Дискретная математика
Тема 3. Алгебраические структуры

Е.А.Перепелкин

Санкт-Перербургский государственный университет аэрокосмического приборостроения

2021

3.1 Основные понятия

Определение

Отображение

$$\alpha : A^n \to A$$

называется n-арной алгебраической операцией на множестве A.

Далее будем рассматривать бинарные алгебраические операции

$$\alpha : A^2 \to A.$$

Бинарную алгебраическую операцию будем обозначать:

$$a * b, \quad ab, \quad a + b, \quad a, b \in A.$$

Пример

Бинарными алгебраическими операциями являются:

- операции сложения $x + y$ и умножения xy на множестве действительных чисел R;
- операции объединения $A \cup B$ и пересечения $A \cap B$ множеств ;
- операции дизъюнкции $x \vee y$ и конъюнкции $x \wedge y$ на множестве $B = \{0; 1\}$;
- операция сложения векторов на плоскости $\vec{v} + \vec{u}$;
- операции сложения $a(x) + b(x)$ и умножения $a(x)b(x)$ полиномов с действительными коэффициентами

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$
$$b(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m.$$

Определение

Множество A с заданными на нём алгебраическими операциями $\alpha_1, \ldots, \alpha_n$ называется алгебраической структурой и обозначается

$$\langle A; \alpha_1, \ldots, \alpha_n \rangle.$$

Пример

Множество квадратных матриц M_n заданной размерности n с операциями сложения и умножения образуют алгебраическую структуру $\langle M_n; +, \cdot \rangle$ с двумя алгебраическими операциями.

Определение

Алгебраическая структура называется конечной, если число её элементов конечно.

Конечную алгебраическую структуру

$$\langle A; * \rangle, \quad A = \{a_1; a_2; \ldots; a_n\},$$

с бинарной алгебраической операцией $*$ можно задать таблицей Кэли

$*$	a_1	$\ldots$	a_n
a_1	b_{11}	$\ldots$	b_{1n}
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_n	b_{n1}	$\ldots$	b_{nn}

где $b_{ij} = a_i * a_j \in A$.

Пример

На множестве $A = \{0; 1; 2\}$ задана бинарная алгебраическая операция $a + b \pmod 3$. Таблица Кэли для этой алгебраической структуры имеет следующий вид

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Определение

Бинарная алгебраическая операция, заданная на множестве A, называется коммутативной, если

$$\forall a, b \in A : ab = ba.$$

Называется ассоциативной, если

$$\forall a, b, c \in A : (ab)c = a(bc).$$

Пример

Операция сложения матриц коммутативна.
Операция умножения матриц не коммутативна.
Обе эти операции ассоциативные.

Под a^n понимается

$$a^n = \underbrace{aa\ldots a}_{n}.$$

Справедливы соотношения

$$a^n a^m = a^{n+m}, \quad (a^n)^m = a^{nm}.$$

Если $ab = ba$, то $(ab)^n = a^n b^n$.

Определение

Элемент $e \in A$ такой, что

$$\forall a \in A : ae = ea = a$$

называется единичным (нейтральным). Единичный элемент будем также обозначать a^0.

Пример

В алгебраической структуре $\langle M_n; +, \cdot \rangle$ по отношению к операции сложения нейтральным элементом является нулевая матрица, по отношению к операции умножения нейтральным элементом является единичная матрица.

Единичный элемент, если существует, всегда единственный.

Пусть существуют два единичных элемента e_1 и e_2.

По определению единичного элемента

$$e_1 e_2 = e_1, \quad e_1 e_2 = e_2.$$

Следовательно, $e_1 = e_2 = e$.

Определение

Обратным для a называется элемент a^{-1} такой, что

$$aa^{-1} = a^{-1}a = e.$$

Пусть для элемента a существует обратный a^{-1}. Тогда

$$(a^n)^{-1} = (a^{-1})^n, \quad n \in N.$$

В дальнейшем $(a^{-1})^n$ будем обозначать a^{-n}.

Определение

Две алгебраические структуры

$$\langle A; \alpha_1, \ldots, \alpha_n \rangle \quad \text{и} \quad \langle B; \beta_1, \ldots, \beta_n \rangle$$

с бинарными алгебраическими операциями называются изоморфными, если существует биекция $f : A \leftrightarrow B$ такая, что

$$\forall a_1, a_2 \in A \; \forall \alpha_i : \; f(a_1 \alpha_i a_2) = f(a_1) \beta_i f(a_2).$$

Пример

Алгебраические структуры: $\langle B; \wedge \rangle$, $\langle B; \vee \rangle$, $B = \{0; 1\}$ изоморфны.
Биекцию $f : B \leftrightarrow B$ установим по правилу $f(x) = \bar{x}$.
Это означает, что $f(0) = 1, \quad f(1) = 0$.
Применяя закон де Моргана, получим

$$\forall x, y \in B : f(x \vee y) = \overline{x \vee y} = \bar{x} \wedge \bar{y} = f(x) \wedge f(y).$$

Следовательно, рассматриваемые алгебраические структуры изоморфны.

3.2 Группы

Определение

Алгебраическая структура $G = \langle A; \cdot \rangle$ с бинарной ассоциативной операцией называется полугруппой.

Определение

Алгебраическая структура $G = \langle A; \cdot \rangle$ с бинарной ассоциативной операцией называется группой, если в G существует единичный элемент и для для каждого элемента G существует обратный.

Коммутативную группу принято называть абелевой группой.

Определение

Группа называется конечной порядка n, если она содержит ровно n различных элементов.

Пример

Множество целых чисел относительно операции умножения образует полугруппу, относительно операции сложения образует абелеву группу.

Пример

Множество невырожденных квадратных матриц одной размерности образует группу относительно операции умножения.
Произведение двух невырожденных матриц AB – невырожденная матрица.
Единичным элементом является единичная матрица E.
Для каждой невырожденной матрицы существует обратная матрица A^{-1} такая, что $A^{-1}A = E$, $AA^{-1} = E$.
Данная группа не является абелевой. В общем случае, $AB \neq BA$.

