

МГТУ ФН-12 МГТУ ФН-12 МГТУ

Московский государственный технический университет
имени Н.Э. Баумана

Факультет «Фундаментальные науки»
Кафедра «Математическое моделирование»

А.Н. Канатников

**ИЗБРАННЫЕ ЛЕКЦИИ
ПО АЛГЕБРЕ**

Конспект лекций

Для студентов факультета ФН

Москва
2009

МГТУ ФН-12 МГТУ ФН-12 МГТУ

19. ПОЛУКОЛЬЦА И БУЛЕВЫ АЛГЕБРЫ

19.1. Определение полукольца

Полукольцо — алгебраическая система с двумя бинарными операциями „+“ и „·“ (сложение и умножение), причем относительно сложения эта алгебра есть коммутативный моноид, относительно умножения — тоже моноид, кроме того, умножение дистрибутивно (слева и справа) относительно сложения, а нейтральный элемент сложения (ноль полукольца) есть аннулирующий элемент умножения. Всего восемь аксиом. Коммутативное полукольцо и идемпотентное полукольцо ($x + x = x$). Примеры ($\mathbb{R}^* = \{x \in \mathbb{R}: x \geq 0\}$):

- а) любое кольцо с единицей;
- б) $\mathcal{R}^* = (\mathbb{R}^*, +, \cdot, 0, 1)$ — коммутативное неидемпотентное полукольцо;
- в) $\mathcal{S}_A = (2^A, \cup, \cap, \emptyset, A)$ — коммутативное идемпотентное полукольцо;
- г) $\mathcal{R}_A = (2^{A \times A}, \cup, \circ, \emptyset, \text{id}_A)$ — идемпотентное некоммутативное полукольцо;
- д) $\mathcal{U}_{a,b} = ([a, b], \max, \min, a, b)$ — коммутативное идемпотентное полукольцо;
- е) $\mathcal{L}_{a,b} = ([a, b], \min, \max, b, a)$ — коммутативное идемпотентное полукольцо;
- ж) $\mathcal{R}^+ = (\mathbb{R}^* \cup \{+\infty\}, \min, +, +\infty, 0)$ — коммутативное идемпотентное полукольцо.

Отношение порядка в полукольце: $x \leq y \Leftrightarrow x + y = y$. Свойства: а) $0 \leq a, a \in K$; б) $a \leq a + b, a, b \in K$; в) $a \leq b, c \leq d \Rightarrow a + c \leq b + d$; г) $a + b = 0 \Rightarrow a = 0$ и $b = 0$; д) $a \leq c, b \leq c \Rightarrow a + b \leq c$; е) $a \leq b \Rightarrow ac \leq bc$. Теорема 1: если A конечное множество идемпотентного полукольца, то сумма всех элементов A есть $\sup A$.

Полукольцо — алгебраическая система с двумя бинарными операциями „+“ и „·“ (сложение и умножение), причем:

- относительно сложения эта алгебра есть коммутативный моноид;
- относительно умножения — тоже моноид;
- умножение дистрибутивно (слева и справа) относительно сложения;
- нейтральный элемент по сложению (*ноль полукольца*) есть аннулирующий элемент по умножению.

Эти четыре условия дают восемь аксиом:

- 1) $x + y = y + x$;
- 2) $(x + y) + z = x + (y + z)$;
- 3) $x + 0 = x$;
- 4) $(xy)z = x(yz)$;
- 5) $x \cdot 1 = 1 \cdot x = x$;
- 6) $(x + y)z = xz + yz$;
- 7) $z(x + y) = zx + zy$;
- 8) $x \cdot 0 = 0 \cdot x = 0$.

Полукольцо называется **коммутативным**, если умножение полукольца коммутативно. Мы ограничимся рассмотрением **идемпотентных полуколец**, т.е. полуколец, в которых операция сложения **идемпотентна**: $x + x = x$.

Пример 19.1. а. Первым примером полукольца является любое кольцо с единицей. Отметим, что в кольце сложение не может быть идемпотентным, так как из равенства $x + x = x$ в силу свойства сокращения следует, что $x = 0$.

б. Второй пример — система $\mathcal{R}^* = (\mathbb{R}^*, +, \cdot, 0, 1)$, являющаяся коммутативным полукольцом, но не кольцом. Это полукольцо не идемпотентно.

в. Алгебраическая система $\mathcal{S}_A = (2^A, \cup, \cap, \emptyset, A)$ является коммутативным идемпотентным полукольцом. В этом можно убедиться непосредственной проверкой.

г. Алгебраическая система $\mathcal{R}_A = (2^{A \times A}, \cup, \circ, \emptyset, \text{id}_A)$, носителем которой является множество отношений на множестве A , сложением — объединение отношений, а умножением — композиция отношений, представляет собой идемпотентное некоммутативное полукольцо.

д. Алгебраическая система $\mathcal{U}_{a,b} = ([a, b], \max, \min, a, b)$ — коммутативное идемпотентное полукольцо. В этом можно убедиться непосредственно, проверяя аксиомы полукольца. Однако следует заметить, что пример а полукольца нетрудно модифицировать: можно рассмотреть не все множество всех подмножеств множества A (булеан множества A), а любое семейство подмножеств множества A , замкнутое относительно операций объединения и пересечения двух множеств и включающее подмножества $\emptyset$ и A . Если в качестве указанного семейства множеств выбрать совокупность отрезков вида $[a, x]$, обозначаемых правым концом x , то объединение отрезков с концами x и y будет отрезком с концом $\max\{x, y\}$, а пересечение этих отрезков — отрезком с концом $\min\{x, y\}$. Иными словами полукольцо $\mathcal{U}_{a,b}$ можно интерпретировать как частный случай полукольца $\mathcal{S}_A$.

е. Еще один пример коммутативного идемпотентного полукольца — алгебраическая система $\mathcal{L}_{a,b} = ([a, b], \min, \max, b, a)$. Любопытно, что если в полукольцах $\mathcal{S}_A$ и $\mathcal{U}_{a,b}$ поменять местами две бинарные операции и две нульарные, то также получим полукольцо. Действительно, $\mathcal{S}_A$ является коммутативным моноидом и относительно объединения, и относительно пересечения. Каждая из этих операций дистрибутивна относительно другой, а нейтральный элемент одной операции является аннулирующим элементом другой.

е. Алгебраическая система $\mathcal{R}^+ = (\mathbb{R}^* \cup \{+\infty\}, \min, +, +\infty, 0)$, где $\mathbb{R}^*$ — множество неотрицательных действительных чисел, является коммутативным идемпотентным полукольцом.

В идемпотентном полукольце K отношение $\{(x, y): x + y = y\}$ есть отношение порядка, которое обозначают символом $\leq$ и называют **естественным порядком полукольца**.

Покажем, что введенное отношение действительно есть отношение порядка. Во-первых, из условий $x \leq y$ и $y \leq x$ делаем вывод, что $x + y = y$ и $y + x = x$, откуда в силу коммутативности сложения вытекает, что $x = y$. Следовательно, введенное нами отношение антисимметрично. Во-вторых, это отношение транзитивно, так как условия $x \leq y$ и $y \leq z$ означают, что $x + y = y$ и $y + z = z$, а следовательно, $x + z = x + y + z = y + z = z$ и $x \leq z$. Наконец, рефлексивность отношения, т.е. выполнение условия $x \leq x$ означает выполнение для любого $x \in K$ равенства $x + x = x$, т.е. идемпотентность сложения.

Пример 19.2. В полукольце $\mathcal{S}_A = (2^A, \cup, \cap, \emptyset, A)$ условие $B \cup C = C$ равносильно включению $B \subset C$. Следовательно в этом полукольце отношение естественного порядка есть отношение включения.

В полукольце $\mathcal{U}_{a,b} = ([a, b], \max, \min, a, b)$ отношение естественного порядка полукольца совпадает с естественным числовым порядком, а в полукольце $\mathcal{L}_{a,b}$ естественное отношение порядка является обратным к естественному числовому порядку.

Отношение естественного порядка полукольца K обладает следующими свойствами:

- а) $0 \leq a, a \in K$;
- б) $a \leq a + b, a, b \in K$;
- в) $a \leq b, c \leq d \Rightarrow a + c \leq b + d$;
- г) $a + b = 0 \Rightarrow a = 0$ и $b = 0$;
- д) $a \leq c, b \leq c \Rightarrow a + b \leq c$;
- е) $a \leq b \Rightarrow ac \leq bc$.

Первые четыре свойства повторяют соответствующие свойства отношения естественного порядка на множестве действительных неотрицательных чисел. А вот два последних свойства не имеют аналога среди отношений порядка на числовых множествах, хотя для отношения включения множеств оно очевидно. Проверка свойств элементарна и не вызывает затруднений. Поэтому доказательство их мы опускаем.

Поскольку на идемпотентном полукольце естественным образом возникает отношение порядка, такое полукольцо всегда можно рассматривать как упорядоченное множество. Напомним, что для таких множеств введены понятия наибольшего (наименьшего) элемента, максимального (минимального элемента), верхней (нижней) грани множества и точной верхней (нижней) грани.

Теорема 19.1. Если A конечное множество элементов идемпотентного полукольца, то сумма всех элементов A есть $\sup A$.

