Лекция №4

20.09.24

6. Отношения порядка и упорядоченные множества

Определение и примеры

Упорядоченная пара $\mathbf{A} = (A, \leq)$, где A - непустое множество, называемое *носителем*, а $\leq$ - некоторое отношение порядка на носителе, называется *упорядоченным множеством*.

Примеры

1) $(\mathbb{R}, \leq)$ - множество действительных чисел с обычным отношением порядка («меньше или равно»), которое называется *естественным числовым порядком*.
2) $(2^M, \subseteq)$ - булеан некоторого (возможно, даже пустого) множества M с отношением включения.
3) Рассмотрим отношение делимости на множестве целых чисел: $x \mid y$ (x делит y).
   Это отношение рефлексивно (каждое число делит само себя) и транзитивно, так как $x \mid y, y \mid z \Rightarrow y = kx, z = my (k, m \in \mathbb{Z}) \Rightarrow z = mkx \Rightarrow x \mid z$.
   Но это отношение не антисимметрично, так как $x \mid y, y \mid x \Rightarrow x = \pm y$. То есть отношение делимости на множестве целых чисел есть только предпорядок. Если же ограничиться неотрицательными целыми числами, то отношение делимости становится порядком.
   Из этого примера видно также, что на одном и том же носителе можно определять разные отношения порядка и получать тем самым разные упорядоченные множества: на множестве $\mathbb{N}_0$ неотрицательных целых чисел можно задать естественный числовой порядок и отношение делимости; получим два разных упорядоченных множества: $(\mathbb{N}_0, \leq)$ и $(\mathbb{N}_0, |)$.

Отношения, связанные с исходным порядком

1) *Строгий порядок*: $x < y \rightleftharpoons (x \leq y) \& (x \neq y)$; это отношение иррефлексивно, антисимметрично и транзитивно.

2) *Двойственный порядок* – порядок, обратный исходному (легко показать, что отношение, обратное отношению порядка, также является отношением порядка).

3) *Индуцированный порядок*: если $\mathbf{A} = (A, \leq)$ упорядоченное множество, а $B \subseteq A$ - подмножество носителя, то можно определить отношение порядка на подмножестве B как ограничение исходного порядка на данное подмножество: $x \leq_B y \rightleftharpoons x \leq y; x, y \in B$. Этот порядок называют *порядком на подмножестве* B, *индуцированным исходным порядком на всем множестве* A. В сущности, это то же самое отношение порядка, но сравниваются только элементы выбранного подмножества. Для индуцированного порядка обычно используют то же обозначение, что и для исходного.

4) *Доминирование*: говорят, что *элемент* y *упорядоченного множества доминирует над элементом* x того же множества, если $x < y$ и не существует такого z, что $x < z < y$. Будем обозначать это так: $x \lhd y$. Например, для целых чисел можно написать $(\forall x)(x \lhd x+1)$. Но для естественного числового порядка на множестве рациональных (и, тем более, всех действительных) чисел отношение доминирования пусто, так как для любых таких двух чисел $p < q$ существует «промежуточное» число r такое, что $p < r < q$ (свойство плотности рациональной и действительной прямой). Доминирующий элемент – ближайший больший, и он не всегда существует.

5) *Несравнимость*: говорят, что *элементы* x *и* y *упорядоченного множества несравнимы*, если неверно, что $x \le y$, а также неверно и обратное: $y \le x$. Будем обозначать это так: $x \updownarrow y$.

Отношение порядка, в котором нет несравнимых элементов, называется *линейным*. Естественный числовой порядок линеен, а порядок, определяемый отношением включения (множеств) или определяемый делимостью, не является линейным.

Наименьший (наибольший) и минимальный (максимальный) элементы

Элемент $a \in A$ упорядоченного множества $\mathbf{A} = (A, \le)$ называется *наименьшим* (соответственно, *наибольшим*) элементом данного множества, если $(\forall x \in A)(a \le x)$ (соответственно, $(\forall x \in A)(a \ge x)$).

Такие элементы упорядоченного множества существуют не всегда.

Например, множество неотрицательных целых чисел имеет наименьший элемент (0), но не имеет наибольшего. Множество всех целых чисел не имеет ни наименьшего, ни наибольшего элемента.

Интервал на числовой прямой не имеет ни наименьшего, ни наибольшего элемента, а отрезок имеет и тот, и другой.

Имеет место следующая

Теорема. Если упорядоченное множество имеет наименьший (наибольший) элемент, то он единственный.

Доказательство. Пусть $a, a' \in A$ два наименьших элемента упорядоченного множества $\mathbf{A} = (A, \le)$. Тогда $a \le a'$, так как a наименьший, и $a' \le a$, так как a' наименьший. Отсюда, в силу антисимметричности отношения порядка, $a' = a$, что и означает единственность наименьшего элемента.

Единственность наибольшего элемента доказывается точно так же.

Можно заметить, что определение наибольшего элемента получается из определения наименьшего заменой обозначения исходного порядка ($\le$) обозначением двойственного (обратного) порядка ($\ge$). Как говорят, второе определение *двойственно* исходному (или «двойственным образом определяется»).

В теории упорядоченных множеств имеет место следующий принцип:

Принцип двойственности: 1) если в определении, касающемся упорядоченного множества, всюду заменить обозначение исходного порядка обозначением двойственного порядка и наоборот, то получим определение, которое называют двойственным к исходному; 2) любое утверждение, доказанное для упорядоченного множества, остается справедливым, если в нем произвести указанную выше взаимную замену.