Определение

Группа называется мультипликативной, если алгебраическая операция имеет смысл произведения. В мультипликативной группе алгебраическая операция обозначается «$\cdot$». Нейтральный элемент обозначается «1». Обратный элемент обозначается «a^{-1}». Произведение n элементов $a \dots a$ обозначается «a^n ».

Определение

Группа называется аддитивной, если алгебраическая операция имеет смысл сложения. В аддитивной группе алгебраическая операция обозначается «$+$». Нейтральный элемент обозначается «0». Обратный элемент называется противоположным и обозначается «$-a$». Сумма n элементов $a + \dots + a$ обозначается «na».

Теорема (Свойства группы)

Пусть G – группа. Тогда

1) *Для любого $a \in G$ обратный элемент a^{-1} является единственным.*
2) *Для любых $a, b \in G$ уравнение $ax = b$ имеет единственное решение $x = a^{-1}b$.*
   Для любых $a, b \in G$ уравнение $xa = b$ имеет единственное решение $x = ba^{-1}$.
3) *Для любых $a, b \in G$ справедливо равенство $(ab)^{-1} = b^{-1}a^{-1}$.*

Доказательство.

Предположим, что для элемента a существуют два обратных элемента a_1 и a_2. Тогда

$$a_1 a a_2 = a_1(a a_2) = a_1 e = a_1,$$
$$a_1 a a_2 = (a_1 a) a_2 = e a_2 = a_2.$$

Следовательно, $a_1 = a_2$.
Подставим $x = a^{-1}b$ в уравнение $ax = b$. Получим

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

Следовательно, $x = a^{-1}b$ является решением уравнения $ax = b$.

Пусть существуют два решения x_1 и x_2. Тогда из равенств $ax_1 = b$, $ax_2 = b$ следует, что $ax_1 = ax_2$. Умножим левую и правую часть последнего равенства на a^{-1}. Получим

$$(a^{-1}a)x_1 = (a^{-1}a)x_2, \quad ex_1 = ex_2, \quad x_1 = x_2.$$

Аналогично можно показать, что уравнение $xa = b$ имеет единственное решение $x = ba^{-1}$.

Докажем третью часть теоремы. Для любых $a, b \in G$ справедливы равенства

$$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e,$$
$$ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

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

Определение

Пусть G – группа. Подмножество $H \subseteq G$ называется подгруппой G, если H само является группой.

Теорема

Пересечение двух подгрупп является подгруппой.

Доказательство.

Пусть H и P подгруппы группы G. Обозначим $Q = H \cap P$. Пусть $a, b \in Q$. Необходимо показать, что $ab \in Q$, $e \in Q$, $a^{-1} \in Q$.

Из условия $a, b \in Q$ следует, что $a, b \in H$ и $a, b \in P$. Следовательно, $ab \in H$ и $ab \in P$. Таким образом, $ab \in Q$.

Единичный элемент является единственным, при этом $e \in H$ и $e \in P$. Следовательно, $e \in Q$.

Пусть $a \in Q$. Тогда $a \in H$ и $a \in P$. Обратный элемент $a^{-1} \in H$ и $a^{-1} \in P$. Следовательно, $a^{-1} \in Q$. □

Теорема

Для любого элемента a группы G множество

$$\{a\} = \left\{ a^k \mid k \in Z \right\} \subseteq G$$

является абелевой подгруппой.

Доказательство.

Для любых $k, j \in Z$ произведение

$$a^k a^j = a^j a^k = a^{k+j} \in \{a\}.$$

Единичный элемент $e = a^0 \in \{a\}$.
Для любого $a^k \in \{a\}$ существует обратный $(a^k)^{-1} = a^{-k} \in \{a\}$.
Следовательно, $\{a\}$ является абелевой подгруппой G. □

Определение

Подгруппа $\{a\}$ называется циклической подгруппой, порождённой элементом a.

Пример

Пусть $G = \langle Z; + \rangle$ – группа целых чисел относительно операции сложения.
Подмножество чётных чисел является подгруппой G.
Сумма двух чётных чисел является чётным числом.
Противоположное число к чётному числу является чётным числом.
Нейтральный элемент, число 0, является чётным числом.
Подгруппа чётных чисел является циклической подгруппой $\{2\}$, поскольку любое четное число записывается в виде $2k$, $k \in Z$.

3.3 Циклические группы

Определение

Группа G называется циклической, если она совпадает с одной из своих циклических подгрупп, т.е. её можно представить в виде

$$G = \{a\}, \quad a \in G.$$

Теорема

Любая подгруппа циклической группы является циклической.

Доказательство.

Пусть H есть подгруппа циклической группы $G = \{a\}$.
Если $a^k \in H$, то и $(a^k)^{-1} = a^{-k} \in H$.
Пусть k – минимальное положительное число такое, что $a^k \in H$.
Покажем, что любой элемент H может быт записан в виде $(a^k)^p = a^{pk}$. Докажем от противного.
Пусть $a^n \in H$, $n > k$ и n не делится на k. Тогда $n = pk + r$, где $0 < r < k$.
Следовательно, $a^r = a^n a^{-pk} \in H$, что противоречит выбору k.
Таким образом, мы показали, что a^k является порождающим элементом подгруппы $H = \{a^k\}$. □

Определение

Порядком элемента a группы G называется наименьшее положительное число n такое, что $a^n = e$.

Теорема

Пусть G – группа и $a \in G$ имеет порядок n. Тогда циклическая подгруппа $\{a\}$ является конечной порядка n и состоит из элементов

$$\{a\} = \{e; a; a^2; \ldots; a^{n-1}\}.$$

Доказательство.

Все элементы последовательности $e, a, a^2, \ldots, a^{n-1}$ различны.
Докажем от противного. Пусть

$$a^k = a^r, \quad k, r < n, \quad k > r.$$

Тогда $a^{k-r} = e$, $k - r < n$. Следовательно, порядок элемента a меньше n, что противоречит исходному предположению.
Любая другая степень a, положительная или отрицательная, совпадает с одним из элементов этой последовательности.
Пусть $|k| \geq n$. Тогда k можно записать в виде $k = np + r$, $0 \leq r < n$.
Следовательно,

$$a^k = (a^n)^p a^r = e^p a^r = a^r \in \{e, a, a^2, \ldots, a^{n-1}\}.$$

Таким образом,

$$\{a\} = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Определение

Пусть G – группа. Подмножество $H \subset G$ называется системой образующих группы G, если любой элемент G есть произведение конечного числа элементов, каждый из которых является элементом H или обратным к элементу H.

