

ЭЛЕМЕНТЫ ОБЩЕЙ АЛГЕБРЫ

Циклические полугруппы и группы

Определение 8.1.

В полугруппе $(A, *)$ **n -я степень элемента a** есть элемент $\underbrace{a * a * \dots * a}_{n \text{ раз}}$, обозначаемый a^n , причем $a^1 = a$ и $a^n = a * a^{n-1}$,
 $n = 2, 3, \dots$

Определение 8.1.

В полугруппе $(A, *)$ **n -я степень элемента a** есть элемент $\underbrace{a * a * \dots * a}_{n \text{ раз}}$, обозначаемый a^n , причем $a^1 = a$ и $a^n = a * a^{n-1}$,

$n = 2, 3, \dots$

Если $(A, *, \mathbf{1})$ — моноид, то вводят нулевую степень $a^0 = \mathbf{1}$.

Определение 8.1.

В полугруппе $(A, *)$ **n -я степень элемента a** есть элемент $\underbrace{a * a * \dots * a}_{n \text{ раз}}$, обозначаемый a^n , причем $a^1 = a$ и $a^n = a * a^{n-1}$, $n = 2, 3, \dots$

Если $(A, *, \mathbf{1})$ — моноид, то вводят нулевую степень $a^0 = \mathbf{1}$.

Если $(A, *, \mathbf{1})$ — группа, то для любого элемента a вводят отрицательную степень согласно равенству: $a^{-n} = (a^{-1})^n$, $n = 1, 2, \dots$

Определение 8.1.

В полугруппе $(A, *)$ **n -я степень элемента a** есть элемент $\underbrace{a * a * \dots * a}_{n \text{ раз}}$, обозначаемый a^n , причем $a^1 = a$ и $a^n = a * a^{n-1}$, $n = 2, 3, \dots$

Если $(A, *, \mathbf{1})$ — моноид, то вводят нулевую степень $a^0 = \mathbf{1}$.

Если $(A, *, \mathbf{1})$ — группа, то для любого элемента a вводят отрицательную степень согласно равенству: $a^{-n} = (a^{-1})^n$, $n = 1, 2, \dots$ (Отрицательная степень элемента a группы есть положительная степень элемента, обратного к a .)

Определение 8.1.

В полугруппе $(A, *)$ **n -я степень элемента a** есть элемент $\underbrace{a * a * \dots * a}_{n \text{ раз}}$, обозначаемый a^n , причем $a^1 = a$ и $a^n = a * a^{n-1}$, $n = 2, 3, \dots$

Если $(A, *, \mathbf{1})$ — моноид, то вводят нулевую степень $a^0 = \mathbf{1}$.

Если $(A, *, \mathbf{1})$ — группа, то для любого элемента a вводят отрицательную степень согласно равенству: $a^{-n} = (a^{-1})^n$, $n = 1, 2, \dots$ (Отрицательная степень элемента a группы есть положительная степень элемента, обратного к a .)

Свойства степеней

Определение 8.1.

В полугруппе $(A, *)$ **n -я степень элемента a** есть элемент $\underbrace{a * a * \dots * a}_{n \text{ раз}}$, обозначаемый a^n , причем $a^1 = a$ и $a^n = a * a^{n-1}$,
 $n = 2, 3, \dots$

Если $(A, *, \mathbf{1})$ — моноид, то вводят нулевую степень $a^0 = \mathbf{1}$.

Если $(A, *, \mathbf{1})$ — группа, то для любого элемента a вводят отрицательную степень согласно равенству: $a^{-n} = (a^{-1})^n$, $n = 1, 2, \dots$
(Отрицательная степень элемента a группы есть положительная степень элемента, обратного к a .)

Свойства степеней

Утверждение 8.1.

1) Для любой полугруппы $a^m * a^n = a^{m+n}$; $(a^m)^n = a^{mn}$ ($m, n \in \mathbb{N}$);

Определение 8.1.

