Лекция №7

04.10.24

2. Группоиды, полугруппы, группы (продолжение)

Далее операцию группы обозначаем «точкой», которая обычно опускается (как при записи числового умножения).

Теорема. В каждой группе:

1) выполняются *законы сокращения*:
2) $ab = ac \Rightarrow b = c;$
   $ba = ca \Rightarrow b = c.$
3) однозначно разрешимы уравнения:
   $ax = b(1),$
   $xa = b(2),$
   $axb = c(3).$
   (относительно неизвестного *x*.)

Доказательство. 1) Если $ab = ac$, то, умножая обе части равенства слева на a^{-1}, получим, что получим $b = c.$ Второе условие доказывается также (но нужно умножать на a^{-1} справа).

2) Рассмотрим уравнение (1). Легко проверить, что $x = a^{-1}b$ есть решение:

$a(a^{-1}b) = (aa^{-1})b = b$.

Теперь надо доказать, что это единственное решение.

Пусть x_0 есть решение уравнения (1). Подстановка решения в уравнение превращает его в равенство: $ax_0 = b$. Умножая обе части этого равенства слева на элемент a^{-1}, $a^{-1}(ax_0) = a^{-1}b \Rightarrow x_0 = a^{-1}b$, что и означает, что только $x = a^{-1}b$ есть решение.

Аналогично доказывается, что решениями уравнений (2) и (3) соответственно будут $x = ba^{-1}$ и $x = a^{-1}cb^{-1}$.

Понятие степени элемента группы

В *полугруппе* можно определить любую натуральную (положительную целую) степень элемента, полагая $a^n = (a^{n-1})a, n \geq 2; a^1 = a$.

В *моноиде* дополнительно определяется нулевая степень любого элемента как равная нейтральному элементу.

В *группе* может быть определена произвольная *целая* степень, и отрицательная степень определяется следующим образом: $a^{-n} \rightleftharpoons (a^n)^{-1}, n \geq 0$

Без доказательства сформулируем теорему о свойствах степеней:

Теорема. Для произвольных целых чисел *m* и *n* выполняется:

1) $a^{m+n} = a^m a^n$
2) $a^{mn} = (a^m)^n$ (в частности, $a^{-n} = (a^{-1})^n$)
3) Если элементы *a* и *b* коммутируют, то есть $ab = ba$, то $(ab)^n = a^n b^n$

Способы записи группы

В общих рассуждениях о группах используют два способа обозначения (записи)операций группы: *мультипликативную запись* и *аддитивную запись*. При мультипликативной записи бинарную операцию обозначают точкой, которую часто опускают, и называют *умножением* (результат, соответственно, *произведением*), обратный к a элемент обозначают a^{-1}, а нейтральный называют *единицей* и записывают часто, как число 1 (хотя в общем случае это совсем не число). Выше мы и пользовались именно такой записью.

При аддитивной записи бинарную операцию обозначают «плюсом» (+) и называют *сложением* (результат – *сумма*). Нейтральный элемент называют *нулем* и обозначают, как число 0 (и опять надо понимать, что в общем случае это никакое не число). Обратный к a элемент обозначают $-a$ и называют *противоположным к* a.

Аддитивную запись в основном используют при изучении коммутативных групп.

При использовании аддитивной записи вводят такое обозначение степени элемента:

$$n \circ a \rightleftharpoons \underbrace{(a + a + \ldots + a)}_{n},$$

$$-n \circ a \rightleftharpoons -(n \circ a) = n \circ (-a) = \underbrace{(-a - a - \ldots - a)}_{n}, n > 0;$$

$$0 \circ a \rightleftharpoons 0.$$

Так вводится аддитивная степень элемента при использовании аддитивной записи группы.

Вычитание и деление

Пусть дана коммутативная группа в аддитивной записи: $(G, +, 0)$.

Рассмотрим уравнение

$a + x = b$.

Его решение $x = -a + b = b + (-a)$. Сумму $b + (-a)$ обозначают как $b - a$ и называют *разностью* элементов *b* и *a*. Так, в частности, определяется разность векторов в произвольном линейном пространстве,

Коммутативная группа может быть представлена и в мультипликативной записи (например, упомянутые выше мультипликативные числовые группы).

В этом случае решение уравнения $ax = b$ можно записать так: $x = a^{-1}b = ba^{-1} \rightleftharpoons \frac{b}{a}$.

Так вводится понятие *частного от деления* (и, соответственно, сама операция *деления*, как выше – *вычитания*). Но это имеет смысл только для коммутативных групп!

Легко видеть, что в коммутативной группе все виды уравнений сводятся к уравнению (1).

3. Группы подстановок

Пусть $M = \{1, 2, ..., n\}$ - конечное множество, далее, как правило, отождествляемое с множеством первых *n* натуральных чисел.

Симметрическая группа этого множества, называемая симметрической группой степени *n* и обозначаемая S_n, состоит из биекций его на себя; эти биекции, взаимно однозначные отображения, называются *подстановками* и стандартно записываются в виде двустрочной матрицы:

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

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

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

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[1].

4) Циклы, разложение на независимые циклы

Пусть фиксированы элементы $1 \le i_1, i_2, ..., i_k \le n, 1 \le k \le n$ и подстановка σ действует так:

$$i_1 \to i_2 \to i_3 \to ... \to i_k \to i_1 ,$$

то есть $\sigma(i_j) = i_{j+1}, 1 \le j \le k-1$ и $\sigma(i_k) = i_1$, причем для всякого $m \in M \setminus \{i_1, ..., i_k\}$ $\sigma(m) = m$.

Такая подстановка называется циклом длины k и записывается в виде $(i_1 i_2 i_3 ... i_k)$. Из определения ясно, что любая циклическая перестановка элементов цикла, то есть элементов $i_1, i_2, ..., i_k$, даст тот же самый цикл, ту же самую подстановку. Например, (12345)=(23451)=(34512) и т. д. Кроме того, цикл оставляет неподвижными все элементы исходного множества, которые не входят в цикл. Цикл длины 1 есть, как нетрудно сообразить, тождественная подстановка. Наибольшая длина цикла в группе S_n равна n.

Полезно заметить, что число циклов длины n в таком случае равно $\frac{n!}{n} = (n-1)!$, так как существует ровно n циклических перестановок элементов цикла.

Понятно также, что цикл, обратный данному, получается инвертированием элементов исходного цикла: $(i_1 i_2 ... i_{k-1} i_k)^{-1} = (i_k i_{k-1} ... i_2 i_1)$.

Два цикла называются независимыми, если они не имеют общих элементов. Важное свойство независимых циклов состоит в том, что они коммутируют по композиции, то

[1] С начала п. 3 до этого места – повторение конца лекции №6.

есть, если κ_1 и κ_2 - независимые циклы, то $\kappa_1\kappa_2 = \kappa_2\kappa_1$ (значок композиции будем, как правило, опускать).

Доказывается теорема, согласно которой любая подстановка может быть разложена на композицию (иногда говорят – произведение) попарно независимых циклов.

Покажем это на примере.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 3 & 8 & 5 & 7 & 1 & 6 & 9 & 2 \end{pmatrix} = (14576)(2389)$$

Чтобы построить такое разложение, нужно проследить «орбиту» каждого элемента под действием данной подстановки. Строим цикл, содержащий 1:

1→4→5→7→6→1 – замкнули первый цикл.

Берем любой элемент, например, 2, не попавший в построенный цикл, и строим цикл, содержащий 2:

2→3→8→9→2.

Так действуем до исчерпания всех элементов, не попавших в очередной цикл. Заметим, что сумма длин всех циклов в этом разложении должна быть равна числу элементов множества, на котором действует подстановка. В этом примере – 9. Заметим также, что в разложении могут быть циклы длины 1. Цикл длины 1 – это тождественная подстановка. Появление цикла длины 1 означает, что исходная подстановка оставляет соответствующий элемент неподвижным (переводит его в себя).

Разложение подстановки на попарно независимые циклы позволяет легко вычислять любые целые степени подстановок. А именно, если $\sigma = \kappa_1\kappa_2...\kappa_m$, где циклы κ_i попарно независимы, то для любого целого s $(\kappa_1\kappa_2...\kappa_m)^s = \kappa_1^s\kappa_2^s...\kappa_m^s$.