Пример

Для циклической группы $G = \{a\}$ система образующих состоит из одного элемента a.

Пример

Множество $A = \{(x, y) \mid x, y \in Z\}$ с операцией сложения

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

образует абелеву группу. Система образующих этой группы состоит из двух элементов: $(0, 1)$ и $(1, 0)$.

3.4 Симметрическая группа

Пусть задано множество A. Обозначим через F множество биекций

$$f : A \leftrightarrow A.$$

Рассмотрим операцию композиции биекций $f \circ g$.

Для любого $x \in A$ значение композиции определяется по правилу

$$(f \circ g)(x) = g(f(x)).$$

Операция композиции биекций является алгебраической операцией, поскольку композиция биекций также является биекцией.

Эта операция является ассоциативной

$$\forall f, g, h \in F : (f \circ g) \circ h = f \circ (g \circ h).$$

Действительно,

$$((f \circ g) \circ h)(x) = h((f \circ g)(x)) = h(g(f(x))),$$
$$(f \circ (g \circ h))(x) = (g \circ h)(f(x)) = h(g(f(x))).$$

Рассмотрим биекцию $e : A \leftrightarrow A$, заданную правилом

$$e(x) = x, \quad x \in A.$$

Справедливы равенства

$$(e \circ f)(x) = f(e(x)) = f(x), \quad (f \circ e)(x) = e(f(x)) = f(x).$$

Следовательно, e является нейтральным элементом по отношению к операции композиции.

Обратным элементом для $f \in F$ является обратная функция

$$f^{-1} : A \leftrightarrow A, \quad x = f^{-1}(y), \quad y = f(x),$$

которая также является биекцией. Справедливы соотношения

$$f \circ f^{-1} = e, \quad f^{-1} \circ f = e.$$

Таким образом, множество F относительно операции композиции образует группу.

Определение

Симметрической группой множества A называется группа биекций $f : A \leftrightarrow A$ относительно операции композиции. Симметрическую группу обозначают $S(A)$.

Теорема (Теорема Кэли)

Пусть $G = \langle A; \cdot \rangle$ – группа. Существует подгруппа H группы $S(A)$, такая, что G изоморфна H.

Доказательство.

Пусть $a \in A$. Построим функцию $f_a : A \to A$ по правилу

$$\forall x \in A : f(x) = ax.$$

Эта функция является биекцией.
Для любого $y \in A$ уравнение $ax = y$ имеет единственное решение $x = a^{-1}y$.
Следовательно, f_a является сюръекцией и инъекцией, то есть биекцией.

Обозначим через $F_A = \{f_a | \ a \in A\}$ множество таких биекций. Пусть $a, b \in A$. Тогда

$$\forall x \in A : (f_a \circ f_b)(x) = f_b(f_a(x)) = f_b(ax) = bax = f_{ba}(x).$$

Следовательно, $f_a \circ f_b = f_{ba} \in F_A$.
Обозначим через 1 нейтральный элемент группы G. Нейтральный элемент группы $S(A)$ равен $e = f_1 \in F_A$. Обратный элемент $f_a^{-1} = f_{a^{-1}} \in F_A$.

Таким образом, относительно операции композиции множество F_A образует подгруппу $H = \langle F_A; \circ \rangle$ группы $S(A)$.
Установим биекцию $g : A \leftrightarrow F_A$ по правилу

$$\forall a \in A : g(a) = f_a.$$

Эта биекция порождает изоморфизм групп G и H. □

Определение

Симметрическая группа $S(A)$ конечного множества A с n элементами называется группой симметрий и обозначается S_n.

Группа симметрий S_n является конечной. Порядок группы симметрий S_n равен числу биекций $n!$.

Теорема Кэли справедлива и для группы симметрий. Это означает, что любая конечная группа порядка n изоморфна некоторой подгруппе группы симметрий S_n.

Группу симметрий называют также группой подстановок. Это название происходит от формы записи биекции в виде подстановки.

Определение

Подстановкой порядка n называется таблица

$$P_k = \begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix},$$

где нижняя строка есть перестановка элементов верхней строки.

Каждая подстановка есть биекция $f : A \leftrightarrow A$, где $A = \{1; 2; \dots; n\}$.
Всего различных подстановок $n!$

Под произведением подстановок

$$P_i = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \quad P_j = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

понимается подстановка

$$P_i P_j = \begin{pmatrix} 1 & 2 & \dots & n \\ j_{i_1} & j_{i_2} & \dots & j_{i_n} \end{pmatrix}.$$

Произведение подстановок есть композиция соответствующих подстановкам биекций.

Пример

При $n = 3$ подстановки можно записать в следующем виде

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Пример произведения подстановок

$$P_4 P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = P_6.$$

Множество подстановок порядка n относительно операции умножения образуют группу. В этой группе единичным элементом является подстановка

$$P_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Для каждой подстановки P_i существует обратная P_j такая, что

$$P_i P_j = P_1, \quad P_j P_i = P_1.$$

Обратной для

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

является подстановка P_j, которая может быть построена следующим образом. Сначала составим таблицу

$$\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Затем переставим столбцы этой таблицы так, чтобы она приняла вид подстановки

$$P_j = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}.$$

Это и будет, обратная для P_i подстановка.