В полугруппе $(A, *)$ **n -я степень элемента a** есть элемент $\underbrace{a * a * \dots * a}_{n \text{ раз}}$, обозначаемый a^n , причем $a^1 = a$ и $a^n = a * a^{n-1}$,
 $n = 2, 3, \dots$

Если $(A, *, \mathbf{1})$ — моноид, то вводят нулевую степень $a^0 = \mathbf{1}$.

Если $(A, *, \mathbf{1})$ — группа, то для любого элемента a вводят отрицательную степень согласно равенству: $a^{-n} = (a^{-1})^n$, $n = 1, 2, \dots$
(Отрицательная степень элемента a группы есть положительная степень элемента, обратного к a .)

Свойства степеней

Утверждение 8.1.

- 1) Для любой полугруппы $a^m * a^n = a^{m+n}$; $(a^m)^n = a^{mn}$ ($m, n \in \mathbb{N}$);
- 2) для любой группы $a^{-n} = (a^n)^{-1}$ ($n \in \mathbb{N}$), $a^m * a^n = a^{m+n}$ ($m, n \in \mathbb{Z}$).

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a .

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Далее $1 \cdot 1 = 1$,

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Далее $1 \cdot 1 = 1$, $2 \cdot 1 = 1 + 1 = 2$ и т.д.

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Далее $1 \cdot 1 = 1$, $2 \cdot 1 = 1 + 1 = 2$ и т.д.

Для произвольного n имеем

$$n \cdot 1 = \underbrace{1 + \dots + 1}_{n \text{ раз}} = n.$$

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Далее $1 \cdot 1 = 1$, $2 \cdot 1 = 1 + 1 = 2$ и т.д.

Для произвольного n имеем

$$n \cdot 1 = \underbrace{1 + \dots + 1}_{n \text{ раз}} = n.$$

б) Группа $(\mathbb{Z}_5, \odot_5, 1)$ — циклическая с образующим элементом 2.

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Далее $1 \cdot 1 = 1$, $2 \cdot 1 = 1 + 1 = 2$ и т.д.

Для произвольного n имеем

$$n \cdot 1 = \underbrace{1 + \dots + 1}_{n \text{ раз}} = n.$$

б) Группа $(\mathbb{Z}_5, \odot_5, 1)$ — циклическая с образующим элементом 2. Действительно, для 2 имеем $2^0 = 1$,

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Далее $1 \cdot 1 = 1$, $2 \cdot 1 = 1 + 1 = 2$ и т.д.

Для произвольного n имеем

$$n \cdot 1 = \underbrace{1 + \dots + 1}_{n \text{ раз}} = n.$$

б) Группа $(\mathbb{Z}_5, \odot_5, 1)$ — циклическая с образующим элементом 2. Действительно, для 2 имеем $2^0 = 1$, $2^1 = 2$,

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Далее $1 \cdot 1 = 1$, $2 \cdot 1 = 1 + 1 = 2$ и т.д.

Для произвольного n имеем

$$n \cdot 1 = \underbrace{1 + \dots + 1}_{n \text{ раз}} = n.$$

б) Группа $(\mathbb{Z}_5, \odot_5, 1)$ — циклическая с образующим элементом 2.

Действительно, для 2 имеем $2^0 = 1$, $2^1 = 2$, $2^2 = 2 \odot_5 2 = 4$,

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Далее $1 \cdot 1 = 1$, $2 \cdot 1 = 1 + 1 = 2$ и т.д.

Для произвольного n имеем

$$n \cdot 1 = \underbrace{1 + \dots + 1}_{n \text{ раз}} = n.$$

б) Группа $(\mathbb{Z}_5, \odot_5, 1)$ — циклическая с образующим элементом 2.

Действительно, для 2 имеем $2^0 = 1$, $2^1 = 2$, $2^2 = 2 \odot_5 2 = 4$,
 $2^3 = 2 \odot_5 2^2 = 2 \odot_5 4 = 3$,

Определение 8.2. Полугруппу (группу) $(A, *)$ называют **циклической**, если существует такой элемент a , что любой элемент x полугруппы (группы) является некоторой (целой) степенью элемента a . Элемент a называют **образующим элементом полугруппы (группы)**.

Замечание. При аддитивной форме записи вместо a^n пишут $n \cdot a$.

