ПРИДНЕСТРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. Т.Г. ШЕВЧЕНКО

Факультет физико-математический
Кафедра алгебры, геометрии и МПМ

КУРС ЛЕКЦИЙ
ПО ЧИСЛОВЫМ СИСТЕМАМ

Учебное пособие

Тирасполь - 2016

УДК 511(072.8)
ББК В13р30
Ч67

Составители:

Г.Н. Ермакова, к.п.н., доцент, и.о. зав. кафедрой алгебры, геометрии и МПМ ПГУ им. Т.Г. Шевченко.

Н.Н. Дидурик, ст. преподаватель кафедры алгебры, геометрии и МПМ, ПГУ им. Т.Г. Шевченко.

Рецензенты:

Ю.М. Рябухин, д.ф-м.н., профессор кафедры алгебры, геометрии и МПМ, ПГУ им. Т.Г. Шевченко.

В.И. Арнаутов, академик, д.ф-м.н., профессор, гл. научный сотрудник института математики и информатики АН РМ.

Курс лекций по числовым системам: Учебное пособие сост.: Г.Н. Ермакова, Н.Н. Дидурик – Тирасполь, 2016 - 79 с. – Электронный вариант.

Учебное пособие по числовым системам предназначено для самостоятельной работы студентов физико-математического факультета. Пособие содержит учебный материал для студентов II-IV курсов заочного отделения направления «Математика и информатика».

УДК 511(072.8)
ББК В13р30

Рекомендовано к изданию Научно-методическим советом ПГУ им. Т.Г. Шевченко

ЛИТЕРАТУРА

1. Блох А.Ш. Числовые системы: Уч. пособ. – Мн.: Вышейш. шк., 1982. – 158с.
2. Бухштаб А.А. Теория чисел: Уч. пособ. – М.: Просвещение, 1966. – 384с.
3. Виноградов И.М. Основы теории чисел: Учебник. – М.: Наука, 1972. – 167с. 1965. – 172с.
4. Галочкин А.И. и др. введение в теорию чисел: Уч. пособ. – М.: МГУ, 1984. – 147с.
5. Кононов С.Г. и др. Введение в математику. В 3-х ч.: Уч. пособ. – Мн.: БГУ. Ч. 1. 2003. – 171с. Ч. 2. 2003. – 126с. Ч. 3. 2003. – 74с.
6. Нечаев В.И. Числовые системы, М., Просвещение, 1975.
7. Нечаев В.И. Числовые системы, М., Просвещение, 1975.
8. Арнольд И.В. Теоретическая арифметика, Учпедгиз, 1939.
9. Драбкин М.Е. Основания арифметики, Минск, 1962.

Учебное издание
Курс лекций по числовым системам
Составители:
Галина Николаевна Ермакова
Наталия Николаевна Дидурик

Формат 60×84/16 Уч.-изд. л. 8,3
Электронное издание

$i \cdot i_5 + i_5 i = 2 \cdot c_1$, $j \cdot i_5 + i_5 \cdot j = 2 \cdot c_2$, $k \cdot i_5 + i_5 \cdot k = 2 \cdot c_3$. Из этих равенств найдем $i_5 \cdot k$.

Так как $k = i \cdot j = i$, то $i_5 \cdot k = i_5 \cdot (i \cdot j) = (i_5 \cdot i) \cdot j = (2 \cdot c_1 - i \cdot i_5) \cdot j =$
$= 2 \cdot c_1 \cdot j - i \cdot (i_5 \cdot j) == 2 \cdot c_1 \cdot j - i \cdot (2 \cdot c_2 - j \cdot i_5) = 2 \cdot c_1 \cdot j - 2 \cdot c_2 \cdot i +$
$+ (i \cdot j) \cdot i_5 = 2 \cdot c_1 \cdot j - 2 \cdot c_2 \cdot i + k \cdot i_5 = 2 \cdot c_1 \cdot j - 2 \cdot c_2 \cdot i + 2 \cdot c_3 - i_5 \cdot k.$
Отсюда $i_5 k = c_1 j - c_2 i + c_3$ или $i_5 k = c_3 - c_2 i + c_1 j$. Умножим обе части последнего равенства на k справа $i_5 k^2 = c_3 k - c_2 ik + c_1 jk$, получим $(-i_5) = c_3 k + c_2 j + c_1 i$, откуда $i_5 = -c_1 i - c_2 j - c_3 k$. Но это означает, что i_5 линейно зависит от i, j, k. Мы пришли к противоречию с допущением, следовательно, не существует алгебры с делением ранга $n > 4$.

Теорема Фробениуса замечательна тем, что устанавливает предел расширения числовых полей, а именно, последним числовым полем, включающим все предшествующие числовые поля и кольца в порядке их расширения, является некоммутативное поле кватернионов. Если же не требовать, чтобы числовая система была полем, то есть алгеброй с делением, то возможно построение сколько угодно гиперкомплексных систем или алгебр любого ранга, притом не только над полем действительных чисел, но и над другими полями. Так, например, над полем комплексных чисел можно построить алгебру бикватернионов. Элемент этой алгебры бикватернион имеет вид $a + b \cdot i + c \cdot j + d \cdot k$, причем a, b, c, d комплексные числа, а $1, i, j, k$ – базисные единицы с такой же таблицей умножения, как в алгебре кватернионов. Но алгебра бикватернионов не обладает делением.

ОГЛАВЛЕНИЕ

Умножив левую и правую части последнего равенства слева на i_2, получим $-j = c_0 i_2 - c_1 + c_2 i_2 j = c_0 c i_2 - c_1 + c_2(c_0 + c_1 i_2 + c_2 j) =$

$= (c_0 c_2 - c_1) + (c_0 + c_1 c_2) i_2 + c_2^2 j$

Откуда $(c_0 c_2 - c_1) + (c_0 + c_1 c_2) i_2 + (c_2^2 + 1) j = 0$.

Так как $1, i_2, j$, то $(c_0 c_2 - c_1) = (c_0 + c_1 c_2) = (c_2^2 + 1) = 0$. Но $c_2^2 \neq -1$, так как $c_2 \in R$. Таким образом, сделанное допущение неверно, значит $i_2 j = k$ линейно независимо от $1, i_2, j$.

Итак, при $n > 2$ алгебра A содержит не менее четырех линейно независимых элементов $1, i_2, j, k$. Значит, нет алгебры A с делением ранга $n = 3$.

Заменим базис $1, i_2, i_3, ,..., i_n$ новым базисом $1, i, j, k, i_5, ..., i_n$, где $i = i_2$ I,

$j = \dfrac{c i_2 + i_3}{\sqrt{1 - c^2}}$, $k = ij$.

При $n = 4$ имеем базис $1, i, j, k$. Всякий элемент алгебры принимает вид $t = a + bi + cj + dk$. Таблица умножения базисных элементов такая же, как для кватернионов:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Итак при $n = 4$ алгебра A с делением есть тело T кватернионов. $A = T$.

4) Остается убедиться в том, что ранг алгебры A с делением не может превышать $n = 4$.

Допустим противное. Пусть $n > 4$, то есть, базис алгебры A состоящий из элементов $1, i, j, k, i_5, ..., i_n$ содержит, по меньшей мере, пять линейно независимых элементов $1, i, j, k, i_5$. Согласно (5) можно записать:

Из равенства (1) следует, что в качестве α и β можно взять i_2 и i_3, тогда согласно равенству (5), получим

$$i_2 i_3 + i_3 i_2 = 2c. \qquad (6)$$

Покажем теперь, что в A существует такой элемент

$$j = a_0 + a_1 i_2 + a_2 i_3, \qquad (7)$$

что $j^2 = -1$ и $i_2 j + j i_2 = 0,$ т.е. $\left(a_0 + a_1 i_2 + a_2 i_3\right)^2 = -1$ и $i_2\left(a_0 + a_1 i_2 + a_2 i_3\right) + \left(a_0 + a_1 i_2 + a_2 i_3\right) i_2 = 0$.

Из последнего равенства с учетом (6), получим

$$a_0 i_2 + a_1 i_2^2 + a_2 i_2 i_3 + a_0 i_2 + a_1 i_2^2 + a_2 i_3 i_2 = 2a_0 i_2 - 2a_1 +$$
$$+ a_2\left(i_2 i_3 + i_3 i_2\right) = 2a_0 i_2 - 2a_1 + 2a_2 c = 0,$$

откуда $a_0 i_2 - a_1 + a_2 c = 0$ или $a_0 i_2 + \left(a_2 c - a_1\right) = 0$.

Ввиду линейной независимости i_2 и 1, получим $a_0 = 0$ и $a_2 c - a_1 = 0,$ откуда $a_1 = a_2 c.$ Подставив в равенство (7) $a_0 = 0$ и $a_2 c - a_1 = 0,$ получим $\left(c a_2 i_2 + a_2 i_3\right)^2 = -1,$ откуда $a_2^2\left(c i_2 + i_3\right) = -1$ или $a_2^2\left(-c^2 + c i_2 i_3 + c i_3 i_2 - 1\right) = -1.$

Учитывая равенство (6), получим $a_2^2\left(-c^2 + 2c^2 - 1\right) = -1$ или $a_2^2\left(c^2 - 1\right) = -1,$ откуда $a_2^2 = \dfrac{1}{1 - c^2}$ или $a_2 = \dfrac{1}{\sqrt{1 - c^2}}$.

Искомый элемент $j = a_0 + a_1 i_2 + a_2 i_3 = a_2 c i_2 + a_2 i_3 = a_2\left(c i_2 + i_3\right) =$

$$= \frac{c i_2 + i_3}{\sqrt{1 - c^2}}.$$

Итак, j линейно выражается через i_2 и i_3. Система $1, i_2, i_3$ и i_3 линейно независима, тогда система $1, i_2, j$ также линейно независима.

Докажем теперь, что элемент $i_2 j = k$ линейно независим от $1, i_2, j$.

Допустим противное, т.е. допустим, что $i_2 j$ линейно зависим от $1, i_2, j$, т.е. $i_2 j = c_0 + c_1 i_2 + c_2 j,$ где $c_0, c_1, c_2 \in R$.

ВВЕДЕНИЕ

1. Бинарные отношения. Отношение эквивалентности и разбиение множества на классы. Фактор множества.

Пусть a, b произвольные объекты, различные или одинаковые, заданные в определенном порядке (сначала a, затем b). Будем говорить, что эти объекты образуют ***упорядоченную пару*** и записывать (a,b).

Определение. Если (a,b) и (c,d) – упорядоченные пары, то

$$1)\,(a,b) = (c,d) \Leftrightarrow a = c \wedge b = d$$
$$2)\,a \neq b \Leftrightarrow (a,b) \neq (b,a)$$

Определение. Прямым произведением множества A на множество B называют множество P, состоящее из всех упорядоченных пар (a,b), первые компоненты которых – элементы множества A, а вторые – элементы множества B.

$$P = A \times B = \left\{(a,b) \,\middle|\, a \in A \wedge b \in B\right\}$$

Примеры.

$A = \{a,b,c\},\ B = \{a,d\}$

$A \times B = \{(a,a),(a,d),(b,a),(b,d),(c,a),(c,d)\}$

$B \times A = \{(a,a),(a,b),(a,c),(d,a),(d,b),(d,c)\} \neq A \times B$

2) R – множество действительных чисел (числовая прямая);

$R \times R$ – совокупность всех пар действительных чисел (числовая плоскость).

Прямое произведение n множеств определяется следующим образом:

$A_1 \times A_2 \times A_3 \times \ldots \times A_n = \left\{(a_1, a_2, a_3, \ldots, a_n) \,\middle|\, a_i \in A_i, i = 1, \ldots n\right\}$, где

$(a_1, a_2, a_3, \ldots, a_n)$ – упорядоченный кортеж.

Определение. Подмножество $\rho \subseteq A \times B$ называется **бинарным отношением** между элементами множеств A и B (или отношением, определенном на паре множеств A, B). Если $A = B$, то ρ называют отношением на множестве A. Если $(a,b) \in \rho$, то $a \rho\, b$ (a и b находятся в отношением ρ).

Определение. **Областью определения** отношения ρ называется множество первых координат элементов из $\rho : Dom\rho$. **Областью значений** отношения ρ называется множество вторых координат элементов из $\rho : Im\,\rho$.

Определение. $\rho = A \times B$ называется универсальным бинарным отношением на паре множеств A, B.

Определение. Если $\rho \subseteq A \times B,$ тогда $\rho^{-1} = \{(b,a) | (a,b) \in \rho\}$.

Определение. Отношение α определенное на множестве A $(\alpha \subseteq A^2)$ обладающее свойством:

1) $\forall x \in A, (x,x) \in \alpha -$ называется **рефлексивным**;

2) $(x,y) \in \alpha \Rightarrow \quad (y,x) \in \alpha$ – называется **симметричным**;

3) $(x,y) \in \alpha \wedge (y,z) \in \alpha \Rightarrow (x,z) \in \alpha$ – называется **транзитивным**;

4) если $(x,y) \in \alpha \wedge (y,x) \in \alpha \Rightarrow x = y$ или если $(x,y) \in \alpha \Rightarrow (y,x) \notin \alpha$, то отношение называется **антисимметричным**;

5) если $\forall x \in A \Rightarrow (x,x) \notin \alpha$, то отношение называется **антирефлексивным**.

Определение. Отношение α определенное на множестве A называется $n-$арным, если $\alpha \subseteq A^n$.

Определение. Отношение α, определенное на множестве A называется **отношением эквивалентности**, если оно рефлексивное, симметричное, транзитивное.

Примеры. 1. Отношение равенства множеств – отношение эквивалентности

а) $\forall A \in I \Rightarrow A = A$ – рефлексивность;

б) $A = B \Leftrightarrow B = A$ – симметричность;

в) $A = B \wedge B = C \Rightarrow A = C$ – транзитивность.

Определение. Разбиением непустого множества A называется совокупность $S(A)$ непустых попарно непересекающихся подмножеств множества A, таких, что объединение всех множеств A_i равно множеству A, т.е.

Так как элементы $\alpha, \beta, 1$ линейно независимы, то $\alpha + \beta$ и $\alpha - \beta$ не могут быть действительными числами. Докажем это.

Допустим, например, что $\alpha + \beta = a$, где $a \in R$, получим, $\alpha \cdot 1 + \beta \cdot 1 - 1 \cdot a = 0,$ а это значит, что система $\alpha, \beta, 1$ линейно зависима, что противоречит выбору элементов системы $\alpha, \beta, 1$.

Итак, $\alpha + \beta, \alpha - \beta \notin R$, тогда по свойству 3 они служат корнями некоторых квадратных уравнений: $x^2 + px + q = 0$ и $x^2 + p_1 x + q_1 = 0$, где $p, q. p_1, q_1 \in R$.