При возведении же цикла в целую степень нужно учитывать, что цикл, возведенный в степень, равную его длине, даст тождественную подстановку. Следовательно, при возведении цикла в произвольную целую степень показатель степени нужно взять по модулю длины цикла (то есть вычислить остаток от деления показателя степени на длину цикла). Например, для построенного выше разложения

$$[(14576)(2389)]^{2022} = (14576)^{2022 \bmod 5}(2389)^{2022 \bmod 4} = (14576)^2(2389)^2 = (15647)(28)(39).$$

Схема вычисления положительно целой степени s цикла $(i_1 i_2 ... i_k)$ такова:

$$i_1 \to i_{1+s} \to i_{2+s} \to ...$$

Так, образно говоря, шагаем через s-1 элемент и действуем так до тех пор, пока не получим произведение попарно независимых циклов (в частности, один цикл).

Например:

$(123456789)^2 = (135792468); (123456789)^3 = (147)(258)(369);$

$(123456)^2 = (135)(246); (123456)^3 = (14)(25)(36); (123456)^4 = (153)(264).$

Полезно заметить и следующее.

Пусть дан цикл длины k, а положительное целое m<k.

Тогда

$(i_1 i_2 ... i_k)^m = (i_1 i_2 ... i_k)^k (i_1 i_2 ... i_k)^{m-k} = (i_k i_{k-1} ... i_1)^{k-m}$,

так как $(i_1 i_2 ... i_k)^k = \varepsilon = \begin{pmatrix} 12...n \\ 12...n \end{pmatrix}$ - тождественная подстановка.

Если число k-m>0 достаточно мало, то удобнее, для вычисления исходной m-й степени, возвести в степень k-m цикл, обратный данному.

Например,

$(123456789)^7 = (987654321)^2 = (975318642) = (186429753)$.

Последний цикл мы получили бы, если бы «в лоб» шагали через 6 элементов в приведенной выше схеме (напомним, что цикл не меняется при любой циклической перестановке его элементов: $\begin{matrix} (i_1 i_2 ... i_k) = (i_2 i_3 ... i_k i_1) = (i_3 i_4 ... i_{k-2} i_1 i_2) = ... \\ (1234) = (2341) = (3412) = (4123). \end{matrix}$).

В частности, если m=k-1, то m-я степень цикла длины k равна обратному циклу:

$(i_1 i_2 ... i_k)^{k-1} = (i_1 i_2 ... i_k)^{-1} = (i_k i_{k-1} ... i_1)$

$(123456789)^8 = (987654321)$.

Сделаем теперь замечание о разложении в произведение попарно независимых циклов подстановки, представленной в виде произведения (композиции) циклов, не являющихся независимыми.

Поясним это на примере. Пусть в группе S_9 дана подстановка $(123)(23489)(5678)$. Как видно, циклы в этой композиции не являются независимыми.

Действуем так: имеем три подстановки, действующие последовательно. Строим «орбиту» каждого элемента под действием этих трех последовательно применяемых подстановок. Можно начать с 1: первый цикл переводит 1 в 2, второй переводит 2 в 3, а в третьем 3 отсутствует. В итоге 1 перешла в 3. Дальше следим за «судьбой» тройки (3): 3→1, и всё, так как единицы во втором и третьем цикле нет. Значит, мы замкнули цикл (13). Действуя таким же образом, получим цикл, содержащий двойку (2): (2456789).

Итак, $(123)(23489)(5678) = (13)(2456789)$.

(Подробнее -

Орбита двойки (2): 2→3→4; в итоге 2 перейдет в 4, так как 4 в третьем цикле нет.

Орбита 4: 4→8 (2-й цикл), 8→5 (3-й цикл); в итоге 4 переходит в 5.

5→6→7 (эти элементы находятся только в третьем цикле). Далее 7→8, 8 есть во втором цикле, поэтому сначала 8→9, после чего 9→2, и второй цикл в строящемся разложении замыкается.)

Пример. В группе S_4 решить уравнение:

$$\begin{pmatrix}1234\\4213\end{pmatrix}^{2021} X \begin{pmatrix}1234\\3214\end{pmatrix}^{-2019} = (12)^{829}\ .$$

Решение

Чтобы решить это уравнение, нужно сначала вычислить все степени указанных подстановок. Для этого надо каждую подстановку разложить на попарно независимые циклы, после чего каждый цикл возвести в степень, взяв показатель степени по модулю длины цикла.

Будем иметь:

$$\begin{pmatrix}1234\\4213\end{pmatrix}^{2021} = [(143)(2)]^{2021} = (143)^2 = (341);$$

$$\begin{pmatrix}1234\\3214\end{pmatrix}^{-2019} = [(13)(2)(4)]^{-2019} = (13);$$

$$(12)^{829} = (12).$$

Исходное уравнение примет вид:

$$(341)\,X\,(13) = (12).$$

Решение:

$$X = (341)^{-1}(12)(13)^{-1} = (143)(12)(13) = (14)(23).$$

4. Конечные группы. Циклические группы

Число элементов конечной группы называется ее *порядком*.

Порядком элемента a конечной группы называется наименьшее положительное число s такое, что $a^s = 1$.

Через некоторое время мы докажем, что если G - конечная группа, $a \in G$ и s - порядок a, то $a^{|G|} = a^s = 1$ (где $|G|$ - порядок группы G). Поэтому, чтобы возвести элемент конечной группы в произвольную целую степень, надо показатель степени взять по модулю порядка группы, или по модулю порядка данного элемента (который предварительно надо найти).

Рассмотрим один пример конечной группы.

Мультипликативная группа вычетов по модулю 7.

На множестве положительных целых чисел $\{1,2,3,4,5,6\}$ определим операцию умножения по модулю 7, полагая $a \odot_7 b = \mathrm{mod}(ab,7)$, то есть берется остаток от деления на 7 обычного произведения. Можно доказать, что такая алгебра есть группа. Она называется мультипликативной группой вычетов по модулю 7.

Таблица Кэли (см. стр. 143, пример 2.14) такой группы выглядит так:

$\odot_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

По этой таблице легко найти пары взаимно обратных элементов. Скажем, надо найти обратный к 3. По строке «3» идем до клетки с «1». Номер соответствующего столбца даст обратный. В данном случае это будет 5.

Дальше будет показано, что такая мультипликативная группа вычетов может быть построена для любого простого числа p. Такую группу называют мультипликативной группой вычетов по модулю p и обозначают $\mathbb{Z}_p^*$. Ее операцию умножения по модулю p, определяемую в общем случае аналогично определению умножения по модулю 7, часто обозначают просто точкой, которую обычно опускают (если это не вредит пониманию).

Пример. Решить в группе $\mathbb{Z}_7^*$ уравнение

$$3^{2026} \odot_7 x = 5^{-2020}.$$

Имеем:

$x = 3^{-2026} \odot_7 5^{-2020} = 3^2 \odot_7 5^2 = 2 \odot_7 4 = 1$.

Вычисление степеней с показателями, меньшими порядка группы (равного 6) можно проводить «в лоб», используя формулу $a^n = a^{n-1}a$ (в любой группе; обозначение операции опущено), но можно заметить, что для конечной группы G имеет место равенство $a^n = a^{n-|G|} (n \lhd |G|)$. Поэтому, если бы надо было вычислить 3^4, то $3^4 = 3^{-2} = (3^2)^{-1} = 2^{-1} = 4.$

Циклические группы

Группа $\mathbf{G} = (G, \cdot, 1)$ называется *циклической*, если существует такой элемент $a \in G$, что любой элемент группы является некоторой целой степенью элемента a, который называется *образующим элементом* данной циклической группы.

Сразу надо заметить, что вместе с каждым образующим элементом обратный к нему также будет образующим. Действительно, если любой элемент группы $g = a^n, n \in \mathbb{Z}$,

то $g = (a^{-1})^{-n}$. Позже мы увидим, что таких пар образующих элементов может быть много.