◀ Пусть $A = \{a_1, a_2, \dots, a_n\}$. Чтобы доказать утверждение, достаточно показать, что, с одной стороны, сумма $a = a_1 + a_2 + \dots + a_n$ есть верхняя грань множества A , а с другой она не превышает никакой другой верхней грани множества A .

Используя свойства естественного порядка, заключаем, что

$$a_i \leq a_i + a = a_i + a_1 + a_2 + \dots + a_i + \dots + a_n = a, \quad i = \overline{1, n}.$$

Таким образом, сумма a есть верхняя грань множества A .

Пусть b — какая-либо грань множества A , т.е. $a_i \leq b$, $i = \overline{1, n}$. Тогда в силу свойства д) естественного порядка полукольца

$$a_1 + a_2 \leq b, \quad (a_1 + a_2) + a_3 \leq b, \quad \dots, \quad (a_1 + a_2 + \dots + a_{n-1}) + a_n \leq b.$$

Следовательно, $a \leq b$ и сумма a не превышает любой произвольно взятой верхней грани множества A . ▶

19.2. Ряды в полукольцах

Ряд в идемпотентном полукольце. Частичные суммы и сумма ряда; неубывающая последовательность частичных сумм. Теорема 2: если ряд сходится, то его сумма является точной верхней гранью последовательности членов ряда; если последовательность членов ряда имеет точную верхнюю грань, то ряд сходится. Следствие: $a_i \leq a \Rightarrow \sum_{i=1}^{\infty} a_i \leq a$. Группировки и перестановки в рядах.

Теорема 3: если ряд сходится, то и любая его перестановка сходится к той же сумме. Теорема 4: Если ряд сходится, то сходится любая его группировка; если группировка ряда сходится, то и сам ряд сходится (в основе утверждение: точная верхняя грань неубывающей последовательности совпадает с точной верхней гранью любой ее подпоследовательности). Бесконечная ассоциативность и бесконечная коммутативность. Теорема 5: Пусть $\{a_{mn}\}$ — посл. с двойной нумерацией, ряд $\sum_n a_{mn}$ сходится $\forall n$ и $\sum_n a_{mn} = b_m$. Если $\sum b_m$ сходится, то любой ряд c_k , полученный перенумерацией $\{a_{mn}\}$, сходится к $\sum b_m$. Следствие: $\sum (a_n + b_n) = \sum a_n + \sum b_n$. Покомпонентная непрерывность операции сложения относительно естественного порядка.

Пусть $\{a_n\}$ — некоторая последовательность элементов полукольца K . Символическая запись

$$a_1 + a_2 + \dots + a_n + \dots = \sum_{i=1}^{\infty} a_i$$

называется **рядом**. Тема „ряды“ — одна из важнейших в курсе математического анализа, при этом теория числовых рядов активно использует понятие предела числовой последовательности.

В полукольцах нет понятия предела последовательности. Однако можно построить элементарную теорию рядов, похожую на теорию *закноположительных рядов*.

Итак, пусть дан ряд $\sum_{i=1}^{\infty} a_i$. Значения

$$S_1 = a_1, \quad S_2 = a_1 + a_2 = S_1 + a_2, \quad \dots, \quad S_{n+1} = S_n + a_n, \quad \dots$$

называются **частичными суммами** рассматриваемого ряда. Из равенств $S_{n+1} = S_n + a_n$, $n \in \mathbb{N}$, следует, что $S_1 \leq S_2 \leq \dots \leq S_n \leq \dots$, т.е. последовательность $\{S_n\}$ частичных сумм

является **монотонной**. Если эта последовательность имеет точную верхнюю грань S , то рассматриваемый ряд будем называть **сходящимся**, а элемент S — его **суммой**.

Теорема 19.2. Последовательность частичных сумм сходящегося ряда имеет точную верхнюю грань, равную сумме ряда. Если последовательность членов ряда имеет точную верхнюю грань, то ряд сходится к этой точной верхней грани.

◀ Для доказательства утверждения теоремы достаточно показать, что у последовательности $\{a_n\}$ членов ряда и последовательности $\{S_n\}$ его частичных сумм множества верхних граней совпадают. Тогда из существования наименьшего элемента у одного множества следует существование наименьшего элемента у другого множества, причем это будет один и тот же элемент полукольца.

Поскольку $a_n \leq S_n$, то любая верхняя грань последовательности $\{S_n\}$ является верхней гранью и последовательности $\{a_n\}$. Пусть b — верхняя грань последовательности $\{a_n\}$. Тогда $a_n \leq b$, $n \in \mathbb{N}$. В силу свойства д) естественного порядка полукольца

$$S_n = a_1 + a_2 + \dots + a_n \leq b, \quad n \in \mathbb{N}.$$

Следовательно, b есть верхняя грань последовательности $\{S_n\}$. ▶

Следствие 19.1. $a_i \leq a \Rightarrow \sum_{i=1}^{\infty} a_i \leq a$.

Это следствие формулирует результат второй части доказательства теоремы: верхняя грань последовательности членов ряда есть в то же время верхняя грань последовательности частичных сумм.

Ряд $\sum_{k=1}^{\infty} b_k$, называется **группировкой ряда** $\sum_{i=1}^{\infty}$, если

$$b_k = \sum_{i=n_k+1}^{n_{k+1}} a_i = a_{n_k+1} + a_{n_k+2} + \dots + a_{n_{k+1}},$$

где $\{n_k\}$ — возрастающая последовательность натуральных чисел, начинающаяся с $n_1 = 1$. Отметим очевидный факт, что последовательность частичных сумм группированного ряда является подпоследовательностью последовательности частичных сумм негруппированного ряда.

Теорема 19.3. Если ряд сходится, то любая его группировка сходится к той же сумме. Для сходимости ряда достаточно сходимости какой-либо его группировки.

◀ В основе теоремы лежит утверждение, что точная верхняя грань неубывающей последовательности совпадает с точной верхней гранью любой ее подпоследовательности.

Поскольку подпоследовательность есть подмножество последовательности, любая верхняя грань последовательности есть верхняя грань и любой ее подпоследовательности. Если последовательность монотонная, то верно и обратное. Действительно, рассмотрим монотонную последовательность $\{S_n\}$ и произвольную ее подпоследовательность $\{S_{n_k}\}$. Пусть b — верхняя грань последовательности $\{S_{n_k}\}$, т.е. $S_{n_k} \leq b$, $k \in \mathbb{N}$. Для произвольного номера m можно выбрать такой номер k , что $m \leq n_k$. Следовательно, $S_m \leq S_{n_k} \leq b$. Значит, b является верхней гранью всей последовательности.

Итак, множества верхних граней последовательности $\{S_n\}$ и ее подпоследовательности $\{S_{n_k}\}$ совпадают. Значит, совпадают и их точные верхние грани, причем для существования точной верхней грани одной последовательности достаточно существования точной верхней грани другой. ▶

Утверждение доказанной теоремы можно рассматривать как свойство бесконечной ассоциативности сложения в полукольце.

Пусть $\{n_k\}$ — последовательность натуральных чисел, представляющая собой биективное отображение множества натуральных чисел на себя (т.е. любое натуральное число появляется в последовательности, и притом ровно один раз). Тогда из любого ряда $\sum_{k=1}^{\infty} a_k$ можно образовать новый ряд $\sum_{k=1}^{\infty} a_{n_k}$, называемый **перестановкой ряда** $\sum_{k=1}^{\infty} a_k$. Последовательность элементов полукольца K естественно интерпретировать как отображение вида $\varphi: \mathbb{N} \rightarrow K$. Образ $\varphi(n)$ номера n при этом отображении является n -м членом последовательности. При такой трактовке перестановка членов последовательности (и, соответственно, членов ряда) есть композиция $\varphi \circ h$, где $h: \mathbb{N} \rightarrow \mathbb{N}$ — биекция множества натуральных чисел на себя, записываемая как последовательность $\{n_k\}$. При такой трактовке ясно, что если последовательность $\{b_k\}$ получена перестановкой последовательности $\{a_n\}$, то и последовательность $\{a_n\}$ может быть получена перестановкой последовательности $\{b_k\}$. Такая перестановка порождается отображением h^{-1} , обратным к отображению h .

Теорема 19.4. Если ряд в полукольце сходится, то и любая перестановка этого ряда тоже сходится, причем к той же сумме.

◀ Доказательство теоремы, как и в случае предыдущей теоремы, повторяет доказательство своего аналога для положительных числовых рядов. Пусть $\{S_n\}$ — последовательность частичных сумм ряда $\sum_{k=1}^{\infty} a_k$, а $\{D_k\}$ — последовательность частичных сумм перестановки $\sum_{k=1}^{\infty} a_{n_k}$. Отметим, что

$$D_k = a_{n_1} + a_{n_2} + \dots + a_{n-k}.$$

Положим $m = \max\{n_1, n_2, \dots, n_k\}$. Тогда сумма

$$S_m = a_1 + a_2 + \dots + a_m$$

среди слагаемых будет содержать все элементы a_{n_j} , $j = \overline{1, k}$. Из этого вытекает, что для любого $k \in \mathbb{N}$ существует номер m при котором $D_k \leq S_m$. Из этого нетрудно сделать вывод, что любая верхняя грань последовательности $\{S_m\}$ является верхней гранью и последовательности $\{D_k\}$. Иначе говоря, множество верхних граней последовательности частичных сумм любого ряда включается в множество верхних граней последовательности частичных сумм любой его перестановки. Всеобщность этого утверждения и обратимость перестановки позволяют сделать вывод, что на самом деле множества верхних граней последовательности частичных сумм ряда и последовательности частичных сумм произвольной его перестановки совпадают. Следовательно, из сходимости одного ряда следует сходимость другого к той же сумме. ►

Утверждение доказанной теоремы можно рассматривать как свойство бесконечной коммутативности. В рамках бесконечной коммутативности можно рассматривать и следующее свойство.