Пример 1. а) Полугруппа $(\mathbb{N}, +, 0)$ — циклическая, с образующим элементом 1.

Следуя определению 8.1, получим $0 \cdot 1 = 0$.

Далее $1 \cdot 1 = 1$, $2 \cdot 1 = 1 + 1 = 2$ и т.д.

Для произвольного n имеем

$$n \cdot 1 = \underbrace{1 + \dots + 1}_{n \text{ раз}} = n.$$

б) Группа $(\mathbb{Z}_5, \odot_5, 1)$ — циклическая с образующим элементом 2.

Действительно, для 2 имеем $2^0 = 1$, $2^1 = 2$, $2^2 = 2 \odot_5 2 = 4$, $2^3 = 2 \odot_5 2^2 = 2 \odot_5 4 = 3$, $2^4 = 2 \odot_5 3 = 1$.

Порядком конечной группы называют количество ее элементов.

Порядком конечной группы называют количество ее элементов.
Аддитивная группа вычетов по модулю k имеет порядок k .

Порядком конечной группы называют количество ее элементов.
Аддитивная группа вычетов по модулю k имеет порядок k .
Группа подстановок S_n есть группа порядка $n!$.

Порядком конечной группы называют количество ее элементов.

Аддитивная группа вычетов по модулю k имеет порядок k .

Группа подстановок S_n есть группа порядка $n!$.

Мультипликативная группа вычетов по модулю p (p — простое число!) имеет порядок $p - 1$.

Порядком конечной группы называют количество ее элементов.

Аддитивная группа вычетов по модулю k имеет порядок k .

Группа подстановок S_n есть группа порядка $n!$.

Мультипликативная группа вычетов по модулю p (p — простое число!) имеет порядок $p - 1$.

Определение 8.3.

Группу $\mathcal{H} = (H, *, {}^{-1}, \mathbf{1})$ называют **подгруппой** группы $\mathcal{G} = (G, *, {}^{-1}, \mathbf{1})$, если

H есть подмножество G , замкнутое относительно операции $*$,

Порядком конечной группы называют количество ее элементов.

Аддитивная группа вычетов по модулю k имеет порядок k .

Группа подстановок S_n есть группа порядка $n!$.

Мультипликативная группа вычетов по модулю p (p — простое число!) имеет порядок $p - 1$.

Определение 8.3.

Группу $\mathcal{H} = (H, *, {}^{-1}, \mathbf{1})$ называют **подгруппой** группы $\mathcal{G} = (G, *, {}^{-1}, \mathbf{1})$, если

H есть подмножество G , замкнутое относительно операции $*$, содержащее *единицу* $\mathbf{1}$ группы \mathcal{G}

Порядком конечной группы называют количество ее элементов.

Аддитивная группа вычетов по модулю k имеет порядок k .

Группа подстановок S_n есть группа порядка $n!$.

Мультипликативная группа вычетов по модулю p (p — простое число!) имеет порядок $p - 1$.

Определение 8.3.

Группу $\mathcal{H} = (H, *, ^{-1}, \mathbf{1})$ называют **подгруппой** группы $\mathcal{G} = (G, *, ^{-1}, \mathbf{1})$, если

H есть подмножество G , замкнутое относительно операции $*$, содержащее *единицу* $\mathbf{1}$ группы \mathcal{G}

и вместе с каждым элементом $x \in H$ содержащее элемент x^{-1} , обратный к x .

Порядком конечной группы называют количество ее элементов.

Аддитивная группа вычетов по модулю k имеет порядок k .

Группа подстановок S_n есть группа порядка $n!$.

Мультипликативная группа вычетов по модулю p (p — простое число!) имеет порядок $p - 1$.

Определение 8.3.

Группу $\mathcal{H} = (H, *, ^{-1}, \mathbf{1})$ называют **подгруппой** группы $\mathcal{G} = (G, *, ^{-1}, \mathbf{1})$, если

H есть подмножество G , замкнутое относительно операции $*$, содержащее *единицу* $\mathbf{1}$ группы \mathcal{G}

и вместе с каждым элементом $x \in H$ содержащее элемент x^{-1} , обратный к x .