Тогда

$(\alpha + \beta)^2 + p(\alpha + \beta) + q = 0$ и $(\alpha - \beta)^2 + p_1(\alpha - \beta) + q_1 = 0$, откуда получаем

$$\left.\begin{aligned}(\alpha+\beta)^2 &= -p(\alpha+\beta) - q \\ (\alpha-\beta)^2 &= -p_1(\alpha-\beta) - q_1\end{aligned}\right\} \qquad (2)$$

С другой стороны,

$$\left.\begin{aligned}(\alpha+\beta)^2 &= \alpha^2 + \beta^2 + \alpha\cdot\beta + \beta\cdot\alpha = -2 + \alpha\cdot\beta + \beta\cdot\alpha; \\ (\alpha-\beta)^2 &= \alpha^2 + \beta^2 - \alpha\cdot\beta - \beta\cdot\alpha = -2 - \alpha\cdot\beta - \beta\cdot\alpha.\end{aligned}\right\} \qquad (3)$$

Сравнивая правые части равенств (2) и (3) получим

$$\left.\begin{aligned}-2 + \alpha\cdot\beta + \beta\cdot\alpha &= -p(\alpha+\beta) - q \\ -2 - \alpha\cdot\beta - \beta\cdot\alpha &= -p_1(\alpha-\beta) - q_1\end{aligned}\right\} \qquad (4)$$

Сложив почленно равенства (4), получим

$(-4) = -(p + p_1)\alpha - (p - p_1)\beta - (q + q_1)$ или

$(p + p_1)\alpha + (p - p_1)\beta + (q + q_1 - 4) = 0.$

Учитывая, что элементы $\alpha, \beta, 1$ линейно независимы, получим, что $p + p_1 = p - p_1 = q + q_1 - 4 = 0$, откуда $p = p_1 = 0.$ Тогда равенства (4) принимают следующий вид:

$$\left.\begin{aligned}-2 + \alpha\cdot\beta + \beta\cdot\alpha &= -q \\ -2 - \alpha\cdot\beta - \beta\cdot\alpha &= -q_1\end{aligned}\right\} \quad \text{или} \quad \alpha\cdot\beta + \beta\cdot\alpha = 2c, \quad \text{где}$$

$2c = -q + 2 = q_1 - 2$, т.е. $2c \in R$ (5)

1) Если ранг алгебры A равен 1, то все элементы из A будут иметь вид $a \cdot \varepsilon_1 = a \cdot 1 = a$, т.е. будут действительными числами. Следовательно, $A = R$.

2) Если ранг алгебры A больше или равен 2, то поле R будет частью A, и в A будут содержаться элементы, не совпадающие с действительными числами. В частности, базисные элементы $\varepsilon_2, \varepsilon_3, ..., \varepsilon_n$ не являются действительными числами.

Докажем это. Допустим, что какое-либо $\varepsilon_s \neq \varepsilon_1 = 1$ – действительное число, тогда $\varepsilon_s = a = a \cdot 1 = a \cdot \varepsilon_1$, это значит, что ε_S линейно выражается через $\varepsilon_1 = 1$, что невозможно, ввиду линейной независимости базисных элементов.

Согласно третьему свойству всякий элемент из A, не являющийся действительным числом, есть корень некоторого квадратного уравнения $(x-c)^2 + d^2 = 0$, где c и $d \neq 0$ – действительные числа. Следовательно, ε_s, где $s \in \{2,3,...,n\}$ является корнем уравнения такого вида, т. е. $(\varepsilon_s - c)^2 + d^2 = 0$, откуда $\left(\frac{\varepsilon_s - c}{d}\right)^2 + 1 = 0$, тогда $\left(\frac{\varepsilon_S - c}{d}\right)^2 = -1$ (1)

Обозначим $\left(\frac{\varepsilon_s - c}{d}\right) = i_s$ и заменим базис $1, \varepsilon_2, ..., \varepsilon_n$ новым базисом $1, i_2, i_3, ,..., i_n$, для элементов которого выполняется свойство (1), т.е. $i_2^2 = i_3^2 = ... = i_n^2 = -1$.

Если ранг алгебры равен 2, то базис состоит из двух элементов 1 и $i_s = i$, где $i^2 = -1$, а всякий элемент из A имеет вид $a \cdot 1 + b \cdot i$, где $a, b \in R$. Умножение базисных элементов производится следующим образом: 1·1=1, $1 \cdot i = i \cdot 1 = i$, $i^2 = -1$.

Таким образом, при $n = 2$ $A = C$.

3) Посмотрим, что будет представлять собой A при $n > 2$. Возьмем такие независимые элементы $\alpha, \beta, 1 \in A$, чтобы $\alpha^2 = \beta^2 = -1$.

$$S(A) = \left\{ A_i \middle| A_i \neq \varnothing,\ A_i \subseteq A,\ \bigcup A_i = A;\ A \cap A_j = \varnothing,\ i \neq j \right\}$$

Теорема: Каждому бинарному отношению эквивалентности множества A соответствует некоторое разбиение множества. И наоборот, каждому разбиению множества A соответствует бинарное отношение эквивалентности.

Определение. Отношение α, определенное на множестве A назовем отношением «строгого» порядка, если оно антирефлексивно, антисимметрично, транзитивно.

Определение. Отношение $\alpha \subseteq A^2$ назовем отношением «нестрогого» порядка, если оно рефлексивно, антисимметрично, транзитивно.

Примеры.

1. На множестве R $''<''$ – отношение «строгого» порядка;
   $''\leq''$ – отношение «нестрогого» порядка.
2. На множестве J: $''\subseteq''$ – отношение «нестрогого» порядка;
   $''\subset''$ – отношение «строгого» порядка.

Определение. Бинарное отношение f называется **функцией** (отображением), если $\left(\left(\forall x, y, z \in A \quad (x, y) \in f \wedge (x, z) \in f\right) \Rightarrow y = z\right)$.

Определение. Две функции называются равными, если они равны как множества, т.е.

$$(f = g) \Leftrightarrow \left(Domf = Domg \wedge \forall x \in Domf\ f(x) = g(x)\right)$$

Определение. Если $f \subseteq A \times B,\ A = Domf,\ Im\, f \subset B$, то f отображение множества A в B, если при этом из $f(x) = f(y)$ следует, $x = y$ то отображение называют **инъективным** или инъекцией.

Определение. Если $f \subseteq A \times B,\ Domf = A,\ Im\, f = B$, т.е. для любого $y \in B$ существует $x \in A$, такой что $y = f(x)$, то f отображение множества A на B (сюръекция).

Определение. Функция $f : A \to B$ называется **биективной** (взаимно–однозначным отображением), если она сюръективна и инъективна.

Определение. Семейство всех смежных классов множества A по эквивалентности α называется фактор множеством множества A по α и обозначается $S(A) = A/\alpha$.

2. Определение группы, примеры групп, простейшие свойства групп.

Определение. Непустое множество G на котором определена бинарная алгебраическая операция $(\cdot)$ называется группой, если выполняются следующие аксиомы.

$A1.\ \forall a,b,c \in G \Rightarrow (a\cdot b)\cdot c = a\cdot(b\cdot c)$ –ассоциативность

$A2.\ \exists e \in G \,|\, \forall a \in G,\ a\cdot e = a$, где e – правая единица

$A3.\ \forall a \in G\ \exists a^{-1} \in G \,|\, a\cdot a^{-1} = e$, где a^{-1} – правый обратный элемент.

Определение. Если для элементов группы $G(\cdot)$ выполняется

$A4.\ \forall a,b \in G \Rightarrow a\cdot b = b\cdot a$ – коммутативность,

то $G(\cdot)$ – коммутативная группа.

Примеры.

$M=\{1\},\ K=\{1;-1\},\ R^*=R\setminus\{0\},\ Q^*=Q\setminus\{0\},\ C^*=C\setminus\{0\}$ – коммутативные группы;

$$G=\left\{A=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\middle| a_{ij}\in R, |A|\neq 0\right\}$$ – не коммутативная группа;

Свойства.

1. В произведении из n элементов группы скобки можно расставлять произвольно.
2. $\exists! e \in G \,|\, \forall a \in G\ a\cdot e = e\cdot a = a$,
3. $\forall a \in G\ \exists! a^{-1} \in G \,|\, a\cdot a^{-1} = a^{-1}\cdot a = e$.
4. Уравнение $ax = b\ (ya = b)$ имеем в группе $G(\cdot)$ единственное решение.

Определение. Непустое подмножество N группы $G(\cdot)$ называется подгруппой группы $G(\cdot)$ если относительно операции $(\cdot)$ N является группой.

Теорема (критерий подгруппы). Непустое подмножество N группы $G(\cdot)$ является подгруппой группы $G(\cdot)$ тогда и только тогда, когда:

$1.\ \forall h_1,h_2 \in H \Rightarrow h_1\cdot h_2 \in H$;

Пусть A – алгебра с делением ранга n и $\alpha \in A$. Тогда любая система, состоящая из $n+1$ элемента множества A является линейно зависимой, в частности, система элементов $\alpha^n,\alpha^{n-1},...,\alpha,1$ множества A является линейно зависимой. Тогда по определению линейно зависимых систем существует упорядоченный не нулевой набор $a_n,a_{n-1},...,a_1,a_0$ действительных чисел такой, что $a_n\cdot\alpha^n + a_{n-1}\cdot\alpha^{n-1} +,,,+a_1\cdot\alpha + a_0 = 0$. Следовательно, α является корнем не нулевого многочлена степени n с действительными коэффициентами $f(x) = a_n\cdot x^n + a_{n-1}\cdot x^{n-1} +,,,+a_1\cdot x + a_0$.

Известно, что любой многочлен с действительными коэффициентами степени $n \geq 1$ раскладывается в произведение многочленов первой и второй степени с действительными коэффициентами, то есть.

Элемент $\alpha \in A$ является корнем многочлена $f(x) = f_1(x)\cdot f_2(x)\cdot\ldots\cdot f_s(x)$, и значит, $f(\alpha) = f_1(\alpha)\cdot f_2(\alpha)\cdot\ldots\cdot f_s(\alpha)$. Откуда по свойству 1 по крайней мере один из множителей $f_1(\alpha), f_2(\alpha),..., f_s(\alpha)$ равен нулю. Если элемент $\alpha \in R$, то он будет корнем множителя $f_i(x) = x-\alpha$, если $\alpha \notin R$, то оно должно быть корнем только множителя второй степени вида $f_i(x) = x^2 + px + q$, который неприводим над полем действительных чисел, тогда $\frac{p^2}{4} - q < 0$, что возможно, лишь при $q > 0$. Тогда уравнение $x^2 + px + q = 0$ можно представить в виде $(x-c)^2 + d^2 = 0$, где $c,d \in R$.

Докажем теорему, отвечающую на поставленный выше вопрос.

Теорема Фробениуса. Алгебра с делением над полем действительных чисел является или полем действительных чисел, или полем комплексных чисел, или телом кватернионов.

Доказательство.

Пусть A – алгебра с делением ранга n над полем действительных чисел и $\varepsilon_1,\varepsilon_2,...,\varepsilon_n$ её базис. По второму свойству $R \subset A$, а это значит, что $1 \in A$. Так как базис можно выбирать произвольно, то выберем $\varepsilon_1 = 1$.

Возникает вопрос, ограничиваются ли алгебры с делением над полем R тремя перечисленными видами, возможны ли дальнейшие расширения числовых полей? Чтобы доказать теорему, отвечающую на этот вопрос, рассмотрим некоторые свойства алгебр с делением.

***Свойство* 1.** Алгебра с делением не имеет делителей нуля.

Доказательство.

Пусть A – алгебра с делением и пусть $\alpha \times \beta = 0$, где $\alpha, \beta \in A$.

Если $\beta \neq 0$, тогда по свойствам алгебр с делением для него существует элемент $\beta^{-1} \in A$ такой, $\beta \times \beta^{-1} = 1$.

Умножим левую и правую части равенства $\alpha \times \beta = 0$ на β^{-1}, получим $(\alpha \times \beta) \times \beta^{-1} = 0 \times \beta^{-1}$, откуда следует, что $\alpha \cdot (\beta \cdot \beta^{-1}) = 0$ или $\alpha \cdot 1 = 0$, откуда получим, что $\alpha = 0$.

Таким образом, из равенства нулю произведения вытекает равенство нулю по крайней мере одного из сомножителей.

***Свойство* 2.** Алгебра с делением над полем действительных чисел содержит поле действительных чисел.

Доказательство.

Пусть A – алгебра с делением над полем действительных чисел.

Известно, что всякая алгебра с делением содержит единицу ε, следовательно, содержит и элементы $a \cdot \varepsilon$, где $a \in R$. Поставим в соответствие каждому элементу вида $a \cdot \varepsilon \in A$ действительное число. Очевидно, что это соответствие взаимно однозначное.

Пусть $a \cdot \varepsilon \leftrightarrow a$ и $b \cdot \varepsilon \leftrightarrow b$, тогда

$$a \cdot \varepsilon + b \cdot \varepsilon = (a+b) \cdot \varepsilon \leftrightarrow a + b$$
$$(a \cdot \varepsilon) \times (b \cdot \varepsilon) = (a \cdot b) \cdot (\varepsilon \times \varepsilon) = (a \cdot b) \cdot \varepsilon \leftrightarrow a \cdot b.$$

Откуда по определению изоморфизма следует, что множество всех элементов вида $a \cdot \varepsilon$ изоморфно полю действительных чисел R. Отождествим элемент $a \cdot \varepsilon \in A$ с действительным числом $a \in R$, тогда $R \subset A$.

***Свойство* 3.** Каждый элемент алгебры с делением, отличный от действительного числа, служит корнем некоторого квадратного уравнения вида $(x-c)^2 + d^2 = 0$, где c и $d \neq 0$ – действительные числа.

Доказательство.

2. $\forall h \in H \Rightarrow h^{-1} \in H$.

Примеры.

1. $Z(+)$ – аддитивная группа целых чисел. Z_2 – подгруппа группы $Z(+)$;

2. $L_n = \left\{ A = \begin{pmatrix} a_{11} \ldots a_{1n} \\ a_{n1} \ldots a_{nn} \end{pmatrix} \middle| \, a_{ij} \in R, |A| \neq 0 \right\}$ – некоммутативная группа невырожденных квадратных матриц, $S = \{ A \in L_n \| A | = 1 \}$ подгруппа.

3. Кольцо, примеры колец, простейшие свойства кольца.

Определение. Алгебра $K(+,\cdot)$ называется кольцом, если относительно операций сложения и умножения она удовлетворяет аксиомам.

I. $K(+)$ – абелева группа, т.е.

1. $\forall x, y \in K \Rightarrow x + y = y + x$ (коммутативность);

2. $\forall x, y, z \in K \Rightarrow (x+y) + z = x + (y+z)$ (ассоциативность);

3. $\exists 0 \in K \mid \forall x \in K \; x + 0 = x$ (0 – правый нулевой элемент);

4. $\forall x \in K \; \exists (-x) \in K \mid x + (-x) = 0$ ($(-x)$–правый противоположный элемент).

II. $K(\cdot)$ – полугруппа

5. $\forall x, y, z \in K \Rightarrow (x \cdot y) \cdot z = x \cdot (y \cdot z)$

III.

6. $\forall x, y, z \in K \Rightarrow (x+y) \cdot z = x \cdot z + y \cdot z$;

7. $\forall x, y, z \in K \Rightarrow z \cdot (x+y) = z \cdot x + z \cdot y$.

Определение. Кольцо $K(+,\cdot)$ называется коммутативным кольцом, если выполняется аксиома:

8. $\forall x, y \in K \Rightarrow x \cdot y = y \cdot x$ (коммутативность)

Определение. Кольцо $K(+,\cdot)$ называется кольцом с единицей если:

9. $\exists e \in K \mid \forall x \in K, x \cdot e = e \cdot x = x$ (e – единица кольца K)

Примеры.

1. $Z(+,\cdot)$ $Q(+,\cdot)$, $R(+,\cdot)$, $C(+,\cdot)$ – коммутативные кольца с единицей.
2. $m \in N$, $Z_m = \{\overline{0},\overline{1},\overline{2},...,\overline{m-1}\}$, где

$\forall \overline{a},\overline{b} \in Z_m \;\; \overline{a} \oplus \overline{b} = \overline{a+b}; \; \overline{a} \otimes \overline{b} = \overline{a \cdot b}$.

$Z_m(\oplus,\otimes)$ – коммутативное кольцо с единицей.

3. $Z[\sqrt{\alpha}] = \{(a + b\sqrt{2}),\, a,b, \in Z\}$ –коммутативное кольцо с единицей.
4. $Z[i] - \{a + bi \,|\, a,b, \in Z\}$ – коммутативное кольцо с единицей (кольцо целых Гуссовых чисел).
5. $Z_2 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in Z \right\}$ –не коммутативное кольцо с единицей.

Свойства колец.

1. $\mathrm{K}(+)$– абелева группа. Поэтому всякое кольцо обладает свойствами абелевых групп:

$1^0 \; \exists_! \, 0 \in K | \forall x \in K, \; x + 0 = x;$

$2^0 \; \forall a \in K \; \exists_! (-a) \in K | \; a + (-a) = (-a) + a = 0;$

$3^0 \; \forall a,b \in K$ уравнение $a + x = b \; (y + a = b)$ имеет в K единственное решение;

4^0 в сумме из n элементов кольца скобки можно расставлять произвольно.