Строгое доказательство второго утверждения дается в математической логике.

Понятно, что двойственное к двойственному есть исходное по той простой причине, что отношение, обратное к обратному, есть исходное.

Можно говорить, следовательно, о *взаимно двойственных* определениях (например, определения наименьшего и наибольшего элемента) или утверждениях (например, в записанной выше теореме).

От наименьшего (наибольшего) элемента следует отличать минимальный (максимальный) элемент.

Элемент $a \in A$ упорядоченного множества $\mathbf{A} = (A, \leq)$ называется *минимальным* (*максимальным*) элементом данного множества, если $(\forall x \in A)(a \leq x \vee a \updownarrow x)$ (соответственно, $(\forall x \in A)(a \geq x \vee a \updownarrow x)$).

Таким образом минимальный (максимальный) элемент либо меньше (больше) остальных, либо не сравним с ними.

И минимальных (максимальных) элементов может быть много (и даже бесконечно много).

Например, на множестве собственных (строгих) делителей числа 36 (то есть делителей, отличных от самого числа и единицы: 2, 3, 4, 6, ,9, 12, 18), упорядоченных отношением делимости, 2 и 3 будут минимальными, а 12 и 18 – максимальными элементами.
Далее, на множестве точек плоскости $\mathbb{R}^2$ определим отношение $(a,b) \leq (c,d) \rightleftharpoons (a \leq b, c \leq d)$.

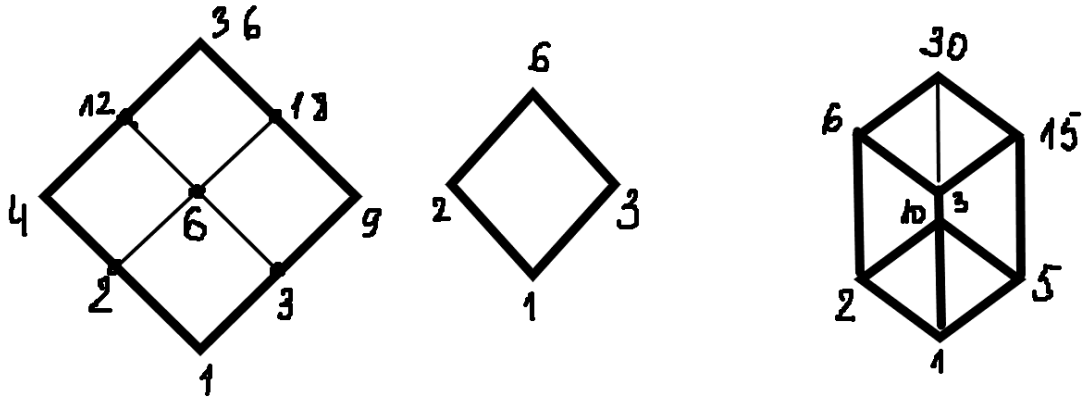
Легко проверить, что это отношение порядка, в котором точки сравниваются покоординатно: абсцисса первой точки не больше абсциссы второй и, соответственно, ордината первой точки не больше ординаты второй. Но тогда, например, точки (1, 2) и (2, 1) окажутся несравнимыми.

Теперь, если взять произвольную точку $M = (a,b)$ и провести через нее две перпендикулярные прямые, параллельные осям координат, то в пределах прямого угла, который левее и ниже точки будут все точки, меньшие данной, в пределах прямого угла, который правее и выше точки будут все точки, больше данной, а в пределах двух других вертикальных прямых углов (левее – выше и правее-ниже) – все точки, не сравнимые с данной.

Тогда для множества точек $B = \{(x,y) : x + y \leq 1\}$ (с индуцированным порядком), то есть для всех точек, расположенных не выше прямой $x + y = 1$, все точки на этой прямой будут максимальными элементами множества B (и не будет ни одного

наибольшего), а для множества $B_1 = \{(x, y) : x + y \geq 1\}$ точки этой же прямой будут минимальными элементами (и не будет ни одного наименьшего).

Диаграммы Хассе.



Верхние и нижние грани

Пусть снова $\mathbf{A} = (A, \leq)$ упорядоченное множество, а $B \subseteq A$ - подмножество носителя.

Элемент $a \in A$ называется *верхней (нижней) гранью подмножества* $B \subseteq A$, если $(\forall b \in B)(b \leq a)$ (соответственно, $(\forall b \in B)(b \geq a)$). Множество всех верхних граней подмножества $B \subseteq A$ называется *верхним конусом* этого подмножества и обозначается

B^{∇}. Двойственно определяется *нижний конус* как множество всех нижних граней. Обозначение: B^{Δ}.

Следует заметить, что подмножество может не иметь верхних, или нижних, граней, и даже ни тех и ни других. Например, рассмотренное выше множество точек плоскости, лежащих не выше (или не ниже) прямой $x + y = 1$. Такие множества можно назвать *неограниченными*. Ясно, что неограниченными будут множества всех действительных, рациональных и целых чисел (если не включать в них бесконечно удаленные точки $\pm\infty$).