Определение 8.4.

Подгруппу группы \mathcal{G} , заданную на множестве всех *степеней* фиксированного *элемента* a , называют **циклической подгруппой** группы \mathcal{G} , порожденной элементом a .

Порядком конечной группы называют количество ее элементов.

Аддитивная группа вычетов по модулю k имеет порядок k .

Группа подстановок S_n есть группа порядка $n!$.

Мультипликативная группа вычетов по модулю p (p — простое число!) имеет порядок $p - 1$.

Определение 8.3.

Группу $\mathcal{H} = (H, *, ^{-1}, \mathbf{1})$ называют **подгруппой** группы $\mathcal{G} = (G, *, ^{-1}, \mathbf{1})$, если

H есть подмножество G , замкнутое относительно операции $*$, содержащее *единицу* $\mathbf{1}$ группы \mathcal{G}

и вместе с каждым элементом $x \in H$ содержащее элемент x^{-1} , обратный к x .

Определение 8.4.

Подгруппу группы \mathcal{G} , заданную на множестве всех *степеней* фиксированного *элемента* a , называют **циклической подгруппой** группы \mathcal{G} , порожденной элементом a .

Задача 1. Найти циклическую подгруппу \mathcal{H} группы Z_{11}^{\odot} с образующим элементом

Порядком конечной группы называют количество ее элементов.

Аддитивная группа вычетов по модулю k имеет порядок k .

Группа подстановок S_n есть группа порядка $n!$.

Мультипликативная группа вычетов по модулю p (p — простое число!) имеет порядок $p - 1$.

Определение 8.3.

Группу $\mathcal{H} = (H, *, ^{-1}, \mathbf{1})$ называют **подгруппой** группы $\mathcal{G} = (G, *, ^{-1}, \mathbf{1})$, если

H есть подмножество G , замкнутое относительно операции $*$, содержащее *единицу* $\mathbf{1}$ группы \mathcal{G}

и вместе с каждым элементом $x \in H$ содержащее элемент x^{-1} , обратный к x .

Определение 8.4.

Подгруппу группы \mathcal{G} , заданную на множестве всех *степеней* фиксированного *элемента* a , называют **циклической подгруппой** группы \mathcal{G} , порожденной элементом a .

Задача 1. Найти циклическую подгруппу \mathcal{H} группы Z_{11}^{\odot} с образующим элементом

а) $a = 4$;

Порядком конечной группы называют количество ее элементов.

Аддитивная группа вычетов по модулю k имеет порядок k .

Группа подстановок S_n есть группа порядка $n!$.

Мультипликативная группа вычетов по модулю p (p — простое число!) имеет порядок $p - 1$.

Определение 8.3.

Группу $\mathcal{H} = (H, *, ^{-1}, \mathbf{1})$ называют **подгруппой** группы $\mathcal{G} = (G, *, ^{-1}, \mathbf{1})$, если

H есть подмножество G , замкнутое относительно операции $*$, содержащее *единицу* $\mathbf{1}$ группы \mathcal{G}

и вместе с каждым элементом $x \in H$ содержащее элемент x^{-1} , обратный к x .

Определение 8.4.

Подгруппу группы \mathcal{G} , заданную на множестве всех *степеней* фиксированного *элемента* a , называют **циклической подгруппой** группы \mathcal{G} , порожденной элементом a .

Задача 1. Найти циклическую подгруппу \mathcal{H} группы Z_{11}^{\odot} с образующим элементом

а) $a = 4$;

б) $a = 2$.

Пусть $\mathcal{G} = (G, *, 1)$ — группа, а $\mathcal{H} = (H, *, 1)$ — ее подгруппа.

Пусть $\mathcal{G} = (G, *, 1)$ — группа, а $\mathcal{H} = (H, *, 1)$ — ее подгруппа.

Определение 8.5. Левым смежным классом подгруппы \mathcal{H} по элементу $a \in G$ называют множество

$$aH = \{y \mid y = a * h, h \in H\}.$$

Пусть $\mathcal{G} = (G, *, 1)$ — группа, а $\mathcal{H} = (H, *, 1)$ — ее подгруппа.