Из свойства следует, что в кольце можно определить операцию – вычитание, по правилу:

$\forall x, y \in K \Rightarrow x - y = x + (-y)$

$5^0 \quad \forall a_1, a_2, ..., a_n \in K \Rightarrow -(a_1 + a_2 + ... + a_n) = (-a_1) +$

$+ (-a_2) + ... + (-a_n)$

$6^0. \forall a \in K, \forall n \in N \Rightarrow n(-a) = -na$

$7^0. \; \forall a,b \in K, \forall m,n \in Z \Rightarrow (n \pm m) \cdot a = n \cdot a \pm m \cdot a;$

$n(a \pm b) = na \pm nb; \;\; m \cdot (n \cdot a) = (m \cdot n) \cdot a.$

Из ассоциативности операции умножения вытекают следующие свойства:

Исходя из свойств умножения векторов на действительные числа (определение 2), имеем

$(a_i \varepsilon_i) \times (b_k \varepsilon_k) = a_i [\varepsilon_i (b_k \varepsilon_k)] = a_i [b_k (\varepsilon_i \times \varepsilon_k)] = (a_i b_k) \cdot (\varepsilon_i \times \varepsilon_k)$

Таким образом, $\alpha \cdot \beta = \sum_{i=1}^{n} a_i \varepsilon_i \times \sum_{k=1}^{n} b_k \varepsilon_k = \sum_{i,k=1}^{n} (a_i b_k) \cdot (\varepsilon_i \times \varepsilon_k)$.

Итак, произведение гиперкомплексных чисел выражается через всевозможные произведения базисных элементов $\varepsilon_1, \varepsilon_2, ..., \varepsilon_n$. Таких парных произведений $\varepsilon_i \times \varepsilon_k$ будет $\varepsilon_i \times \varepsilon_k$, так как $i \in \{1,2,...,n\}$ и $\varepsilon_i \times \varepsilon_k \neq \varepsilon_k \times \varepsilon_i$.

Всякое произведение $\varepsilon_i \times \varepsilon_k$ представляет собой гиперкомплексное число, в свою очередь выражаемое (как всякое гиперкомплексное число) через базисные элементы $\varepsilon_1, \varepsilon_2, ..., \varepsilon_n$, то есть $\varepsilon_i \varepsilon_k = C_{ik1}\varepsilon_1 + C_{ik2}\varepsilon_2 + ... + C_{ikn}\varepsilon_n = \sum_{t=1}^{n} C_{ikt}\varepsilon_t$. Здесь t означает порядковый номер коэффициента C_{ikt} при ε_t в линейном выражении $\varepsilon_i \times \varepsilon_k$. Зная n^3 коэффициентов C_{ikt} (так как произведений $\varepsilon_i \times \varepsilon_k$ всего $\varepsilon_i \times \varepsilon_k$, а каждое из них выражается через n коэффициентов), называемых структурными постоянными умножения данной алгебры, можно однозначно определить произведение любых гиперкомплексных чисел данной алгебры: $\alpha \cdot \beta = \sum_{i,k,t=1}^{n} (a_i b_k) C_{ikt} \varepsilon_t$. Постоянные C_{ikt} могут быть выбраны произвольно. От того или иного выбора n^3 чисел C_{ikt} зависит умножение в данной алгебре, а значит и сама алгебра. Можно построить сколько угодно алгебр любого ранга над полем действительных чисел. Для этого нужно выбрать базис $\varepsilon_1, \varepsilon_2, ..., \varepsilon_n$ и n^3 действительных чисел в качестве структурных постоянных

3. Предел расширения числовых полей. Теорема Фробениуса.

Алгебра с делением над полем R ранга $n = 1$ является полем действительных чисел, ранга $n = 2$ – полем комплексных чисел, ранга $n = 4$ – полем кватернионов.

таких систем вводят в n-мерное векторное пространство операцию умножения.

***Определение* 2.** n −мерное векторное пространство L над полем действительных чисел называется *алгеброй* (или *гиперкомплексной системой*) *ранга* n над этим полем, если в L определена всегда выполнимая и однозначная операция умножения, ассоциативная, дистрибутивная относительно сложения и связанная с умножением элементов из L на действительные числа равенством $k\cdot(\alpha\times\beta)=(k\cdot\alpha)\times\beta=\alpha\times(k\cdot\beta)$, где $\alpha,\beta\in L$, $k\in R$.

Из определения видно, что алгебра ранга n является некоммутативным кольцом.

Если в алгебре ранга n, помимо указанного, выполнимо деление, то она является телом, то есть некоммутативным полем и называется алгеброй с делением ранга n.

Элементы алгебры называются гиперкомплексными (сверхкомплексными) числами.

Алгебра ранга n имеет некоторый базис $\varepsilon_1,\varepsilon_2,...,\varepsilon_n$ и каждый ее элемент $\alpha=(a_1,a_2,...,a_n)$ можно представить в виде

$$\alpha=a_1\varepsilon_1+a_2\varepsilon_2+\ldots+a_n\varepsilon_n=\sum_{i=1}^{n}a_i\varepsilon_i.$$

Посмотрим, что представляет собой произведение двух гиперкомплексных чисел $\alpha=a_1\varepsilon_1+a_2\varepsilon_2+\ldots+a_n\varepsilon_n=\sum_{i=1}^{n}a_i\varepsilon_i$ и

$$\beta=b_1\varepsilon_1+b_2\varepsilon_2+\ldots+b_n\varepsilon_n=\sum_{k=1}^{n}b_k\varepsilon_k.$$

По определению 2 умножение дистрибутивно, поэтому

$$\alpha\times\beta=\alpha\times(b_1\varepsilon_1+b_2\varepsilon_2+\ldots+b_n\varepsilon_n)=\alpha\times(b_1\varepsilon_1)+\alpha\times(b_2\varepsilon_2)+\ldots+\alpha\times(b_n\varepsilon_n)=$$
$$=(a_1\varepsilon_1+a_2\varepsilon_2+\ldots+a_n\varepsilon_n)\times(b_1\varepsilon_1)+(a_1\varepsilon_1+a_2\varepsilon_2+\ldots+a_n\varepsilon_n)\times(b_2\varepsilon_2)+\ldots+$$
$$+(a_1\varepsilon_1+a_2\varepsilon_2+\ldots+a_n\varepsilon_n)\times(b_n\varepsilon_n)==(a_1\varepsilon_1)\times(b_1\varepsilon_1)+(a_2\varepsilon_2)\times(b_1\varepsilon_1)+\ldots+(a_n\varepsilon_n)\times(b_1\varepsilon_1)+$$
$$+(a_1\varepsilon_1)\times(b_2\varepsilon_2)+(a_2\varepsilon_2)\times(b_2\varepsilon_2)+\ldots+(a_n\varepsilon_n)\times(b_2\varepsilon_2)+\ldots+(a_1\varepsilon_1)\times(b_n\varepsilon_n)+$$
$$+(a_2\varepsilon_2)\times(b_n\varepsilon_n)+\ldots+(a_n\varepsilon_n)\times(b_n\varepsilon_n)=\sum_{i,k=1}^{n}(a_i\varepsilon_i)\times(b_k\varepsilon_k)$$

8^0. В произведении из n элементов скобки можно расставлять произвольно.

9^0. $\forall a\in K\ \forall m,n\in Z\Rightarrow a^m\cdot a^n=a^{m+n},\ (a^m)^n=a^{m\cdot n}$

Из дистрибутивного закона умножения относительно сложения вытекает справедливость свойств:

10^0. $\forall a_1,a_2,...,a_m\in K\ \forall b\in\mathrm{K}\Rightarrow(a_1+a_2+\ldots+a_m)\cdot b=$
$=a_1\cdot b+a_2\cdot b+\ldots+a_m\cdot b$

11^0. $\forall a_1,a_2,...,a_m\in K\ \forall b\in\mathrm{K}\Rightarrow b\cdot(a_1+a_2+\ldots+a_m)=$
$=b\cdot a_1+b\cdot a_2+\ldots+b\cdot a_m$

12^0. В каждом кольце K справедливо обычное правило умножения суммы на сумму (без изменения порядка множителей), т.е.

$\forall a_1,a_2,...,a_n,b_1,b_2,...,bm\in K\ \Rightarrow$
$(a_1+a_2+\ldots+a_n)\cdot(b_1+b_2+\ldots+b_m)=$
$=a_1b_1+a_1b_2+\ldots+a_1b_m+a_2b_1+a_2b_2+\ldots+a_2b_m+$
$+a_nb_1+a_nb_2+\ldots+a_nb_m$

13^0. $\forall a,b,c,\in K\Rightarrow(a-b)\cdot c=ac-bc\,;\,c\cdot(a-b)=$
$=c\cdot a-c\cdot b.$

14^0. $\forall a\in K\Rightarrow a\cdot 0=0\cdot a=0$.

15^0. $\forall a,b\in K\Rightarrow(-a)\cdot b=-a\cdot b,\ a\cdot(-b)=-a\cdot b,$
$(-a)\cdot(-b)=ab$

Определение. Кольцо $K(+,\cdot)$ называется кольцом без делителей нуля если:

$$\begin{bmatrix}(\forall a,b\in K\quad a\neq 0\wedge b\neq 0)\Rightarrow(a\cdot b\neq 0)\\(\forall a,b\in K\quad a\cdot b=0)\Rightarrow(a=0\vee b=0)\end{bmatrix}$$

Определение. Кольцо $K(+,\cdot)$ называется кольцом с делителями нуля если:

$$(\exists a,b\in K\ a\neq 0\wedge b\neq 0)\Rightarrow a\cdot b=0$$

Примеры.

1. $Z(+,\cdot)$ $Q(+,\cdot)$, $R(+,\cdot)$, $C(+,\cdot)$ – кольца без делителей нуля.

$2.\ S=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} a,b,c,d\in Z\right\}$ –кольцо с делителями нуля

$A\times B=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix};\ (A\neq O\ B\neq O)\Rightarrow A\times B=O$

3. Все поля являются кольцами без делителей нуля.

$4.\ Z_m=\left\{\overline{0},\overline{1},...\overline{m-1}\right\}$ – кольцо классов вычетов по модулю m. Если m – простое, то Z_m –кольцо без делителей нуля , если m – составное , то Z_m – кольцо с делителями нуля.

Определение. Непустое подмножество A кольца $K(+,\cdot)$ называется подкольцом кольца $K(+,\cdot)$, если $(A+,\cdot)$ – кольцо.

Примеры.

$1.\ K=\left\{A\middle|\ A=\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix}, a_{ij}\in R\right\}$ – кольцо квадратных матриц второго порядка.

$D=\left\{B\middle|B=\begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix}, a_{ij}\in R\right\}$ – подкольцо диагональных матриц кольца K , $K<D$

$2.\ Z(+,\cdot)<Q(+,\cdot)<R(+,\cdot)<C(+,\cdot)$

$3.\ Z_2=\left\{2x\mid x\in Z\right\}<Z$

$4.\ M_2=\left\{\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, a_{ij}\in Z\right\}$ – кольцо матриц второго порядка

$L_2=\left\{\begin{pmatrix} a & 3b \\ b & a \end{pmatrix}, a,b\in Z\right\}<M_2$.

***Теорема* (*критерий подкольца*).** Непустое множество A кольца $K(+,\cdot)$ является подкольцом кольца K тогда и только тогда, когда:

$1.\ \forall x,y\in A\Rightarrow x-y\in A$

$2.\ \forall x,y\in A\Rightarrow x\cdot y\in A.$

Доказательство.

Допустим противное, пусть $\overline{e_1},\overline{e_2},...,\overline{a_k},...,\overline{e_n}$ линейно зависимая система векторов, тогда существует совокупность из n действительных чисел $m_1,m_2,...,m_k,...,m_n$, среди которых есть отличные от нуля, такая что $m_1\overline{e_1}+m_2\overline{e_2}+...+m_k\overline{a_k}+...+m_n\overline{e_n}=\overline{0}$, откуда, после подстановки, получим $m_1\overline{e_1}+m_2\overline{e_2}+...+m_k\left(a\cdot\overline{e_s}+b\cdot\overline{e_t}\right)+...+m_n\overline{e_n}=\overline{0}$. Применяя свойства векторного пространства, преобразуем левую часть последнего равенства, получим равенство

$m_1\overline{e_1}+m_2\overline{e_2}+...+(am_k+m_s)\cdot\overline{e_s}+...+(bm_k+m_t)\cdot\overline{e_t}+m_n\overline{e_n}=\overline{0}$,

коэффициенты которого не обращаются в ноль одновременно. Следовательно, система векторов $\overline{e_1},\overline{e_2},...,\overline{e_s},...,\overline{e_t},...,\overline{e_n}$ линейно зависима, но тогда линейно зависима и система векторов $\overline{e_1},\overline{e_2},...,\overline{e_n}$, как система, содержащая линейно зависимую подсистему, что противоречит выбору системы $\overline{e_1},\overline{e_2},...,\overline{e_n}$.

Полученное противоречие показывает, что предположение о линейной зависимости векторов системы $\overline{e_1},\overline{e_2},...,\overline{a_k},...,\overline{e_n}$ неверно, остаётся, что система векторов $\overline{e_1},\overline{e_2},...,\overline{a_k},...,\overline{e_n}$ – линейно независима и может служить базисом пространства V_n .

2. Алгебра ранга n.

Всякое комплексное число $\alpha=a+b\cdot i$ линейно выражается через две линейно независимые единицы поля комплексных чисел $1=(1,0)$, $i=(0,1)$, а именно: $\alpha=a\cdot 1+b\cdot i$, где a и b – действительные числа.

Естественно, возникает вопрос, нельзя ли построить числа более общие, чем комплексные, которые линейно выражались бы более, чем через две единицы, то есть могли бы характеризовать пространство при $n>2$.

Английским математиком Гамильтоном (1805 – 1865) и немецким математиком Грассманом (1809 – 1877) были построены теории гиперкомплексных систем (или алгебр), в частности Гамильтоном в 1853 году была создана такая система для $n=4$ (система кватернионов). Для построения

ГИПЕРКОМПЛЕКСНЫЕ ЧИСЛА.

1. n-мерное векторное пространство.

Из курса высшей алгебры известно, что алгебра с операциями сложения векторов и умножения вектора на число $V_n = \left\{ \overline{a} = (a_1, a_2 ..., a_n) \,\middle|\, a_i \in R, i = \overline{1,n} \right\}$ является векторным пространством и называется n-мерным арифметическим векторным пространством над полем действительных чисел.

Для элементов алгебры V_n выполняются все общие свойства векторных пространств, рассмотренные в вопросах 6,7 введения.

Следует обратить внимание на то, что в определение n-мерного векторного пространства не входит умножение вектора на вектор.

Известно, что в n-мерном векторном пространстве существуют совокупности из n линейно независимых векторов, но любые $n+1$ векторов линейно зависимы. Число n, указывающее на максимальное количество линейно независимых векторов пространства, называется *размерностью* (рангом) этого пространства.

Совокупность n единичных векторов $\overline{e_1}, \overline{e_2}, ..., \overline{e_n}$ через которую выражается всякий вектор пространства, называется *базисом* этого пространства. Заметим, что базис может быть выбран различным образом, но при любом выборе базис должен состоять из n линейно независимых векторов. Например, в качестве базисных векторов системы координат плоскости можно взять в произвольном масштабе 2 вектора по выбранным направлениям двух осей Ox и Oy, считая их единичными, причем оси могут быть и не перпендикулярными.

Пусть $\overline{e_1}, \overline{e_2}, ..., \overline{e_n}$ – векторы, образующие базис n-мерного векторного пространства над полем R.