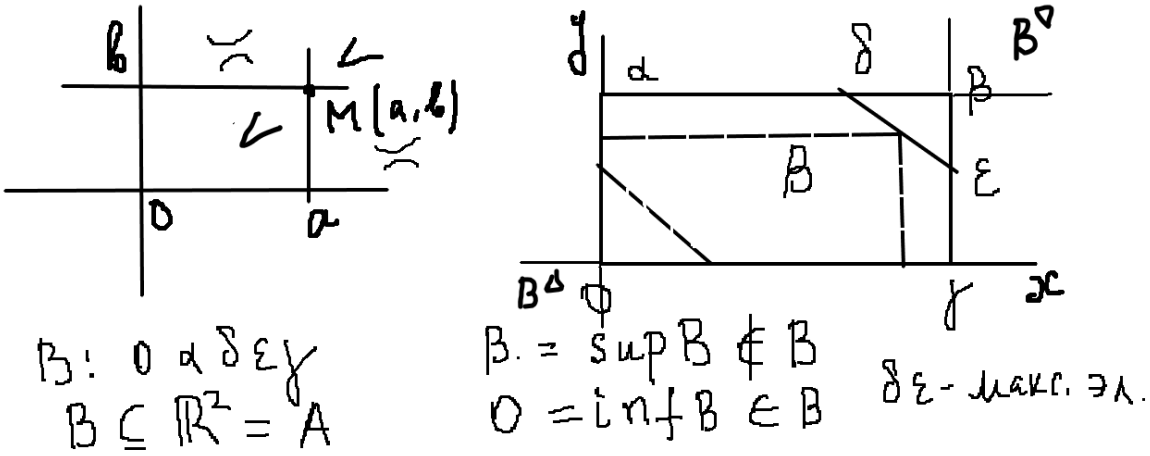
Если множество имеет хотя бы одну верхнюю (нижнюю) грань, оно называется *ограниченным сверху (снизу)*. Например, множество натуральных чисел ограничено снизу (и не ограничено сверху).

Точная верхняя (точная нижняя) грань

Если верхний конус ограниченного сверху подмножества $B \subseteq A$ имеет наименьший элемент, то он называется *точной верхней гранью* этого подмножества и обозначается $\sup B$ (supremum).

Двойственным образом определяется *точная нижняя грань* (как наибольший элемент нижнего конуса). Обозначение: $\inf B$ (infimum).

Поскольку наименьший (или наибольший) элемент множества существует не всегда, то и точные грани тоже не всегда существуют.



Нижний конус для B – все точки 3-го квадранта (включая начало координат), верхний конус – все точки четверть-плоскости с вершиной в точке β правее и выше.

Точная верхняя (нижняя) грань последовательности

Пусть дана некоторая последовательность $a_1, a_2, ..., a_n, ...$ элементов какого-то упорядоченного множества. Тогда ее точной верхней (нижней) гранью считается точная верхняя (нижняя) грань области значений этой последовательности как функции натуральной переменной.

Обозначение: $\sup a_n (\inf a_n)$.

Цепи и антицепи

Цепь в упорядоченном множестве – любое линейно упорядоченное подмножество. *Максимальная цепь* – цепь, максимальная по включению, то есть не являющаяся собственным подмножеством никакой другой цепи.

Например, на множестве точек плоскости с покоординтным порядком множество точек, лежащих на любой прямой с положительным тангенсом угла наклона, а также на любой прямой, параллельной какой-либо оси координат, образует максимальную цепь.

Антицепь в упорядоченном множестве – любое подмножество попарно не сравнимых элементов. *Максимальная антицепь* – антицепь, максимальная по включению, то есть не являющаяся собственным подмножеством никакой другой антицепи.

Например, на множестве точек плоскости с покоординтным порядком множество точек, лежащих на любой прямой с отрицательным тангенсом угла наклона, образует максимальную антицепь.

Заметим, что одноэлементное подмножество будет цепью и антицепью одновременно.

Понятно также, что в линейно упорядоченном множестве никаких антицепей, кроме одноэлементных, не может быть.

Лекция №5

25.09.24

7. Индуктивно упорядоченные множества. Теорема о неподвижной точке

Индуктивно упорядоченное множество

Упорядоченное множество $\mathbf{A} = (A, \leq)$ называется *индуктивно упорядоченным* (или *индуктивным упорядоченным*), если

1) оно имеет наименьший элемент

и

2) любая неубывающая последовательность его элементов имеет точную верхнюю грань.

В дальнейшем используется аббревиатура ИУМ.

Рассмотрим некоторые примеры

1) Отрезок числовой прямой с естественным числовым порядком: $([a,b], \leq)$. В данном случае наименьший элемент – число a (левая граница отрезка), а существование точной верхней грани у любой неубывающей последовательности вытекает из известной теоремы Вейерштрасса, согласно которой любая неубывающая и ограниченная сверху числовая последовательность имеет предел, который в данном случае и оказывается точной верхней гранью последовательности.
2) Множество всех подмножеств произвольного множества M отношением включения: $(2^M, \subseteq)$

Здесь наименьший элемент – пустое множество, а точная верхняя грань произвольной последовательности определяется как

$$\sup A_n = \bigcup_{n=0}^{\infty} A_n = \{x : (\exists n)(x \in A_n)\}^1.$$

Рассмотрим это подробнее. Здесь уместно и важно показать, как доказывается, что элемент упорядоченного множества является точной верхней гранью последовательности (или подмножества). Сначала доказывается, что это просто верхняя грань. В данном случае это легко усматривается из того, что если элемент $x \in A_n$ для некоторого n, то, просто

[1] О бесконечных объединениях и пересечениях см. Учебник, п. 1.5.

в силу определения бесконечного объединения множеств, $x \in \bigcup_{n=0}^{\infty} A_n$. Следовательно, это объединение есть верхняя грань последовательности.