Примеры. 1) Аддитивная группа целых чисел $(\mathbb{Z}, +, 0)$ - циклическая с образующими элементами 1 и -1, так как для любого $n \in \mathbb{Z}$ можно записать $n = n \circ 1 = -n \circ (-1)$ (см. выше определение аддитивной степени элемента аддитивно записанной группы).

Замечание. Подробнее: если $n > 0$, то $n = \underbrace{1+1+...+1}_{n} = n \circ 1 = -(\underbrace{1-1-...-1}_{n}) = -n \circ (-1)$.

Последнее число есть число, противоположное n-й степени минус единицы, то есть противоположное числу -n, то есть n.

Если же $n < 0$, то пусть $n = -m, m > 0$. Тогда
$n = -m = -(\underbrace{1+1+...+1}_{m}) = -m \circ 1 = m \circ (-1) = -\underbrace{1-1-...-1}_{m}$, то есть опять получаем, что
$n = n \circ 1 = -n \circ (-1)$.

2) Легко проверить, что рассмотренная выше мультипликативная группа вычетов по модулю 7 также циклическая с образующими элементами 3 и 5 (которые взаимно обратны). А в группе $\mathbb{Z}_{11}^*$ будет уже две пары образующих элементов: 2 и 6, 7 и 8, что нетрудно проверить.

Позже будет дана формула, по которой можно найти число всех образующих элементов в любой мультипликативной группе вычетов $\mathbb{Z}_p^*$ [2], а также мы рассмотрим определенный способ их перечисления.

Циклическую группу с образующим элементом a будем обозначать $[a]$, называя ее *циклической группой, порожденной элементом* a. Очень важно понять, что каждый образующий элемент – один на всю группу, но не в том смысле, что он единственный (а он не единственный хотя бы потому, что и обратный к нему, в общем случае отличный от него, тоже будет образующим), а в том, что он через свои степени порождает всю группу.

Вспомним теперь, что порядком элемента a конечной группы называется наименьшее положительное число s такое, что $a^s = 1$.

Замечание. На самом деле, порядок элемента так же определяется и для любой группы, не обязательно конечной. Просто в этом параграфе мы рассматриваем почти исключительно конечные группы.

Имеет место следующая важная теорема:

Теорема. Порядок образующего элемента конечной циклической группы равен порядку (числу элементов) этой группы.

Доказательство. Пусть a - образующий элемент некоторой конечной циклической группы, и его порядок равен *n*. Докажем, что в группе $[a]$ ровно *n* элементов, которые

[2] Доказывается, что любая такая группа является циклической.

являются степенями a, то есть $[a]=\{a^0=1,a,a^2,...,a^{n-1}\}$. Прежде всего докажем, что все эти элементы, степени a, попарно различны.

Предположим, что нашлись два таких различных числа *p* и *q* таких, что $a^p=a^q$, причем $1\le p<q\le n-1$. Умножая записанное выше равенство на a^{-p}, получим $a^{q-p}=1$, но $0<q-p<n$, а число *n*, как порядок образующего элемента, есть *наименьшее* положительное число такое, что $a^n=1$. Отсюда следует, что равенство $a^{q-p}=1$ невозможно и указанные выше два числа *p* и *q* также невозможны. Значит, все степени $a^0=1,a,a^2,...,a^{n-1}$ попарно различны и их, стало быть, ровно *n*.

Теперь докажем, что любая целая степень a есть одна из них. Произвольное целое число *m* представим в виде: $m=kn+r$, где *r* – остаток от деления *m* на *n*, то есть $0\le r\le n-1$. Тогда $a^m=a^{kn+r}=a^{kn}a^r=(a^n)^k a^r=1^k\cdot a^r=1\cdot a^r=a^r\in\{1,a,a^2,...,a^{n-1}\}$.

Теорема доказана.

Замечание. Легко показать, что ***любая циклическая группа коммутативна***. Действительно, для любых элементов a^m и a^n циклической группы $[a]$ имеем:

$$a^m\cdot a^n=a^{m+n}=a^{n+m}=a^n\cdot a^m.$$

Подчеркнем, что это относится к *любой* циклической группе, а не только к конечной.

Лекция №8

09.10.24

5. Кольца, тела, поля

Определение кольца

Кольцо – это алгебра типа (2, 2, 0, 0), то есть алгебра с двумя бинарными и двумя нульарными операциями

$$\mathbf{R}=(R,+,\cdot,0,1),$$

называемыми соответственно *сложением, умножением, нулем и единицей* данного кольца и, по определению, обладающими следующими свойствами:

1) $a+(b+c)=(a+b)+c$ (сложение кольца ассоциативно),
2) $a+b=b+a$ (сложение кольца коммутативно),
3) $a+0=a$ (нуль есть нейтральный элемент по сложению),
4) $(\forall a)(\exists a')(a+a'=0)$ (каждый элемент кольца имеет обратный по сложению, называемый противоположным к a и обозначаемый $-a$),
5) $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ (умножение кольца ассоциативно),
6) $a\cdot 1=1\cdot a=a$ (единица есть нейтральный элемент по умножению),

7) $\begin{matrix} a(b+c)=ab+ac; \\ (b+c)a=ba+ca \end{matrix}$ (умножение дистрибутивно относительно сложения как слева, так и справа)[3].

Записанные выше тождества, выражающие свойства операций любого кольца, называются *основными тождествами*, или *аксиомами*, кольца.

Равносильно кольцо можно определить так: это алгебра типа (2, 2, 0, 0), где

1) $(R,+,0)$ - по сложению кольцо есть коммутативная группа (аксиомы 1-4), называемая *аддитивной группой данного кольца*,
2) $(R,\cdot,1)$ - по умножению кольцо есть моноид (аксиомы 5 и 6), называемый *мультипликативным моноидом кольца*,
3) Выполняется аксиома дистрибутивности 7 (эта аксиома связывает две указанные алгебры друг с другом).

Замечание. В алгебраической литературе есть другие определения кольца. Одно из самых распространенных отличается от приведенного выше тем, что по умножению кольцо только лишь группоид. Такой структурой будет, например, множество геометрических (трехмерных) векторов с операциями сложения и векторного умножения.

После этого тогда определяются частные случаи ассоциативного кольца (по умножению кольцо становится полугруппой) и ассоциативного кольца с единицей, что соответствует приведенному выше определению. Нам будет сразу удобно рассматривать именно такой вид кольца и называть его просто кольцом, тем более что других видов «кольцеобразных» структур мы рассматривать не будем.

Отметим сразу важный частный случай *коммутативного кольца*: кольцо называется коммутативным, если его операция умножения коммутативна, то есть имеет место тождество $a\cdot b=b\cdot a$.

Примеры

Перед рассмотрением примеров необходимо заметить следующее.

Когда мы определяем какую-то конкретную алгебру и утверждаем, допустим, что это кольцо, мы обязаны проверить выполнение всех аксиом кольца, то есть подвести частный случай под общее определение.

Переходим к рассмотрению конкретных колец.

1) Кольцо целых чисел $(\mathbb{Z},+,\cdot,0,1)$.
   Аксиомы легко проверяются с учетом известных свойств числовых операций. Структура кольца точно так же может быть определена на множестве рациональных, действительных и даже комплексных чисел, но не может быть определена на множестве неотрицательных целых (рациональных,

[3] Знак умножения («точка») опущен. Это делается часто при таком обозначении операции (абстрактного) умножения.

действительных) чисел в силу невыполнения аксиомы 4 (существования противоположного элемента).
Это кольцо (как и все числовые кольца) коммутативно.