Пример

Таблица Кэли для группы подстановок S_3 имеет следующий вид

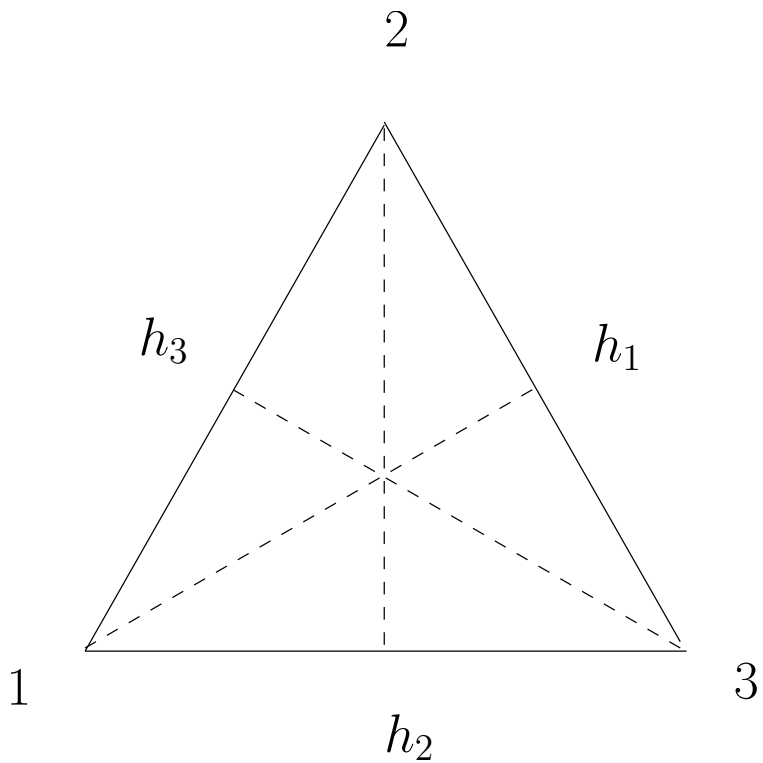
$*$	P_1	P_2	P_3	P_4	P_5	P_6
P_1	P_1	P_2	P_3	P_4	P_5	P_6
P_2	P_2	P_3	P_1	P_6	P_4	P_5
P_3	P_3	P_1	P_2	P_5	P_6	P_4
P_4	P_4	P_5	P_6	P_1	P_2	P_3
P_5	P_5	P_6	P_4	P_3	P_1	P_2
P_6	P_6	P_4	P_5	P_2	P_3	P_1

Группа подстановок не является абелевой. В общем случае $P_iP_j \neq P_jP_i$. Например,

$$P_2P_4 = P_6, \quad P_4P_2 = P_5.$$

Пример

Группа симметрий правильного треугольника



Будем рассматривать самосовмещения треугольника, то есть такие перемещения треугольника, при которых изображение треугольника на плоскости не меняется.

Такие самосовмещения возможны при повороте треугольника относительно центра против часовой стрелки на на углы 0^0, 120^0, 240^0, а также при повороте треугольника относительно трёх высот h_1, h_2, h_3.

Алгебраической операцией в данном случае является операция последовательного перемещения треугольника.

Операции поворота треугольника можно описать в виде подстановок:

P_1 – поворот на 0^0;

P_2 – поворот на 120^0;

P_3 – поворот на 240^0;

P_4 – поворот относительно высоты h_1;

P_5 – поворот относительно высоты h_2;

P_6 – поворот относительно высоты h_3;

Например, последовательное выполнение поворотов треугольника относительно высоты h_1 и против часовой стрелки на 240^0 описывается подстановкой $P_4 P_3 = P_6$.

Группа симметрий правильного треугольника является группой симметрий S_3.

3.5 Разложение группы по подгруппе

Пусть H есть подгруппа группы G. Рассмотрим бинарное отношение на множестве G

$$R_H = \{(a, b) |\ a^{-1}b \in H\}.$$

Теорема

Отношение R_H является отношением эквивалентности.

Доказательство.

Необходимо показать, что отношение R_H является рефлексивным, симметричным и транзитивным.

Рефлексивность

$$a^{-1}a = e \in H \;\Rightarrow\; (a,a) \in R_H.$$

Симметричность

$$(a,b) \in R_H \;\Rightarrow\; a^{-1}b = h \in H \Rightarrow\; b^{-1}a = h^{-1} \in H \;\Rightarrow\; (b,a) \in R_H.$$

Транзитивность

$$(a,b) \in R_H,\ (b,c) \in R_H \;\Rightarrow\; a^{-1}b = h_1 \in H,\ b^{-1}c = h_2 \in H \;\Rightarrow$$
$$a^{-1}c = h_1h_2 \in H \;\Rightarrow\; (a,c) \in R_H.$$

Отношение эквивалентности порождает разбиение группы на классы эквивалентности

$$[a] = \{b \mid a \sim b\}.$$

Определение

Левые смежные классы группы G по подгруппе H есть множества

$$aH = \{ah \mid h \in H\}.$$

Теорема

Классы эквивалентности отношения R_H есть левые смежные классы G по H

$$[a] = aH.$$

Доказательство.

Докажем методом включения

$$b \in [a] \Leftrightarrow a^{-1}b = h \in H \Leftrightarrow b = ah \in aH$$

Левые смежные классы образуют разбиение группы. Это означает, что

$$G = \bigcup_{a \in G} aH$$

и любые два смежных класса aH, bH либо совпадают, либо не пересекаются.

Аналогично определяются правые смежные классы Ha.

Если группа G абелева, то левые и правые смежные классы совпадают, $aH = Ha$.

Теорема (Теорема Лагранжа)

Пусть G конечная группа порядка n, H – подгруппа G порядка k. Тогда n делится на k.

Доказательство.