Теперь пусть множество B является произвольной верхней гранью рассматриваемой последовательности, то есть для каждого $n \geq 0$ имеет место включение $A_n \subseteq B$. Тогда, если $x \in \bigcup_{n=0}^{\infty} A_n$, то для некоторого $n \geq 0$ $x \in A_n$, и, следовательно, $x \in B$, то есть $\bigcup_{n=0}^{\infty} A_n \subseteq B$, откуда следует, что данное объединение всех членов последовательности будет наименьшим по включению множеством, содержащем все члены последовательности, то есть будет точной верхней гранью последовательности.

Еще раз обратим внимание на то, что этот супремум определен для любой последовательности множеств, а не только для неубывающей.

3) Множество неотрицательных целых чисел с отношением делимости: $(\mathbb{N}_0, |)$, где по определению $a | b \rightleftharpoons b = ka, k \in \mathbb{N}_0$.

Любая конечная монотонно возрастающая последовательность имеет, очевидно, супремум в виде наибольшего (по делимости) числа этой последовательности.

Если же взять монотонно возрастающую бесконечную последовательность $a_0 | a_1 | ... | a_n | a_{n+1} | ...$, то единственное число, которое делится на все члены этой последовательности, будет равно нулю, то есть $\sup a_n = 0$. Отсюда же следует, что упорядоченное множество $(\mathbb{N}, |)$, носитель которого не содержит нуля, уже не будет ИУМ.

Наименьший элемент, очевидно, единица.

Этот пример несколько парадоксален, но поучителен.

Заметим, что в конечном упорядоченном множестве любая цепь имеет наибольший элемент, который будет ее точной верхней гранью. Поэтому, конечное упорядоченное множество будет индуктивным, если оно имеет наименьший элемент.

Докажем теперь некоторые утверждения об индуктивно упорядоченных множествах.

Лемма 1. Если у произвольной неубывающей последовательности элементов ИУМ отбросить любое конечное число начальных членов, то ее точная верхняя грань не изменится.

Доказательство. Пусть $\mathbf{A} = (A, \leq)$ - ИУМ и пусть $\{a_n\}_{n \geq 0}$ - неубывающая последовательность его элементов.

Для некоторого $k > 0$ рассмотрим подпоследовательность $\{a_n\}_{n \geq k > 0}$, убрав тем самым первые $k-1$ членов последовательности. Докажем, что $a \rightleftharpoons \sup_{n \geq 0} a_n = \sup_{n \geq k} a_n$. То, что элемент a является просто верхней гранью «усеченной» последовательности, очевидно. Допустим, что b есть верхняя грань подпоследовательности $\{a_n\}_{n \geq k > 0}$. Тогда для любого $n \geq k$ $a_n \leq b$, но поскольку последовательность $\{a_n\}_{n \geq 0}$ не убывает, то

$a_0 \le a_1 \le ... \le a_{k-1} \le a_k \le b$, то есть элемент b является верхней гранью всей последовательности $\{a_n\}_{n\ge 0}$, откуда $a \le b$ и $a = \sup_{n\ge k} a_n$.

Утверждение леммы аналогично известной теореме математического анализа, согласно которой предел сходящейся последовательности не изменится, если у последовательности отбросить произвольное число первых членов. Но никогда нельзя забывать, что понятия точной верхней грани неубывающей последовательности ИУМ и понятие предела числовой последовательности – совсем разные вещи.

Отображение $f : A \to B$ (произвольного) упорядоченного множества $\mathbf{A} = (A, \le)$ в упорядоченное множество $\mathbf{B} = (B, \preceq)$ называется монотонным, если $(\forall x, y \in A)(x \le y \Rightarrow f(x) \preceq f(y))$.

В условиях предыдущего определения, если множества являются индуктивно упорядоченными, то отображение $f : A \to B$ называется непрерывным, если для любой неубывающей последовательности $\{x_n\}_{n\ge 0}$ последовательность $\{f(x_n)\}_{n\ge 0}$ образов имеет точную верхнюю грань, причем $f(\sup x_n) = \sup f(x_n)$.

Заметим, что в этом определении априори не предполагается, что последовательность образов не убывает.

Теорема 1. Всякое непрерывное отображение одного ИУМ в другое монотонно.

Доказательство. Пусть $x \le y; x, y \in A$ (в условиях данных выше определений). Рассмотрим последовательность $x, y, y, ..., y, ...$, в которой все элементы, начиная со второго, равны одному и тому же y. Тогда $\sup\{f(x), f(y), f(y), ..., f(y), ...\} = \sup\{f(x), f(y)\} = f(\sup\{x, y\}) = f(y)$, в силу непрерывности отображения f, откуда $f(x) \preceq f(y)$, то есть отображение монотонно.

Отсюда и следует, что последовательность образов неубывающей последовательности тоже будет неубывающей (для непрерывного отображения).

Из теоремы 1 вытекает также, что понятия непрерывности отображений ИУМ и непрерывности в классическом анализе далеко не тождественны, хотя определенное сходство между этими типами непрерывности и есть.

Замечание. В конечном случае, как можно доказать, монотонность равносильна непрерывности, но в общем случае монотонное отображение может не быть непрерывным (см. Учебник, пример 1.19).

Основной, и важнейший для приложений, результат теории индуктивно упорядоченных множеств, есть теорема о наименьшей неподвижной точке:

Теорема 2. Всякое непрерывное отображение ИУМ в себя имеет наименьшую неподвижную точку.