Теорема 19.5. Если ряды $\sum_{n=1}^{\infty} a_n$ и $\sum_{n=1}^{\infty} b_n$ сходятся, то и ряд $\sum_{n=1}^{\infty} (a_n + b_n)$ сходится, причем

$$\sum_{n=1}^{\infty} (a_n + b_n) = \sum_{n=1}^{\infty} a_n + \sum_{n=1}^{\infty} b_n.$$

Здесь участвуют группировка слагаемых бесконечной суммы и их перестановка. Однако рассмотренные выше перестановки не позволяют „собрать“ два ряда в один или, наоборот, разделить один ряд на два. Кроме того, сходящийся ряд может делиться на два так, что обе составляющие сходятся не будут (этот эффект проще всего наблюдать в множестве знакоположительных числовых рядов с рациональными членами). Это указывает на то, что из доказанных выше теорем 19.3 и 19.4 сформулированная теорема 19.5 не может быть выведена.

Мы докажем обобщение сформулированной теоремы

Теорема 19.6. Пусть $\{a_{mn}\}$ — последовательность с двойной нумерацией, ряд $\sum_{n=1}^{\infty} a_{mn}$ сходится для каждого номера n к сумме b_m , т.е. $\sum_{n=1}^{\infty} a_{mn} = b_m$. Если ряд $\sum_{m=1}^{\infty} b_m$ сходится к сумме b , то любой ряд $\sum_{k=1}^{\infty} c_k$, полученный перенумерацией последовательности $\{a_{mn}\}$ в единую последовательность $\{c_k\}$, сходится к b .

◀ Во-первых, по определению суммы ряда в полукольце имеем $b_m \leq b$, $m \in \mathbb{N}$, и $a_{mn} \leq b_m$, $m, n \in \mathbb{N}$. Следовательно, $a_{mn} \leq b$, $m, n \in \mathbb{N}$. Но тогда b есть верхняя грань последовательности членов ряда $\sum_{k=1}^{\infty} c_k$, а значит, и последовательности частичных сумм этого ряда. Во-вторых, любая верхняя грань b' последовательности частичных сумм ряда $\sum_{k=1}^{\infty} c_k$ есть верхняя грань последовательности членов этого ряда. Поэтому для любого номера m элемент b' является верхней гранью последовательности членов ряда $\sum_{n=1}^{\infty} a_{mn}$, поскольку все члены этой последовательности являются членами последовательности $\{c_k\}$. Значит, сумма этого ряда, являющаяся точной верхней гранью последовательности членов ряда, не превышает b' , т.е. $b_m \leq b'$. Но тогда и $b = \sup \{b_m\} \leq b'$.

Тем самым доказано, что b есть верхняя грань последовательности частичных сумм ряда $\sum_{k=1}^{\infty} c_k$, причем наименьшая верхняя грань. В соответствии с определением суммы ряда заключаем, что ряд $\sum_{k=1}^{\infty} c_k$ сходится к b . ▶

Доказательство теоремы 19.5 можно получить, модифицируя подходящим образом доказательство теоремы 19.6. Можно также рассуждать следующим образом.

Пусть ряды $\sum_{n=1}^{\infty} a_n$ и $\sum_{n=1}^{\infty} u_n$ сходятся к суммам a и b соответственно. Рассмотрим двухиндексную последовательность

$$r_{mn} = \begin{cases} a_n, & m = 1; \\ b_n & m = 2; \\ 0, & m > 2. \end{cases}$$

Эта последовательность удовлетворяет условиям теоремы 19.6, причем нетрудно увидеть, что суммой ряда с общим членом $\sum_{n=1}^{\infty} r_{mn}$, т.е. ряда

$$a + b + 0 + 0 + 0 + \dots,$$

является сумма $a + b$. Следовательно, любой ряд, полученный перенумерацией двухиндексной последовательности r_{mn} , будет сходиться к $a + b$. Нетрудно построить такую нумерацию последовательности r_{mn} , при которой ненулевые слагаемые идут в порядке a_1, b_1, a_2, b_2 и т.д. В полученном ряде многие члены нулевые. Наличие таких членов означает, что некоторые члены в последовательности частичных сумм повторяются. Выбрасывание нулевых слагаемых не скажется на множестве значений последовательности частичных сумм, а потому на существовании и значении точной верхней грани этой последовательности. Но, выбросив все нулевые слагаемые, мы получим ряд

$$a_1 + b_1 + a_2 + b_2 + \dots,$$

который как показано, сходится к $a + b$. Сгруппировав в последнем ряде слагаемые парами, мы придем к заключению теоремы 19.5.

Теорема 19.5 может рассматриваться не только с точки зрения бесконечной коммутативности. Рассмотрим функцию $S_l(x) = x + a$. Эта функция удовлетворяет условию $x_1 \leq x_2 \Rightarrow S_l(x_1) \leq S_l(x_2)$, т.е. эта функция оказывается монотонной. Точно так же монотонна и функция* $S_r(x) = a + x$. Об этом свойстве говорят как о **монотонности сложения по своим аргументам**. Оказывается, что сложение является и **непрерывной по своим аргументам**. Действительно, непрерывность функции $S_l(x)$ означает, что

$$\sup S_l(x_n) = S_l(\sup x_n).$$

Поскольку в случае идемпотентного полукольца точная верхняя грань последовательности есть сумма ряда членов этой последовательности, приходим к следующей интерпретации непрерывности сложения:

$$\sum_{n=1}^{\infty} (x_n + a) = \sum_{n=1}^{\infty} x_n + a.$$

Заменив элемент a в правой части рядом с одинаковыми слагаемыми a , придем к утверждению, вытекающему из теоремы 19.5.

Итак, утверждение теоремы 19.5 можно рассматривать как обобщение свойства непрерывности сложения по своим аргументам. Отметим, что умножение в общем случае таким свойством не обладает.

19.3. Замкнутые полукольца

Замкнутое полукольцо — идемпотентное полукольцо, в котором любой ряд сходится, а умножение непрерывно относительно естественного порядка. Непрерывность умножения как бесконечная дистрибутивность. Пример: конечное идемпотентное полукольцо замкнутое. Теорема: $\sum x_n y_m = (\sum x_n)(\sum y_m)$. Итерация $x^* = \sum x^n$.

Замкнутое полукольцо — идемпотентное полукольцо, в котором любой ряд сходится, а умножение непрерывно по своим аргументам относительно естественного порядка полукольца. Непрерывность умножения, например, по второму аргументу означает, что функция $m_a(x) = ax$ является непрерывной относительно естественного порядка полукольца, т.е. для любой монотонной последовательности $\{x_n\}$

$$\sup m_a(x) = m_a(\sup x_n).$$

Учитывая вид функции $m_a(x)$ и свойство $\sup x_n = \sum_{n=1}^{\infty} x_n$, свойство непрерывности умножения можно записать в виде

$$\sum_{n=1}^{\infty} ax_n = a \sum_{n=1}^{\infty} x_n.$$

В таком виде непрерывность умножения можно рассматривать как свойство бесконечной дистрибутивности.

Пример 19.3. Полукольцо $\mathcal{S}_A = (2^A, \cup, \cap, \emptyset, A)$ является замкнутым. В самом деле, операция объединения распространяется не только на счетное, а на любое семейство множеств, причем даже в этом случае пересечение остается дистрибутивным по отношению к сложению.

Полукольцо $\mathcal{S}_{[a,b]} = ([a, b], \max, \min, a, b)$ также замкнуто (его можно рассматривать как модификацию предыдущего полукольца).

Теорема 19.7. Конечное идемпотентное полукольцо замкнуто.

* На самом деле функции $S_l(x)$ и $S_r(x)$ совпадают.

Основная идея доказательства в том, что любой ряд в конечном полукольце фактически является конечной суммой. Действительно, в любом ряде $\sum_{n=1}^{\infty} a_n$ в конечном полукольце члены ряда могут принимать конечное число значений. Поэтому можно указать такой номер N , что все значения встречаются среди первых N членов ряда. Но тогда

$$\sum_{i=1}^N a_i + a_{N+1} + \dots + a_{N+p} = \sum_{i=1}^N a_i.$$

Нетрудно показать, что $S_N = \sum_{i=1}^N a_i$ есть точная верхняя грань последовательности частичных сумм $\{S_n\}$. Таким образом, любой ряд в конечном идемпотентном полукольце сходится.