Заменим какой-либо из базисных элементов, например $\overline{e_k}$, некоторым вектором $\overline{a_k} \neq \overline{0}$ линейно выраженным через какие-либо базисные элементы; пусть $\overline{a_k} = a \cdot \overline{e_s} + b \cdot \overline{e_t}$, где a и b действительные числа, не равные одновременно нулю.

Теорема. Совокупность векторов $\overline{e_1}, \overline{e_2}, ..., \overline{a_k}, ..., \overline{e_n}$ линейно независима.

Определение. Отображение $\varphi : K(+,\cdot) \overset{в\,(на)}{\to} K'(\oplus,\otimes)$ называется гомоморфизмом кольца $K(+,\cdot)$ в (на) кольцо $K'(\oplus,\otimes)$ если оно удовлетворяет аксиомам:

1. $\forall x, y \in K \Rightarrow \varphi(x+y) = \varphi(x) \oplus \varphi(y)$
2. $\forall x, y \in K \Rightarrow \varphi(x \cdot y) = \varphi(x) \otimes \varphi(y)$

Определение. Гомоморфизм $\varphi : K(+,\cdot) \overset{на}{\to} K'(\oplus,\otimes)$ называется изоморфизмом кольца $K(+,\cdot)$ на кольцо $K'(\oplus,\otimes)$ если φ взаимно однозначное отображение.

4. Поле. Простейшие свойства поля. Примеры полей. Числовые поля. Упорядоченное поле.

Определение. Коммутативное кольцо P называется **полем**, если в нём содержится по крайней мере один элемент, отличный от нуля, и если в нем выполняется операция деления, кроме деления на нуль, т.е. $\forall a, b \in P, a \neq 0, \exists (q \in P \,|\, a \cdot q = b$

Примеры.

1. Коммутативное кольцо рациональных чисел Q является полем.
2. Коммутативное кольцо действительных чисел R является полем.
3. Коммутативное кольцо $Q\left[\sqrt{2}\right] = \left\{ a + b\sqrt{2} \,\middle|\, a, b \in Q \right\}$ является полем.

Свойства поля.

1. В каждом поле существует, и притом только одна единица.
2. В каждом поле P для любого элемента $a \neq 0$ существует, и притом только один обратный элемент a^{-1}.
3. Любое поле не содержит делителей нуля.
4. Каждое поле является коммутативным кольцом. Поэтому все свойства колец выполняются для полей.

Определение. Непустое подмножество P' поля P называют **подполем** этого поля, если оно само является полем относительно алгебраических операций, определенных на поле P. Поле P называют расширением поля P'.

***Теорема* (*критерий подполя*).** Для того чтобы непустое подмножество P' поля P, содержащее по крайне мере один не нулевой элемент, было подполем поля P, необходимо и достаточно,

чтобы множество P' было замкнуто относительно операций поля.

***Примеры* (*подполей*).**

1. Поле рациональных чисел Q является подполем поля $Q\left[\sqrt{2}.\right]$.
2. Поле рациональных чисел Q является подполем поля R действительных чисел.
3. Поле $Q\left[\sqrt{2}\right]$ является подполем поля R.

Определение. Поля элементами которых являются числа называют числовыми полями.

Теорема. Поле рациональных чисел является минимальным числовым полем.

Определение. Алгебраическая система $(F,<)$ называется линейно упорядоченным множеством, если выполняются следующие условия:

$1.\left(\forall a,b,c\in F\ из\ a<b\wedge b<c\right)\Rightarrow\left(a<c\right)$

$2.\left(\forall a,b\in F\right)\Rightarrow\left(a<b\vee b<a\vee a=b\right)$

Определение. Упорядоченным полем называется алгебраическая система $(F,+,\cdot,<)$ удовлетворяет условиям:

(1) алгебра $\left(F,+,\cdot\right)$ – поле;

(2) система $\left(F,<\right)$ линейно упорядоченное множество;

(3) если $a<b$, то $a+c<b+c$, где $a,b,c\in F$ (*монотонность сложения*)

(4) если $a<b$ и $c>0$, то $a\cdot c<b\cdot c$, где $a,b,c\in F$ (*монотонность умножения*)

5. Векторное пространство. Примеры и простейшие свойства векторных пространств. Линейная зависимость и независимость системы векторов. Базис и ранг конечной системы векторов.

Определение. Множество $L=\left\{\bar{a},\bar{b},\bar{c},...\right\}$ «векторов» называется векторным (линейным) пространством над полем $P=\left\{a,b,c,..\right\}$, если относительно операций сложения векторов и умножения вектора на элемент поля P выполняются условия:

$1^0.\ \forall\bar{a},\bar{b}\in L\Rightarrow\bar{a}+\bar{b}=\bar{b}+\bar{a}$;

$2^0.\forall\bar{a},\bar{b},\bar{c}\in L\Rightarrow\left(\bar{a}+\bar{b}\right)+\bar{c}=\bar{a}+\left(\bar{b}+\bar{c}\right)$;

Определение. Тело $\left(K,\oplus\otimes\right)$ называется телом кватернионов, а его элементы – кватернионами.

Запишем, тело кватернионов в виде $T=\left\{a+bi+cj+dk\,\middle|\,a,b/c.d\in R,i^2=j^2=k^2=-1\right\}$

Пусть $t=a+bi+cj+dk\in T$, элемент $\bar{t}=a-bi-cj-dk\in T$ назовём сопряжённым к элементу t. Найдём произведение сопряжённых элементов:

$t\cdot\bar{t}=\left(a+bi+cj+dk\right)\cdot\left(a-bi-cj-dk\right)=a^2-\left(bi+cj+dk\right)^2=$

$=a^2+b^2+c^2+d^2\in R.$

$$= a\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + b\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} + c\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} + d\begin{pmatrix}0 & i\\ i & 0\end{pmatrix} = aE + bI + cJ + dK,$$

где $E = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $I = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}$, $J = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $K = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$.

Найдём

$$E^2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \otimes \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = E;$$

$$I^2 = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} \otimes \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = -\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = -E;$$

$$J^2 = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} \otimes \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = -\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = -E;$$

$$K^2 = \begin{pmatrix}0 & i\\ i & 0\end{pmatrix} \otimes \begin{pmatrix}0 & i\\ i & 0\end{pmatrix} = \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix} = -\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = -E.$$

Итак, любой элемент тела $(T,\oplus,\otimes)$ имеет вид: $aE + bI + cJ + dK = a + bI + cJ + dK$, где $a,b,c,d \in R$, $I^2 = J^2 = K^2 = -E$.

Для матриц E,I,J,K составим таблицу умножения:

	E	I	J	K
E	E	I	J	K
I	I	$-E$	K	$-J$
J	J	$-K$	$-E$	I
K	K	J	$-I$	$-E$

Замечаем, что $I \otimes J = K$, а $J \otimes I = -K$, откуда $I \otimes J \neq J \otimes K$, следовательно, тело $(T,\oplus,\otimes)$ не является полем.

Таким образом, доказана, следующая теорема.

Теорема. Алгебра $(K,\oplus\otimes)$ является телом.

$3^0.\ \exists\,\bar{0} \in L \mid \forall \bar{a} \in L \Rightarrow \bar{a} + \bar{0} = \bar{a}$;

$4^0.\ \forall \bar{a} \in L\ \exists(-\bar{a}) \in L \mid \bar{a} + (-\bar{a}) = \bar{0}$;

$5^0.\ \forall \bar{a} \in L\ 1 \cdot \bar{a} = \bar{a}$, где 1 – единица поля P;

$6^0.\ \forall k,t \in \mathrm{P}, \forall \bar{a} \in L \Rightarrow k \cdot (t \cdot \bar{a}) = (k \cdot t) \cdot \bar{a}$;

$7^0.\ \forall k \in \mathrm{P}, \forall \bar{a},\bar{b} \in L \Rightarrow k \cdot (\bar{a} + \bar{b}) = k \cdot \bar{a} + k \cdot \bar{b}$;

$8^0.\ \forall k,t \in \mathrm{P}, \forall \bar{a} \in L \Rightarrow (k + t) \cdot \bar{a} = k \cdot \bar{a} + t \cdot \bar{a}$

Примеры.

1. $V_n = \left\{\bar{a} \mid \bar{a} = (a_1, a_2, ..., a_n), a_i \in R, i = \overline{1,n}\right\}$ – арифметическое $n-$ мерное векторное пространство, где R – поле действительных чисел.

2. $L_n = \left\{A \mid A = (a_{ij})_n, a_{ij} \in Q\right\}$ – векторное пространство квадратных матриц над полем рациональных чисел.

Определение. Система векторов $\bar{a}_1, \bar{a}_2, ..., \bar{a}_s$ векторного пространства L над полем P называется **линейно зависимой** если существует система ненулевых элементов $t_1, t_2, ..., t_s$ поля P для которых $t_1 \cdot \bar{a}_1 + t_2 \cdot \bar{a}_2 + ... + t_s \bar{a}_s = \bar{0}$.

Определение. Система векторов $\bar{a}_1, \bar{a}_2, ..., \bar{a}_s$ векторного пространства L над полем P называется линейно независимой, если векторное равенство $x_1 \cdot \bar{a}_1 + x_2 \cdot \bar{a}_2 + ... + x_s \bar{a}_s = \bar{0}$ выполняется тогда и только тогда, когда $x_1 = x_2 = ... = x_s = 0$, т.е.

$$\left(x_1 \bar{a}_1 + x_2 \bar{a}_2 + ... + x_s \bar{a}_s = \bar{0}\right) \Leftrightarrow \left(x_1 = x_2 = ... = x_s = 0\right)$$

Примеры.

1. $L_2 = \left\{A = \begin{pmatrix}a & b\\ c & d\end{pmatrix}, a,b,c,d \in Q\right\}$ – векторное пространство матриц второго порядка над полем рациональных чисел.

Система векторов–матриц $A_1=\begin{pmatrix}-3 & 4\\ 5 & 0\end{pmatrix}$, $A_2=\begin{pmatrix}1 & 2\\ -1 & 0\end{pmatrix}$, $A_3=\begin{pmatrix}2 & 4\\ -2 & 0\end{pmatrix}$ линейно зависима так как $0\cdot A_1+(-2)A_2+1\cdot A_3=0$.

Система векторов–матриц $E_1=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$, $E_2=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}$, $E_3=\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$, $E_4=\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}$ линейно независима, так как

$$\left(x_1E_1+x_2E_2+x_3E_3+x_4E_4=0\right)\Leftrightarrow\left(\begin{pmatrix}x_1 & x_2\\ x_3 & x_4\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\right)\Leftrightarrow$$

$$\Leftrightarrow\left(x_1=x_2=x_3=x_4=0\right)$$

Определение. Вектор $\overline{b}\in R$ называется линейной комбинацией векторов $\overline{a_1},\overline{a_2},...,\overline{a_s}\in L$ векторного пространства над полем P, если в поле P найдется система элементов $k_1,k_2,...,k_s$ для которой $\overline{b}=k_1\cdot\overline{a_1}+k_2\cdot\overline{a_2}+...+k_s\overline{a_s}$.

Теорема. Система векторов $\overline{a_1},\overline{a_2},...,\overline{a_s}$ векторного пространства L над полем P линейно зависима тогда и только тогда, когда хотя бы один вектор системы линейно выражается через остальные.

Свойства.

1. Если в системе векторов векторного пространства R над полем P хотя бы один вектор нулевой, то система линейно зависима.
2. Система, состоящая из одного вектора, линейно независима тогда и только тогда, когда этот вектор не нулевой.
3. Если некоторая подсистема системы векторов векторного пространства L над полем P линейно зависима, то и сама система линейно зависима.

Следствие. Если некоторая система векторов линейно независимая, то всякая ее подсистема линейно независимая.

4. Если система $\overline{a_1},\overline{a_2},...,\overline{a_s}$ – линейно независима, а система $\overline{a_1},\overline{a_2},...,\overline{a_s},\overline{b}$ – линейно зависима, то вектор $\overline{b}$ – линейно выражается через вектора первой системы.

Пусть $\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}=\begin{pmatrix}a+bi & c+di\\ -c+di & a-bi\end{pmatrix}$, тогда $\begin{vmatrix}a+bi & c+di\\ -c+di & a-bi\end{vmatrix}=a^2+b^2+c^2+d^2\neq 0$, следовательно, матрица $\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}$ – невырожденная, а значит, является обратимой матрицей,

$$\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}^{-1}=\frac{1}{a^2+b^2+c^2+d^2}\begin{pmatrix}\overline{\alpha} & -\beta\\ \overline{\beta} & \alpha\end{pmatrix}=$$

$$=\frac{1}{a^2+b^2+c^2+d^2}\begin{pmatrix}\overline{\alpha} & -\beta\\ -\overline{(-\beta)} & \overline{\alpha}\end{pmatrix}\in T,$$

тогда $X=\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}^{-1}\otimes\begin{pmatrix}\alpha_1 & \beta_1\\ -\overline{\beta_1} & \overline{\alpha_1}\end{pmatrix}\in T$.

Аналогично, уравнение $Y\otimes\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}=\begin{pmatrix}\alpha_1 & \beta_1\\ -\overline{\beta_1} & \overline{\alpha_1}\end{pmatrix}$, где $\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}\neq\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$, имеет корень

$$Y=\begin{pmatrix}\alpha_1 & \beta_1\\ -\overline{\beta_1} & \overline{\alpha_1}\end{pmatrix}\otimes\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}^{-1}\in T.$$

Итак, кольцо $(T,\oplus,\otimes)$ является телом.

Покажем, что тело $(T,\oplus,\otimes)$ не является полем.

Пусть $\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}\in T$, тогда

$$\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}=\begin{pmatrix}a+bi & c+di\\ -c+di & a-bi\end{pmatrix}=\begin{pmatrix}a & 0\\ 0 & a\end{pmatrix}+\begin{pmatrix}bi & 0\\ 0 & -bi\end{pmatrix}+\begin{pmatrix}0 & c\\ -c & 0\end{pmatrix}+\begin{pmatrix}0 & di\\ di & 0\end{pmatrix}=$$

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ -\overline{\beta_1} & \overline{\alpha_1} \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{pmatrix} = \begin{pmatrix} \alpha_1\alpha_2 - \beta_1\overline{\beta_2} & \alpha_1\beta_2 + \beta_1\overline{\alpha_2} \\ -\overline{\beta_1}\alpha_2 - \overline{\alpha_1}\beta_2 & -\overline{\beta_1}\beta_2 + \overline{\alpha_1}\overline{\alpha_2} \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_1\alpha_2 - \beta_1\overline{\beta_2} & \alpha_1\beta_2 + \beta_1\overline{\alpha_2} \\ -\overline{\alpha_1\beta_2 + \beta_1\overline{\alpha_2}} & \overline{\alpha_1\alpha_2 - \beta_1\overline{\beta_2}} \end{pmatrix} = \begin{pmatrix} \alpha_4 & \beta_4 \\ -\overline{\beta_4} & \overline{\alpha_4} \end{pmatrix} \in T,$$ где

$\alpha_4 = \alpha_1\alpha_2 - \beta_1\overline{\beta_2} \in C$ и $\beta_4 = \alpha_1\beta_2 + \beta_1\overline{\alpha_2} \in C$.

Итак, операции $\oplus$ и $\otimes$ являются алгебраическими на множестве T, а значит, $(T,\oplus,\otimes)$ – алгебра.