Доказательство. Пусть $\mathbf{A} = (A, \leq)$ - ИУМ, и $f : A \to A$ - непрерывное отображение. Обозначим через O наименьший элемент множества A.

Построим последовательность

$$\mathrm{O}, f(\mathrm{O}), f(f(\mathrm{O})), ..., f^n(\mathrm{O}), ...,$$

где $f^n(x) = f(f^{n-1}(x)), n \geq 1; f^0(x) = x$ - результат n-кратного применения функции f к элементу x.

Докажем, что эта последовательность не убывает. Так как O наименьший элемент, то $\mathrm{O} \leq f(\mathrm{O})$. Если для любого $k \leq n > 0$ предположить, что $f^{k-1}(\mathrm{O}) \leq f^k(\mathrm{O})$, то в силу монотонности непрерывного отображения f получим при $k = n$

$$f(f^{n-1}(\mathrm{O})) = f^n(\mathrm{O}) \leq f(f^n(\mathrm{O})) = f^{n+1}(\mathrm{O}),$$

откуда, в силу принципа индукции, для любого $n \geq 0$ имеет место $f^n(\mathrm{O}) \leq f^{n+1}(\mathrm{O})$, что и означает неубывание последовательности $\{f^n(\mathrm{O})\}_{n \geq 0}$.

Тогда эта последовательность имеет точную верхнюю грань.

Положим $a = \sup_{n \geq 0} f^n(\mathrm{O})$.

Докажем, что $f(a) = a$.

Имеем:

$$f(a) = f(\sup_{n \geq 0} f^n(\mathrm{O})) = \sup_{n \geq 0} f(f^n(\mathrm{O})) = \sup_{n \geq 0} f^{n+1}(\mathrm{O}) =$$
$$= \sup\{f(\mathrm{O}), f^2(\mathrm{O}), ..., f^n(\mathrm{O}), ...\} = \sup_{n \geq 1} f^n(\mathrm{O}) = a$$

На втором шаге этой цепочки используется непрерывность отображения f, а не последнем – лемма 1: вычисляется супремум последовательности, полученной из исходной отбрасыванием нулевого члена.

Итак, доказано существование неподвижной точки отображения f.

Докажем теперь, что это именно наименьшая неподвижная точка.

Пусть для какого-то $b \in A$ выполняется $f(b) = b$. Так как $\mathrm{O} \leq b$, то в силу монотонности любого непрерывного отображения

$$f(\mathrm{O}) \leq f(b) = b, f(f(\mathrm{O})) \leq f(f(b)) = b, ..., f^n(\mathrm{O}) \leq b$$

для любого $n \geq 0$, и, тем самым, элемент $b \in A$ является верхней гранью исходной последовательности, откуда $a = \sup_{n \geq 0} f^n(\mathrm{O}) \leq b$.

Теорема полностью доказана.

Ее доказательство конструктивно, так как дает формулу вычисления наименьшей неподвижной точки любого непрерывного отображения ИУМ в себя.

Теорему о наименьшей неподвижной точке можно трактовать, как утверждение о существовании наименьшего решения уравнения $x = f(x)$ в произвольном ИУМ. Это важно с точки зрения приложений этой теоремы в теории полуколец и основанных на ней методах анализа графов и автоматов.

Рассмотрим в этой связи такой пример.

В ИУМ всех подмножеств произвольного множества M (см. пример 2 выше) решим уравнение

$$X = (A \cap X) \cup B$$

относительно неизвестного множества X .

Можно доказать, что правая часть этого уравнения $f(X) = (A \cap X) \cup B$ непрерывна (это доказывается в теории полуколец).

Вычисляем последовательные приближения к решению:

$f(\varnothing) = B$, $f(B) = (A \cap B) \cup B = B$, то есть для любого $n \geq 1$ $f^n(\varnothing) = B$. Это и есть наименьшее решение уравнения.

Интересно показать попутно анализ этого уравнения независимым от теоремы о неподвижной точке методом.

Рассматриваемое уравнение можно трактовать, как утверждение о равенстве двух множеств. Используя известный критерий равенства множеств, состоящий в том, что множества равны тогда и только тогда, когда их симметрическая разность пуста, получим:

$$X \Delta ((A \cap X) \cup B) = \varnothing \ ,$$

откуда

$$\begin{matrix} X \cap \overline{((A \cap X) \cup B)} = \varnothing, \\ \bar{X} \cap ((A \cap X) \cup B) = \varnothing \end{matrix} .$$

Преобразуем 1-е пересечение:

$$X \cap (\overline{(A \cap X)} \cap \bar{B}) = X \cap (\bar{A} \cup \bar{X}) \cap \bar{B} = X \cap \bar{A} \cap \bar{B} = X \cap \overline{A \cup B} = \varnothing,$$

откуда $X \subseteq A \cup B$.

Далее:

$$\bar{X} \cap ((A \cap X) \cup B) = \bar{X} \cap B = \varnothing,$$

откуда $B \subseteq X$.

Итак, $B \subseteq X \subseteq A \cup B$. Это значит, что любое множество X, удовлетворяющее такому условию (и только такое), будет решением исходного уравнения, а $X = B$ есть решение наименьшее.

Лекция №6

27.09.24

II. Элементы общей алгебры

1. Основные понятия

Понятие операции

Отображение вида

$$\omega: A^n \to A, n \geq 0$$

называется n - *арной операцией на множестве* A. Это множество предполагается непустым.