Все левые смежные классы содержат ровно k элементов, т.к. из равенства $ah_1 = ah_2$, $h_1, h_2 \in H$ следует $h_1 = h_2$.
Пусть p есть число различных смежных классов. Тогда $n = kp$. □

Пример

Рассмотрим группу подстановок S_3. Порядок этой группы равен 6. По теореме Лагранжа в группе S_3 могут быть подгруппы порядка 1,2,3. Запишем эти подгруппы

$$\{P_1\}, \quad \{P_1; P_4\}, \quad \{P_1; P_5\}, \quad \{P_1; P_6\}, \quad \{P_1; P_2; P_3\}.$$

3.6 Определение и свойства колец

Определение

Кольцом называется алгебраическая структура $\langle K; +, \cdot \rangle$ с двумя алгебраическими операциями: сложение «$+$» и умножение «$\cdot$», в которой выполняются следующие условия:

1) $\langle K; + \rangle$ является аддитивной абелевой группой;
2) $\langle K; \cdot \rangle$ является полугруппой;
3) выполняется закон дистрибутивности

$$\forall a, b, c \in K: \ (a+b)c = ac + bc, \quad c(a+b) = ca + cb.$$

Пример

Множество целых чисел с операциями сложения и умножения $\langle Z; +, \cdot \rangle$ является кольцом.

Множество $F(x)$ многочленов

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

с действительными коэффициентами образует кольцо $\langle F(x); +, \cdot \rangle$.

Определение

Кольцо $\langle K; +, \cdot \rangle$ называется коммутативным, если умножение коммутативная операция.
Кольцо $\langle K; +, \cdot \rangle$ называется кольцом с единицей, если в полугруппе $\langle K; \cdot \rangle$ существует единица 1.

Теорема (Свойства кольца)

Пусть $\langle K; +, \cdot \rangle$ *– кольцо. Тогда*

1) $\forall a \in K \ : \ a0 = 0a = 0$
2) $\forall a, b \in K \ : \ (-a)b = a(-b) = -ab$

Доказательство.

Для любых $a, b \in K$ справедливы утверждения:

$$a(a+0) = aa + a0,\ a(a+0) = aa \ \Rightarrow\ a0 = 0,$$
$$(a+0)a = aa + 0a,\ (a+0)a = aa \ \Rightarrow\ 0a = 0,$$
$$0 = 0b = (a-a)b = ab + (-a)b \ \Rightarrow\ (-a)b = -ab,$$
$$0 = a0 = a(b-b) = ab + a(-b) \ \Rightarrow\ a(-b) = -ab.$$

Здесь мы применили закон дистрибутивности и определение нулевого и противоположного элемента аддитивной группы. □

Определение

Элементы $a, b \neq 0$ кольца $\langle K; +, \cdot \rangle$ называются делителями нуля, если $ab = 0$.

Пример

Множество квадратных матриц с действительными элементами размерности n образуют кольцо $\langle M_n; +, \cdot \rangle$. В этом кольце существуют делители нуля. Например, при $n = 2$

$$\begin{bmatrix} 1 & 2 \\ -2 & -4 \end{bmatrix} \begin{bmatrix} 3 & 5 \\ -1,5 & -2,5 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Определение

Подмножество L кольца $\langle K; +, \cdot \rangle$ является подкольцом, если L само является кольцом $\langle L; +, \cdot \rangle$.

Теорема

Подмножество L кольца $\langle K; +, \cdot \rangle$ является подкольцом тогда и только тогда, когда

$$\forall a, b \in L \ : a - b \in L \quad \textit{и} \quad ab \in L.$$

Доказательство.

Необходимость очевидна. Докажем достаточность. Пусть $a, b \in L$. Тогда

$$0 = a - a \in L, \quad 0 - a = -a \in L, \quad a - (-b) = a + b \in L,$$
$$a + b = b + a, \quad ab \in L.$$

Следовательно, $\langle L; + \rangle$ – абелева группа, $\langle L; \cdot \rangle$ – полугруппа. Также выполняется закон дистрибутивности

$$\forall a, b, c \in L : a(b + c) = ab + ac, \quad (a + b)c = ac + bc.$$

Тем самым мы показали, что $\langle L; +, \cdot \rangle$ является кольцом. □

Пример

Рассмотрим кольцо целых чисел $\langle Z; +, \cdot \rangle$. Множество целых чисел $L = \{pn | \ n \in Z\}$, кратных заданному натуральному числу p, является подкольцом кольца Z.
Действительно, пусть $a, b \in L$. Тогда $a = pn$, $b = pm$ и $a - b = p(n - m) \in L$, $ab = p(npm) \in L$. Следовательно, L есть подкольцо кольца $\langle Z; +, \cdot \rangle$.

Пример

Рассмотрим кольцо многочленов $\langle F(x); +, \cdot \rangle$ и множество $L(x)$ многочленов $f(x) = a_1 x + a_2 x^2 + \cdots + a_n x^n$ с нулевым коэффициентом a_0. Пусть $f(x), g(x) \in L(x)$. Тогда $f(x) - g(x) \in L(x)$, $f(x)g(x) \in L(x)$. Следовательно, $L(x)$ является подкольцом кольца $\langle F(x); +, \cdot \rangle$.

3.7 Идеалы, классы вычетов, фактор-кольца

Пусть $\langle K; +, \cdot \rangle$ – коммутативное кольцо.

Определение

Идеалом кольца K называется подкольцо L такое, что для любого $a \in L$ и любого $b \in K$ произведение $ab \in L$.

Пример

Рассмотрим кольцо целых чисел $\langle Z; +, \cdot \rangle$. Множество целых чисел $L = \{pn | \ n \in Z\}$, кратных заданному натуральному числу p, является идеалом кольца Z.
Действительно, множество L является подкольцом кольца $\langle Z; +, \cdot \rangle$ и для любых $a = pn \in L$, $b \in Z$ произведение $ab = pnb \in L$.

Теорема

Для любого $a \in K$ множество $aK = \{ab \mid b \in K\}$ является идеалом кольца K. Этот идеал называется главным.

Доказательство.

Пусть $a, b, c \in K$. Тогда $ab \in aK$, $ac \in aK$. При этом

$$ab - ac = a(b - c) \in aK, \quad (ab)(ac) = a(bac) \in aK.$$

Следовательно, множество aK является подкольцом K.
Подкольцо aK является идеалом, поскольку $(ab)c = a(bc) \in aK$. □

Определение

Кольцо называется кольцом главных идеалов, если в этом кольце других идеалов кроме главных нет.