2) Кольцо квадратных матриц заданного порядка $\mathbf{M}_n = (M_n, +, \cdot, O, E)$.
И здесь аксиомы легко проверить, помня свойства матричных операций.
Это кольцо не коммутативно (матричное умножение не коммутативно).
3) Кольцо множеств $\mathbf{R}_M = (2^M, \Delta, \cap, \varnothing, M)$, в котором сложение – симметрическая разность, умножение – пересечение, нуль – пустое множество, единица – всё множество M, подмножества которого образуют носитель данной алгебры.
Выполнение аксиом кольца следует из доказанных ранее свойств операций над множествами:
(1) $A\Delta(B\Delta C) = (A\Delta B)\Delta C$ - симметрическая разность ассоциативна,
(2) $A\Delta B = B\Delta A$ - симметрическая разность коммутативна,
(3) $A\Delta\varnothing = A$ - пустое множество нейтрально по симметрической разности,
(4) $A\Delta A = \varnothing$ - каждый элемент противоположен самому себе,
(5) $A\cap(B\cap C) = (A\cap B)\cap C$ - пересечение ассоциативно,
(6) $A\cap M = A$ - всё множество нейтрально по пересечению,
(7) $A\cap(B\Delta C) = (A\cap B)\Delta(A\cap C)$ - пересечение дистрибутивно относительно симметрической разности.

Это кольцо коммутативно, так как пересечение – операция коммутативная.

4) Кольцо вычетов по модулю k $\mathbb{Z}_k = (\{0,1,...,k-1\}, \oplus_k, \odot_k, 0, 1)$.
Это конечное кольцо, носителем которого является множество первых k неотрицательных целых чисел, а операции сложения и умножения по модулю k определяются известным образом (берется остаток от деления на k обычных суммы и произведения соответственно). Можно доказать (упражнение!), что все аксиомы кольца выполняются[4]. Это кольцо коммутативно.
Заметим, что в противоположность кольцу множеств алгебра бинарных отношений (того же типа) $\mathrm{Rl}(M) = (2^{M\times M}, \cup, \circ, , \varnothing, \mathrm{id}_M)$ не является кольцом, так как не выполняется аксиома 4 (нет противоположного элемента по операции объединения[5]).

Рассмотрим теперь свойства кольца, вытекающие из его определения.

Теорема. В любом кольце выполняются следующие тождества:

1) $a\cdot 0 = 0\cdot a = 0$ (аннулирующее свойство нуля);
2) $a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$
3) $a\cdot(b-c) = a\cdot b - a\cdot c; (b-c)\cdot a = b\cdot a - c\cdot a$ - дистрибутивность умножения относительно вычитания.

---

[4] См. ниже дополнения к лекциям 7-9.

[5] Действительно, если предположить, что существуют два множества, объединение которых пусто, то оба эти множества должны быть пустыми.

Доказательство. В дальнейших выкладках точка как знак операции умножения опускается (если это не приводит к недоразумению).

1) $a + a \cdot 0 = a \cdot 1 + a \cdot 0 = a(1+0) = a \cdot 1 = a$.

Итак, $a + a \cdot 0 = a$. Это можно рассматривать как уравнение в аддитивной группе кольца относительно неизвестного значения $a \cdot 0$. Решая это уравнение, получим $a \cdot 0 = a - a = 0$. Окончательно $a \cdot 0 = 0$. Точно так же получаем, что $a + 0 \cdot a = a$, откуда $0 \cdot a = 0$.

2) Рассмотрим сумму $a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$, но это значит, что $a \cdot (-b) = -(a \cdot b)$. Заметим, что использовано свойство (1).
Точно так же доказывается, что $(-a) \cdot b = -(a \cdot b)$.
Отсюда, в частности, легко получается, что $-a = (-1) \cdot a = a \cdot (-1)$. Также, основываясь на этом свойстве, можно доказать, что в любом кольце $(-a)^{2m} = a^{2m}, m \in \mathbb{Z}$ (любая четная степень противоположного к данному элемента совпадает с той же степенью исходного элемента – как в элементарной арифметике).
3) $a \cdot (b - c) = a(b + (-c)) = ab + a(-c) = ab - ac$ - в силу свойства (2).
Правая дистрибутивность доказывается точно так же.

Замечание. Свойство четной степени удобно применять при вычислениях в кольцах вычетов по большому модулю. Например, пусть надо возвести в квадрат число 76 в кольце вычетов по модулю 97. Тогда проще возвести квадрат противоположное число 21 и получить 441(mod 97)=53. А в кольце вычетов по меньшему модулю можно полностью устно провести такое вычисление. Например, в кольце вычетов по модулю 33: $27^2 = (-6)^2 = 3$. Подобные действия приходится совершать в некоторых алгоритмах шифрования и дешифрования, о чем позже будет немного сказано.

Обратимость. Понятия тела и поля

Некоторые элементы кольца могут быть обратимыми по умножению. Например, в кольце матриц это будут все невырожденные матрицы, а в кольцах рациональных и действительных чисел все ненулевые числа.

Но если мы потребуем, чтобы ***все*** элементы кольца были обратимы, то получим для нуля: $0 \cdot 0^{-1} = 1$, откуда следует, что в таком кольце $0 = 1$. Это не парадокс и не утверждение о равенстве числа 0 числу 1. Это означает, что, если в кольце все элементы обратимы, то в нем оба нейтральных элемента совпадают, то есть это кольцо состоит из одного единственного элемента, условно обозначаемого нулем: 0. Это одноэлементное кольцо в конкретных случаях может быть, например, кольцом, состоящем из одного числа 0, или кольцом подмножеств пустого множества.

Констатировав существование такого кольца, мы им больше заниматься не будем.

Если потребовать обратимости (по умножению) всех ненулевых элементов кольца, то примеров таких колец уже много. Хотя бы перечисленные выше числовые кольца (кроме кольца целых чисел).

Определение. Кольцо, все ненулевые элементы которого обратимы по умножению, называется *телом*. Тело, умножение которого коммутативно, называется *полем*.

Можно доказать, что все обратимые элементы кольца образуют группу. Это следует из того, что произведение обратимых элементов обратимо, элемент, обратный к обратимому, также обратим и единица обратима (см. в лекции №6 свойства обратимых элементов любого моноида). Поэтому ***тело можно определить как кольцо, все ненулевые элементы которого образуют группу по умножению.*** Эта группа называется мультипликативной группой данного тела.

Все записанные выше числовые кольца (кроме кольца целых чисел) являются полями. Самый «близкий» пример некоммутативного тела – тело кватернионов (см. Учебник, приложение к главе 2).

Делители нуля. Область целостности

Ненулевые элементы a и b кольца называются делителями нуля, если $ab = 0$ или $ba = 0$.

Ясно, что в теле не может быть делителей нуля. Но, например, их нет и в кольце целых чисел.

Определение. Коммутативное кольцо без делителей нуля называется областью целостности (или целостным кольцом).

Поэтому как раз кольцо целых чисел является областью целостности (термин, видимо, связан как раз с тем, что любая область целостности «устроена» подобно кольцу целых чисел). Одним из примеров бесконечной области целостности может служить кольцо многочленов с вещественными коэффициентами с определяемыми стандартно операциями сложения и умножения (см. Дополнения).

Нас особенно будут интересовать конечные области целостности.

Теорема. Конечная область целостности является полем.

Доказательство. Пусть $\mathbf{R} = (R, +, \cdot, 0, 1)$ - конечная область целостности. Нужно доказать, что любой ненулевой элемент обратим, то есть для каждого $a \neq 0$ существует единственный $x \neq 0$ такой, что $ax = 1$(в силу коммутативности достаточно найти правый обратный к $a \neq 0$).

Для произвольного $a \neq 0$ определим отображение $f_a : R \setminus \{0\} \to R \setminus \{0\}$ так, что

$f_a(x) \rightleftharpoons ax$ (это отображение называют правым сдвигом на a). Докажем, что это отображение инъективно.

Пусть $ax = ay$. Тогда $ax - ay = a(x - y) = 0$. Так как в области целостности нет делителей нуля и $a \neq 0$, то $x - y = 0$, то есть $x = y$, что и доказывает инъективность отображения сдвига.

Но, как было замечено ранее, инъекция конечного множества в себя является биекцией[6], откуда следует, что для любого $y \neq 0$ существует единственный $x \neq 0$ такой, что $ax = y$ (любой ненулевой элемент имеет единственный прообраз при отображении сдвига). В частности, при $y = 1$ получаем $ax = 1$. Но это и значит, что этот элемент $x \neq 0$ будет обратным к произвольно взятому $a \neq 0$. Другими словами, обратный к заданному $a \neq 0$ есть не что иное, как прообраз единицы при отображении правого сдвига на a.