Здесь важно понимать следующее: 1) операция определена на любом кортеже $(a_1,...,a_n) \in A^n$ и 2) принимает значение, элемент $b \rightleftharpoons \omega(a_1,...,a_n)$, также принадлежащий тому же множеству A. Если хотя бы одно из этих условий не выполняется, то это не операция в только что определённом смысле. Например, деление на множестве действительных чисел не есть операция (на ноль делить нельзя), матричные операции не являются операциями, так как не любые две матрицы можно сложить и не любые две матрицы можно перемножить. Скалярное (и смешанное) умножение векторов не является операцией, так как аргументы (компоненты кортежа) – векторы, а значение (результат) – число.

Обобщая данное выше определение, можно ввести понятие частичной операции (записанное выше отображение частично) и многосортной операции как отображения вида

$$\omega: A_1 \times ... \times A_n \to B, n \geq 0,$$

то есть аргументы и результат принадлежат, вообще говоря, разным множествам (которые иногда называют типами или сортами). Можно, конечно, ввести понятие частичной многосортной операции. Эти обобщения понятия операции мы в нашем курсе не рассматриваем.

Рассмотрим теперь некоторые частные случаи операций в зависимости от значения числа n.

1) $n = 0$
   Формально нульарная операция на множестве A есть отображение $\omega: A^0 = \{\lambda\} \to A; \omega(\lambda) \in A$.

Результат $\omega(\lambda)$ есть какой-то элемент множества A (разные нульарные операции определят разные элементы множества A). Поэтому обычно (и менее

формально) нульарную операцию определяют как произвольно фиксированный элемент множества A. Иногда бывает необходимо фиксировать какие-то элементы множества, обладающие особыми свойствами. Например, число 0 при умножении на любое число дает 0, а при прибавлении нуля к любому числу это число не меняется; умножение на единицу также оставляет исходное число без изменений.

2) $n=1$ (унарные операции)
   Это переход к противоположному числу, возведение числа в фиксированную степень, дополнение множества, соответствие, обратное к данному соответствию.
3) $n=2$ (бинарные операции)
   Это очень широкий класс операций, которыми мы и будем преимущественно заниматься. Это числовые операции сложения и умножения, сложение и векторное умножение векторов, сложение и умножение квадратных матриц одинакового порядка, операции над множествами (кроме дополнения), соответствиями (кроме диагонали – нульарной операции- и взятия обратного).

Операции более высоких «арностей» встречаются редко, и мы ими заниматься не будем.

Понятие алгебраической структуры

Неформально, *алгебраическая структура* есть множество (непустое) с некоторыми операциями на нем.

Строго, алгебраическая структура есть упорядоченная пара

$\mathbf{A}=(A,\Omega)$,

где A - непустое множество, называемое *носителем*, а Ω - некоторое множество операций на носителе, называемое *сигнатурой*.

Вместо термина «алгебраическая структура» обычно говорят просто «алгебра» (при том, что слово «алгебра» обозначает и всю науку, изучающую алгебраические структуры).

Сигнатура разбивается на подмножества операций разных арностей:

$\Omega=\Omega^{(0)}\cup\Omega^{(1)}\cup\Omega^{(2)}\cup...\cup\Omega^{(n)}\cup...$,

где $\Omega^{(k)}(k=0,1,2,...,n,...)$ - подмножество операций арности k. Некоторые из этих множеств могут быть пустыми. Сигнатура может быть бесконечной (и даже несчетной), хотя дальше мы будем заниматься алгебрами с конечными сигнатурами.

Примеры

1) Числовые алгебры
   $\mathbf{R}=(\mathbb{R},+,\cdot,0,1)$, $\mathbf{Q}=(\mathbb{Q},+,\cdot,0,1)$, $\mathbf{Z}=(\mathbb{Z},+,\cdot,0,1)$, $\mathbf{R}=(\mathbb{R},+,\cdot,0,1)$, $\mathbf{N}_0=(\mathbb{N}_0,+,\cdot,0,1)$ - множества действительных, рациональных, целых и натуральных (неотрицательных целых) чисел с операциями сложения, умножения, а также нулем и единицей в качестве нульарных операций.

2) Векторные алгебры

$\mathbf{L} = (L, +, \overline{0}, \alpha\cdot|_{\alpha\in\mathbb{R}})$ - векторное (линейное) пространство с операциями сложения векторов, нулевым вектором (нульарная операция) и бесконечным множеством унарных операций умножения вектора на действительное число α.

$\mathbf{V} = (V, +, \times, \overline{0})$ - множество геометрических векторов с операциями сложения, векторного умножения и нулевым вектором (как нульарной операцией).

3) Матричные алгебры

$\mathbf{M}_n = (M_n, +, \cdot, O, E)$ - множество квадратных матриц n-го порядка со стандартными операциями сложения и умножения и нулевой и единичной матрицами (как нульарными операциями).

4) Алгебры множеств и отношений

$Set(M) = (2^M, \cup, \cap, \setminus, \Delta, \bar{}, \varnothing, M)$ - булеан (множество всех подмножеств) множества M с операциями объединения, пересечения, разности, симметрической разности, дополнения, пустым и универсальным, то есть всем множеством M как нульарными операциями.

$\mathrm{Rel}(M) = (2^{M\times M}, \cup, \circ, ^{-1}, \varnothing, \mathrm{id}_M)$ - множество всех бинарных отношений на множестве M с операциями объединения, композиции, взятия обратного, пустым отношением и диагональю как нульарными операциями.

