным элементом для $a \in \{0, 1, 2, \ldots, n-1\}$ служит число $n - a$.

Таким образом, для каждого $n \in \mathbb{N}$ мы получаем абелеву группу из n элементов, будем обозначать ее через $\mathbb{Z}_n$.

Пример 6. Если рассмотреть алгебру матриц $M_n(\mathbb{R})$ и выбрать из нее все обратимые матрицы, то мы получим группу $\mathrm{GL}_n(\mathbb{R})$ обратимых матриц порядка n, также называемую общей линейной группой.

Если внутри группы $\mathrm{GL}_n(\mathbb{R})$ рассмотреть только матрицы с определителем 1, то такое множество матриц будет замкнуто относительно умножения и взятия обратных матриц, поэтому такое множество матриц также будет является группой, ее обозначают через $\mathrm{SL}_n(\mathbb{R})$, называется она специальной линейной группой.

Заметим, что в случае группы понятие степени элемента расширяется: можно вводить не только натуральные степени элементов и нулевую, но и вообще любые целые степени.

Именно, для $n \in \mathbb{Z}$ и для $a \in G$

$$a^n = \begin{cases} a \cdot a \times \cdots \times a \ (n \text{ раз}) \text{ при } n > 0; \\ e \text{ при } n = 0; \\ a^{-1} \cdot a^{-1} \times \cdots \times a^{-1} \ (|n| \text{ раз}) \text{ при } n < 0. \end{cases}$$

Легко проверить, что выполняются те же самые соотношения, что и для натуральных степеней в моноиде/полугруппе.

ЦИКЛИЧЕСКИЕ ГРУППЫ

Пусть G — мультипликативная группа (то есть с операцией умножения), a — ее фиксированный элемент.

Если любой элемент $g \in G$ можно записать как a^n для некоторого целого n, то говорят, что $G = \langle a \rangle$ — *циклическая группа* с образующим a (или циклическая группа, порожденная элементом a).

Аналогично циклическая группа определяется в аддитивном случае:

$$\langle a \rangle = \{na \mid n \in \mathbb{Z}\}.$$

Это, конечно, не означает, что все элементы a^n попарно различны.

Простейшим примером циклической группы служит аддитивная группа целых чисел $(\mathbb{Z}, +)$, которая порождена обычной единицей 1 или -1.

Примером циклической группы из n элементов служит недавно введенная группа вычетов $\mathbb{Z}_n$. Она тоже порождается единицей 1, хотя может порождаться и другими элементами, в некоторых случаях — вообще любым ненулевым элементом.

Пусть снова G — произвольная группа, a — ее произвольный элемент. Имеются две возможности:

(1) Все степени элемента a различны, то есть

$$m \neq n \Longrightarrow a^m \neq a^n.$$

В этом случае говорят, что элемент a имеет *бесконечный порядок.*

(2) Имеются совпадения $a^m = a^n$ при некоторых $m \neq n$. Если, например, $m > n$, то $a^{m-n} = e$, то есть существует положительная степень элемента $a \in G$, равная единичному элементу.

Пусть q — наименьший положительный показатель, для которого $a^q = e$.

Тогда говорят, что a — элемент конечного порядка q.

В конечной группе G все элементы, естественно, будут иметь конечный порядок.

Теорема 1. *Порядок любого элемента $a \in G$ равен порядку группы $\langle a \rangle$.*

Если a — элемент конечного порядка q, то $\langle a \rangle = \{e, a, a^2, \ldots, a^{q-1}\}$,

$$a^k = e \Longleftrightarrow k = lq, \quad l \in \mathbb{Z}.$$

Доказательство. В случае элемента бесконечного порядка доказывать нечего.

Если a — элемент порядка q, то по определению все элементы $e, a, a^2, \ldots, a^{q-1}$ различны.

Любая другая степень a^k совпадает с одним из этих элементов, то есть

$$\langle a \rangle = \{e, a, \ldots, a^{q-1}\}.$$

В самом деле, воспользовавшись алгоритмом деления целых чисел с остатком, запишем показатель k в виде

$$k = lq + r, \quad 0 \leqslant r < k,$$

после чего получим

$$a^k = (a^q)^l a^r = ea^r = a^r.$$

В частности,

$$a^k = e \Longrightarrow r = 0 \Longrightarrow k = lq.$$

□

ИЗОМОРФИЗМЫ

Рассмотрим сначала два примера.

Пример 7. Рассмотрим равносторонний треугольник ABC и рассмотрим все движения, которые переводят его самого в себя.

Понятно, что их шесть:

(1) Тождественное движение

(2) Поворот по часовой стрелке на 120°

(3) Поворот против часовой стрелки на 120°

(4)–(6) Отражения треугольника относительно медиан, проходящих через вершины A, B и C соответственно.

Понятно, что на этих движениях можно ввести операцию композиции, которая, конечно же, будет ассоциативна (как любая композиция). При этом существует тождественное движение, превращающее множество движений треугольника в моноид. Кроме того, для каждого движения существует обратное: надо просто перевести все точки в обратном направлении.

В нашем случае движения (1) и (4)–(6) будут обратны сами себе, а повороты — взаимно обратны.