Заменяя бесконечные суммы (ряды) конечными, легко свести свойство бесконечной дистрибутивности (непрерывность умножения) к свойству обычной дистрибутивности. ►

Теорема 19.8. Для любых двух последовательностей $\{x_n\}$ и $\{y_m\}$ в замкнутом полукольце выполняется равенство

$$\sum_{n,m} x_n y_m = \left(\sum_{n=1}^{\infty} x_n \right) \left(\sum_{m=1}^{\infty} y_m \right).$$

Под суммой в равенстве слева можно понимать двойную сумму

$$\sum_{n=1}^{\infty} \sum_{m=1}^{\infty} x_n y_m,$$

равно как и сумму любой перенумерации двухиндексной последовательности (см. теорему 19.6). Используя свойство бесконечной дистрибутивности, получаем

$$\left(\sum_{n=1}^{\infty} x_n \right) \left(\sum_{m=1}^{\infty} y_m \right) = \sum_{n=1}^{\infty} \left(x_n \left(\sum_{m=1}^{\infty} y_m \right) \right) = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} x_n y_m. \quad \blacktriangleright$$

Для любого элемента x в замкнутом полукольце определена сумма

$$x^* = 1 + x + x^2 + \dots + x^n + \dots = \sum_{i=0}^{\infty} x_i,$$

которую называют *итерацией элемента x* .

19.4. Системы линейных уравнений в полукольцах

Теорема: наименьшими решениями уравнений $x = ax + b$ и $x = xa + b$ в замкнутом полукольце являются $x = a^*b$ и $x = ba^*$. Системы линейных уравнений. Теорема: если S — идемпотентное (замкнутое) полукольцо, то $M_n(S)$ — идемпотентное (замкнутое) полукольцо. Наименьшее решение системы $X = AX + B$ и $X = XA + B$ в случае квадратных матриц. Применение к системам с прямоугольной матрицей B (в частном случае столбцом). Метод Гаусса для линейных систем в полукольцах. Пример: система в $\mathcal{U}_{0,1}$ $x_1 = 0,5x_1 + 0,4x_2 + 0,2$; $x_2 = 0,3x_1 + 0,9x_2 + 0,6$.

В полукольцах нельзя использовать теорию линейных систем в том же виде, как и в полях и кольцах, поскольку операция сложения не имеет обратной. Однако некоторые виды систем линейных уравнений можно решать.

Остановимся на простейших линейных уравнениях $x = ax + b$ и $x = xa + b$. Несложно увидеть, что эти уравнения, как правило, имеют много решений. Однако можно поставить вопрос о поиске наименьшего (или минимального) решения такого уравнения.

Теорема 19.9. В любом замкнутом полукольце уравнение $x = ax + b$ ($x = xa + b$) имеет наименьшее решение $x_{\min}$, причем $x_{\min} = a^*b$ ($x_{\min} = ba^*$).

◀ Рассмотрим уравнение $x = ax + b$. Для уравнения второго типа $x = xa + b$ все рассуждения аналогичны.

В основе доказательства — непрерывность функции $\varphi(x) = ax + b$ в смысле естественного порядка полукольца. Эта функция есть композиция двух функций: $y = ax$ и $z = y + b$. Непрерывность первой есть непрерывность умножения и диктуется определением замкнутого полукольца. Непрерывность второй — это непрерывность сложения, установленная выше.

Поскольку замкнутое полукольцо является индуктивным множеством, уравнение $x = \varphi(x)$, определяемое непрерывной функцией $\varphi(x)$, имеет наименьшее решение, равное точной верхней грани последовательности $\varphi^n(0)$, где $\varphi^1(x) = \varphi(x)$, $\varphi^{k+1}(x) = \varphi(\varphi^k(x))$, $k \in \mathbb{N}$.

В нашем случае $\varphi(0) = b$, $\varphi^2(0) = \varphi(b) = ab + b$, $\varphi^3(0) = \varphi(ab + b) = a^2b + ab + b$. Нетрудно уловить закономерность:

$$\varphi^n(0) = a^{n-1}b + a^{n-2}b + \dots ab + b.$$

Строго это равенство можно доказать методом математической индукции. Из полученного равенства вытекает, что последовательность $\{\varphi^n(0)\}$ есть последовательность частичных сумм ряда

$$b + ab + a^2b + \dots + a^nb + \dots$$

Значит, наименьшее решение $x_{\min}$ уравнения $x = ax + b$ есть сумма этого ряда. Но

$$\sum_{n=0}^{\infty} a^n b = \left(\sum_{n=0}^{\infty} a^n \right) b = a^* b.$$

Поэтому $x_{\min} = a^*b$. ►

Переход к системе линейных уравнений вида

[illegible]

можно рассматривать как переход от скалярного уравнения $x = ax + b$ к матричному уравнению $X = AX + B$, где A — квадратная матрица порядка n , а X и B — матрицы-столбцы высоты n . Можно более широко трактовать матрицы X и B и рассматривать матричное уравнение $X = AX + B$, в котором X и B есть матрицы, состоящие из k столбцов высоты n .

Наиболее интересным оказывается случай уравнения $X = AX + B$, в котором все матрицы квадратные. Такое уравнение можно интерпретировать как скалярное уравнение в полукольце квадратных матриц порядка n . Действительно, нетрудно показать, что множество $M_n(K)$ квадратных матриц порядка n с элементами из данного полукольца K есть полукольцо. При этом, если K идемпотентное полукольцо, то и $M_n(K)$ — идемпотентное полукольцо.

Как устроено отношение порядка в полукольце матриц? Равенство $A+B=B$, где $A=(a_{ij})$, $B=(b_{ij})$, означает, что $a_{ij}+b_{ij}=b_{ij}$, или $a_{ij}\leq b_{ij}$, для любых пар индексов i и j . Таким образом, неравенство $A\leq B$ означает, что $a_{ij}\leq b_{ij}$, $i, j=\overline{1, n}$.

Теорема 19.10. Если K — замкнутое полукольцо, то и $M_n(K)$ — замкнутое полукольцо.

◀ Несложно увидеть, что для ряда $\sum_{k=1}^{\infty} A_k$ частичные суммы будут представлять собой матрицы, составленные из покомпонентных частичных сумм. Пусть $A_k = (a_{ij}^{(k)})$. Тогда $S_m = A_1 + \dots +$

A_m есть матрица $S_m = (s_{ij}^{(m)})$, составленная из частичных сумм $s_{ij}^{(m)}$ рядов, составленных из элементов матриц A_k с одинаковым положением. Пусть матрица $S = (s_{ij})$ состоит из сумм рядов

$$s_{ij} = \sum_{k=1}^{\infty} a_{ij}^{(k)}, \quad i, j = \overline{1, n}.$$

Тогда, во-первых, $S_m \leq S$, $m \in \mathbb{N}$, так как это неравенство выполняется покомпонентно, а во-вторых, для любой матрицы $S' = (s'_{ij})$, удовлетворяющей условию $S_m \leq S'$, $m \in \mathbb{N}$, для каждой пары индексов i и j выполняются соотношения $s_{ij}^{(m)} \leq s'_{ij}$. Поэтому $s_{ij} \leq s'_{ij}$, $i, j = \overline{1, n}$, и $S \leq S'$. Значит, S — точная верхняя грань последовательности $\{S_m\}$ и сумма ряда $\sum_{k=1}^{\infty} A_k$.

Убедимся в непрерывности операции умножения по своим аргументам. Для этого нужно при произвольном ряде $\sum_{k=1}^{\infty} A_k$ и произвольной матрице B проверить равенства

$$\left(\sum_{k=1}^{\infty} A_k\right)B = \sum_{k=1}^{\infty} A_k B, \quad D \sum_{k=1}^{\infty} A_k = \sum_{k=1}^{\infty} B A_k.$$

Проверка неравенств проводится по одной схеме. Поэтому можно ограничиться одним из них, например первым.

Положим, как и выше, $A_k = (a_{ij}^{(k)})$, а также $B = (b_{ij})$. Тогда элементами $[SB]_{ij}$ произведения SB суммы ряда S на матрицу B будут

$$[SB]_{ij} = \sum_{p=1}^n s_{ip} b_{pj} = \sum_{p=1}^n \sum_{k=1}^{\infty} a_{ip}^{(k)} b_{pj} = \sum_{k=1}^{\infty} \sum_{p=1}^n a_{ip}^{(k)} b_{pj} = \sum_{k=1}^{\infty} [A_k B]_{ij}.$$

Здесь мы воспользовались свойством бесконечной коммутативности, а затем свойством бесконечной дистрибутивности (непрерывности умножения). Таким образом,

$$\left(\sum_{k=1}^{\infty}\right)B = SB = \sum_{k=1}^{\infty} A_k B,$$

т.е. бесконечная дистрибутивность в полукольце $M_n(K)$ доказана. ►

Итак, если полукольцо K замкнуто, то и полукольцо $M_n(K)$ тоже замкнуто. В этом случае матричное уравнение $X = AX + B$ (также $X = XA + B$) имеет наименьшее решение. Но такое уравнение на самом деле распадается на совокупность матричных уравнений $X_j = AX_j + B_j$, где B_j — j -й столбец матрицы B . При этом наименьшие решения X_j этих систем в совокупности составляют наименьшее решение уравнения $X = AX + B$. Поскольку наименьшее решение $X_{\min}$ уравнения $X = AX + B$ задается равенством $X_{\min} = A^*B$, то исходя из правил вычисления произведения матриц заключаем, что $X_j = A^*B_j$.