Теорема доказана.

Замечание. Доказанную теорему можно обобщить, доказав, что любое *конечное кольцо без делителей нуля (не обязательно коммутативное!) есть тело*. Идея доказательства такая же, но нужно определять два отображения сдвига – правого и левого, которые уже не будут совпадать. Рекомендуется доказать это самостоятельно.

Поля вычетов

В кольце вычетов $\mathbb{Z}_k = (\{0,1,...,k-1\}, \oplus_k, \odot_k, 0, 1)$ отсутствие делителей нуля равносильно условию простоты числа k. Действительно, если это число составное, то делителями нуля будут любые два числа (строго меньшие k), произведение которых (в обычном умножении) делится на k. Так в кольце $\mathbb{Z}_{21}$ делителями нуля будут 3 и 7, 6 и 7, 7 и 15, 3 и 14 и т. д.

Если же k простое, то, как нетрудно показать, произведение двух чисел делится на k тогда и только тогда, когда хотя бы одно из них делится на k (доказать самостоятельно!). Но это значит, что
$ab = 0(\mathrm{mod}\, k) \Leftrightarrow k \mid ab \Leftrightarrow k \mid a \vee k \mid b \Leftrightarrow a = 0(\mathrm{mod}\, k) \vee b = 0(\mathrm{mod}\, k)$.

Возникает, таким образом, обширный класс конечных полей – полей $\mathbb{Z}_p$ вычетов по простому модулю *p*. Мультипликативная группа поля $\mathbb{Z}_p$ называется мультипликативной группой вычетов по модулю *p* и обозначается $\mathbb{Z}_p^*$. Некоторые из этих групп мы уже рассматривали. Заметим, что порядок всех групп вычетов (кроме тривиальной группы вычетов по модулю 2, состоящей из одной единицы) является четным числом *p*-1.

Поля вычетов не исчерпывают многообразие всех конечных полей, которые определенным образом строятся как расширения полей вычетов[7]. Конечные поля называются полями Галуа (в честь гениального французского математика Эвариста Галуа

https://ru.wikipedia.org/wiki/Галуа,_Эварист)

Поля Галуа имеют существенные приложения в теории кодирования и разработке алгоритмов защиты информации.

---

[6] См. Учебник, теорема 1.8, с. 86.

[7] Простые примеры расширения полей рассмотрены в Дополнениях.

В конечных полях можно делать всё то же, что мы привыкли делать в поле действительных (или комплексных) чисел. В частности, на них распространяется вся теория и практика решения систем линейных уравнений (включая теорию определителей). Нужно только не забывать, что все арифметические действия следует выполнять по соответствующему простому модулю *p*, оставляя в качестве результата остаток от деления на *p*.

Замечание. То, что мультипликативная группа вычетов (по простому модулю) является мультипликативной группой соответствующего поля, позволяет упростить вычисления в самой группе, переходя, например, к противоположному числу при возведении исходного числа в какую-то степень.

Решим уравнение $7^{-1998}\cdot x\cdot 5^{115}=21^{21}$ в группе Z_{23}^{*}.

Так как группа коммутативна, можно, конечно, это уравнение вида $axb=c$ свести к уравнению вида $ax=b$, переставив все коэффициенты слева от неизвестного.

Но можно решать, используя формулу $x=a^{-1}cb^{-1}$. Тогда надо получить значения всех коэффициентов. ***При вычислении надо твердо помнить, что показатели степеней следует брать по модулю порядка группы, равного 22, а все вычисления проводить по модулю 23***.

Имеем:

$$a^{-1}=7^{1998}=7^{1998\bmod 22}=7^{18}=7^{-4}=(7^4)^{-1}=(3^2)^{-1}=9^{-1}.$$

Позже мы выведем формулу для вычисления мультипликативного обратного в любом поле вычетов, а сейчас заметим, что $9\cdot 5=-1(\mathrm{mod}\,23)$. Значит, $9^{-1}=-5=18$. Итак, $a^{-1}=18=-5$.

Далее: $c=21^{21}=(-2)^{-1}=-12=11$,
$b^{-1}=5^{-115}=5^{-110-5}=5^{-5}=(5^5)^{-1}=(5^4\cdot 5)^{-1}=(2^2\cdot 5)^{-1}=(-3)^{-1}=-8=15$.

Решение: $x=18\cdot 11\cdot 15=(-5)\cdot 11\cdot(-8)=(-6)\cdot 11=3$.

Использовалась записанная ранее формула (лекция №7) для вычисления степеней в конечных группах:

$$a^n=a^{n-|G|},n\in\mathbb{Z}.$$

Лекция №9

11.10.24

6. Полукольца

Полукольцо – это алгебра того же типа (2, 2, 0, 0) и с теми же названиями операций, что и кольцо, свойства которых устанавливают следующие основные тождества (аксиомы):

1) $a+(b+c)=(a+b)+c$ (сложение полукольца ассоциативно),
2) $a+b=b+a$ (сложение полукольца коммутативно),

3) $a+0=a$ (нуль есть нейтральный элемент по сложению),
4) $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ (умножение полукольца ассоциативно),
5) $a\cdot 1=1\cdot a=a$ (единица есть нейтральный элемент по умножению),
6) $a(b+c)=ab+ac;$ $(b+c)a=ba+ca$ (умножение дистрибутивно относительно сложения как слева, так и справа),
7) $a\cdot 0=0\cdot a=0$ (аннулирующее свойство нуля).

В существенном отличии от кольца полукольцо по сложению есть только коммутативный моноид (нет противоположных элементов). Кроме этого, аннулирующее свойство нуля вводится по определению (как аксиома), и можно показать, что это свойство нельзя вывести из остальных аксиом.

Важные частные случаи: 1) *коммутативное полукольцо* – это полукольцо с коммутативной операцией умножения; 2) *идемпотентное полукольцо* – это полукольцо, в котором операция сложения идемпотентна, то есть $a+a=a$

для любого a. Этот класс полуколец особенно важен для нас. Более того, только такими полукольцами мы и будем заниматься.

Примеры

1) Полукольцо неотрицательных целых чисел: $(\mathbb{N}_0,+,\cdot,0,1)$. Это полукольцо коммутативно и не идемпотентно.
2) Полукольцо множеств: $\mathbf{S}_M=(2^M,\cup,\cap,\varnothing,M)$. Это полукольцо коммутативно и идемпотентно.
3) Полукольцо бинарных отношений: $\mathrm{Rl}(M)=(2^{M\times M},\cup,\circ,,\varnothing,\mathrm{id}_M)$. Это полукольцо не коммутативно и идемпотентно.
4) Полукольцо $\mathbf{B}=(\{0,1\},+,\cdot,0,1)$, состоящее всего из двух элементов, операции которого определяются следующими таблицами:

+	0	1	.	0	1
0	0	1	0	0	0
1	1	1	1	0	1

Это полукольцо коммутативно и идемпотентно.
5) Полукольцо $\mathbf{R}^+=(\mathbb{R}^+\cup\{+\infty\},\min,+,+\infty,0)$. Это полукольцо несколько необычно. Его носитель – множество всех неотрицательных действительных чисел, пополненное «плюс бесконечностью»; операция сложения – взятие числового минимума для произвольных двух чисел (например, min (5, 7)=5); операция умножения – обычное числовое сложение; «нуль», то есть нейтральный элемент по сложению - $+\infty$ (тем самым по определению принимается, что для любого элемента a этого полукольца, включая $+\infty$, выполняется $\min(a,+\infty)=a$, то есть $+\infty$ является наибольшим элементом носителя данного полукольца в естественном числовом порядке); «единица» же этого полукольца есть число 0 – нейтральный элемент по числовому сложению). Полукольцо $\mathbf{R}^+$ коммутативно и идемпотентно.
Полукольца примеров (4) и (5) очень важны в теории графов.