Известно, что множество $M_2 = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \middle| \alpha,\beta,\gamma,\delta \in C \right\}$ квадратных матриц является некоммутативным кольцом относительно операций сложения и умножения матриц, при этом $T \subset M_2$. Покажем, что алгебра $(T,\oplus,\otimes)$ является подкольцом кольца $(M_2,\oplus,\otimes)$. Для этого осталось показать, что для элементов $(T,\oplus,\otimes)$ определена операция вычитания. Действительно,

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ -\overline{\beta_1} & \overline{\alpha_1} \end{pmatrix} - \begin{pmatrix} \alpha_2 & \beta_2 \\ -\overline{\beta_2} & \overline{\alpha_2} \end{pmatrix} = \begin{pmatrix} \alpha_1 - \alpha_2 & \beta_1 - \beta_2 \\ -\overline{\beta_1} + \overline{\beta_2} & \overline{\alpha_1} - \overline{\alpha_2} \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_1 - \alpha_2 & \beta_1 - \beta_2 \\ -\overline{(\beta_1 - \beta_2)} & \overline{\alpha_1 - \alpha_2} \end{pmatrix} = \begin{pmatrix} \alpha_5 & \beta_5 \\ -\overline{\beta_5} & \overline{\alpha_5} \end{pmatrix} \in T,$$

где $\alpha_5 = \alpha_1 - \alpha_2 \in C$, $\beta_5 = \beta_1 - \beta_2 \in C$.

Итак, алгебра $(T,\oplus,\otimes)$ является подкольцом кольца $(M_2,\oplus,\otimes)$, а значит, $(T,\oplus,\otimes)$ является кольцом.

Покажем, что кольцо $(T,\oplus,\otimes)$ является телом.

Рассмотрим уравнение $\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \otimes X = \begin{pmatrix} \alpha_1 & \beta_1 \\ -\overline{\beta_1} & \overline{\alpha_1} \end{pmatrix}$, где

$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Теорема. Если $\overline{a_1},\overline{a_2},...,\overline{a_m}$ и $\overline{b_1},\overline{b_2},...,\overline{b_n}$ две системы векторов где $m > n$ и первая система линейно выражается через вторую, то первая система линейно зависима.

Следствия.

1. Если система векторов $\overline{a_1},\overline{a_2},...,\overline{a_m}$ линейно независима и каждый вектор системы линейно выражается через вектора системы $\overline{b_1},\overline{b_2},...,\overline{b_n}$, то $m \le n$.
2. Если каждая из двух линейно независимых систем векторов линейно выражается через другую, то количество векторов в системах одинаковое.

Определение. Базисом конечной системы векторов называется непустая линейно независимая ее подсистема, через которую линейно выражаются все вектора системы**.**

Примеры.

$\overline{a_1} = (1,0,0), \overline{a_2} = (0,1,0), \overline{a_3} = (0,0,1), \overline{a_4} = (1,2,3), \overline{a_5} = (0,3,4) \in V_3$. Каждая из систем векторов $(\overline{a_1},\overline{a_2},\overline{a_3})$, $(\overline{a_4},\overline{a_5},\overline{a_3})$, $(\overline{a_4},\overline{a_2},\overline{a_3})$ является базисом данной системы векторов.

Теорема. Любая система векторов, содержащая хотя бы один ненулевой вектор обладает базисом.

Теорема. Любые два базиса системы векторов содержат одинаковое число векторов.

Определение. Рангом конечной системы векторов называется число векторов входящих в базис системы.

6. Базис и размерность конечномерного векторного пространства. Подпространства. Линейные многообразия. Изоморфизм векторных пространств.

Пусть L векторное пространство над полем P.

Определение. Система векторов $\overline{e_1},\overline{e_2},...,\overline{e_n} \in L$ называется базисом векторного пространства L над полем P, если $\overline{e_1},\overline{e_2},...,\overline{e_n}$ линейно независимая система через которую линейно выражается каждый вектор пространства, т.е.

$\forall \overline{x} \in L\ \exists x_1,x_2,...,x_n \in P \,|\, \overline{x} = x_1\overline{e_1} + x_2\overline{e_2} + ... + x_n\overline{e_n}$.

Примеры.

1. $\overline{e_1}=(1,0,0,\ldots 0),\overline{e_2}=(0,1,0,\ldots,0),\ldots,\overline{e_n}=(0,0,0,\ldots,1)$ базис арифметического векторного пространства V_n.

2. $E_1=\begin{pmatrix}1&0\\0&0\end{pmatrix}$, $E_2=\begin{pmatrix}0&1\\0&0\end{pmatrix}$, $E_3=\begin{pmatrix}0&0\\1&0\end{pmatrix}$, $E_4=\begin{pmatrix}0&0\\0&1\end{pmatrix}$ базис векторного пространства матриц второго порядка на полем действительных чисел $L_2=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\middle|\ a,b,c,d\in R\right\}$.

Теорема. Любые два базиса линейного пространства имеют одинаковое число векторов.

Определение. Пространство L над полем P называется $n-$мерным ($dim\,R=n$), если:

1) в L существует по крайней мере одна система из n линейно независимых векторов;
2) любая система из $(n+1)$-го вектора является линейно зависимой.

Теорема. Размерность пространства L над полем P равна n тогда и только тогда, когда оно имеет базис из n векторов.

Определение. Непустое подмножество M пространства L называется подпространством пространства L если оно замкнуто относительно операций пространства, т.е.

1) $\forall\overline{x},\overline{y}\in M\Rightarrow\overline{x}+\overline{y}\in M$;
2) $\forall t\in P\ \forall\overline{x}\in M\Rightarrow t\cdot\overline{x}\in M$.

Примеры.

1. Подмножество состоящее только из одного нулевого вектора данного пространства $\overline{0}$ является подпространством.
2. Само пространство является подпространством самому себе.
3. Множество решений однородной системы n линейных уравнений с n неизвестными является подпространством арифметического векторного пространства над полем действительных чисел.

Определение. Множество $H=\left\{\overline{x_0}+\overline{u}\ \middle|\ \overline{u}\in M\right\}=\overline{x}_0+M$ называется **линейным многообразием** пространства, при этом M называ-

Если $\alpha=a+bi$, тогда: $\sqrt{\alpha}=\begin{cases}\pm(u+vi),\text{ при } b>0\\ \pm(u-vi),\text{ при } b<0\end{cases}$, где $u=\sqrt{\dfrac{a+\sqrt{a^2+b^2}}{2}}$, $v=\sqrt{\dfrac{a-\sqrt{a^2+b^2}}{2}}$.

5.Тело кватернионов.

Определение. Кольцо $(A,+,\cdot)$ называется телом, если для любых элементов $a,b\in A$, при $a\neq 0$ уравнения $a\cdot x=b$ и $y\cdot a=b$ имеют в A единственное решение.

***Следствие* 1.** Любое поле является телом.

***Следствие* 2.** Существуют некоммутативные тела.

***Следствие* 3.** Коммутативное тело является полем.

Пусть $(C,+,\cdot)$ – поле комплексных чисел. Обозначим через

$$T=\left\{\begin{pmatrix}\alpha&\beta\\-\overline{\beta}&\overline{\alpha}\end{pmatrix}\middle|\ \alpha,\beta\in C\right\}=\left\{\begin{pmatrix}a+bi&c+di\\-c+di&a-bi\end{pmatrix}\middle|\ a,b,c,d\in R\right\}=$$

$$=\left\{\begin{pmatrix}a&0\\0&a\end{pmatrix}+\begin{pmatrix}0&c\\-c&0\end{pmatrix}+\begin{pmatrix}bi&0\\0&-bi\end{pmatrix}+\begin{pmatrix}0&di\\di&0\end{pmatrix}\right\}\Rightarrow C\subseteq T.$$

Для элементов множества K введём операции $\oplus$ и $\otimes$, по правилам сложения и умножения квадратных матриц, т.е. если $\begin{pmatrix}\alpha_1&\beta_1\\-\overline{\beta_1}&\overline{\alpha_1}\end{pmatrix}\cdot,\begin{pmatrix}\alpha_2&\beta_2\\-\overline{\beta_2}&\overline{\alpha_2}\end{pmatrix}\in T$, тогда:

$$\begin{pmatrix}\alpha_1&\beta_1\\-\overline{\beta_1}&\overline{\alpha_1}\end{pmatrix}\oplus\begin{pmatrix}\alpha_2&\beta_2\\-\overline{\beta_2}&\overline{\alpha_2}\end{pmatrix}=\begin{pmatrix}\alpha_1+\alpha_2&\beta_1+\beta_2\\-\overline{\beta_1}-\overline{\beta_2}&\overline{\alpha_1}+\overline{\alpha_2}\end{pmatrix}=$$

$$=\begin{pmatrix}\alpha_1+\alpha_2&\beta_1+\beta_2\\-\overline{(\beta_1+\beta_2)}&\overline{\alpha_1+\alpha_2}\end{pmatrix}=\begin{pmatrix}\alpha_3&\beta_3\\-\overline{\beta_3}&\overline{\alpha_3}\end{pmatrix}\in T,$$

где $\alpha_3=\alpha_1+\alpha_2\in C$, $\beta_3=\beta_1+\beta_2\in C$.

Свойства сопряженных чисел.

1. $\forall \alpha \in C \Rightarrow \alpha \cdot \overline{\alpha} = a^2 + b^2 \in R$.
2. $\forall \alpha \in C \Rightarrow \alpha + \overline{\alpha} = 2a \in R$.
3. $\forall a \in C \Rightarrow \overline{a} = a \in R$.
4. $\forall \alpha, \beta \in C \Rightarrow \overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$.
5. $\forall \alpha, \beta \in C \Rightarrow \overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$.
6. $\forall \alpha, \beta \in C, \beta \neq 0 \Rightarrow \overline{\left(\frac{\alpha}{\beta}\right)} = \frac{\overline{\alpha}}{\overline{\beta}}$.

Все свойства доказываются непосредственно.

4.Тригонометрическая форма комплексного числа.

Пусть $C = \{\alpha = a + b \cdot i | a, b \in R\}$, тогда любое число $\alpha = a + bi$ можно представить в виде $\alpha = r \cdot (\cos\varphi + i \sin\varphi)$, где $r = \sqrt{a^2 + b^2}$, $\cos\varphi = \frac{a}{r}$, $\sin\varphi = \frac{b}{r}$, $tg\varphi = \frac{b}{a}$, $0 \le \varphi < 2\pi$, r – модуль комплексного числа α, а φ – аргумент комплексного числа α.

Если $\alpha_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$, $\alpha_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$, тогда:

$$\alpha_1 \cdot \alpha_2 = r_1 \cdot r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2));$$

$$\frac{\alpha_1}{\alpha_2} = \frac{r_1}{r_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2)).$$

Если $\alpha = r(\cos\varphi + i\sin\varphi)$, тогда:

$$\alpha^n = r^n(\cos(n \cdot \varphi) + i\sin(n \cdot \varphi)):$$

$$\sqrt[n]{\alpha} = \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right), \text{ где } k = \overline{0, n-1}.$$

ется направляющим пространством многообразия H, а $\overline{x}_0$ – вектором сдвига многообразия H.

Определение. Линейные пространства L и L' над полем P назовем изоморфными, если существует взаимно однозначное отображение $\varphi : L \xrightarrow{на} L'$, такое что

1) $\forall \overline{a}, \overline{b} \in L \quad \varphi(\overline{a} + \overline{b}) = \varphi(\overline{a}) + \varphi(\overline{b})$;
2) $\forall \overline{a} \in L, \forall t \in P \Rightarrow \varphi(t\overline{a}) = t\varphi(\overline{a})$.

Свойства. Пусть $L \cong L'$.

1 нулевой вектор пространства L переходит в нулевой вектор пространства L'.

2 вектор противоположный произвольному вектору пространства L переходит в вектор пространства L' противоположный его образу.

3 линейно независимая система векторов пространства L переходит в линейно независимую систему векторов пространства L'.

4. базис пространства L переходит в базис пространства L'.

Теорема. Любые два пространства над полем P имеющие одинаковую размерность изоморфны.

Следствие. Любое $n-$мерное пространство изоморфно арифметическому $n-$мерному пространству V_n.

СИСТЕМА НАТУРАЛЬНЫХ ЧИСЕЛ

1.Аксиоматическое определение системы натуральных чисел.

Определение. Системой натуральных чисел называется алгебра $(N,+,\cdot,',1)$, где $(+,\cdot)$ – две бинарные алгебраические операции, $(')$ (штрих) – унарная алгебраическая операция, определенные на N, 1 – нульарная алгебраическая операция определенная на N. Причем имеют место следующие аксиомы Пеано:

A_1. $\forall a \in N \; a \neq 1$;

A_2. $\forall a,b \in N \; a' = b' \Rightarrow a = b$

A_3. $\forall a \in N \quad a + 1 = a'$

A_4. $\forall a \in N \quad a \cdot 1 = a$

A_5. $\forall a,b \in N \quad a + b' = (a + b)'$

A_6. $\forall a,b \in N \quad a \cdot b' = ab + a$

A_7 (аксиома индукции): Если для некоторого подмножество $M \subseteq N$ – имеют место свойства:

$1) 1 \in M$, $2) \forall a \in M \Rightarrow a' \in M$, тогда $M = N$.

Элементы алгебры $N(+,\cdot,',1)$ удовлетворяющие аксиомам $A_1 - A_7$ называют **натуральными числами**.

***Замечание* 1.1.** Операция $(')$ – штрих называется операцией следования, число a' это число следующее за числом a. Из A_1 вытекает, что натуральное число 1 не следует ни за каким натуральным числам. Из A_2 вытекает, что любое натуральное число следует не более чем за одним натуральным числом, если $a' = b$, то число a предшествующее для b. A_7 (аксиома индукции) является основной для доказательства свойств методом методической индукции, остальные аксиомы связывают операции системы между собой.

II. Алгебра $C_1 = \{a \oplus b \otimes i \,|\, a,b \in R\} = \{(a,b) \,|\, a,b \in R\}$ является полем комплексных чисел, относительно операций $\oplus$ и $\otimes$, введенных по правилам:

$$(a,b) \oplus (c,d) = (a + c, b + d);$$
$$(a,b) \otimes (c,d) = (a \cdot c - b \cdot d, a \cdot d + b \cdot c).$$

III. Любая пара действительных чисел на координатной плоскости представляет собой вполне определенную точку. И любая точка координатной плоскости определяет пару действительных чисел, вполне определенную. Следовательно, между точками координатной плоскости и парами действительных чисел существует взаимно-однозначное соответствие.

Обозначим через C_2 – множество точек координатной плоскости. Для элементов множества C_2 вводим следующие операции:

пусть $A,B \in C_2$. Точка $A(a,b)$, $B(c,d)$

$$A \oplus B = C(a + c, b + d)$$
$$A \otimes B = D(a \cdot c - b \cdot d, a \cdot d + b \cdot c)$$

Можно доказать, что алгебры $(C_2,\oplus,\otimes)$ и $(C,+,\cdot)$ – изоморфны.

Следовательно $(C_2,\oplus,\otimes)$ – поле комплексных чисел.

IV. Любая точка плоскости однозначно определят вектор с началом в начале системы координат (радиус-вектор точки). Известно, что между множеством точек плоскости и множеством их радиус векторов существует взаимно-однозначное соответствие, поэтому между множеством C и множеством радиус векторов плоскости C_3 можно установить взаимно-однозначное соответствие по правилу:

$$\forall a + b \cdot i \leftrightarrow A(a,b) \leftrightarrow \overline{OA}(a,b)$$

Доказав, что алгебры $(C_2,\oplus,\otimes)$ и $(C_3,\oplus,\otimes)$ изоморфны, получим, что $(C_3,\oplus,\otimes)$ – поле комплексных чисел.

3.Сопряженные комплексные числа и их свойства.

Пусть $C = \{\alpha = a + b \cdot i \,|\, a,b \in R\}$. Число $\overline{\alpha} = \overline{a + bi} = a - bi \in C$ называют числом сопряженным к числу α.

Итак, для алгебры $(\overline{C},\oplus,\otimes)$ выполняются аксиомы 1–4 из определения поля комплексных чисел.

По аксиоме 5 алгебра $(C,\oplus,\otimes)$ является минимальной для которой выполняются условия 1, 2, 3, 4, следовательно, $C \subseteq \overline{C}$.

Итак, для алгебр $(C,\oplus,\otimes)$ и $(\overline{C},\oplus,\otimes)$ выполняются аксиомы 1–4 из определения поля комплексных чисел, кроме этого $\overline{C} \subseteq C$ и $C \subseteq \overline{C}$, откуда следует, что $C = \overline{C}$. Тогда для любого $z \in C$ существуют $a,b \in R$ такие, что $z = a \oplus b \otimes i$.