Выберем произвольный столбец $\mathbf{b}$ и рассмотрим матричное уравнение $\mathbf{x} = A\mathbf{x} + \mathbf{b}$. Положив $B = (\mathbf{b}, \mathbf{b}, \dots, \mathbf{b})$ (квадратная матрица B получена повторением одного столбца), найдем решение $X = A^*B$, у которого в силу выбора матрицы B все столбцы будут одинаковые. Эти столбцы будут решениями матричного уравнения $\mathbf{x} = A\mathbf{x} + \mathbf{b}$, они равны $\mathbf{x}_{\min} = A^*\mathbf{b}$.

Вычисление итерации элемента может быть трудной задачей даже в „полукольце скаляров“ K , а уж тем более в полукольце матриц $M_n(K)$. Поэтому непосредственное использование формулы $\mathbf{x}_{\min} = A^*\mathbf{b}$ для наименьшего решения $\mathbf{x}_{\min}$ системы $\mathbf{x} = A\mathbf{x} + \mathbf{b}$ может натолкнуться на трудности.

Существует, однако, способ поиска наименьшего решения системы (19.1), по духу близкий к методу исключения Гаусса. Суть его такова. Из первого уравнения, рассматривая неизвестные $x_2, x_3, \dots, x_n$ как параметры, находим наименьшее решение

$$x_1 = a_{11}^*(a_{12}x_2 + a_{13}x_3 + \dots + a_{1n}x_n + b_1) \quad (19.2)$$

и подставляем это решение вместо x_1 в остальные уравнения системы. В результате мы получим $n - 1$ уравнений с $n - 1$ неизвестным: неизвестное x_1 из уравнений будет исключено. Повторяя процедуру исключения, мы, в конце концов, получим уравнение с одним неизвестным x_n . Решив его, найдем x_n . Зная x_n , по предыдущему уравнению найдем x_{n-1} . Повторяя эту процедуру, получим значения всех неизвестных.

В описанном методе просматривается два этапа. На первом этапе исключения мы приходим к системе с треугольной матрицей. Этот этап называют **прямым ходом метода исключения**. На втором этапе определяются значения неизвестных, начиная с последнего и заканчивая первым. Этот этап **обратный ход метода исключения**.

В отличие от обычных систем линейных уравнений замена первого уравнения системы (19.1) уравнением (19.2) не является эквивалентной в том смысле, что такая замена изменяет множество решений всей системы уравнений. Можно в этой ситуации лишь утверждать, что такая замена приводит к уменьшению множества решений: каждой решение новой системы будет и решением исходной системы. Отсюда можно сделать заключение, что наименьшее решение системы, полученной исключением переменного x_1 , не может быть меньше наименьшего решения исходной системы. Это же относится к решению, полученному методом исключения: оно является решением исходной системы, но, возможно, не наименьшим.

Оказывается, что в действительности метод исключения, хотя и приводит к сокращению множества решений, дает наименьшее решение системы. Чтобы перейти к обоснованию этого факта, отметим следующий важный момент. Наименьшее решение системы линейных уравнений, как функция правых частей системы, является монотонным.

Лемма. Пусть x_1 — наименьшее решение системы $x = Ax + b_1$, а x_2 — наименьшее решение системы $x = Ax + b_2$. Если $b_1 \leq b_2$, то $x_1 \leq x_2$.

◀ Это свойство вытекает из записи наименьшего решения через итерацию матрицы A . Действительно, верны равенства $x_1 = A^*b_1$ и $x_2 = A^*b_2$. В силу монотонности умножения по своим аргументам и неравенства $b_1 \leq b_2$ заключаем, что

$$x_1 = A^*b_1 \leq A^*b_2 = x_2 \quad \blacktriangleright$$

Теорема 19.11. Решение системы $x = Ax + b$, получаемое методом Гаусса, является наименьшим.

◀ Используем блочную запись векторов x, b в виде $x = (x_1, \tilde{x})^T$, $b = (b_1, \tilde{b})^T$, где $\tilde{x}, \tilde{b}$ — соответствующие векторы без первой компоненты. Тогда рассматриваемую систему можно записать в виде

$$\begin{cases} x_1 = a_{11}x_1 + \tilde{a}_{12}^T\tilde{x} + b_1, \\ \tilde{x} = \tilde{a}_{21}x_1 + A_{22}\tilde{x} + \tilde{b}_2. \end{cases}$$

Пусть $x^0 = (x_1^0, \tilde{x}^0)^T$ — наименьшее решение этой системы. Рассмотрим элемент $x_{1*} = a_{11}^*(\tilde{a}_{12}^T\tilde{x}^0 + b_1)$ — наименьшее решение первого уравнения относительно x_1 при значениях остальных неизвестных, соответствующих наименьшему решению всей системы (ниже она будет называться исходной). Поскольку x_1^0 — решение уравнения $x_1 = a_{11}x_1 + \tilde{a}_{12}^T\tilde{x}^0 + b_1$, то $x_{1*} \leq x_1^0$. Используя решение системы x^0 , делаем заключение, что

$$\tilde{x}^0 = \tilde{a}_{21}x_1^0 + A_{22}\tilde{x}^0 + \tilde{b}_2.$$

Следовательно, в силу монотонности сложения и умножения

$$\tilde{a}_{21}x_{1*} + A_{22}\tilde{x}^0 + \tilde{b}_2 \leq \tilde{a}_{21}x_1^0 + A_{22}\tilde{x}^0 + \tilde{b}_2 = \tilde{x}^0.$$

Положив $\tilde{\mathbf{b}}_{2*} = \tilde{\mathbf{b}}^2 + \tilde{\mathbf{x}}^0$, получим равенство

$$\tilde{\mathbf{x}}^0 = \tilde{a}_{21}x_{1*} + A_{22}\tilde{\mathbf{x}}^0 + \tilde{\mathbf{b}}_{2*},$$

означающее, что вектор $(x_{1*}, \tilde{\mathbf{x}}^0)^T$ является решением системы

$$\begin{cases} x_1 = a_{11}x_1 + \tilde{a}_{12}^T\tilde{\mathbf{x}} + b_1, \\ \tilde{\mathbf{x}} = \tilde{a}_{21}x_1 + A_{22}\tilde{\mathbf{x}} + \tilde{\mathbf{b}}_{2*}. \end{cases}$$

Но тогда наименьшее решение $\mathbf{x}^{00}$ этой системы не превышает $\mathbf{x}^0$. Следовательно, выполняются неравенства

$$\mathbf{x}^{00} \leq (x_{1*}, \tilde{\mathbf{x}}^0)^T \leq \mathbf{x}^0 = (x_1^0, \tilde{\mathbf{x}}^0)^T.$$

Однако, при этом правые части второй системы превышают правые части первой, и мы имеем и такое неравенство: $\mathbf{x}^0 \leq \mathbf{x}^{00}$. Поэтому в действительности

$$\mathbf{x}^{00} = (x_{1*}, \tilde{\mathbf{x}}^0)^T = \mathbf{x}^0 = (x_1^0, \tilde{\mathbf{x}}^0)^T$$

и $x_1^0 = x_{1*}$.

Подставив во вторую часть исходной системы вместо x_1 выражение $x_1 = a_{11}^*(\tilde{a}_{12}^T\tilde{\mathbf{x}} + b_1)$, получим систему, для которой столбец $\mathbf{x}^0$ является решением. Поскольку все решения новой системы в то же время являются решениями исходной системы, то $\mathbf{x}^0$ будет наименьшим решением новой системы.

Тем самым мы доказали, что в результате исключения неизвестного x_1 мы получаем систему с тем же наименьшим решением, что и исходная, т.е. в смысле наименьшего решения исключение неизвестных — эквивалентное преобразование. ►

Пример 19.4. Рассмотрим систему в полукольце $\mathcal{U}_{[0,1]}$

$$\begin{cases} x_1 = 0,5x_1 + 0,4x_2 + 0,2; \\ x_2 = 0,3x_1 + 0,9x_2 + 0,6. \end{cases}$$

В рассматриваемом полукольце итерация любого элемента равна единице полукольца:

$$1 + x + x^2 + x^3 + \dots = 1,$$

так как $x^n \leq 1$ для любой степени n .

Из первого уравнения

$$x_1 = 0,5^*(0,4x_2 + 0,2) = 0,4x_2 + 0,2.$$

Подставив найденное представление во второе уравнение, получим:

$$x_2 = 0,3(0,4x_2 + 0,2) + 0,9x_2 + 0,6,$$

или

$$x_2 = (0,3 \cdot 0,4 + 0,9)x_2 + (0,3 \cdot 0,2 + 0,6).$$

Выполнив операции (сумма — максимум, произведение — минимум), находим:

$$x_2 = 0,9x_2 + 0,6.$$

Следовательно, $x_2 = 0,9^* \cdot 0,6 = 0,6$ и $x_1 = 0,4 \cdot 0,6 + 0,2 = 0,4$. Итак, наименьшее решение рассматриваемой системы: $x_1 = 0,4$, $x_2 = 0,6$.