6) Полукольцо $\mathbf{S}_{[a,b]} = ([a,b], \max, \min, a, b)$ - полукольцо, носителем которого является отрезок $[a,b]$ числовой прямой, операция сложения – наибольшее число из двух, операция умножения – наименьшее число из двух, «нуль» число a (левая граница отрезка), «единица» - число b (правая граница отрезка), Это полукольцо коммутативно и идемпотентно.
7) Полукольцо $D_n = (Div(n), НОК, НОД, 1, n)$ делителей натурального числа n с операциями НОК (сложения) и НОД (умножения), где «нуль» - число 1, «единица» - всё число n. Это полукольцо коммутативно и идемпотентно.

Проверка аксиом полукольца во всех этих примерах не вызывает затруднений (с учетом известных свойств числовых операций, операций над множествами и отношениями. Подробный анализ свойств операций max и min содержится в конце текста семинара №4. А операции НОК и НОД, как можно показать, сводятся к операциям max и min (см. Учебник, пример 3.9, с. 195, а также пример 3.1, с. 167-168).

Далее будут рассматриваться только идемпотентные полукольца. Поэтому всюду в дальнейшем термин «полукольцо» понимается как «идемпотентное полукольцо».

Естественный порядок (идемпотентного) полукольца

На носителе произвольного полукольца[8] можно определить такое отношение: $a \le b \rightleftharpoons a + b = b$. Легко проверяется, что это отношение порядка. Действительно:
$a + a = a \Rightarrow a \le a$, то есть отношение рефлексивно;
$a \le b, b \le a \Rightarrow a + b = b, b + a = a = a + b \Rightarrow a = b$, то есть отношение антисимметрично;
$a \le b, b \le c \Rightarrow a + b = b, b + c = c \Rightarrow a + c = a + (b + c) = (a + b) + c = b + c = c \Rightarrow a \le c$, то есть отношение транзитивно.

Получаем тем самым отношение порядка, которое называется *естественным порядком* данного полукольца.

Посмотрим теперь, чем будет естественный порядок в полукольцах приведенных выше примеров (кроме первого – единственного среди них неидемпотентного полукольца).

В полукольце множеств $A \le B \Leftrightarrow A \cup B = B \Leftrightarrow A \subseteq B$. Это значит, что в данном полукольце естественный порядок есть не что иное как отношение включения.

Поскольку в полукольце бинарных отношений сложение есть тоже объединение множеств, то и в этом полукольце естественный порядок совпадает с включением.

В полукольце $\mathbf{B}$ тривиально 0 < 1.

[8] Подчеркнем еще раз, что везде далее полукольцо есть всегда идемпотентное полукольцо.

В полукольце $\mathbf{R}^+$ $a \le_{R^+} b \Leftrightarrow \min(a,b) = b \Leftrightarrow b \le_{числ} a$. Это значит, что естественный порядок полукольца $\mathbf{R}^+$ является порядком, обратным (двойственным) естественному числовому.

В полукольце $\mathbf{S}_{[a,b]}$ естественный порядок, очевидно, совпадает с естественным числовым, а в полукольце делителей есть отношение делимости (доказать самостоятельно).

Так как $0 + a = a$ для любого a, то для любого a $0 \le a$, то есть ***нуль полукольца оказывается наименьшим элементом по естественному порядку.***

Докажем теперь простой, но важный результат.

Теорема. Сумма произвольного числа слагаемых в полукольце является точной верхней гранью множества слагаемых: $\sum_k^n a_k = \sup\{a_1, ..., a_k\}$.

Доказательство. Рассмотрим сумму

$$a_i + \sum_k^n a_k = a_i + (a_1 + ... + a_i + ... + a_n) = a_1 + ... + a_i + a_i + ... + a_n = a_1 + ... + a_i + ... + a_n = \sum_k^n a_k .$$

Берем произвольно фиксированное i-е слагаемое и прибавляем к нему всю сумму. Дальнейшее следует из свойств ассоциативности, коммутативности и идемпотентности сложения.

Итак, $a_i + \sum_k^n a_k = \sum_k^n a_k \Rightarrow (\forall i = 1, ..., n)(a_i \le \sum_k^n a_k)$, то есть сумма есть верхняя грань множества слагаемых.

Докажем, что это точная верхняя грань. Пусть для некоторого b и любого $i = 1, ..., n$ выполняется $a_i \le b$, то есть элемент b является какой-то верхней гранью множества слагаемых. Тогда $b + \sum_k^n a_k = b + (a_1 + ... + a_n) = b + a_1 + ... + a_n = b + a_2 + ... + a_n = ... = b + a_n = b$, то есть элемент b по очереди «съедает» (поглощает) все слагаемые и остается один. Значит, сумма $\sum_k^n a_k \le b$, откуда и следует, что она есть точная верхняя грань множества слагаемых.

Теорема доказана.

Следствие. В любом полукольце любое конечное множество имеет точную верхнюю грань, совпадающую с суммой его элементов.

7. Замкнутые полукольца

Полукольцо называется *замкнутым*, если выполняются два условия: 1) любая последовательность имеет точную верхнюю грань по естественному порядку; 2)

операция умножения непрерывна, то есть для любого элемента a и любой последовательности $\{b_n\}_{n\geq 0}$ выполняются равенства

$$a\sup b_n = \sup(ab_n), (\sup b_n)a = \sup(b_n a).$$

Из определения следует, что ***замкнутое полукольцо является индуктивно упорядоченным множеством*** (см. Лекцию №5).

Это очень важный факт. Заметим, что в замкнутом полукольце ***любая*** (а не только неубывающая) последовательность имеет точную верхнюю грань.

Замечание. Непрерывность умножения означает тогда непрерывность функций $f(x) = ax$ (умножение каждого x на фиксированный элемент a слева) и $g(x) = xa$ (умножение каждого x на фиксированный элемент a справа). Действительно, вспоминая определение непрерывного отображения индуктивно упорядоченного множества в себя, получим для первой функции $f(\sup x_n) = a\sup x_n = \sup ax_n = \sup f(x_n)$. Для второй функции – аналогично.

Сразу отметим такой простой, но важный результат:

Теорема. Любое конечное полукольцо замкнуто.

Доказательство. В конечном полукольце любая последовательность $\{b_n\}_{n\geq 0}$ имеет конечную область значений, и точная верхняя грань равна сумме элементов этой области значений. Непрерывность умножения тогда выражает обычное свойство дистрибутивности умножения относительно сложения:

$$a\sum_{k=0}^{n} b_k = \sum_{k=0}^{n} ab_k, (\sum_{k=0}^{n} b_k)a = \sum_{k=0}^{n} b_k a.$$

Можно показать, что все рассмотренные выше в примерах идемпотентные полукольца замкнуты. Подробнее см. Учебник, пример 3.5, с. 180-182.

Понятие бесконечной суммы

Под бесконечной суммой элементов $a_1, \ldots a_n, \ldots$ замкнутого полукольца понимается точная верхняя грань последовательности $\{a_n\}_{n\geq 0}$, то есть, по определению

$$\sum_{n=0}^{\infty} a_n = \sup a_n.$$

Нижний предел суммирования может быть и больше нуля. Как правило, будем пользоваться обозначением $\sum a_n$, полагая по умолчанию, что суммирование ведется от нуля до бесконечности. В случае, когда нижний предел отличен от нуля, будем это указывать.

Рассмотрим здесь важнейшие свойства бесконечной суммы.

Теорема 1. Для произвольных последовательностей $\{x_n\}_{n\geq 0}$ и $\{y_n\}_{n\geq 0}$ имеет место равенство

$$\sum(x_n + y_n) = \sum x_n + \sum y_n .$$

Доказательство. Пусть $a = \sum x_n + \sum y_n$. Докажем, что элемент a есть точная верхняя грань последовательности $\{x_n + y_n\}$. Имеем: для любого $n \in \mathbb{N}$ вычислим

$$a + x_n + y_n = \sum x_n + \sum y_n + x_n + y_n = \sum x_n + \sum y_n = a .$$

Если b - верхняя грань указанной последовательности, то $b + a = b + \sum x_n + \sum y_n = b,$ так как для любого $n \in \mathbb{N}$ $b \geq x_n + y_n \geq x_n, y_n$ (конечная сумма есть, как известно, точная верхняя грань множества слагаемых), т.е. элемент b является верхней гранью каждой из рассматриваемых двух последовательностей и, следовательно, не меньше точных верхних граней этих последовательностей, которые в указанной выше сумме поглощаются по очереди. Итак, $b + a = b$ и $a \leq b$, откуда $a = \sum(x_n + y_n)$

Из доказанной теоремы вытекает важное свойство непрерывности операции сложения в замкнутом полукольце, а именно имеет место

Следствие 1. Для любых последовательности $\{x_n\}_{n\geq 0}$ и элемента a замкнутого полукольца выполняется

$$\sum(x_n + a) = \sum(a + x_n) = a + \sum x_n = (\sum x_n) + a .$$

Доказательство. Частный случай утверждения теоремы 1, когда вторая последовательность постоянна, то есть при $y_n = a$ для каждого n.