Определение 8.5. **Левым смежным классом** подгруппы \mathcal{H} по элементу $a \in G$ называют множество

$$aH = \{y \mid y = a * h, h \in H\}.$$

Соответственно, **правый смежный класс** подгруппы \mathcal{H} по элементу $a \in G$ — это множество $Ha = \{y \mid y = h * a, h \in H\}$.

Пусть $\mathcal{G} = (G, *, 1)$ — группа, а $\mathcal{H} = (H, *, 1)$ — ее подгруппа.

Определение 8.5. Левым смежным классом подгруппы \mathcal{H} по элементу $a \in G$ называют множество

$$aH = \{y \mid y = a * h, h \in H\}.$$

Соответственно, **правый смежный класс** подгруппы \mathcal{H} по элементу $a \in G$ — это множество $Ha = \{y \mid y = h * a, h \in H\}$.

Задача 2. Найти левый смежный класс aH циклической подгруппы \mathcal{H} с образующим элементом $b = 4$ мультипликативной группы Z_{11}^* по элементу $a = 3$.

Теорема 1. (Лагранж) *Порядок конечной группы* делится на порядок любой ее подгруппы.

Теорема 1. (Лагранж) *Порядок конечной группы* делится на порядок любой ее подгруппы.

Задача 3. Может ли некоторая подгруппа мультипликативной группы Z_{97}^* содержать 23 элемента?

Теорема 1. (Лагранж) *Порядок конечной группы* делится на порядок любой ее подгруппы.

Задача 3. Может ли некоторая подгруппа мультипликативной группы Z_{97}^* содержать 23 элемента? 24 элемента?

Теорема 1. (Лагранж) *Порядок конечной группы* делится на порядок любой ее подгруппы.

Задача 3. Может ли некоторая подгруппа мультипликативной группы Z_{97}^* содержать 23 элемента? 24 элемента? 32 элемента?

ЭЛЕМЕНТЫ ОБЩЕЙ АЛГЕБРЫ

Кольца. Поля. Решение СЛАУ

Определение 8.6. Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями

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

такая, что:

Определение 8.6. Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями

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

такая, что:

1) алгебра $(R, +, 0)$ — коммутативная группа;

Определение 8.6. Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями

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

такая, что:

- 1) алгебра $(R, +, 0)$ — коммутативная группа;
- 2) алгебра $(R, \cdot, 1)$ — моноид ;

Определение 8.6. Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями

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

такая, что:

- 1) алгебра $(R, +, 0)$ — коммутативная группа;
- 2) алгебра $(R, \cdot, 1)$ — моноид ;
- 3) имеет место дистрибутивность операции $+$ (сложения кольца) относительно операции \cdot (умножения кольца):

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Определение 8.6. Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями

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

такая, что:

- 1) алгебра $(R, +, 0)$ — коммутативная группа;
- 2) алгебра $(R, \cdot, 1)$ — моноид ;
- 3) имеет место дистрибутивность операции $+$ (сложения кольца) относительно операции \cdot (умножения кольца):

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Операцию $+$ называют **сложением кольца**,

Определение 8.6. Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями

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

такая, что:

- 1) алгебра $(R, +, 0)$ — коммутативная группа;
- 2) алгебра $(R, \cdot, 1)$ — моноид ;
- 3) имеет место дистрибутивность операции $+$ (сложения кольца) относительно операции \cdot (умножения кольца):

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Операцию $+$ называют **сложением кольца**, \cdot — **умножением кольца**,

Определение 8.6. Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями

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

такая, что:

- 1) алгебра $(R, +, 0)$ — коммутативная группа;
- 2) алгебра $(R, \cdot, 1)$ — моноид ;
- 3) имеет место дистрибутивность операции $+$ (сложения кольца) относительно операции \cdot (умножения кольца):

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Операцию $+$ называют **сложением кольца**, \cdot — **умножением кольца**, элемент 0 — **нулем кольца**,

Определение 8.6. Кольцо — это алгебра с двумя бинарными и двумя нульарными операциями

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

такая, что:

- 1) алгебра $(R, +, 0)$ — коммутативная группа;
- 2) алгебра $(R, \cdot, 1)$ — моноид ;
- 3) имеет место дистрибутивность операции $+$ (сложения кольца) относительно операции \cdot (умножения кольца):

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Операцию $+$ называют **сложением кольца**, \cdot — **умножением кольца**, элемент 0 — **нулем кольца**, элемент 1 — **единицей кольца**.