Пример

Кольцо целых чисел $\langle Z; +, \cdot \rangle$ является кольцом главных идеалов. Действительно, пусть L есть идеал кольца Z. Обозначим через a наименьшее натуральное число в L. Покажем, что $L = aZ$. По определению идеала $aZ \subseteq L$. Пусть $b \in L$ и $b \notin aZ$. Существуют $q, r \in N$ такие, что $b = aq + r$ и $0 < r < a$. Тогда $r = b - aq \in L$, что противоречит выбору a. Следовательно, $L = aZ$.

Пусть L – идеал кольца $\langle K; +, \cdot \rangle$. Рассмотрим аддитивную коммутативную группу $\langle K; + \rangle$. Подкольцо L также является и подгруппой $\langle L; + \rangle$ группы $\langle K; + \rangle$. Рассмотрим смежные классы

$$[a] = a + L = \{a + b \mid b \in L\}$$

группы $\langle K; + \rangle$ по подруппе $\langle L; + \rangle$. В теории колец эти смежные классы называют классами вычетов и обозначают C_a.

На множестве классов вычетов определим операции сложения и умножения

$$C_a + C_b = C_{a+b},$$
$$C_a C_b = C_{ab}.$$

Теорема

Множество классов вычетов образуют коммутативное кольцо относительно операций сложения и умножения. Это кольцо называется факторкольцом и обозначается K/L.

Доказательство.

Справедливы равенства:

$$C_a + C_b = C_{a+b} = C_{b+a} = C_a + C_b,$$
$$C_a + C_0 = C_a, \quad C_a + C_{-a} = C_0,$$
$$C_a C_b = C_{ab} = C_{ba} = C_b C_a.$$

Следовательно, K/L есть коммутативное кольцо. □

Пример

Рассмотрим кольцо целых чисел $\langle Z; +, \cdot \rangle$ и идеал $\langle L; +, \cdot \rangle$ чисел, кратных натуральному числу p.
Обозначим Z_p кольцо классов вычетов, порождённое идеалом L.
Элементы кольца классов вычетов имеют следующий вид

$$C_a = \{a + pn \mid n \in Z\}.$$

В этом кольце существует единичный элемент C_1. Для любого $n \in Z$ класс вычетов $C_{pn} = C_0$.

Кольцо Z_p является конечным и состоит из элементов

$$Z_p = \{C_0, C_1, \ldots, C_{p-1}\}.$$

Действительно, пусть $a \in Z$. Тогда $a = pn + r$, $0 \leq r < p$ и, следовательно,

$$C_a = C_{pn+r} = C_p C_n + C_r = C_0 + C_r = C_r.$$

Противоположный к классу C_m есть класс C_{p-m}, поскольку

$$C_m + C_{p-m} = C_p = C_0.$$

Операции сложения и умножения в кольце Z_p выполняются по следующим правилам

$$C_m + C_n = \begin{cases} C_{m+n}, & m+n < p \\ C_{m+n-p}, & m+n \geq p \end{cases},$$

$$C_m C_n = C_r, \quad mn = pk + r, \quad 0 \leq r < p.$$

3.8 Определение и свойства полей

Определение

Коммутативное кольцо $\langle P; +, \cdot \rangle$ называется полем, если в P существует 1 и для любого $a \in P,\ a \neq 0$, существует a^{-1}.

Алгебраическая структура $\langle P \setminus \{0\}; \cdot \rangle$ является коммутативной группой. Таким образом, поле состоит из двух коммутативных групп, объединённых законом дистрибутивности.

Пример

Множество целых чисел $\langle Z; +, \cdot \rangle$ полем не является. Множество рациональных чисел $\langle Q; +, \cdot \rangle$, множество действительных чисел $\langle R; +, \cdot \rangle$ и множество комплексных чисел $\langle C; +, \cdot \rangle$ являются полями относительно операций сложения и умножения.

В поле нет делителей нуля. Действительно, пусть $ab = 0$, $a \neq 0$, $b \neq 0$. Тогда $a^{-1}(ab) = (a^{-1}a)b = 1b = b = 0$. Что противоречит исходному предположению.

Теорема

Конечное коммутативное кольцо с единицей является полем тогда и только тогда, когда в этом кольце нет делителей нуля.

Доказательство.

Необходимость мы уже доказали. Докажем достаточность. Обозначим элементы кольца

$$K = \{a_1; a_2; \ldots; a_n\}.$$

Среди этих элементов есть нулевой элемент – 0 и единичный – 1.

Пусть $a \in K$ и $a \neq 0$. Рассмотрим последовательность элементов

$$aa_1,\ aa_2,\ \ldots,\ aa_n.$$

Все элементы этой последовательности различны. Действительно, пусть $aa_i = aa_j$, $a_i \neq a_j$. Тогда $a(a_i - a_j) = 0$. Поскольку $a \neq 0$ и в кольце нет делителей нуля, то $a_i - a_j = 0$. То есть, $a_i = a_j$. Получили противоречие.
Таким образом,

$$\{a_1; a_2; \ldots; a_n\} = \{aa_1; aa_2; \ldots; aa_n\}.$$

Следовательно, $aa_i = 1$ некоторого $1 \leq i \leq n$. В силу коммутативности $a_i a = 1$. Это означает, что для каждого элемента $a \in K$ существует обратный a^{-1}. Тем самым мы доказали, что рассматриваемое кольцо является полем. □

Пример

Рассмотрим кольцо вычетов Z_p. Это конечное коммутативное кольцо, состоящее из элементов

$$Z_p = \{C_0; C_1; \ldots; C_{p-1}\}.$$

В этом кольце есть единичный элемент C_1.
Пусть p составное число, $p = mn$. Тогда

$$C_m C_n = C_p = C_0.$$

Следовательно, в кольце Z_p есть делители нуля и поэтому Z_p не является полем.

Пусть p простое число. В этом случае в кольце Z_p делителей нуля нет.
Докажем от противного.
Пусть $C_m C_n = C_0$. Тогда $mn = kp$. Число p простое. Следовательно, k делится на m.
Мы можем записать $k = ml$. После деления на m левой и правой равенства $mn = kp$ получим $n = lp$. Что невозможно, поскольку $n < p$.
Таким образом, при простом p кольцо вычетов Z_p является полем.