Типом алгебры с конечной сигнатурой называется кортеж, составленный из арностей ее операций. Например, типы записанных выше алгебр множеств и отношений будут (2, 2, 2, 2, 1, 0, 0) и (2, 2, 1, 0, 0) соответственно.

Алгебры, имеющие один и тот же тип, называются *однотипными*. Например, рассмотренные выше числовые алгебры и алгебра квадратных матриц однотипны и их тип будет (2, 2, 0, 0).

Заметим, что порядок перечисления операций в сигнатуре произволен, но обычно договариваются перечислять их по убыванию арностей.

2. Группоиды, полугруппы, группы

Алгебра с одной бинарной операцией (то есть алгебра типа (2)) называется *группоидом*.

Например, группоидами будут следующие алгебры: $1)(\mathbb{R}, +), 2)(\mathbb{R}, \cdot), 3)(V, \times), 4)(2^M, \setminus), 5)(2^M, \Delta)$ - 1) группоид действительных чисел с операцией сложения и 2) умножения; 3) группоид геометрических векторов с операцией векторного умножения; 4) и 5) группоид подмножеств некоторого множества M (может быть, даже и пустого) с операциями разности и симметрической разности соответственно.

Пусть $\mathbf{G} = (G, *)$ - некий группоид.

Если его операция ассоциативна, то есть имеет место тождество $a*(b*c) = (a*b)*c \ (a,b,c \in G)$, то такой группоид называется *полугруппой*. В записанных выше примерах группоиды (1), (2) и (5) -полугруппы, а группоиды (3) и (4) не являются полугруппами, так как их операции не ассоциативны.

Элемент $\varepsilon \in G$ группоида называется *нейтральным по операции* * (или просто нейтральным, если бинарная операция подразумевается), если для любого $a \in G$ имеет место $a * \varepsilon = \varepsilon * a = a$.

Теорема. Если группоид имеет нейтральный элемент, то он единственный.

Доказательство. Пусть $\varepsilon, \varepsilon'$ - два нейтральных элемента одного и того же группоида. Тогда $\varepsilon * \varepsilon' = \varepsilon'$, так как ε нейтральный элемент, и $\varepsilon * \varepsilon' = \varepsilon$, так как ε' нейтральный. То есть $\varepsilon = \varepsilon'$. Заметим, что при доказательстве существенно использовано «двустороннее свойство» нейтрального элемента: при «умножении» на него как слева, так и справа, тот элемент, который «умножается», остается неизменным. Операция группоида условно названа «умножением».

Для нас особенно важны полугруппы с нейтральными элементами.

Полугруппа с нейтральным элементом называется *моноидом*.

В общем случае моноид записывают так: $\mathbf{M} = (M, \cdot, \varepsilon)$, где точкой обозначена бинарная операция (точку часто опускают), а ε - нейтральный элемент.

Примеры моноидов:

1) $(\mathbb{R}, \cdot, 1), (\mathbb{R}, +, 0)$ - числовые моноиды всех действительных чисел по умножению (мультипликативный моноид действительных чисел) и по сложению (аддитивный моноид действительных чисел);
2) $(2^{M^2}, \circ, \mathrm{id}_M)$ - моноид бинарных отношений на множестве M (напомним, что операция композиции отношений ассоциативна, а диагональ, то же самое, что тождественное отображение, есть нейтральный элемент по этой операции:
   $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$,
   $\rho \circ \mathrm{id}_M = \mathrm{id}_M \circ \rho = \rho$);
3) $\mathbf{M}_n^{\cdot} = (M_n, \cdot, E)$ - моноид квадратных матриц n-го порядка по умножению:
4) $(2^M, \cup, \varnothing), (2^M, \cap, M), (2^M, \Delta, \varnothing)$ - моноиды на булеане множества M.

Заметим дополнительно, что множество натуральных чисел (положительных целых) по сложению не будет моноидом, так как не содержит нуля – нейтрального элемента по сложению; это будет просто полугруппа. Но по операции умножения получится моноид.

Обратимые элементы моноида

Некоторые элементы моноида могут оказаться *обратимыми*. А именно, элемент a' называется *обратным к элементу* a, если выполняется двойное равенство $a \cdot a' = a' \cdot a = \varepsilon$. Тогда сам элемент a называется обратимым. Например, в моноиде квадратных матриц обратимыми будут невырожденные матрицы, то есть матрицы с ненулевым определителем.

Теорема. Если элемент моноида обратим, то обратный к нему определен однозначно.

Доказательство. Допуская, что для некоторого элемента a существуют два обратных, скажем a' и a''. Тогда строим такую цепочку преобразований: $a'' = a''\varepsilon = a''(aa') = (a''a)a' = \varepsilon a' = a'$(точка, знак операции, опущена). Существенно использована ассоциативность операции моноида, а также «двустороннее свойство» обратного элемента: при «умножении» на обратный как слева, так и справа, получаем нейтральный элемент.

Далее обратный к a обозначаем a^{-1}.

Свойства обратимых элементов

1) $(ab)^{-1} = b^{-1}a^{-1}$

Действительно: $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a\varepsilon a^{-1} = aa^{-1} = \varepsilon$

Точно так же доказывается, что $(b^{-1}a^{-1})(ab) = \varepsilon$. Отсюда, в силу единственности обратного элемента, получаем, что $(ab)^{-1} = b^{-1}a^{-1}$.

2) $(a^{-1})^{-1} = a$

Равенство $aa^{-1} = a^{-1}a = \varepsilon$ следует прочитать как определение обратного к обратному. В силу единственности обратного отсюда и следует, что это будет исходный элемент.