Определение 8.7. Кольцо называют **коммутативным**, если операция умножения в нем коммутативна.

Пример 2.

а) Алгебра $(\mathbb{Z}, +, \cdot, 0, 1)$ есть коммутативное кольцо.

Пример 2.

а) Алгебра $(\mathbb{Z}, +, \cdot, 0, 1)$ есть коммутативное кольцо.

б) Алгебра $(\mathbb{N}, +, \cdot, 0, 1)$ кольцом не будет, поскольку $(\mathbb{N}, +)$ — коммутативный моноид, но не группа.

Пример 2.

а) Алгебра $(\mathbb{Z}, +, \cdot, 0, 1)$ есть коммутативное кольцо.

б) Алгебра $(\mathbb{N}, +, \cdot, 0, 1)$ кольцом не будет, поскольку $(\mathbb{N}, +)$ — коммутативный моноид, но не группа.

б) Алгебра

$$\mathbb{Z}_k = (\{0, 1, 2, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$$

(при $k \geq 1$), аддитивная группа которого есть *аддитивная группа вычетов по модулю k* ,

Пример 2.

а) Алгебра $(\mathbb{Z}, +, \cdot, 0, 1)$ есть коммутативное кольцо.

б) Алгебра $(\mathbb{N}, +, \cdot, 0, 1)$ кольцом не будет, поскольку $(\mathbb{N}, +)$ — коммутативный моноид, но не группа.

б) Алгебра

$$\mathbb{Z}_k = (\{0, 1, 2, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$$

(при $k \geq 1$), аддитивная группа которого есть *аддитивная группа вычетов по модулю k* , а операция умножения по модулю k определена аналогично сложению по модулю k , т.е. $m \odot n$ равно остатку от деления на k числа $m \cdot n$,

Пример 2.

а) Алгебра $(\mathbb{Z}, +, \cdot, 0, 1)$ есть коммутативное кольцо.

б) Алгебра $(\mathbb{N}, +, \cdot, 0, 1)$ кольцом не будет, поскольку $(\mathbb{N}, +)$ — коммутативный моноид, но не группа.

б) Алгебра

$$\mathbb{Z}_k = (\{0, 1, 2, \dots, k-1\}, \oplus_k, \odot_k, 0, 1)$$

(при $k \geq 1$), аддитивная группа которого есть *аддитивная группа вычетов по модулю k* , а операция умножения по модулю k определена аналогично сложению по модулю k , т.е. $m \odot n$ равно остатку от деления на k числа $m \cdot n$, есть коммутативное кольцо. Его называют **кольцом вычетов по модулю k** .

Определение 8.8. Ненулевые элементы a и b кольца \mathcal{R} называют делителями нуля, если $a \cdot b = 0$.

Определение 8.8. Ненулевые элементы a и b кольца \mathcal{R} называют делителями нуля, если $a \cdot b = 0$.

Задача 4. Существуют ли делители нуля в кольце вычетов по модулю 4 Z_4 .

Определение 8.8. Ненулевые элементы a и b кольца \mathcal{R} называют делителями нуля, если $a \cdot b = 0$.

Задача 4. Существуют ли делители нуля в кольце вычетов по модулю 4 Z_4 . В кольце Z_5 ?

Определение 8.8. Ненулевые элементы a и b кольца \mathcal{R} называют делителями нуля, если $a \cdot b = 0$.

Задача 4. Существуют ли делители нуля в кольце вычетов по модулю 4 Z_4 . В кольце Z_5 ? При каких n Z_n не содержит делителей нуля?

Определение 8.9. Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют **телом**.

Определение 8.9. Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют **телом**.
Коммутативное тело называют **полем**.