Определение

Подкольцо L поля $\langle P; +, \cdot \rangle$ называется подполем, если L само является полем.

Определение

Поле P называется расширением поля L, если L является подполем P.

Пример

Поле действительных чисел $\langle R; +, \cdot \rangle$ является расширением поля рациональных чисел $\langle Q; +, \cdot \rangle$. Поле комплексных чисел $\langle C; +, \cdot \rangle$ является расширением поля действительных чисел $\langle R; +, \cdot \rangle$.

Конечные поля называют полями Галуа и обозначают F_q или $GF(q)$, где q – число элементов поля.

Конечное поле с числом элементов q существует тогда и только тогда, когда $q = p^m$,где p – простое число, m – любое натуральное число.

Мултипликативная группа конечного поля $GF(q)$ является циклической. Это означает, что существует элемент поля $a \neq 0$ такой, что все остальные элементы поля, за исключением 0, являются степенями этого элемента. Таким образом

$$GF(q) = \{0; 1; a; a^2; \ldots; a^{q-2}\}.$$

Пример

Простейшим примером конечного поля F_2 является поле $\langle E; \oplus, \cdot \rangle$, где $E = \{0; 1\}$, $\oplus, \cdot$ – логические операции сумма по модулю два и конъюнкция. Это поле изоморфно полю классов вычетов $\langle Z_2; +, \cdot \rangle$.

В общем случае кольцо классов вычетов $\langle Z_p; +, \cdot \rangle$ является полем тогда и только тогда, когда p – простое число.

Все остальные конечные поля можно построить как расширение полей классов вычетов.

Обозначим через $GF(q)[x]$ кольцо многочленов с коэффициентами из поля $GF(q)$. Элементы $GF(q)[x]$ есть многочлены следующего вида

$$f(x) = f_0 + f_1 x + \cdots + f_n x^n, f_i \in GF(q).$$

Многочлен $f(x) \in GF(q)[x]$ называется нормированным, если коэффициент при старшей степени равен $f_n = 1$.

Многочлен $f(x) \in GF(q)[x]$ называется примитивным, если его нельзя представить в виде произведения двух многочленов из $GF(q)[x]$ ненулевой степени.

В кольце $GF(q)[x]$ для любого натурального m всегда существует по крайней мере один примитивный многочлен степени m.

Например в кольце $GF(2)[x]$ примитивными многочленами являются

$$1+x+x^2, \quad 1+x+x^3, \quad 1+x+x^4,$$
$$1+x^2+x^5, \quad 1+x+x^6, \quad 1+x^3+x^7.$$

Примитивными многочленами второй степени в кольце $GF(3)[x]$ являются

$$1+x^2, \quad 2+x+x^2, \quad 2+2x+x^2.$$

Алгоритм построения конечного поля $GF(p^m)$ удобно описать с использованием кольца многочленов $GF(p)[x]$.

Пусть $f(x)$ есть примитивный нормированный многочлен степени m в кольце $GF(p)[x]$.

Элементы поля $GF(p^m)$ есть многочлены $g(x) \in GF(p)[x]$ степени не выше $m-1$. Число таких многочленов равно p^m.

Элементы поля $GF(p^m)$ можно также рассматривать как векторы

$$g = [g_0, g_1, \ldots, g_{m-1}],$$

составленные из коэффициентов многочленов

$$g(x) = g_0 + g_1 x + \cdots + g_{m-1} x^{m-1} \in GF(p)[x].$$

В случае $p = 2$ это будут двоичные векторы.

Операции сложения и умножения элементов поля $GF(p^m)$ выполняются как операции сложения и умножения соответствующих многочленов в кольце $GF(p)[x]$.

При этом результат произведения двух многочленов $g(x)$ и $h(x)$ есть остаток от деления $g(x)h(x)$ на $f(x)$.

Другими словами, произведение $g(x)$ и $h(x)$ в поле $GF(p^m)$ есть $g(x)h(x) \pmod{f(x)}$ в кольце $GF(p)[x]$.

Организовать вычисления в конечном поле можно с использованием порождающего элемента мультипликативной группы поля.

Сумма элементов поля a^i и a^j есть сумма соответствующих векторов с элементами из поля $GF(p)$.

Произведение определяется по правилу

$$a^i a^j = a^{i+j} \pmod{q-1}.$$

Рассмотрим пример построения поля $GF(2^3)$ с использованием примитивного многочлена третьей степени $f(x) = 1 + x + x^3$.

Элементы поля – это все многочлены с двоичными коэффициентами не выше второй степени:

$$0; \quad 1; \quad x; \quad 1+x; \quad x^2; \quad 1+x^2; \quad x+x^2; \quad 1+x+x^2.$$

Можно построить таблицы сложения и умножения элементов поля. Пусть, например,

$$g(x) = 1 + x^2, \quad h(x) = 1 + x + x^2.$$

Тогда

$$g(x) + h(x) = x,$$

$$g(x)h(x) = (1+x^2)(1+x+x^2) \pmod{f(x)} =$$

$$= (1+x+x^3+x^4) \pmod{f(x)} = x + x^2.$$

Элемент поля $a = x$ является порождающим элементом мультипликативной группы поля. Это означает, что элементы поля можно записать в следующем виде:

$$0; \quad 1; \quad a; \quad a^2; \quad a^3; \quad a^4; \quad a^5; \quad a^6.$$

Здесь

$$\begin{aligned}
&a = x, \\
&a^2 = x^2 \pmod{f(x)} = x^2; \\
&a^3 = x^3 \pmod{f(x)} = 1 + x, \\
&a^4 = x^4 \pmod{f(x)} = x + x^2, \\
&a^5 = x^5 \pmod{f(x)} = 1 + x + x^2, \\
&a^6 = x^6 \pmod{f(x)} = 1 + x^2.
\end{aligned}$$

Заметим, что

$$a^7 = x^7 \pmod{f(x)} = 1.$$

Таким образом мы получаем три эквивалентных представления элементов поля: в виде степени порождающего элемента мультипликативной группы поля, в виде многочлена и в виде двоичного вектора

0	0	$[000]$
1	1	$[100]$
a	x	$[010]$
a^2	x^2	$[001]$
a^3	$1+x$	$[110]$
a^4	$x+x^2$	$[011]$
a^5	$1+x+x^2$	$[111]$
a^6	$1+x^2$	$[101]$

Пусть, например, необходимо вычислить сумму и произведение элементов поля a^4 и a^6. Значение суммы можно вычислить как значение суммы соответствующих двоичных векторов в поле $GF(2)$. Получим

$$a^4 + a^6 \equiv [011] + [101] = [110] \equiv a^3.$$

Значение произведения вычисляется по правилу

$$a^4 a^6 = a^{10} \pmod 7 = a^3.$$

При этом не требуется умножать и делить соответствующие элементам a^4 и a^6 многочлены.