19.5. Симметричные полукольца

Идемпотентное полукольцо $(S, +, \cdot)$ симметрично, если алг. система $(S, \cdot, +)$ тоже идемпотентное полукольцо. Дополнительные аксиомы: а) коммутативность умножения; б) дистрибутивность сложения по отношению к умножению; в) идемпотентность умножения; г) аннулирующее свойство единицы по отношению к сложению. Пример: $\mathcal{S}_A = (2^A, \{\cup, \cap, \emptyset, A\})$. Двойственное полукольцо. Двойственность в симметричных полукольцах. Свойства: а) $0 \leq x \leq 1$. б) тождества поглощения $x + xy = x$ и $x(x + y) = x$; в) $x \leq y \Leftrightarrow xy = x$; г) $xy = 1 \Rightarrow x = y = 1$; д) $x_1 x_2 \dots x_k = \inf \{x_1, x_2, \dots, x_k\}$. Булева алгебра — симметричное полукольцо, в котором дополнительно есть унарная операция — дополнение $\bar{x}$, удовлетворяющая аксиомам $x + \bar{x} = 1$, $x \cdot \bar{x} = 0$. Свойства: 1) единственность; 2) нильпотентность $\bar{\bar{x}} = x$; 3) законы де Моргана $\overline{x + y} = \bar{x} \cdot \bar{y}$, $\overline{xy} = \bar{x} + \bar{y}$. Пример булевой алгебры — двухэлементная булева алгебра $\mathcal{B}$. Декартово произведение булевых алгебр, декартова степень булевой алгебры и булев куб $\mathcal{B}^n$. Булевы векторы. Теорема: любая конечная булева алгебра изоморфна $\mathcal{B}^n$.

Идемпотентное полукольцо $(S, +, \cdot)$ симметрично, если алг. система $(S, \cdot, +)$ тоже идемпотентное полукольцо. Дополнительные аксиомы: а) коммутативность умножения; б) дистрибутивность сложения по отношению к умножению; в) идемпотентность умножения; г) аннулирующее свойство единицы по отношению к сложению. Двойственное полукольцо. Двойственность в симметричных полукольцах.

Свойства:

- а) $0 \leq x \leq 1$;
- б) тождества поглощения $x + xy = x$ и $x(x + y) = x$;
- в) $x \leq y \Leftrightarrow xy = x$;
- г) $xy = 1 \Rightarrow x = y = 1$;
- д) $x_1 x_2 \dots x_k = \inf \{x_1, x_2, \dots, x_k\}$;

◀ Первое свойство следует из равенств $x + 0 = x$, $x + 1 = 1$ (второе равенство есть аннулирующее свойство единицы по отношению к сложению).

Первое из тождеств поглощения вытекает из равенств

$$x + xy = x \cdot 1 + xy = x(1 + y) = x \cdot 1 = x$$

(опять использовано аннулирующее свойство единицы по сложению). Второе тождество поглощения является двойственным к первому и следует из принципа двойственности.

Третье свойство можно получить из тождеств поглощения. Если $x \leq y$, то $x + y = y$. В силу второго тождества поглощения $xy = x(x + y) = x$. Наоборот, если $xy = x$, то в соответствии с первым тождеством поглощения $x + y = xy + y = y$, что равносильно неравенству $x \leq y$.

Наконец, последние два свойства вытекают из того, что отношение порядка двойственного полукольца является обратным (двойственным) к естественному порядку полукольца. Поэтому свойство г) двойственно к свойству $a + b = 0 \Rightarrow a = b = 0$, а свойство д) является двойственным по отношению к равенству

$$x_1 + x_2 + \dots + x_k = \sup \{x_1, x_2, \dots, x_k\}. \quad \blacktriangleright$$

Замечание. Принцип двойственности для симметричных полуколец можно расширить, если добавить двойственность $\inf$ – $\sup$.

Булева алгебра — симметричное полукольцо K с дополнительной унарной операцией **дополнения** $x \rightarrow \bar{x}$, которая со сложением и умножением связана условиям

$$x + \bar{x} = 1, \quad x \cdot \bar{x} = 0. \quad (19.3)$$

Примером булевой алгебры является полукольцо $\mathcal{S}_A = (2^A, \{\cup, \cap, \emptyset, A\})$. В этом полукольце каждому множеству X соответствует дополнение $\bar{X} = A \setminus X$, удовлетворяющее условиям

$$X \cup \bar{X} = A, \quad X \cap \bar{X} = \emptyset. \quad (19.4)$$

Это полукольцо часто называют **алгеброй множеств**.

Теорема 19.12. В симметричном полукольце K для каждого $x \in K$ элемент $\bar{x}$, удовлетворяющий условиям (19.3), определен однозначно.

◀ Рассмотрим два элемента x_1 и x_2 , удовлетворяющие равенствам

$$x + x_1 = 1, \quad xx_1 = 0, \quad x + x_2 = 1, \quad xx_2 = 0.$$

Умножив первое равенство на x_2 и учтя, что $xx_2 = 0$, находим

$$x_1x_2 = xx_2 + x_1x_2 = x_2,$$

откуда $x_2 \leq x_1$. Повторив это рассуждение со вторым и третьим равенствами, получаем $x_1 \leq x_2$. Следовательно, $x_1 = x_2$. ►

Из доказанной теоремы вытекает, что дополнение в симметричном полукольце полностью определяется свойствами сложения и умножения. Дополнение в симметричном полукольце может и не существовать, но если его можно ввести, то единственным способом.

Примером симметричного полукольца, в котором нет дополнения, служит алгебра $\mathcal{U}_{a,b} = ([a, b], \max, \min, a, b)$. Если бы дополнение существовало, должны были выполняться равенства $\max\{x, \bar{x}\} = b$, $\min\{x, \bar{x}\} = a$, что возможно только для $x = a$ или $x = b$.

Свойства дополнения:

- 1) нильпотентность $\bar{\bar{x}} = x$;
- 2) законы де Моргана $\overline{x + y} = \bar{x} \cdot \bar{y}$, $\overline{x \cdot y} = \bar{x} + \bar{y}$;
- 3) $x\bar{y} = 0 \Rightarrow x \leq y$;
- 4) $x + \bar{y} = 1 \Rightarrow y \leq x$.

◀ Первое свойство вытекает из симметричности равенств (19.4). Докажем второе свойство — законы де Моргана. Отметим, что два закона де Моргана являются двойственными друг к другу. Поэтому достаточно доказать один из них, например первый.

Первый закон де Моргана можно интерпретировать так: элемент $\bar{x} \cdot \bar{y}$ является дополнением к элементу $x + y$. Чтобы убедиться в этом, достаточно проверить выполнение равенств (19.4). Первое равенство (используем дистрибутивность сложения относительно умножения):

$$\bar{x}\bar{y} + x + y = (\bar{x} + x)(\bar{y} + y) + y = \bar{y} + x + y = 1 + x = 1.$$

Второе равенство:

$$\bar{x}\bar{y}(x + y) = \bar{x}(\bar{y}x + \bar{y}y) = \bar{x}\bar{y}x = 0\bar{y} = 0.$$

Третье и четвертое свойства двойственны друг другу. Можно ограничиться доказательством лишь одного из них. Если $x\bar{y} = 0$, то

$$xy = xy + x\bar{y} = x(y + \bar{y}) = x \cdot 1 = x.$$

Равенство $xy = x$ равносильно условию $x \leq y$. ►

Пример булевой алгебры — двухэлементная булева алгебра $\mathcal{B}$. Всего два элемента 0 и 1. Действие операций таково

$$0 + 0 = 0, \quad 1 + 0 = 0 + 1 = 1 + 1 = 1, \quad 1 \cdot 1 = 1, \quad 0 \cdot 1 = 1 \cdot 0 = 0 \cdot 0 = 0.$$

Операции этой алгебры можно определить как максимум и минимум. При этом минимум совпадает с операцией умножения, а максимум можно определить выражением $\max\{x, y\} = x + y - xy$.

Рассмотрим булевы алгебры $B_1, B_2, \dots, B_k$. Тогда на декартовом произведении $B_1 \times B_2 \times \dots \times B_k$ можно ввести структуру булевой алгебры, рассматривая на кортежах поэлементные операции:

$$\begin{aligned} (x_1, x_2, \dots, x_k) + (y_1, y_2, \dots, y_k) &= (x_1 + y_1, x_2 + y_2, \dots, x_k + y_k), \\ (x_1, x_2, \dots, x_k) \cdot (y_1, y_2, \dots, y_k) &= (x_1 \cdot y_1, x_2 \cdot y_2, \dots, x_k \cdot y_k), \\ \overline{(x_1, x_2, \dots, x_k)} &= (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_k). \end{aligned}$$

Несложно проверить выполнение аксиом булевой алгебры (включая равенства (19.3)). Полученная таким образом булева алгебра называется **декартовым произведением булевых алгебр** $B_1, B_2, \dots, B_k$. Частным случаем этой конструкции является **декартова степень B^n булевой алгебры B** . Декартову степень B^n двухэлементной булевой алгебры B называют n -мерным **булевым кубом**, а элементы этой алгебры, т.е. кортежи длины n из нулей и единиц, — n -мерными **булевыми векторами**.