Определение 8.9. Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют **телом**.

Коммутативное тело называют **полем**.

Группу ненулевых элементов поля по умножению называют **мультипликативной группой** этого **поля**.

Определение 8.9. Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют **телом**.

Коммутативное тело называют **полем**.

Группу ненулевых элементов поля по умножению называют **мультипликативной группой** этого **поля**.

Пример 3.

а) Алгебра $(\mathbb{Q}, +, \cdot, 0, 1)$ есть поле, называемое **полем рациональных чисел**.

Определение 8.9. Кольцо, в котором множество всех ненулевых элементов по умножению образует группу, называют **телом**.

Коммутативное тело называют **полем**.

Группу ненулевых элементов поля по умножению называют **мультипликативной группой** этого поля.

Пример 3.

а) Алгебра $(\mathbb{Q}, +, \cdot, 0, 1)$ есть поле, называемое **полем рациональных чисел**.

б) Алгебра $(\mathbb{R}, +, \cdot, 0, 1)$ есть поле, называемое **полем вещественных чисел**.

Задача 5. Какие из числовых множеств образуют кольцо относительно обычных операций умножения и сложения:

Задача 5. Какие из числовых множеств образуют кольцо относительно обычных операций умножения и сложения:

(а) множество неотрицательных целых чисел;

Задача 5. Какие из числовых множеств образуют кольцо относительно обычных операций умножения и сложения:

- (а) множество неотрицательных целых чисел;
- (б) множество чисел вида $x + \sqrt{2}y$, $x, y \in \mathbb{Q}$?

Задача 5. Какие из числовых множеств образуют кольцо относительно обычных операций умножения и сложения:

- (а) множество неотрицательных целых чисел;
 - (б) множество чисел вида $x + \sqrt{2}y$, $x, y \in \mathbb{Q}$?
- Какие из указанных колец являются полями?

Задача 5. Какие из числовых множеств образуют кольцо относительно обычных операций умножения и сложения:

- (а) множество неотрицательных целых чисел;
- (б) множество чисел вида $x + \sqrt{2}y$, $x, y \in \mathbb{Q}$?

Какие из указанных колец являются полями?

Задача 6. Какие из множеств матриц образуют кольцо относительно матричных операций умножения и сложения? Какие из колец являются полями?

Задача 5. Какие из числовых множеств образуют кольцо относительно обычных операций умножения и сложения:

(а) множество неотрицательных целых чисел;

(б) множество чисел вида $x + \sqrt{2}y$, $x, y \in \mathbb{Q}$?

Какие из указанных колец являются полями?

Задача 6. Какие из множеств матриц образуют кольцо относительно матричных операций умножения и сложения? Какие из колец являются полями?

(а) множество матриц вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $a, b, c \in \mathbb{R}$?

Задача 5. Какие из числовых множеств образуют кольцо относительно обычных операций умножения и сложения:

- (а) множество неотрицательных целых чисел;
- (б) множество чисел вида $x + \sqrt{2}y$, $x, y \in \mathbb{Q}$?

Какие из указанных колец являются полями?

Задача 6. Какие из множеств матриц образуют кольцо относительно матричных операций умножения и сложения? Какие из колец являются полями?

- (а) множество матриц вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $a, b, c \in \mathbb{R}$?

- (б) множество матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in \mathbb{R}$?

Задача 5. Какие из числовых множеств образуют кольцо относительно обычных операций умножения и сложения:

- (а) множество неотрицательных целых чисел;
- (б) множество чисел вида $x + \sqrt{2}y$, $x, y \in \mathbb{Q}$?

Какие из указанных колец являются полями?

Задача 6. Какие из множеств матриц образуют кольцо относительно матричных операций умножения и сложения? Какие из колец являются полями?

- (а) множество матриц вида $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $a, b, c \in \mathbb{R}$?

- (б) множество матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in \mathbb{R}$?

Задача 7. Составить таблицу Кэли для операций сложения и умножения в кольцах вычетов \mathbb{Z}_3 и \mathbb{Z}_5 . Показать, что \mathbb{Z}_3 и \mathbb{Z}_5 являются полями.