Достаточность.

Пусть $(C,\oplus,\otimes)$ алгебра, для элементов которой выполняются аксиомы 1–4 из определения поля комплексных чисел и условие: для любого $z \in C$, существуют $a,b \in R$ такие, что $z = a \oplus b \otimes i$, т.е. $C = \{a \oplus b \otimes i | a,b \in R\}$.

Надо доказать, что для алгебры $(C,\oplus,\otimes)$ выполняется аксиома 5.

Любое поле, с операциями $\oplus$ и $\otimes$, содержащее элементы $a,b \in R$ и элемент содержит и элемент вида: $a \oplus b \otimes i$. Следовательно и алгебра $(C,\oplus,\otimes)$ которая состоит из элементов такого вида $a \oplus b \otimes i$ содержится в названной алгебре, т.е. алгебра $(C,\oplus,\otimes)$ является минимальной, т.е выполняется А.5. Итак, алгебра $(C,\oplus,\otimes)$ является полем комплексных чисел.

***Теорема* 2.** Любые два поля комплексных чисел изоморфны, т.е. система аксиом комплексных чисел полная.

***Теорема* 3.** Существует поле комплексных чисел, т.е. система аксиом комплексных чисел непротиворечивая.

2.Различные модели поля комплексных чисел.

I. Алгебра $C = \{a + b \cdot i | a,b \in R\}$ является полем комплексных чисел, относительно операций $(+,\cdot)$:

$$(a + b \cdot i) + (c + d \cdot i) = (a + c) + (b + d) \cdot i;$$
$$(a + b \cdot i) \cdot (c + d \cdot i) = (a \cdot c - b \cdot d) + (a \cdot d + b \cdot c) \cdot i.$$

2.Основные свойства операции сложения натуральных чисел.

***Теорема* 2.1:** Операция сложения натуральных чисел ассоциативна, т.е.

$$\forall a,b,c \in N \Rightarrow (a+b)+c = a+(b+c) \qquad (1)$$

Доказательство. Докажем теорему методом математической индукции по числу c, т.е. обозначим через M – множество всех натуральных чисел для которых равенство (1) имеет место при любых $a,b \in N$. Пусть $c = 1$, тогда:

$$(a+b)+1 \overset{A3}{=} (a+b)' \overset{A5}{=} a+b' \overset{A3}{=} a+(b+1)$$

Итак, $(a+b)+1 = a+(b+1) \Rightarrow \underline{1 \in M}$.

Пусть $c \in M$, тогда по определению множества M для любых $a,b \in N$ имеет место равенство

$$(a+b)+c = a+(b+c) \qquad (2)$$

Тогда

$$(a+b)+c' \overset{A5}{=} ((a+b)+c)' \overset{(2)}{=} (a+(b+c))' \overset{A5}{=} a+(b+c)' \overset{A5}{=} a+(b+c').$$

Итак, равенство $(a+b)+c' = a+(b+c')$ верно для любого $c \in M$, следовательно, $c' \in M$.

Таким образом, M подмножество множества N, содержащее 1 и для любого элемента множества M, следующий за ним элемент, принадлежит множеству M. Тогда по A_7 множество M совпадает с множеством N – системой натуральных чисел.

***Теорема* 2.2.** Операция сложения натуральных чисел коммутативна, т.е.

$$\forall a,b \in N \quad a+b = b+a \qquad (3)$$

Доказательство. Для доказательство предварительно докажем, что верно:

$$\forall a \in N \quad a+1 = 1+a \qquad (4)$$

Обозначим через M множество всех натуральных чисел для которых (4) верно, тогда в силу однозначности результата операции сложения $1+1 = 1+1$, следовательно, $\underline{1 \in M}$.

Пусть $a \in M$ покажем, что $a' \in M$.

Из того, что $a \in M$ следует, $a+1 = 1+a$ (5)

Тогда $a'+1 \overset{A3}{=} (a+1)+1 \overset{(5)}{=} (1+a)+1 \overset{T2.1}{=} 1+(a+1) \overset{A3}{=} 1+a'$.

Итак, $a'+1 = 1+a'$, следовательно $a' \in M$.

Таким образом, M подмножество множества N, содержащее 1 и для любого элемента множества M, следующий за ним элемент, принадлежит множеству M. Тогда по A_7 множество M совпадает с множеством N – системой натуральных чисел.

Покажем выполнимость (3).

Обозначим, через M – множество всех натуральных чисел, для которых верно (3) для любого $a \in N$.

Тогда из верности (4), следует, что $\underline{1 \in M.}$

Пусть теперь $b \in M$, тогда $a+b = b+a$. (6)

$$a+b' \overset{A5}{=} (a+b)' \overset{(6)}{=} (b+a)' \overset{A5}{=} b+a' \overset{A3}{=} b+(a+1) \overset{(4)}{=} b+(1+a) \overset{T2.1}{=}$$

$$= (b+1)+a \overset{A3}{=} b'+a$$

Получили, что равенство $a+b' = b'+a$ выполняется и для элемента b', следующего за элементом b. А это значит, что $b' \in M$.

Таким образом, M подмножество множества N, содержащее 1 и для любого элемента множества M, следующий за ним элемент, принадлежит множеству M. Тогда по A_7 множество M совпадает с множеством N – системой натуральных чисел.

Замечание. В силу ассоциативности и коммутативности операции сложения имеем:

$$(a+b)+c = a+(b+c) = (b+a)+c = \ldots = a+b+c$$

А это значит, что в любой сумме слагаемые можно складывать произвольным образом.

3.Основные свойства операции умножения натуральных чисел.

***Теорема* 3.1.** Операции сложения и умножения натуральных чисел связаны с правым дистрибутивным законом:

$$\forall a,b,c \in N \Rightarrow (a+b)\cdot c = a\cdot c + b\cdot c \qquad (1)$$

Действительно:

$(a \oplus b \otimes i) \oplus (c \oplus d \otimes i) = (a+c) \oplus (b+d) \otimes i$;

$(a \oplus b \otimes i) \otimes (c \oplus d \otimes i) = (a \cdot c - b \cdot d) \oplus (a \cdot d + b \cdot c)$.

Из того, что $a,b,c,d \in R$, следует, что $a+c, b+d, a \cdot c - b \cdot d, a \cdot d + b \cdot c \in R$, а это значит, что для любых элементов множества $\overline{C}$ их сумма и произведение являются элементами множества $\overline{C}$, т.е. множество $\overline{C}$ замкнуто относительно операций $\oplus$ и $\otimes$.

Из того, что $a,b \in R$, следует, что $(-a),(-b) \in R$, но тогда $(-a) \oplus (-b) \otimes i = -(a \oplus b \otimes i) \in \overline{C}$, т.е. для каждого элемента множества $\overline{C}$ элемент ему противоположный принадлежит $\overline{C}$.

Пусть теперь $a \oplus b \otimes i \neq 0$, то элемент $(a \oplus b \otimes i)^{-1} = \dfrac{1}{a \oplus b \otimes i} = \dfrac{a}{a^2 \oplus b^2} \oplus \dfrac{-b}{a^2 \oplus b^2} \otimes i$.

Из того, что $a,b \in R$, следует, что $\dfrac{a}{a^2 \oplus b^2}, \dfrac{-b}{a^2 \oplus b^2} \in R$, а это значит, что обратный элемент тоже принадлежит $\overline{C}$.

Следовательно, $(\overline{C},\oplus,\otimes)$ подполе поля $(C,\oplus,\otimes)$, а это значит, что $(\overline{C},\oplus,\otimes)$ является полем, т.е. для алгебры $(\overline{C},\oplus,\otimes)$ выполняется аксиома 1 из определения поля комплексных чисел.

Любое действительное число a можно записать в виде $a = a \oplus 0 \otimes i \in \overline{C}$, а это значит, что $R \subset \overline{C}$, т.е. для алгебры $(\overline{C},\oplus,\otimes)$ выполняется аксиома 2 из определения поля комплексных чисел.

Для любых $a,b \in R$ имеем, что $a \oplus b = a+b$ и $a \otimes b = a \cdot b$, т.е. для алгебры $(\overline{C},\oplus,\otimes)$ выполняется аксиома 3 из определения поля комплексных чисел.

Элемент $i = 0 \oplus 1 \otimes i \in \overline{C}$, при этом $i^2 = (0 \oplus 1 \otimes i)^2 = -1$, т.е. для алгебры $(\overline{C},\oplus,\otimes)$ выполняется аксиома 4 из определения поля комплексных чисел.

ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ.

1.Аксиоматическое определение поля комплексных чисел.

В поле действительных чисел уравнение $x^2+1=0$ не имеет решения. Следовательно, возникает вопрос о расширении поля действительных чисел так, чтобы это уравнение решалось. Введем понятие поля комплексных чисел.

Определение. Алгебра $(C,\oplus,\otimes)$ называется полем комплексных чисел если:

1. $(C,\oplus,\otimes)$ – поле;
2. $R\subseteq C$;
3. $\forall a,b\in R\Rightarrow(a\oplus b=a+b,\ a\otimes b=a\cdot b)$;
4. $\exists i\in C\,|\,i^2=i\otimes i=-1$;
5. C минимальное поле со свойствами 1, 2, 3, 4.

***Теорема* 1.** Алгебра $(C,\oplus,\otimes)$ для которой выполняются условия 1, 2, 3, 4, и 5 будет полем комплексных чисел тогда и только тогда, когда для любого $z\in C$ существуют $a,b\in R$ такие, что $z=a\oplus b\otimes i$.

Доказательство.

Необходимость.

Пусть $(C,\oplus,\otimes)$ – поле комплексных чисел. Докажем, что $a\oplus b\otimes i=c\oplus d\otimes i$ тогда и только тогда, когда $a=c$ и $b=d$.

Предположим обратное, что $b\neq d$. Тогда:

$a\oplus b\otimes i=c\oplus d\otimes i\Leftrightarrow(b-d)\otimes i=(c-a)\Leftrightarrow i=(c-a)\otimes(b-d)^{-1}\Leftrightarrow i\in R$,

т.е. $i^2=-1\in R$, что противоречит свойствам действительных чисел. Следовательно, предположение $b\neq d$ является неверным, следовательно, $b=d$.

Из того, что $b=d$ и $a\oplus b\otimes i=c\oplus b\otimes i$ следует, что $a=c$.

Рассмотрим множество $\overline{C}=\{a\oplus b\otimes i\,|\,a,b\in R\}$.

Очевидно, что $\overline{C}\subseteq C$.

Покажем, что $\overline{C}\leq C$. Для этого покажем, что множество $\overline{C}$ замкнуто относительно операций поля C.

Доказательство.

Обозначим через M множество таких $c\in N$ для которых выполнено (1), для любых $a,b\in N$. Тогда при $c=1$. Имеем $(a+b)\cdot 1\overset{A4}{=}a+b\overset{A4}{=}a\cdot 1+b\cdot 1$. Итак, $1\in M$.

Пусть $c\in M$, тогда $(a+b)\cdot c=a\cdot c+b\cdot c$ (2)

$(a+b)\cdot c'\overset{A6}{=}(a+b)\cdot c+(a+b)\overset{(2)}{=}(a\cdot c+b\cdot c)+(a+b)\overset{3l.1}{=}$

$=(ac+a)+(bc+b)\overset{A6}{=}ac'+bc'$

Получили, что $(a+b)\cdot c'=a\cdot c'+b\cdot c'$, следовательно $c'\in M$.

Таким образом, M подмножество множества N, содержащее 1 и для любого элемента множества M, следующий за ним элемент, принадлежит множеству M. Тогда по A_7 множество M совпалает с множеством N – системой натуральных чисел.

***Теорема* 3.2.** Для натуральных чисел имеет место коммутативный закон умножения:

$$\forall a,b\in N\Rightarrow a\cdot b=b\cdot a \qquad (3)$$

Доказательство.

Предварительно докажем, что

$$\forall a\in N\ a\cdot 1=1\cdot a \qquad (4)$$

Обозначим через M множество таких натуральных чисел для которых выполняется (4).

При $a=1$, получим $1\cdot 1=1\cdot 1$, тогда $1\in M$.

Пусть $a\in M$, покажем $a'\cdot 1=1\cdot a'$.

Действительно,

$a'\cdot 1\overset{A3}{=}(a+1)\cdot 1\overset{T3.1}{=}a\cdot 1+1\cdot 1\overset{a\in M}{=}1\cdot a+1\cdot 1\overset{A6}{=}1\cdot(1+a)\overset{T2.2}{=}1\cdot(a+1)\overset{A3}{=}$.

$=1\cdot a'$

Получили $a'\cdot 1=1\cdot a'$, тогда $a'\in M$.

Таким образом, M подмножество множества N, содержащее 1 и для любого элемента множества M, следующий за ним элемент, принадлежит множе-

ству M. Тогда по A_7 множество M совпадает с множеством N – системой натуральных чисел, а значит, (4) – верно.

Покажем, что(3) верно.

Обозначим через M множество натуральных чисел b, для которых (3) верно для любого $a \in N$. Тогда в силу (4) $1 \in M$.

Пусть $b \in M$, тогда

$$b' \cdot a \overset{A3}{=} (b+1) \cdot a \overset{T3.1}{=} b \cdot a + 1 \cdot a \overset{b \in M,\,(4)}{=} a \cdot b + a \cdot 1 \overset{A6}{=} a \cdot (b+1) = ab'$$

Получаем $b' \cdot a = a \cdot b'$, следовательно, $b' \in M$.

Таким образом, M подмножество множества N, содержащее 1 и для любого элемента множества M, следующий за ним элемент, принадлежит множеству M. Тогда по A_7 множество M совпадает с множеством N – системой натуральных чисел, а значит, (3) – верно.

***Теорема* 3.3.** Операция умножения натуральных чисел, ассоциативна, т.е.

$$\forall a,b,c \in N \Rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c) \qquad (5)$$

Доказательство.

Докажем теорему методом математической индукции на число c, для этого обозначим через M множество всех натуральных чисел для которых (5) имеет место для любых $a,b \in N$.

Пусть $c = 1$, тогда $(a \cdot b) \cdot 1 \overset{A4}{=} ab \overset{A4}{=} a \cdot (b \cdot 1)$, а значит, $1 \in M$.

Пусть $c \in M$, т.е. для любых $a,b \in N$ имеет место (5)

$$(a \cdot b) \cdot c' \overset{A3}{=} (a \cdot b)(c+1) \overset{T3.1}{=} (a \cdot b) \cdot c + (a \cdot b) \cdot 1 \overset{c \in M,\, 1 \in M}{=}$$

$$= a \cdot (b \cdot c) + a \cdot (b \cdot 1) \overset{T3.2,\, T3.1}{=} a \cdot (bc + b \cdot 1) \overset{A6}{=} a \cdot (b \cdot c').$$

Итак, $(a \cdot b) \cdot c' = a \cdot (b \cdot c')$, и значит, $c' \in M$.

Таким образом, M подмножество множества N, содержащее 1 и для любого элемента множества M, следующий за ним элемент, принадлежит множеству M. Тогда по A_7 множество M совпадает с множеством N – системой натуральных чисел, а значит, (5) – верно.

12) $\forall a \in R \quad \overline{a < a}$ (антирефлексивность отношения "<")

13) $(\forall a,b \in R\ 0 < a) \Rightarrow (\exists n \in N \mid b < na)$ (архимедовость)

Аксиома полноты.

14) Любая фундаментальная последовательность упорядоченного поля R, имеет в R предел.

Из (1–13) следует, что система действительных чисел является непрерывным полем.

существует такое число $c \in [0, a+1]$, для которого $f(c) = 0$, откуда получаем, что $c^n = a$ или $\sqrt[n]{a} = c$.

3. Аксиоматическое определение поля действительных чисел.