Таким образом, множество движений треугольника ABC оказывается группой из шести элементов.

Теперь пронумеруем вершины треугольника (то есть теперь это будет не треугольник ABC, а треугольник 123) и заметим, что при каждом движении вершины обязательно переходят вершины. Кроме того, если известно, как отобразились в вершины, то движение полностью определено. Значит, можно отобразить каждое движение в перестановку трех вершин.

Введенная группа становится очень похожа на группу S_3.

Пример 8. Теперь рассмотрим две уже рассмотренных группы. Одна из них — $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.

Другая — введенная выше циклическая группа, порожденная элементом a порядка n, которая состоит из элементов $e, a, a^2, \ldots, a^{n-1}$.

Обозначим вторую группу через G.

Попробуем временно заменить элементы вида a^k на числа k (просто как бы заменим обозначения).

Заметим, что если мы перемножим два исходных элемента a^k и a^l, то получим элемент a^{k+l}, то есть при замене элементов их показателями эти самые показатели будут складываться, причем по модулю n.

Благодаря этому группа G отождествляется с группой $\mathbb{Z}_n$.

Два последних примера показывают, что иногда группы внешне выглядят и вводятся по-разному, но при этом по сути очень похожи, получаются друг из друга какими-то переобозначениями.

Эти примеры обобщает понятие изоморфизма.

Определение 1. Две группы G и G' с операциями $*$ и $\circ$ называются *изоморфными*, если существует отображение $f : G \to G'$ такое, что:

(1) $f(a * b) = f(a) \circ f(b)$ для всех $a, b \in G$;

(2) f биективно.

Данное отображение называется *изоморфизмом.*

Факт изоморфизма групп часто обозначается символом $G \cong G'$.

Отметим простейшие свойства изоморфизма.

(1) *Единица переходит в единицу.*

Действительно, если e — единица группы G, то

$$e * a = a * e = a,$$

и, значит,

$$f(e) \circ f(a) = f(a) \circ f(e) = f(a),$$

откуда следует, что

$$f(e) = e'$$

— единица группы G'.

В этом рассуждении использованы, хотя частично, об свойства изоморфизма.

Для первого свойства это очевидно, а свойство (2) обеспечивает сюръективность f, так что элементами $f(g)$ исчерпывается все группа G'.

(2) *Обратный элемент переходит в обратный элемент.*
Пусть $a \in G$, $f : G \to G'$ — изоморфизм групп.
Покажем, что $f(a^{-1}) = (f(a))^{-1}$.
Действительно,

$$a * a^{-1} = e \Longrightarrow f(a) \circ f(a^{-1}) = f(e) = e',$$

откуда получаем, что элементы $f(a)$ и $f(a^{-1})$ взаимно обратны.

(3) Обратное отображение $f^{-1} : G' \to G$ (существующее в силу биективности f) тоже является изоморфизмом.

Мы уже знаем, что обратное к биекции отображение тоже биективно.

Поэтому остается только проверить свойство (1).

Пусть $a', b' \in G'$. Тогда ввиду биективности f имеем

$$a' = f(a), \quad b' = f(b)$$

для каких-то $a, b \in G$.

Поскольку f — изоморфизм,

$$a' \circ b' = f(a) \circ f(b) = f(a * b).$$

Отсюда имеем

$$a * b = f^{-1}(a' \circ b'),$$

а так как в свою очередь

$$a = f^{-1}(a'), \quad b = f^{-1}(b'),$$

то

$$f^{-1}(a' \circ b') = f^{-1}(a') * f^{-1}(b').$$

(4) *Композиция изоморфизмов — изоморфизм.*

Действительно, если $f : G \to G'$ и $h : G' \to G''$ — изоморфизмы, то их композиция $hf : G \to G''$ является биекцией и для всех $a, b \in G$ выполнено

$$hf(a * b) = h(f(a * b)) = h(f(a) \circ f(b)) = \\ = h(f(a)) \cdot h(f(b)) = hf(a) \cdot hf(b),$$

что и требовалось.

Теорема 2. *Все циклические группы одного и того же порядка (в том числе и бесконечного) изоморфны.*

Доказательство. В самом деле, если $\langle g\rangle$ — бесконечная циклическая группа, то все степени g^k образующего g различны и мы получим изоморфизм

$$f : \langle g\rangle \to (\mathbb{Z}, +),$$

полагая

$$g^k \mapsto f(g^k) = k.$$

Биективность f очевидна, а свойство

$$f(g^m g^n) = f(g^n) + f(g^m)$$

вытекает из свойств степени.

Пусть теперь

$$G = \{e, g, \ldots, g^{q-1}\} \text{ и } G' = \{e', g', \ldots, (g')^{q-1}\}$$

— две циклические группы порядка q (для удобства не будем различать операции в G и G').

Определим биективное отображение

$$f : g^k \mapsto (g')^k, \quad k = 0, 1, \ldots, q-1.$$

Полагая $n+m = lq+r, 0 \leqslant r < q$, для любых $n, m = 0, 1, \ldots, q-1$, будем иметь

$$f(g^{n+m}) = f(g^r) = (g')^r = (g')^{n+m} = (g')^n (g')^m = f(g^n) f(g^m).$$

□