Теорема 2. В любом кольце выполняются следующие тождества

Теорема 2. В любом кольце выполняются следующие тождества

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

Теорема 2. В любом кольце выполняются следующие тождества

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

2) $(a - b) \cdot c = a \cdot c - b \cdot c$,

Теорема 2. В любом кольце выполняются следующие тождества

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

2) $(a - b) \cdot c = a \cdot c - b \cdot c$,

$c \cdot (a - b) = c \cdot a - c \cdot b$, где *разность* $a - b$ есть по определению $a - b = a + (-b)$.

Теорема 2. В любом кольце выполняются следующие тождества

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

2) $(a - b) \cdot c = a \cdot c - b \cdot c$,

$c \cdot (a - b) = c \cdot a - c \cdot b$, где *разность* $a - b$ есть по определению $a - b = a + (-b)$.

Следствие 8.1. В любом кольце справедливы тождества:

$$a \cdot (-b) = (-a) \cdot b = -a \cdot b$$

(в частности, $(-1) \cdot x = x \cdot (-1) = -x$).

Теорема 2. В любом кольце выполняются следующие тождества

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

2) $(a - b) \cdot c = a \cdot c - b \cdot c$,

$c \cdot (a - b) = c \cdot a - c \cdot b$, где *разность* $a - b$ есть по определению $a - b = a + (-b)$.

Следствие 8.1. В любом кольце справедливы тождества:

$$a \cdot (-b) = (-a) \cdot b = -a \cdot b$$

(в частности, $(-1) \cdot x = x \cdot (-1) = -x$).

Таким образом, производя вычисления в любом кольце (поле), можно раскрывать скобки и менять знаки так же, как в обычной школьной алгебре.

Задача 8.

Решить в поле \mathbb{Z}_3 и в поле \mathbb{Z}_5 систему уравнений:

$$\begin{cases} x + 2y = 1, \\ y + 2z = 2, \\ 2x + z = 1. \end{cases}$$

Задача 8.

Решить в поле \mathbb{Z}_3 и в поле \mathbb{Z}_5 систему уравнений:

$$\begin{cases} x + 2y = 1, \\ y + 2z = 2, \\ 2x + z = 1. \end{cases}$$

Задача 9.

Решить в поле \mathbb{Z}_5 и в поле \mathbb{Z}_7 систему уравнений:

$$\begin{cases} 2x + 3y = 1, \\ 3x - 4y = 2. \end{cases}$$

Задача 8.

Решить в поле \mathbb{Z}_3 и в поле \mathbb{Z}_5 систему уравнений:

$$\begin{cases} x + 2y = 1, \\ y + 2z = 2, \\ 2x + z = 1. \end{cases}$$

Задача 9.

Решить в поле \mathbb{Z}_5 и в поле \mathbb{Z}_7 систему уравнений:

$$\begin{cases} 2x + 3y = 1, \\ 3x - 4y = 2. \end{cases}$$

Задача 10.

Разрешима ли в кольце \mathbb{Z}_{21} система уравнений:

$$\begin{cases} 5x + 2y = 1, \\ y - 11x = 13? \end{cases}$$

Дополнительные задачи

8.1. Кольцо R называется булевым, если $\forall x \in R \quad x^2 = x$. Доказать:

- (а) в любом булевом кольце $\forall x \in R \quad x + x = 0$;
- (б) любое булево кольцо коммутативно;
- (в) в любом булевом кольце мощности больше 2 есть делители нуля.

8.2. Доказать, что $(2^M, \Delta, \cap, \emptyset, M)$ — булево кольцо. Доказать, что оно изоморфно \mathbb{Z}_2 при $|M| = 1$.

8.3. Будет ли любое кольцо \mathbb{Z}_{2^n} , $n \geq 1$, булевым?

8.4. Доказать:

- (а) если элемент кольца обратим (слева, справа), то он не является делителем нуля (левым, правым);
- (б) в конечном кольце любой односторонне обратимый элемент обратим;
- (в) элемент кольца вычетов по $\text{mod } k$ обратим тогда и только тогда, когда он взаимно прост с k .