Определение. Полем действительных чисел называется любое множество $R = \{a,b,c,...\}$, содержащее, по крайней мере, два различных элемента, на котором определены две бинарные операции: сложение и умножение, и введено отношение "$<$" (меньше) $a < b$ $(a$ *меньше* $b)$, причем выполняются следующие аксиомы:

Аксиомы поля.

1) $\forall a,bc \in R \Rightarrow (a+b)+c = a+(b+c)$ (ассоциативность сложения)

2) $\forall a,b \in R \Rightarrow a+b = b+a$ (коммутативность сложения)

3) $(\forall a,b \in R\ \exists c \in R \mid a+c = b)$ (выполняется операция вычитания).

4) $\forall a,b,c \in R \Rightarrow (a \cdot b)\cdot c = a \cdot (b \cdot c)$ (ассоциативность умножения)

5) $\forall a,b \in R \Rightarrow a \cdot b = b \cdot a$ (коммутативность умножения)

6) $\forall a,b,c \in R \Rightarrow (a+b)\cdot c = a \cdot c + b \cdot c$ (дистрибутивность умножения относительно сложения)

7) $(\forall a,b \in R, a \neq 0\ \exists r \in R \mid a \cdot r = b)$ (выполняется деление, кроме деления на ноль)

Аксиомы упорядоченности поля.

8) $\forall a,b \in R \Rightarrow (a < b \vee b < a \vee a = b)$

9) $(\forall a,b,c \in R\ a < b \wedge b < c) \Rightarrow (a < c)$ (транзитивность отношения "$<$")

10) $(\forall a,b,c \in R\ a < b) \Rightarrow (a + c < b + c)$ (монотонность системы)

11) $\forall a,b,c \in R\ a < b \wedge 0 < c) \Rightarrow (ac < bc)$ (монотонность умножения);

4.Понятие упорядоченности натуральных чисел.

Определение. Отношение α, определенное на множестве A назовем отношением «строгого» порядка, если оно антирефлексивно, антисимметрично, транзитивно.

На множестве натуральных чисел отношение $>$ – больше: антирефлексивно, антисимметрично и транзитивно.

Действительно,

– любое натуральное число не больше самого себя (антирефлексивность);

– из того, что $a > b$ не следует, что $b > a$, для любых натуральных чисел a и b (антисимметричность);

– из $a > b$ и $b > c$, следует, что $a > c$ (транзитивность).

Следовательно, множество натуральных чисел строго упорядоченно.

Определение. Отношение α, определенное на множестве A назовем отношением линейного порядка, если для любых элементов $a,b \in A$: либо $a \alpha b$, либо $b \alpha a$, в этом случае отношение α называют связным.

Таким образом, множество натуральных чисел линейное строго упорядоченное множество относительно отношения $>$ – больше.

5.Вычитание и деление на множество натуральных чисел.

Исходя из свойств системы натуральных чисел, имеем, что $N(+)$ – коммутативная полугруппа, $N(\cdot)$ – коммутативная полугруппа с сокращением.

Определение. Пусть $G(+)$ – коммутативная полугруппа с сокращением. Разностью элементов a и b множества G, назовём элемент $c \in G$ который в сумме с элементом b даёт элемент a, т.е. $b + c = a$.

Разность элементов a и b обозначается $c = a + (-b) = a - b$. Значит, разность, это решение уравнения $b + x = a$.

Замечание. Если для чисел a и b существует разность, то $a - b = c \in G$ единственна.

Определение. Если $G(\cdot)$ – коммутативная полугруппа с сокращением, то элемент $c \in G$ называется частным элементов a и b если $c \cdot b = a$. Обозначается $c = \frac{a}{b}$.

Значит, частное $\frac{a}{b}$ это решение уравнения $b \cdot x = a$.

***Теорема* 5.1.** Для того, чтобы существовала разность натуральных чисел $a \quad и \quad b$ необходимо и достаточно, чтобы $a > b.$

***Теорема* 5.2.** Для того, чтобы существовало частное $\frac{a}{b}$ необходимо, но не достаточно, чтобы $a \geq b.$

Вычитание и деление натуральных чисел не являются бинарными алгебраическими операциями на множестве N, т.к. разность и частное существуют не для любой пары a, b натуральных чисел.

***Определение* 3**. Если поле $(A,+,\cdot)$ полное и упорядочено архимедовски, то говорят , что оно непрерывное.

***Определение* 4.** Непрерывное поле, содержащее поле рациональных чисел называется полем действительных чисел.

***Теорема* 1**. Поле $(R,+,\cdot)$, содержащее поле рациональных чисел будем называть полем действительных чисел_ тогда и только тогда, когда любая фундаментальная последовательность рациональных чисел имеет предел в этом поле.

Теорема 2. Любые два поля действительных чисел изоморфны.

Теорема 3. Существует поле действительных чисел.

Доказательство.

План доказательства.

1. Обозначим через $\overline{R} = \{(a_n), a_i \in Q\}$ множество фундаментальных последовательностей рациональных чисел.

2. Для последовательностей из $\overline{R}$ вводим понятие отношения θ по правилу: $(a_n)\theta(b_n) \Leftrightarrow \lim\limits_{n\to\infty}(a_n - b_n) = 0$.

3. Доказываем, что это отношение является отношением эквивалентности. Следовательно, θ разбивает $\overline{R}$ на классы.

4. Обозначим через R множество классов эквивалентности, для элементов которого вводим операции сложения и умножения по правилам:

$$K(a_n) \oplus K(b_n) = K(a_n + b_n);$$
$$K(a_n) \otimes K(b_n) = K(a_n \cdot b_n)$$

5. Доказываем, что введённые операции $\oplus$, $\otimes$ являются алгебраическими операциями.

6. Доказываем, что это R поле действительных чисел, т.е., что оно архимедовски упорядочено и является полным.

Свойство. Для любых $n \in N$ и любых $a \in R$, $a > 0$ существует $\sqrt[n]{a}$.

Доказательство.

Рассмотрим многочлен $f(x) = x^n - a$, который, как любой многочлен n-ой степени с действительными коэффициентами, является непрерывной, монотонной, возрастающей функцией. При этом $f(0) = -a < 0$, а $f(a+1) = (a+1)\left((a+1)^{n-1} - 1\right) > 0$. Следовательно, функция $f(x)$ на концах отрезка $[0, a+1]$ принимает значения противоположного знака, тогда

***Замечание* 1.** Предложение, что «элемент $a \in A$ предел последовательности (a_n), записывается: $\lim\limits_{n\to\infty} a_n = a$.

***Замечание* 2.** Относительно предела последовательности для элементов расположенного поля имеют место все теоремы, доказываемые в математическом анализе для последовательности действительных чисел.

Определение. Последовательность (a_n) с элементами из расположенного поля $(A,+,\cdot)$ называется фундаментальной последовательностью, если для любого $\varepsilon \in A$, где $\varepsilon > 0$ существует такое $n_0 \in N$, что для всех $n \in A, n > n_0$ и $m \in A$, $m > n_0$, $|a_n - a_m| < \varepsilon$.

Известно, что если последовательность имеет предел, то эта последовательность фундаментальная. Так же известно, что существует фундаментальные последовательности, которые не имеют предела в данном поле.

Пусть $(Q,+,\cdot)$ поле рациональных чисел. Из сказанного выше следует, что поле рациональных чисел – расположенное поле. В этом поле фундаментальная последовательность $1{,}4.\ 1{,}41.\ 1{,}414.\ 1{,}4141.\ldots$ в поле рациональных чисел не имеет предела (известно, что предел этой последовательности $\sqrt{2} \notin Q$). Поэтому возникает необходимость расширить поле Q рациональных чисел, так чтобы любая фундаментальная последовательность рациональных чисел имела предел в расширенном поле. Для этого введём понятие поля действительных чисел.

Пусть $(A,+,\cdot)$ – расположенное поле.

***Определение* 1.** Расположенное поле $(A,+,\cdot)$ является архимедовски упорядоченным, если для любых элементов a и b принадлежащих A, где $b > 0$ существует натуральное число n такое что $n \cdot b >$.

***Определение* 2**. Расположенное поле $(A,+,\cdot)$ называется полным полем, если любая фундаментальная последовательность имеет предел в этом поле.

Поле рациональных чисел не является полным, так как $\lim\sqrt{2} \notin Q$.

КОЛЬЦО ЦЕЛЫХ ЧИСЕЛ.

1.Аксиоматическое определение кольца целых чисел.

Определение. Алгебру $(Z,+,\cdot,0,1,N)$ назовем системой целых чисел, а ее элементы целыми числами, если она удовлетворяет аксиомам:

Z_1. $\forall a,b,c \in Z \Rightarrow a+(b+c)=(a+b)+c$

Z_2. $\forall a,b \in Z \Rightarrow a+b=b+a$

Z_3. $\exists 0 \in Z) \mid \forall a \in Z \quad a+0=a.$

Z_4. $\forall a \in Z\ \exists a_1 \in Z \mid a+a_1=0$.

Z_5. $\forall a,b,c \in Z \Rightarrow (a\cdot b)\cdot c = a\cdot(b\cdot c)$

Z_6. $\forall a,b,c \in Z \Rightarrow \begin{cases} a\cdot(b+c)=a\cdot b+a\cdot c \\ (b+c)\cdot a = b\cdot a + c\cdot a \end{cases}$

Z_7. $(N,+,\cdot,',1)$ – полукольцо натуральных чисел.

Z_8. $N \subset Z$.

Z_9. $(\textit{аксиома минимальности})$: любое множество M подмножество множества Z ($M \subseteq Z$), удовлетворяющее условиям: $a) N \subset M$; $b)\, a,b \in M \Rightarrow a-b \in M$, совпадает множества Z ($M \subseteq Z$)

Из выполнимости $Z_1 - Z_6$ следует что $(Z+,\cdot)$ кольцо (кольцо целых чисел), из выполнимости аксиом $Z_7 - Z_8$ следует, что N полукольцо натуральных чисел включается в систему целых чисел Z, аксиома Z_9 играет роль аксиомы индукции.

2.Необходимое и достаточное условие, чтобы кольцо содержащее N , было кольцом целых чисел.

Теорема. Чтобы кольцо содержащее N было кольцом целых чисел необходимо и достаточно, чтобы любой элемент кольца был представлен в виде разности двух натуральных чисел.

***Теорема* 1.1.** Любое целое число представимо в виде разности двух натуральных чисел, причем для любых $k_1, e_1, m_1, n_1 \in N$ выполняется условие:

$$k_1 - e_1 = m_1 - n_1 \Leftrightarrow \kappa_1 + n_1 = m_1 + e_1$$

Доказательство.

Включим в множество M только те целые числа которые представимы в виде разности двух натуральных чисел, тогда $M \subseteq Z$ (1)

По аксиоме A_3 для любого натурального числа n существует следующее за ним число $n' \in N$, такое что $n' = n + 1$, откуда по определению разности получим, что $n = n' - 1$, а это значит, что любое натуральное число представимо в виде разности целых чисел, так как $N \subset Z$, и значит $N \subset M$ (2)

Выберем два произвольных числа из множества M. Пусть $a, b \in M$, тогда по определению множества M, каждое из этих чисел представимо в виде разности двух натуральных чисел, т.е.

$$(\exists k_1, e_1, m_1, n_1 \in N \mid a = k_1 - e_1, b = m_1 - n_1) \Rightarrow$$

$$\Rightarrow (a - b = (k_1 - e_1) - (m_1 - n_1))) \Rightarrow (a - b = (\kappa_1 + n_1) - (m_1 + e_1),$$ где

$$(\kappa_1 + n_1), (m_1 + e_1) \in N) \Rightarrow (a - b \in M)$$

Таким образом,

$$(\forall a, b \in M \Rightarrow a - b \in M)$$ (3)

Из выполнимости условий (1), (2), (3) по аксиоме минимальности Z_9 следует, что $M = Z$.

Следовательно, любое целое число представимо в виде разности двух натуральных чисел.

Докажем, что для любых $k_1, e_1, m_1, n_1 \in N$ выполняется условие:

$$k_1 - e_1 = m_1 - n_1 \Leftrightarrow \kappa_1 + n_1 = m_1 + e_1$$ (4)

Действительно,

Теорема. Если $(A, +, \cdot)$ расположенное кольцо, то это кольцо характеристики ноль.

Доказательство.

Пусть $a \in A$, где $a \neq 0$ и пусть $n \in N$. Докажем, что $n \cdot a \neq 0$. Для доказательства воспользуемся методом математической индукции по числу n.

Рассмотрим возможные случаи.

I. Число a – положительное.

Пусть $n = 2$ тогда $2a = a + a$ – положительное, а значит, $2 \cdot a \neq 0$. Итак, база индукции доказана.

Предположим, что $k \cdot a \neq 0$, где $k \in N$ и докажем, что $(k+1) \cdot a \neq 0$.

Число $(k+1) \cdot a = k \cdot a + 1 \cdot a = k \cdot a + a$ – положительное, как сумма двух положительных чисел, тогда, по доказанному выше, $(k+1) \cdot a > 0$, а значит, $(k+1) \cdot a \neq 0$.

Таким образом, из предположения, что $k \cdot a \neq 0$ получили, что $(k+1) \cdot a \neq 0$, откуда в силу принципа математической индукции следует, что $n \cdot a \neq 0$ для любого $n \in N$.

II. Число a – отрицательное , тогда $(-a)$ – положительное, откуда по доказанному в пункте I получим, что $n \cdot (-a) \neq 0$, то есть $(-n \cdot a) \neq 0$, тогда и $n \cdot a \neq 0$.

2. Понятие предела в расположенном поле.

Пусть $(A, +, \cdot)$ – расположенное поле, тогда множество A – упорядоченное и пусть "$\leq$" – отношение порядка на множестве A.

Пусть $(a_1, a_2, ..., a_n, ...) = (a_n)$ – последовательность элементов множества A.

Определение. Будем говорить, что элемент $a \in A$ будет пределом последовательности (a_n) если для любого $\varepsilon \in A$, где $\varepsilon > 0$ существует такое $n_0 \in N$, что для всех $n \in A$, $n > n_0$ $|a_n - a| < \varepsilon$.

Теорема. Если $(A,+,\cdot)$ расположенное кольцо, то любое положительное число больше нуля, ноль больше любого отрицательного числа, а любое положительное число больше любого отрицательного.

Доказательство.

Заметим, что если $a \neq 0$, тогда a либо положительное, либо отрицательное, при этом, если a – отрицательное, то $(-a)$ – положительное.

Рассмотрим возможные случаи.

Если a – положительное, то $(a-0)=a$ – положительное, следовательно, $a>0$.

Если a – отрицательное, то $(-a)$ – положительное, тогда $0-a=-a$ – положительное, откуда следует, что $0>a$.

Пусть $a>0$, а $0>b$, докажем, что $a>b$.

$$\left.\begin{array}{l} a>0 \Rightarrow a-0>0 \\ 0>b \Rightarrow 0-b>0 \end{array}\right\} \Rightarrow (a-0)+(0-b)>0 \Rightarrow a-b>0$$

Теорема. Если $(A,+,\cdot)$ расположенное кольцо, то это кольцо без делителей нуля.

Доказательство.

Докажем, что если $a \neq 0$ и $b \neq 0$, тогда $a \cdot b \neq 0$.

если a и b – положительные, тогда по второму пункту из определения расположенного кольца, $a \cdot b > 0$, то есть $ab \neq 0$.

1) если a – положительное, b – отрицательное, тогда a и $(-b)$ – положительные, откуда по второму пункту из определения расположенного кольца, $a \cdot (-b) > 0$, то есть $(-a \cdot b) \neq 0$, тогда и противоположный элемент $a \cdot b \neq 0$.

2) если a – отрицательное, b – положительное, тогда $(-a)$ и b – положительные, откуда по второму пункту из определения расположенного кольца, $(-a) \cdot b > 0$, то есть $(-a \cdot b) \neq 0$, тогда и противоположный элемент $a \cdot b \neq 0$.