3.9 Булева алгебра

Рассмотрим алгебраическую структуру с тремя алгебраическими операциями $\langle B; +, \cdot, ^- \rangle$. Две из них бинарные: «$+$»,«$\cdot$», одна унарная: «$^-$». Элемент $\overline{a}$ будем называть дополнением элемента a.

Определение

Алгебраическая структура $\langle B; +, \cdot, ^- \rangle$ называется булевой алгеброй, если

1) $\langle B; + \rangle$ есть коммутативная полугруппа с нулевым элементом 0;
2) $\langle B; \cdot \rangle$ есть коммутативная полугруппа с единичным элементом 1;
3) выполняются законы дистрибутивности

$$\forall a, b, c \in B: \ a(b+c) = ab + bc, \ a + bc = (a+b)(a+c);$$

4) выполняются законы дополнения

$$\forall a \in B: \ a + \overline{a} = 1, \ a\overline{a} = 0.$$

Пример

Булеан 2^A множества A образует булеву алгебру $\langle 2^A; \cup, \cap, ^- \rangle$ относительно операций объединения, пересечения и дополнения множеств. Роль нуля здесь выполняет пустое множество $\emptyset$, роль единицы само множество A.

Пример

Согласно законам алгебры логики множество $B = \{0; 1\}$ образует булеву алгебру $\langle B; \vee, \wedge, ^- \rangle$ относительно логических операций дизъюнкции, конъюнкции и отрицания.

Рассмотрим следствия, которые вытекают из аксиом булевой алгебры. Сначала заметим, что для любого элемента a, элемент, удовлетворяющий законам дополнения, является единственным и равен $\overline{a}$. Действительно, пусть для некоторого элемента b выполняются равенства

$$a + b = 1, \quad ab = 0.$$

Применяя законы дистрибутивности и дополнения, получим

$$b = b + 0 = b + a\overline{a} = (b + a)(b + \overline{a}) = 1(b + \overline{a}) = (a + \overline{a})(b + \overline{a}) = ab + \overline{a} = 0 + \overline{a} = \overline{a}.$$

Заметим также, что $1 + 0 = 1$, $1 \cdot 0 = 0$. Следовательно, $\overline{1} = 0$, $\overline{0} = 1$.

Теорема

Пусть $\langle B; +, \cdot, ^- \rangle$ *есть булева алгебра. Тогда для любых* $a, b \in B$ *справедливы тождества:*

1) *идемпотентность*

$$2a = a, \quad a^2 = a;$$

2) *свойства констант*

$$a + 1 = 1, \quad a0 = 0.$$

3) *поглощение*

$$a + ab = a, \quad a(a + b) = a;$$

4) двойное дополнение

$$\overline{\overline{a}} = a;$$

5) законы де Моргана

$$\overline{a + b} = \overline{a}\,\overline{b}, \quad \overline{ab} = \overline{a} + \overline{b};$$

6) склеивание

$$\overline{a}b + ab = b, \quad (\overline{a} + b)(a + b) = b;$$

Доказательство.

Идемпотентность.

Из законов дистрибутивности и дополнения получим

$$2a = (a + a)1 = (a + a)(a + \overline{a}) = a + a\overline{a} = a + 0 = a,$$
$$a^2 = a^2 + 0 = a^2 + a\overline{a} = a(a + \overline{a}) = a1 = a.$$

Свойства констант.

Из идемпотентности и законов дополнения следует

$$a + 1 = a + (a + \overline{a}) = (a + a) + \overline{a} = a + \overline{a} = 1,$$
$$a0 = a(a\overline{a}) = a^2\overline{a} = a\overline{a} = 0.$$

Поглощение.
Из законов дистрибутивности и свойств констант следует

$$a + ab = a1 + ab = a(1 + b) = a1 = a,$$
$$a(a + b) = (a + 0)(a + b) = a + 0b = a + 0 = a.$$

Двойное дополнение.
По законам дополнения

$$\overline{a} + \overline{\overline{a}} = 1, \quad \overline{a}\,\overline{\overline{a}} = 0,$$
$$\overline{a} + a = 1, \quad \overline{a}a = 0.$$

В силу единственности дополнения $\overline{\overline{a}} = a$.

Законы де Моргана.
Из законов дистрибутивности и свойств констант получим

$$(a+b)\overline{a}\overline{b} = (a\overline{a})\overline{b} + (b\overline{b})\overline{a} = 0\overline{b} + 0\overline{a} = 0,$$
$$(a+b) + \overline{a}\overline{b} = (a+b+\overline{a})(a+b+\overline{b}) = (1+b)(1+a) = 1.$$

Элемент $\overline{a}\overline{b}$ удовлетворяет законам дополнения для элемента $a+b$.
Следовательно,

$$\overline{a+b} = \overline{a}\overline{b}.$$

Применяя доказанный закон и двойное дополнение, получим

$$\overline{a} + \overline{b} = \overline{\overline{\overline{a} + \overline{b}}} = \overline{\overline{\overline{a}}\,\overline{\overline{b}}} = \overline{ab}.$$

Склеивание.

По законам дистрибутивности и дополнения

$$\bar{a}b + ab = (\bar{a} + a)b = 1b = b,$$
$$(\bar{a} + b)(a + b) = \bar{a}a + b = 0 + b = b.$$