Итак, за бесконечную сумму можно выносить произвольное слагаемое, как и наоборот: вносить отдельное слагаемое в бесконечную сумму. Это и выражает свойство непрерывности операции сложения, то есть непрерывности функции $f(x) = a + x$. Напомним, что операция умножения в замкнутом полукольце непрерывна по определению, то есть для последовательности $\{x_n\}_{n\geq 0}$ и элемента a замкнутого полукольца выполняется

$$\sum ax_n = a\sum x_n \text{ и } \sum x_n a = (\sum x_n)a .$$

Это не что иное, как бесконечный аналог свойства дистрибутивности умножения относительно сложения.

Следующее свойство бесконечной суммы связано с понятием частичной суммы последовательности.

Положим для последовательности $\{x_n\}_{n\geq 0}$

$s_k = \sum_{i=0}^{k} x_i$ при $k \geq 0$ и назовем это *k-ой частичной суммой последовательности* $\{x_n\}_{n\geq 0}$. Так как последовательность $\{s_k\}_{k\geq 0}$ является неубывающей, то $\sum_{k=0}^{\infty} s_k = \sum_{k=m\geq 1}^{\infty} s_k$ для любого m.

Теорема 2. Точная верхняя грань (бесконечная сумма) любой последовательности равна точной верхней грани последовательности ее частичных сумм, то есть

$$\sum x_n = \sum s_n .$$

Доказательство. Для произвольного неотрицательного k имеем:

$$x_k + \sum s_n = x_k + \sum_{n\geq k} s_n = \sum_{n\geq k} (x_k + s_n) = \sum_{m\geq 0} (x_k + x_1 + \ldots + x_k + \ldots + x_{k+m}) =$$

$$= \sum_{m\geq 0} (x_1 + \ldots + x_k + \ldots + x_{k+m}) = \sum_{n\geq k} s_n = \sum s_n$$

(Использованы свойства коммутативности и идемпотентности операции сложения в полукольце.)

Это значит, что точная верхняя грань последовательности частичных сумм есть верхняя грань последовательности $\{x_n\}_{n\geq 0}$. Для произвольной верхней грани этой b последовательности аналогично предыдущему (доказательство теоремы 1), с учетом того, что для любого k $b + x_k = b$ получим:

$$b + \sum s_n = \sum b + s_n = \sum b + (x_1 + \ldots + x_n) = b,$$

откуда и следует доказываемое.

8. Решение линейных уравнений и систем линейных уравнений в замкнутом полукольце

Линейные уравнения

В замкнутом полукольце можно решать *линейные уравнения* вида

$$x = ax + b \qquad (1)$$

или

$$x = xa + b \qquad (2)$$

Уравнение (1) называют *праволинейным*, а уравнение (2) – *леволинейным*.

Подчеркнем, что в существенном отличии от колец тут невозможен никакой перенос слагаемых из одной части уравнения (или равенства) в другую.

Выведем формулу для решения праволинейного уравнения. Это основной вид линейных уравнений в полукольцах, который мы только и будем изучать.

Прежде всего заметим, что правая часть уравнения (1) непрерывна, так как умножение непрерывно по определению, а непрерывность сложения была доказана в лекции №9.

Тогда, полагая $f(x) = ax + b$, применяем формулу для наименьшего решения уравнения (1):

$$x = \sup\{f^n(0)\} = \sup\{0, f(0) = b, f(f(0) = f^2(0) = ab + b = (1 + a)b,$$
$$f^3(0) = a(ab + b) + b = (1 + a + a^2)b, \ldots, f^n(0) = (1 + a + a^2 + \ldots + a^{n-1})b, \ldots\}$$

Отбрасывая 0, запишем это в виде бесконечной суммы:

$$x = \sum_{n=1}^{\infty}(1 + a + a^2 + \ldots + a^{n-1})b = \sum_{n=0}^{\infty}(1 + a + a^2 + \ldots + a^n)b.$$

Используя непрерывность умножения, выносим множитель b за знак бесконечной суммы (справа) и получаем

$$x = (\sum_{n=0}^{\infty}1 + a + a^2 + \ldots + a^n)b$$

Под знаком бесконечной суммы стоит частичная сумма последовательности $\{a^n\}_{n\geq 0}$ степеней элемента a. Согласно одному из свойств бесконечной суммы,

$$\sum_{n=0}^{\infty}(1 + a + a^2 + \ldots + a^n) = \sum_{n=0}^{\infty}a^n$$

(точная верхняя грань последовательности совпадает с точной верхней гранью последовательности ее частичных сумм).

Итак, получаем формулу для наименьшего решения уравнения (1):

$$x = (\sum_{n=0}^{\infty}a^n)b.$$

Точная верхняя грань последовательности степеней элемента a называется *итерацией* (или *замыканием* элемента a) и обозначается a^*. Окончательно тогда формула для наименьшего решения уравнения (1) примет вид:

$$x = a^*b \qquad (3)$$

Для леволинейного уравнения (2) аналогично может быть получена формула $x = ba^*$.

Формула (3) принимает совсем простой вид в полукольцах с тривиальной итерацией, то есть в таких, в которых итерация каждого элемента равна единице полукольца. Тогда наименьшее решение как праволинейного, так и леволинейного уравнения совпадет со свободным членом уравнения: $x = b$.

Дополнения

1)Проверка аксиом для кольца вычетов (лекция №8)

Покажем для примера доказательство ассоциативности операции сложения по модулю k.

Обозначим $\mathrm{mod}(m,k)$ остаток от деления m на k, а $[m]_k$ - наибольшее целое, не превосходящее k и делящееся на k. Ясно, что $\mathrm{mod}(m,k) = m - [m]_k$

По определению $m \oplus_k n \rightleftharpoons \mathrm{mod}(m+n,k)$.

Имеем:

$$m \oplus_k (n \oplus_k p) = \mathrm{mod}(m + \mathrm{mod}(n+p,k),k) =$$
$$= \mathrm{mod}(m+n+p-[n+p]_k,k) = \mathrm{mod}(m+n+p,k).$$

(так как $[n+p]_k = 0 \ (\mathrm{mod}\, k)$.

Поскольку операция $\oplus_k$, как очевидно, коммутативна, то
$(m \oplus_k n) \oplus_k p = p \oplus_k (m \oplus_k n) = \mathrm{mod}(p+m+n,k) = \mathrm{mod}(m+n+p,k).$

Аксиомы 5 и 7 проверяются аналогично, а проверка остальных тривиальна.

2) Кольцо многочленов над полем

Пусть K - некоторое поле.

Многочлен над полем K - это формальная конечная сумма вида

$$P^{(n)}(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n, n \geq 0, (\forall k \in \{0,1,2,\ldots n\})(a_k \in K).$$

где x - формальная переменная.

Часто считают, что эта переменная принимает значение в поле K, и тогда, придавая этой переменной то или иное значение и считая, что записанная выше сумма есть выражение, использующее операции поля K, можно придать многочлену функциональный смысл: он определяет некоторое отображение носителя поля в себя.

Можно также видеть, что многочлен $P^{(n)}(x)$ полностью определяется кортежем коэффициентов $(a_0, a_1, a_2 \ldots, a_n)$. Удобнее, однако, рассматривать такой кортеж как

финитную последовательность, то есть такую бесконечную последовательность, у которой все члены, начиная с некоторого номера, равны нулю. Наибольший номер отличного от нуля члена называется *степенью многочлена*. При этом последовательность, состоящая из одних нулей, определяется как многочлен степени $-\infty$. Последовательность, у которой только первый член отличен от нуля, определяет многочлен степени 0, который можно отождествить с элементом исходного поля.