Булева алгебра B^n — пример конечной булевой алгебры (она содержит 2^n элементов). Оказывается, что других конечных булевых алгебр нет. Чтобы доказать это, выделим в конечной булевой алгебре B определенные элементы. Наряду с естественным порядком $x \leq y$ в B будем рассматривать строгий порядок $x < y$, означающий, что $x \leq y$ и $x \neq y$.

Элемент $x \neq 0$ алгебры B будем называть атомом, если не существует ни одного элемента y , удовлетворяющего условию $0 < y < x$. Если элемент x не является атомом, то для него можно выбрать элемент x_1 , для которого $0 < x_1 < x$. Элемент x_1 либо атом, либо имеет x_2 , удовлетворяющий условию $0 < x_2 < x_1$. Таким образом, каждый элемент алгебры является концом цепочки последовательно убывающих элементов. В бесконечном случае такая цепочка может быть бесконечной (например, в $\mathcal{U}_{0,1}$ цепочка $1, 1/2, 1/3, \dots$). В конечной же алгебре B такая цепочка должна быть конечной. Самый маленький элемент в ней — атом, подчиненный исходному элементу x . Совокупность всех атомов конечной булевой алгебры образует своего рода базис в ней.

Пусть $a_1, a_2, \dots, a_k$ — атомы в булевой алгебре B . Рассмотрим выражение

$$\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_k a_k,$$

где α_i либо нуль, либо единица булевой алгебры. Это выражение уместно назвать линейной комбинацией атомов $a_1, a_2, \dots, a_k$. Фактически линейная комбинация — это сумма некоторого атомов из рассматриваемой системы

Лемма 19.1. Если

$$\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_k a_k = \beta_1 a_1 + \beta_2 a_2 + \dots + \beta_k a_k, \quad (19.5)$$

где $\alpha_i, \beta_i \in \{0, 1\}$, $i = \overline{1, k}$, то $\alpha_i = \beta_i$, $i = \overline{1, k}$.

◀ Отметим, что если $a_1, a_2, \dots, a_k$ — различные атомы, то произведение $a_1 \bar{a}_2 \bar{a}_3 \dots \bar{a}_k$ отлично от нуля. Действительно, если $a_1 \bar{a}_2 \bar{a}_3 \dots \bar{a}_k = 0$, то по свойству дополнения $a_1 \bar{a}_2 \bar{a}_3 \dots \bar{a}_{k-1} \leq a_k$. Но так как a_k — атом, то левая часть либо равна нулю, либо a_k . Но во втором случае заключаем, что $a_1 \leq a_k$, а это для двух различных атомов невозможно. Итак, $a_1 \bar{a}_2 \bar{a}_3 \dots \bar{a}_{k-1} = 0$. Повторяя процедуру, заключаем, что $a_1 = 0$, что противоречит определению атома.

Пусть $a_1, a_2, \dots, a_k$ — различные атомы и имеет место равенство (19.5). Домножим равенство на произведение $\bar{a}_2 \bar{a}_3 \dots \bar{a}_{k-1} \leq a_k$. Тогда в обеих частях равенства уничтожатся все слагаемые кроме первого, поскольку в эти слагаемые будет входить произведение вида $a_i \bar{a}_i$. В результате получим, что

$$\alpha_1 a_1 \bar{a}_2 \bar{a}_3 \dots \bar{a}_{k-1} \leq a_k = \beta_1 a_1 \bar{a}_2 \bar{a}_3 \dots \bar{a}_{k-1} \leq a_k.$$

Отсюда вытекает, что $\alpha_1 = \beta_1$, поскольку иначе один из этих коэффициентов равен нулю, а второй единице, а следовательно, одна часть равенства нулевая, а вторая — нет. Повторяя эти рассуждения для остальных индексов, получим утверждение леммы. ►

Лемма 19.2. Для любого элемента y конечной алгебры B имеет место представление

$$y = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n,$$

где $a_1, a_2, \dots, a_n$ — совокупность всех атомов алгебры B , а коэффициенты α_i определяются следующим образом: $\alpha_i = 1$, если $a_i \leq y$ и $\alpha_i = 0$, если a_i не подчинен y .

◀ Положим $y_* = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$, где $\alpha_i = 1$ при $a_i \leq y$ и $\alpha_i = 0$ в противном случае. Тогда y_* есть сумма всех атомов, подчиненных y и, следовательно, $y_* \leq y$. Рассмотрим $c = y\bar{y}_*$. Нам достаточно показать, что $y \leq y_*$, а это равносильно соотношению $c = y\bar{y}_* = 0$. Предполагая, что это соотношение неверно, заключаем, что c имеет хотя бы один подчиненный атом. Пусть это a_1 (иначе можно просто изменить нумерацию атомов). Значит, $a_1 \leq c$. Но тогда $a_1 \leq y$ и в сумме, представляющей y_1 , $\alpha_1 = 1$. Отсюда заключаем, что

$$a_1 c = a_1 y \cdot \overline{\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n} = a_1 y \prod_{a_j \leq y} \bar{a}_j = 0,$$

так как $\bar{a}_1$ входит в произведение. В то же время в силу неравенства $a_1 \leq c$ имеем $a_1 c = a_1$, откуда $a_1 = 0$, а это противоречит условию, что a_1 — атом. Итак, предположение $c \neq 0$ приводит к противоречию. Значит, $c = 0$ и $y = y_1 = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$. ▶

Теорема 19.13. Любая конечная булева алгебра изоморфна некоторой алгебре $\mathcal{B}^n$.

◀ Пусть $a = 1$, $a_2, \dots, a_n$ — набор всех атомов конечной алгебры B . Согласно доказанным леммам, каждый элемент $y \neq 0$ представим в виде линейной комбинации

$$y = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n,$$

и притом единственным образом. Это верно и для нуля алгебры: достаточно взять линейную комбинацию с нулевыми коэффициентами. Каждому $y \in B$ ставим в соответствие n -мерный булев вектор $(\alpha_1, \alpha_2, \dots, \alpha_n)$ из коэффициентов линейной комбинации. Получим биективное отображение $\varphi: B \rightarrow \mathcal{B}^n$. Покажем, что это отображение есть гомоморфизм булевых алгебр, т.е. оно сохраняет три булевых операции. Для сложения это очевидно, поскольку

$$(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n) + (\beta_1 a_1 + \beta_2 a_2 + \dots + \beta_n a_n) = (\alpha_1 + \beta_1) a_1 + (\alpha_2 + \beta_2) a_2 + \dots + (\alpha_n + \beta_n) a_n,$$

где коэффициенты суммируются по правилу сложения элементов в $\mathcal{B}$. Аналогично проверяется равенство

$$(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n)(\beta_1 a_1 + \beta_2 a_2 + \dots + \beta_n a_n) = (\alpha_1 \beta_1) a_1 + (\alpha_2 \beta_2) a_2 + \dots + (\alpha_n \beta_n) a_n,$$

в котором умножение коэффициентов есть умножение алгебры $\mathcal{B}$ (необходимо учесть, что произведение двух разных атомов равно нулю, поскольку должно быть не более каждого из атомов). Наконец, учитывая полученные равенства, а также равенство

$$a_1 + a_2 + \dots + a_n = 1$$

(элементу 1 подчинены все атомы алгебры), заключаем, что дополнением к элементу $y = \alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n$ является элемент $\bar{y} = \bar{\alpha}_1 a_1 + \bar{\alpha}_2 a_2 + \dots + \bar{\alpha}_n a_n$, так как

$$\begin{aligned} y + \bar{y} &= (\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n) + (\bar{\alpha}_1 a_1 + \bar{\alpha}_2 a_2 + \dots + \bar{\alpha}_n a_n) = \\ &= (\alpha_1 + \bar{\alpha}_1) a_1 + (\alpha_2 + \bar{\alpha}_2) a_2 + \dots + (\alpha_n + \bar{\alpha}_n) a_n = a_1 + a_2 + \dots + a_n = 1 \end{aligned}$$

и

$$y\bar{y} = (\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n)(\bar{\alpha}_1 a_1 + \bar{\alpha}_2 a_2 + \dots + \bar{\alpha}_n a_n) = (\alpha_1 \bar{\alpha}_1) a_1 + (\alpha_2 \bar{\alpha}_2) a_2 + \dots + (\alpha_n \bar{\alpha}_n) a_n = 0.$$

Итак, построенное отображение биективно и сохраняет все операции, т.е. представляет собой изоморфизм. ▶

19.6. Решетки

Полурешетка — коммутативная полугруппа с дополнительным свойством идемпотентности. Отношение порядка в полурешетке. Теорема: упорядоченное множество имеет структуру полурешетки, если любое двухэлементное множество имеет точную верхнюю грань. Двойственность. Верхняя $(L, \sup)$ и нижняя $(L, \inf)$ полурешетки упорядоченного множества. Решетка — алгебра $(R, \vee, \wedge)$, которая относительно каждой операции полурешетка, а обе операции связаны тождествами поглощения $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$. Пример: любое симметричное полукольцо есть решетка. Пример: алгебра $((a, b), \max, \min)$ есть решетка, но не полукольцо (нет нуля и единицы). Двойственность порядков решетки. Теорема: любое упорядоченное множество, в котором любое двухэлементное множество имеет $\sup$ и $\inf$, есть решетка. Решетка и дистрибутивность. Примеры недистрибутивных решеток (пентагон и диамант). Теорема: дистрибутивная решетка с 0 и 1 есть симметричное полукольцо.