3) Нейтральный элемент обратен себе самому.

Моноид, все элементы которого обратимы, называется *группой*.

Примеры групп

1) Числовые группы: $1)(\mathbb{R}\setminus\{0\},\cdot,1), 2)(\mathbb{Q}\setminus\{0\},\cdot,1).3)(\mathbb{R},+,0), 4)(\mathbb{Q},+,0), 5)(\mathbb{Z},+,0)$.

   Эти группы называются: 1) и 2) *мультипликативные группы* действительных и рациональных чисел, 3), 4) и 5) *аддитивные группы* действительных, рациональных и целых чисел. Такие же группы могут быть образованы на множестве комплексных чисел.

2) Группа векторов: $(V,+,\bar{0})$
3) Группа матриц: $\mathrm{GL}(n) = (M_n^+,\cdot,E)$ - группа невырожденных матриц по умножению. Определение этой группы корректно, так как произведение невырожденных матриц является невырожденной матрицей в силу известной теоремы об умножении определителей.
4) Группа множеств: $(2^M,\Delta,\varnothing)$. Эта группа интересна тем, что в ней каждый элемент обратен самому себе: $A\Delta A = \varnothing$.

Группу обычно записывают, как моноид, указывая носитель, бинарную операцию и нейтральный элемент. Иногда в сигнатуру добавляют унарную операцию взятия обратного.

Следующий пример группы очень важен для всего дальнейшего изложения.

Рассмотрим моноид бинарных отношений на некотором непустом множестве $(2^{M^2}, \circ, \mathrm{id}_M)$.

Можно доказать, что *отношение* $\rho \in M^2$ *обратимо тогда и только тогда, когда оно является биекцией данного множества на себя.* Тогда и только тогда выполняется равенство $\rho \circ \rho^{-1} = \rho^{-1} \circ \rho = \mathrm{id}_M$ (рекомендуется доказать самостоятельно, хотя это не совсем тривиально). Следует подчеркнуть, что в общем случае для произвольного отношения и обратного к нему записанное выше двойное равенство не выполняется! (см. Семинар №2).

Замечание. Если $f : A \to A$ биекция, то

$$(\forall x)(\exists! y)(y = f(x)) \,\&\, (\forall y)(\exists! x)(y = f(x));$$
$$f^{-1}(y) = x \rightleftharpoons y = f(x)$$
$$x \xrightarrow{f} y = f(x) \xrightarrow{f^{-1}} x$$
$$y \xrightarrow{f^{-1}} x \xrightarrow{f} y;$$
$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_M$$

Обратное отношение тогда есть $f^{-1} = \{(y, x) : y = f(x)\}$, и поскольку такой x единственный, то можно положить

$$f^{-1}(y) = x \rightleftharpoons y = f(x),$$

то есть обратное отношение есть отображение, как легко понять, тоже взаимно однозначное.

Так как композиция биекций есть снова биекция, обратное отображение тоже биекция и, наконец, тождественное отображение (диагональ) – биекция (проверить эти утверждения!), то получаем группу на множестве биекций (взаимно однозначных отображений), которая называется *симметрической группой данного множества* и обозначается S_M. Для нас особенно важен случай конечного множества. Биекция конечного множества на себя называется *подстановкой* этого множества, а группа подстановок n-элементного множества называется *симметрической группой степени n* и обозначается S_n.

Подстановка стандартно записывается в виде двустрочной матрицы:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

где в верхней строке перечисляются элементы множества *M* в стандартном порядке (по возрастанию), и под каждым элементом в нижней строке подписывается его образ при отображении σ, то есть $i_k = \sigma(k), 1 \le k \le n$.

Таким образом, нижняя строка является некоторой ***пере****становкой* элементов верхней строки. Иногда саму подстановку называют перестановкой, но, строго говоря, это неверно: перестановка – это вектор значений функции (отображения), которая называется подстановкой.

Отсюда же видно, что число элементов в группе S_n равно *n*! (n факториал).

Рассмотрим теперь выполнение операций группы: композиции и обращения.

1) Вычисление композиции

Композиция двух подстановок

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \text{ и } \tau = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

вычисляется очень просто по формуле $\sigma \circ \tau(k) = \tau(\sigma(k)), 1 \le k \le n$, то есть это вычисление значения сложной функции. Первая подстановка переводит элемент k в элемент i_k, а вторая полученный элемент i_k переводит в элемент j_{i_k}.

Например:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

Схема действий:

1→4→4, 2→3→1, 3→1→3, 4→2→2.

При этом

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \neq \sigma \circ \tau,$$

то есть композиция подстановок некоммутативна.

2) Обратная подстановка

Чтобы найти подстановку, обратную данной, нужно переставить строки матрицы, а потом переставить столбцы так, чтобы верхняя строка приняла стандартный вид 1 2 … *n*.

Например,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 3 & 1 \end{pmatrix} \to \begin{pmatrix} 4 & 5 & 2 & 3 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix} = \sigma^{-1}$$

Перестановку строк можно выполнить «в уме» и сразу записать обратную подстановку, читая исходную снизу вверх.

(См. Учебник, пример 2.10.)

В заключение отметим важный частный случай *коммутативной группы*.

Группа называется коммутативной (или абелевой), если ее бинарная операция коммутативна, то есть имеет место тождество $ab = ba$. Все числовые группы коммутативны; группа множеств также коммутативна, а группа матриц и симметрическая группа любого множества не коммутативны.