Рассмотрим теперь операции над многочленами.

1) *Сложение*

Многочлены как финитные последовательности складываются почленно:

$$(a_0, a_1, ..., a_n, 0, 0, ...) + (b_0, b_1, ..., b_n, b_{n+1}, ..., b_m, 0, 0, ...) \rightleftharpoons$$
$$\rightleftharpoons (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, 0 + b_{n+1}, ..., 0 + b_m, 0, 0, ...) =$$
$$= (a_0 + b_0, a_1 + b_1, ..., a_n + b_n, b_{n+1}, ..., b_m, 0, 0, ...); n \le m$$

в предположении, что степень первого многочлена равна n, второго – m.

Тогда понятно, что степень суммы равна наибольшей из степеней слагаемых.

С функциональной точки зрения, здесь просто складываются две суммы, определяющие некоторые элементы базового поля:

$$\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{m} b_k x^k = \sum_{k=0}^{m} (a_k + b_k) x^k (a_{n+1} = ... = a_m = 0); n \le m$$

.

2) *Умножение*

Член c_k произведения двух финитных последовательностей указанного выше вида определяется формулой:

$$c_k = a_0 b_k + a_1 b_{k-1} + ... + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i}$$

(сумма индексов в каждом слагаемом равна k).

Опять-таки с функциональной точки зрения перемножаются две суммы (раскрываются скобки), как в обычной школьной алгебре:

$$(a_0 + a_1 x + ... + a_n x^n)(b_0 + b_1 x + ... + b_m x^m) =$$
$$= a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + ... +$$
$$+ (a_0 b_k + a_1 b_{k-1} + ... + a_k b_0) x^k + ... + a_n b_m x^{n+m}.$$

Очевидно, что степень произведения равна сумме степеней сомножителей.

Обозначим через $K[x]$ множество многочленов над полем K с переменной x.

Тогда можно доказать такую теорему:

Теорема. Алгебра $\mathbf{K}[x]=(K[x],+,\cdot,0,1)$, где сложение и умножение определены выше, 0 и 1 суть нуль и единица поля K [9], является областью целостности.

Рекомендуется доказать это самостоятельно.

Замечание. Утверждение теоремы остается истинным, если вместо базового поля рассматривать любую область целостности.

3)Примеры расширений полей

Задача. Является ли полем множество чисел вида $x+y\sqrt{2}$, где $x,y\in\mathbb{Q}$ (рациональные числа) с обычными операциями сложения и умножения.

Решение

Свойства числовых операций проверять не нужно: они известны. Здесь нужно убедиться в том, что определенное в условии задачи множество $M=\{x+y\sqrt{2}:x,y\in\mathbb{Q}\}$ замкнуто относительно операций сложения и умножения, то есть сумма и произведение двух чисел из M принадлежит M.

Это легко проверить:

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}\in M;$$
$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}\in M$$

Кроме этого, нейтральные элементы 0 и 1 представляются как числа из этого же множества M:

$0=0+0\sqrt{2},1=1+0\sqrt{2}$.

Множество M можно уподобить множеству комплексных чисел, у которых есть действительная и мнимая части. Здесь же мы можем говорить о рациональной и иррациональной части.

Итак, мы имеем числовую алгебру $\mathbf{M}=(M,+,\cdot,0,1)$, которая, очевидно, является кольцом и подалгеброй поля действительных чисел.

Чтобы ответить на вопрос, является ли это кольцо полем, нужно проверить обратимость по умножению произвольного ненулевого числа из множества M.

Имеем:

---

[9] Точнее, нуль кольца многочленов есть нулевая последовательность, а единица – последовательность (1, 0, 0,...).

$$(a+b\sqrt{2})^{-1}=\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}, a^2+b^2\neq 0$$.

Знаменатель этой дроби не может оказаться равным нулю, так как тогда мы получили бы, что $\frac{a}{b}=\sqrt{2}$, но отношение рациональных чисел не может быть иррациональным числом.

Итак, любой ненулевой элемент множества M обратим по умножению, и

$$(a+b\sqrt{2})^{-1}=\frac{a}{a^2-2b^2}-\frac{b}{a^2-2b^2}\sqrt{2}\in M, a^2+b^2\neq 0$$,

так как обе дроби в написанной выше формуле являются рациональными числами (что совершенно очевидно).

Итак, алгебра $\mathbf{M}=(M,+,\cdot,0,1)$ есть поле. Оно является расширением поля рациональных чисел (то есть содержит последнее в качестве подполя).

Это расширение поля рациональных чисел можно рассматривать как полученное путем добавления к этому полю корня уравнения $x^2-2=0$, не имеющего решения в поле рациональных чисел.

В сущности, также строится поле комплексных чисел: множество действительных чисел расширяется путем добавления к нему корня уравнения $x^2+1=0$, обозначаемого i, и рассматриваются все линейные комбинации вида $a+bi; a,b\in\mathbb{R}$. То же самое поле (точнее, поле изоморфное[10] полю комплексных чисел), мы получим, рассматривая в кольце многочленов над полем действительных чисел множество остатков от деления на многочлен x^2+1.

Можно доказать, что множество остатков от деления на многочлен x^2+x+1 (не имеющий действительных корней) также образует поле. Это поле уже не будет изоморфно полю комплексных чисел (см. Учебник, задача 2.14).

Операции сложения и умножения проводятся в этих случаях по модулям соответствующих многочленов.

Поле рациональных чисел можно расширить, добавляя корень уравнения $x^3-2=0$, то есть элемент $\theta=\sqrt[3]{2}$. Но в этом случае, поскольку элемент $\theta^2=\sqrt[3]{4}$ также иррационален, элементами нового поля будут линейные комбинации вида $a+b\theta+c\theta^2; a,b,c\in\mathbb{Q}$. Доказательство того, что они образуют поле аналогично решению рассмотренной выше задачи, но, конечно, сложнее. Так, обратный к заданному, отличному от нуля, элементу, некий элемент $a'+b'\theta+c'\theta^2$ с неизвестными рациональными коэффициентами находится из условия

[10] О гомоморфизмах и изоморфизмах см. Учебник, 2.8, 2.9, 4.3 и 4.4.

$(a'+b'\theta+c'\theta^2)(a+b\theta+c\theta^2)=1$. Раскрывая скобки (с учетом того, что $\theta^3=2$) и приравнивая коэффициенты при одинаковых степенях θ, получим систему относительно неизвестных a',b',c':

$$\begin{cases} aa'+2cb'+2bc'=1 \\ ba'+ab'+2cc'=0 \\ ca'+bb'+ac'=0 \end{cases}$$

Можно доказать, что главный определитель этой системы при рациональных a,b,c отличен от нуля, то есть система имеет единственное решение, что и позволяет определить элемент поля, обратный данному.

В заключение простой пример конечного поля, построенного как расширение поля вычетов по модулю 3, то есть поля $\mathbb{Z}_3$ (состоящего всего из трех элементов). Легко проверить, что в этом поле уравнение $x^2+1=0$ не имеет решений. Введем новый элемент $\theta=\sqrt{-1}$ (наподобие обычной мнимой единицы). Тогда элементами нового поля будут все линейные комбинации вида $a+b\theta; a,b\in\mathbb{Z}_3$. Все операции выполняются с учетом того, что $\theta^2=-1$ и, конечно, в арифметике остатков от деления на 3. Например, $(1+\theta)(1+2\theta)=(1+\theta)(1-\theta)=1-\theta^2=2=-1$. Число элементов в этом поле равно, очевидно, $9=3^2$.

Это простой пример поля Галуа, являющегося расширением поля $\mathbb{Z}_3$. Одним из важных результатов алгебраической теории полей является то, что для любых простого числа p и натурального *n* может быть построено поле Галуа, состоящее из p^n элементов, которое можно рассматривать как расширение поля вычетов по модулю p. Такое поле обозначается $GF(p^n)$. Рассмотренное только что поле есть поле $GF(3^2)$.