К понятию булевой алгебры можно подходить с различных сторон. Во-первых, булеву алгебру легко превратить в кольцо с единицей, если заменить булево сложение $+$ операцией $x \oplus y = x\bar{y} + \bar{x}y$. Можно непосредственно проверить, что относительно этой операции булева алгебра есть аддитивная группа и что умножение дистрибутивно относительно введенной операции. В результате мы получаем кольцо с идемпотентным умножением — булево кольцо. Наоборот, булево кольцо всегда коммутативно, а сложение удовлетворяет условию $x + x = 0$. Заменяя в булевом кольце сложение операцией $x + y + xy$, получим симметричное полукольцо. В нем нетрудно ввести дополнение по формуле $\bar{x} = x + 1$. В этом случае $x\bar{x} = x(x + 1) = x^2 + x = x + x = 0$, $x + \bar{x} = x + x + 1 = 0 + 1 = 1$.

Таким образом, теории булевых алгебр и булевых колец легко трансформируются одна в другую. Еще один подход связан с понятием решетки.

Полурешетка — коммутативная полугруппа, в которой операция идемпотентна. Идемпотентность операции означает, что в полурешетке, как и в полукольце, возникает отношение порядка $x \leq y \Leftrightarrow x + y = y$. На полурешетку переносится теорема из теории полуколец о том, что конечное множество имеет точную верхнюю грань, равную сумме элементов множества. Поэтому операция полурешетки восстанавливается по отношению порядка согласно формуле $x + y = \sup \{x, y\}$.

Отметим, что не всякое упорядоченное множество можно превратить в полурешетку, в упорядоченном множестве не всякое конечное множество может иметь точную верхнюю грань. Например, зададим на множестве из трех элементов $-1, 0, 1$ отношение $x \preceq y \Leftrightarrow |x| < |y|$ или $x = y$. Тогда двухэлементное множество $\{-1, 1\}$ не будет иметь ни одной верхней грани, а потому и точной верхней грани.

Теорема 19.14. Каждое упорядоченное множество $(M, \leq)$, в котором каждое двухэлементное множество имеет точную верхнюю грань, есть полурешетка с операцией $x + y = \sup \{x, y\}$.

◀ Очевидно, что формула $x + y = \sup \{x, y\}$ задает корректную операцию на упорядоченном множестве, если каждое двухэлементное множество имеет точную верхнюю грань*. Остается проверить аксиомы решетки. Но коммутативность и идемпотенность очевидны. Кроме того, очевидно и соотношение

$$\sup \{\sup \{x, y\}, z\} = \sup \{x, y, z\}.$$

Во-первых, по условиям теоремы левая часть определена и является верхней гранью множества, составленного из элементов x, y, z . Во-вторых, любая верхняя грань g множества из элементов x, y, z является верхней гранью множества из элементов $\sup \{x, y\}$ и z , т.е. $\sup \{\sup \{x, y\}, z\} \leq g$. Следовательно, $\sup \{\sup \{x, y\}, z\}$ — точная верхняя грань множества $\{x, y, z\}$. В силу произвольности x, y, z заключаем, что

$$\sup \{\sup \{x, y\}, z\} = \sup \{x, y, z\} = \sup \{x, \sup \{y, z\}\}. \quad \blacktriangleright$$

*Здесь следует выделить случай $x = y$, в котором элементы x и y есть на самом деле один элемент и двухэлементного множества не возникает. В этом случае полагаем $x + x = x$.

На упорядоченном множестве M могут возникнуть две решеточных операции: одна — точная верхняя грань, другая — точная нижняя грань (это точная верхняя грань для обратного порядка). Для этого достаточно, чтобы любое двухэлементное множество имело и точную верхнюю грань, и точную нижнюю. При этом алгебру $(M, \sup)$ называют **верхней полурешеткой**, а алгебру $(V, \inf)$ — **нижней полурешеткой**.

Решеткой называют алгебру $(M, \vee, \wedge)$ с двумя бинарными операциями $\vee$ (решеточное объединение) и $\wedge$ (решеточное пересечение), которая, во-первых, является полурешеткой относительно каждой из двух операций, а во-вторых, эти операции связаны **тождествами поглощения**

$$a \wedge (a \vee b) = a, \quad a \vee (a \wedge b) = a.$$

Примером полурешетки является любое симметричное полукольцо. Однако этим примером понятие полурешетки не исчерпывается. Алгебра $((a, b); \max; \min)$ является полурешеткой, но не является симметричным полукольцом, так как обе операции не имеют нейтрального элемента.

В полурешетке каждая из операций порождает свое отношение порядка, но два порядка в силу тождеств поглощения являются взаимно обратными. В самом деле, если $x \vee y = y$, то $x \wedge y = x \wedge (x \vee y) = x$. Иначе говоря из отношения $x \leq_u y$, соответствующего решеточному объединению, вытекает отношение $y \leq_l x$, соответствующее решеточному пересечению. В силу симметрии верно и обратное.

Уже отмечено, что симметричное полукольцо есть решетка, а решетка может не быть симметричным полукольцом из-за отсутствия нуля и единицы. Второе расхождение между двумя алгебраическими структурами — свойство дистрибутивности каждой из операций относительно другой. В решетке свойство дистрибутивности может отсутствовать.

Пример 19.5. Рассмотрим объединение двух линейно упорядоченных множеств M_1 и M_2 , имеющих общие наименьший x_* и наибольший x^* элементы (например, левая и правая полуокружности на плоскости, точки которых упорядочены по ординате). Выберем два элемента x_1 и x_2 . Если эти элементы принадлежат одному линейно упорядоченному множеству, то они сравнимы, например $x_1 \leq x_2$. Тогда $\sup \{x_1, x_2\} = x_2$ и $\inf \{x_1, x_2\} = x_1$. Если же эти элементы из разных частей, то $\sup \{x_1, x_2\} = x^*$ и $\inf \{x_1, x_2\} = x_*$. Теперь нетрудно убедиться в том, что равенство

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

может нарушаться. Пусть $x, y \in M_1, z \in M_2$, причем $y < x$. Тогда $y \vee z = x^*$ и $x \wedge (y \vee z) = x \wedge x^* = x$. В то же время $(x \wedge y) \vee (x \wedge z) = y \vee x_* = y$.

Частным случаем рассмотренной схемы является **пентагон** — упорядоченное множество их пяти элементов (рис. 19.1). Отношением неравенства связаны любые два элемента, расположенных на одном пути снизу вверх.

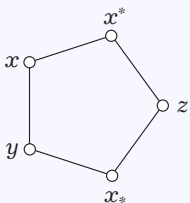


Рис. 19.1

Решетка называется **дистрибутивной**, если каждая из ее операций дистрибутивна относительно другой.

Теорема 19.15. Дистрибутивная решетка, у которой каждая операция имеет нейтральный элемент (0 относительно объединения, 1 относительно пересечения) является симметричным полукольцом.

◀ В силу симметрии достаточно убедиться, что выполняются аксиомы основного полукольца. Отметим, что в силу условий теоремы решетка является коммутативным моноидом с идемпотентной операцией и относительно решеточного объединения, и решеточного пересечения. Решеточное пересечение дистрибутивно относительно решеточного объединения. Остается установить аннулирующее свойство нуля. Используя одно из тождеств поглощения, для любого элемента a решетки получаем

$$0 \wedge a = 0 \vee (0 \wedge a) = 0,$$

а это и есть аннулирующее свойство нуля решетки. ►

ОГЛАВЛЕНИЕ

4. Псевдорешения и псевдообратная матрица	1
4.1. Метод наименьших квадратов	1
4.2. Псевдорешения	3
4.3. Скелетное разложение	4
4.4. Псевдообратная матрица	6
4.5. Проектирование на подпространство	10
9. Жорданова нормальная форма	12
9.1. Корневые подпространства	12
9.2. Жорданова нормальная форма	14
9.3. Комплексные корни	19
9.4. Теорема Кэли — Гамильтона	20
13. Операции над тензорами	22
13.1. Понятие тензора	22
13.2. Матричная запись тензоров	23
13.3. Преобразование тензоров, записанных в матричной форме	24
14. Множества и отношения	26
14.1. Алгебра множеств	26
14.2. Отображения и соответствия	30
14.3. Отношения и операции	32
14.4. Элементы математической логики	34
14.5. Мощность множеств	35
16. Кольца и поля	36
16.1. Кольца	36
16.2. Специальные типы колец	36
16.3. Гомоморфизмы колец и факторизация	36
16.4. Модули и алгебры	36
16.5. Алгебры на поле	40
17. Кольцо многочленов	43
17.1. Определение кольца многочленов	43
17.2. Деление с остатком и его свойства	45
17.3. Разложение на неприводимые множители	49
17.4. Использование делимости в теории шифрования	49
17.5. Кватернионы	50
19. Полукольца и булевы алгебры	51
19.1. Определение полукольца	51
19.2. Ряды в полукольцах	53
19.3. Замкнутые полукольца	57
19.4. Системы линейных уравнений в полукольцах	58
19.5. Симметричные полукольца	63
19.6. Решетки	67