3) если a – отрицательное, b – отрицательное, тогда $(-a)$ и $(-b)$ – положительные, откуда по второму пункту из определения расположенного кольца, $(-a) \cdot (-b) > 0$, то есть $a \cdot b \neq 0$.

1) из $k_1 - e_1 = m_1 - n_1 \Rightarrow (k_1 - e_1) + n_1 = (m_1 - n_1) + n_1 \Rightarrow$
$\Rightarrow (k_1 - e_1) + n_1 + e_1 = (m_1 - n_1) + n_1 + e_1 \Rightarrow k_1 + n_1 = m_1 + e_1$.

2) $k_1 + n_1 = m_1 + e_1 \Rightarrow$
$\Rightarrow (k_1 + n_1) + (-n_1) + (-e_1) = m_1 + e_1 + (-n_1) + (-e_1) \Rightarrow$
$\Rightarrow k_1 - e_1 = m_1 - n_1$.

3.Построение кольца целых чисел.

***Теорема* 1.2.** Любое целое число либо ноль, либо натуральное число, либо число противоположное натуральному.

Доказательство.

По теореме 1.1 любое целое число a представимо в виде $a = k - m$, где $k, m \in N$.

Известно, что множество натуральных чисел линейно упорядочено, тогда для любых $k, m \in N$ верно одно из следующих утверждений: либо $k = m$, либо $k > m$, либо $m > k$.

Если $k = m$, $a = k - m = m - m = 0$.

Если $k > m$, либо $m > k$ тогда, согласно критерия существования разности двух натуральных чисел, существуют натуральные числа s и r для которых $k - m = s$ и $m - k = r$. Откуда $a = k - m = s$, либо $a = k - m = -(m - k) = -r$.

Теорема. Кольцо целых чисел является коммутативным кольцом с единицей.

Доказательство.

Из выполнимости $Z_1 - Z_6$ следует что $(Z,+,\cdot)$ кольцо.

1. Покажем, что для любых $a, b \in Z$ выполняется коммутативный закон: $a \cdot b = b \cdot a$.

$$\left.\begin{array}{l} a \in Z \Rightarrow \exists\, k_1, e_1 \in N \,|\, a = k_1 - e_1 \\ b \in Z \Rightarrow \exists\, m_1, n_1 \in N \,|\, b = m_1 - n_1 \end{array}\right\} \Rightarrow a \cdot b = (k_1 - e_1) \cdot (m_1 - n_1) =$$

$$(k_1 - e_1) \cdot m_1 - (k_1 - e_1) \cdot n_1 = k_1 \cdot m_1 - e_1 \cdot m_1 - k_1 \cdot n_1 + e_1 \cdot n_1 =$$
$$= (k_1 \cdot m_1 - k_1 \cdot n_1) + (-e_1 \cdot m_1 + e_1 \cdot n_1) = (m_1 \cdot k_1 - n_1 \cdot k_1) + (-m_1 \cdot e_1 + n_1 \cdot e_1) =$$
$$= (m_1 - n_1) \cdot k_1 + (m_1 - n_1) \cdot (-e_1) = (m_1 - n_1) \cdot (k_1 - e_1) = b \cdot a$$

Таким образом, $(\forall a,b \in Z \Rightarrow a \cdot b = b \cdot a)$

2. Покажем, что $(Z+,\cdot)$ кольцо с единицей. По аксиоме Z_8. $N \subset Z$, а значит, $1 \in Z$. Докажем, что $1 \cdot a = a \cdot 1$ для любого целого числа a.

$$\left.\begin{array}{l} 1 \cdot a = 1 \cdot (k_1 - e_1) = 1 \cdot k_1 - 1 \cdot e_1 = k_1 - e_1 = a \\ a \cdot 1 = (k_1 - e_1) \cdot 1 = k_1 \cdot 1 - e_1 \cdot 1 = k_1 - e_1 = a \end{array}\right\} \Rightarrow 1 \cdot a = a \cdot 1.$$

4.Понятие категоричности системы аксиом. План доказательства. Категоричность системы аксиом целых чисел.

Определение. Данная аксиоматическая теория является категоричной тогда и только тогда, когда любые две модели, удовлетворяющие аксиомам, изоморфны.

Теорема. Система аксиом целых чисел категорична.

Доказательство.

Построим две модели системы аксиом целых чисел и покажем, что они изоморфизмы.

I. План.

Рассмотрим две модели кольца целых чисел $(Z_1,+,\cdot, 0_1,1_1, N_1)$ и $(Z_2,\oplus,\otimes,0_2,1_2 N_2)$.

Для доказательства изоморфизма надо показать, что существует взаимнооднозначное отображение $f : Z_1 \xrightarrow{на} Z_2$ удовлетворяющее условиям:

1) $\forall a_1, b_1 \in Z_1 \Rightarrow f(a_1 + b_1) = f(a_1) \oplus f(b_1)$;
2) $\forall a_1 b_1 \in Z_1 \Rightarrow f(a_1 \cdot b_1) = f(a_1) \otimes f(b_1)$;
3) $f(0_1) = 0_2$;
4) $f(1_1) = 1_2$.

II. Реализация плана.

Пусть $(N_1,1_1,+,\cdot)$ и $(N_2,1_2,\oplus,\otimes)$ – подкольца натуральных чисел, соответствующие кольцам Z_1 и Z_2. Причем N_1 и N_2 изомрфны, т.е. существует отображение $\varphi : N_1 \xrightarrow{на} N_2$ такое, что

1. $\forall a_1, b_1 \in N_1 \Rightarrow \varphi(a_1 + b)_1 = \varphi(a_1) \oplus \varphi(b_1)$;
2. $\forall a_1, b_1 \in N_1 \Rightarrow \varphi(a_1 \cdot b_1) = \varphi(a_1) \otimes \varphi(b_1)$;

СИСТЕМА ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ.

1. Расположенные кольца

Определение. Кольцо $(A,+,\cdot)$ называется расположенным кольцом, если для элементов множества A введено понятие быть положительным (быть больше нулевого элемента – нуля), относительно которого выполняются следующие условия:

1) для любого $a \in A$ имеет место одно из следующих утверждений: либо $a > 0$, либо $a = 0$, либо $(-a) > 0$;
2) если элементы a и b положительные, то $a + b$ и $a \cdot b$ также положительные.

Теорема. Если $(A,+,\cdot)$ расположенное кольцо, то множество A упорядоченное.

Доказательство.

Действительно, вводим отношение α следующим образом: $(a \alpha b \Leftrightarrow a - b > 0)$. Тогда бинарное отношение α : антирефлексивное, антисимметричное, транзитивное.

Действительно, если $a \in A$, то по свойствам кольца $a - a = 0$, а это значит, что $(a,a) \notin \alpha$, а это значит, что α антирефлексивное отношение.

Пусть теперь, тогда $a - b > 0$, откуда по свойствам элементов кольца $(b - a) = -(a - b) \le 0$, т.е. если $(a - b)$ положительный элемент, то $(b - a)$ – не положительный. Итак, если элементы a и b кольца A связаны отношением α, то элементы b и a этим отношением не связаны, откуда следует, что отношение α – антисимметричное.

Пусть теперь $a \alpha b$ и $b \alpha c$, докажем, что $a \alpha c$.

$$\left.\begin{array}{l} a \alpha b \Rightarrow a - b > 0 \\ b \alpha c \Rightarrow b - c > 0 \end{array}\right\} \Rightarrow (a - b) + (b - c) > 0 \Rightarrow a + (-b + b) - c > 0 \Rightarrow a - c > 0 \Rightarrow a \alpha c$$

Из того, что бинарное отношение α : антирефлексивное, антисимметричное, транзитивное следует по определению, что кольцо A упорядоченное.

Обозначим отношение α – символом $>$, то есть $a \alpha b = a > b$.

Действительно, пусть $\varphi\left(\frac{m}{n}\right)=\varphi\left(\frac{k}{l}\right)$, тогда по определению отображения $\frac{m}{n}=\frac{k}{l}$ и $\frac{m}{n},\frac{k}{l}\in Q_2$ откуда, по теореме 1, $m\cdot l=n\cdot k$, откуда по свойствам целых чисел получим, что $m\otimes l=n\otimes k$, тогда по теореме 1 $\frac{m}{n}=\frac{k}{l}$ и $\frac{m}{n},\frac{k}{l}\in Q_1$.

Покажем теперь, что для любых $\frac{m}{n},\frac{k}{l}\in Q_1$ выполняются равенства:

$$\varphi\left(\frac{m}{n}\oplus\frac{k}{l}\right)=\varphi\left(\frac{m}{n}\right)+\varphi\left(\frac{k}{l}\right);$$

$$\varphi\left(\frac{m}{n}\otimes\frac{k}{l}\right)=\varphi\left(\frac{m}{n}\right)\cdot\varphi\left(\frac{k}{l}\right)$$

Итак,

$$\varphi\left(\frac{m}{n}\oplus\frac{k}{l}\right)=\varphi\left(\frac{m\otimes l\oplus k\otimes l}{n\otimes l}\right)=\varphi\left(\frac{m\cdot l+k\cdot l}{n\cdot l}\right)=\frac{m\cdot l+k\cdot l}{n\cdot l}=$$

$$=\frac{m}{n}+\frac{k}{l}\varphi\left(\frac{m}{n}\right)+\varphi\left(\frac{k}{l}\right);$$

$$\varphi\left(\frac{m}{n}\otimes\frac{k}{l}\right)=\varphi\left(\frac{m\otimes k}{n\otimes l}\right)=\varphi\left(\frac{m\cdot k}{n\cdot l}\right)=\frac{m\cdot k}{n\cdot l}=\frac{m}{n}\cdot\frac{k}{l}=\varphi\left(\frac{m}{n}\right)\cdot\varphi\left(\frac{k}{l}\right).$$

3. $\varphi(1_1)=1_2$
4. $\varphi(a+1_1)=\varphi(a)\oplus 1_2$

Определим отображение $f: Z_1\to Z_2$ по правилу:

$$\forall a_1\in Z_1\Rightarrow f(a_1)=\varphi(k_1)-\varphi(e_1),$$

где $a_1=k_1-e_1,\quad k_1,e_1\in N$.

1) покажем, что отображение $f: Z_1\to Z_2$ определено коректно (т.е. оно не зависит от вида разложения числа a_1).

Пусть $a_1=k_1-e_1=m_1-n_1$, где $k_1,e_1,m_1,n_1\in N$, тогда $f(a_1)=\varphi(k_1)-\varphi(e_1)=\varphi(m_1)-\varphi(n_1)$

2) покажем, что $f: Z_1\to Z_2$ взаимно-однозначное отображение:

Пусть $a_1=k_1-e_1$ и $b_1=m_1-n_1$ два числа из Z_1, где $k_1,e_1,m_1,n_1\in N_1$ и пусть $f(a_1)=f(b_1)$, докажем, что $a_1=b_1$.

Из

$$f(a_1)=f(b_1)\Rightarrow\varphi(k_1)-\varphi(e_1)=\varphi(m_1)-\varphi(n_1)\Rightarrow$$
$$\varphi(k_1)+\varphi(n_1)=\varphi(m_1)+\varphi(e_1)\Rightarrow\varphi(k_1+n_1)=\varphi(m_1+e_1)\Rightarrow$$
$$\Rightarrow k_1+n_1=m_1+e_1\Rightarrow k_1-e_1=m_1-n_1\Rightarrow a_1=b_1$$

Пусть целое число $a_2\in Z_2$, покажем, что существует целое число $a_1\in Z_1$ такое что $f(a_1)=a_2$.

(Из $a_2\in Z_2$) $\Rightarrow$ ($\exists k_2,e_2\in N_2 \mid a_2=k_2-e_2$) (1)

(Из $k_2\in N_2$) $\Rightarrow$ ($\exists k_1\in N_1 \mid \varphi(k_1)=k_2$) (2)

(Из $e_2\in N_2$) $\Rightarrow$ ($\exists e_1\in N_1 \mid \varphi(e_1)=e_2$) (3)

(Из (2) и (3)) $\Rightarrow k_2-e_2=\varphi(k_1)-\varphi(e_1)=f(a_1)$, где $a_1=k_1-e_1\in Z_1$.

3) покажем верность условий 1) – 4) (п.**I**)

Пусть $a_1,b_1\in Z_1$, тогда условию существования кольца целых чисел $a_1=m_1-n_1$ и $b_1=k_1-l_1$, где $m_1,n_1,k_1,l_1\in N_1$, тогда

1) $a_1+b_1=(m_1-n_1)+(k_1-l_1)=(m_1+k_1)-(n_1+l_1)$. Найдём $f(a_1+b_1)$:

$$f(a_1+b_1)=\varphi(m_1+k_1)-\varphi(n_1+l_1)=\varphi(m_1)\oplus\varphi(k_1)-\varphi(n_1)\oplus\varphi(l_1)=$$

$= \varphi(m_1) - \varphi(n_1) \oplus \varphi(k_1) - \varphi(l_1) = f(m_1 - n_1) \oplus f(k_1 - l_1) =$

$= f(a_1) \oplus f(b_1)$;

2) $a_1 \cdot b_1 = (m_1 - n_1) \cdot (k_1 - l_1) = (m_1 \cdot k_1 + n_1 \cdot l_1) - (m_1 \cdot l_1 + n_1 \cdot k_1)$. Найдём $f(a_1 \cdot b_1)$:

$f(a_1 \cdot b_1) = \varphi(m_1 \cdot k_1 + n_1 \cdot l_1) - \varphi(m_1 \cdot l_1 + n_1 \cdot k_1) =$

$= \varphi(m_1) \otimes \varphi(k_1) \oplus \varphi(n_1) \otimes \varphi(l_1) - \varphi(m_1) \otimes \varphi(l_1) \oplus \varphi(n_1) \otimes \varphi(k_1) =$

$= (\varphi(m_1) - \varphi(n_1)) \otimes (\varphi(k_1) - \varphi(l_1)) = f(a_1) \otimes f(b_1)$

3) пусть $0_1 \in Z_1$, тогда его можно представить в виде $0_1 = a_1 - a_1$, где $a_1 \in Z_1$. Найдём

$f(0_1) = \varphi(a_1) - \varphi(a_1) = \varphi(m_1 - n_1) - \varphi(m_1 - n_1) = \varphi(m_1) - \varphi(n_1) -$

$- \varphi(m_1) \oplus \varphi(n_1) == (\varphi(m_1) - \varphi(m_1)) \oplus (\varphi(n_1) - \varphi(n_1)) =$

$= \varphi(m_1 - m_1) \oplus \varphi(n_1 - n_1) = \varphi(0_1) \oplus \varphi(0_1) = \varphi(0_1 + 0_1) == \varphi(0_1) = 0_2$;

4)пусть $1_1 \in Z_1$, тогда $1_1 \in N_1$, и значит, для любого $a_1 \in N_1$ имеем, что $a_1 + 1_1 = a_1'$, но тогда $1_1 = a_1' - a_1$. Найдём

$f(1_1) = f(a_1' - a_1) = \varphi(a_1') - \varphi(a_1) = \varphi(a_1 + 1_1) - \varphi(a_1) =$

$\varphi(a_1) \oplus \varphi(1_1) - \varphi(a_1) == (\varphi(a_1) - \varphi(a_1)) \oplus \varphi(1_1) = \varphi((a_1 - a_1) + 1_1) =$

$= \varphi(1_1) = 1_2.$

Доказательство.

Пусть $(Q_1, \oplus, \otimes)$ и $(Q_2, +, \times)$ две модели поля рациональных чисел, докажем, что они изоморфны.

По теореме1 для любого $q_1 \in Q_1$ существуют $k_1, l_1 \in Z$ такие что $q_1 = \frac{k_1}{l_1}$, где $l_1 \neq 0$.

Определим отображение φ. $Q_1 \to Q_2$ по следующему правилу:

$$\forall q_1 \in Q_1 \ \varphi(q_1) = \frac{k_1}{l_1}.$$

Покажем, что отображение $\varphi : Q_1 \overset{в}{\to} Q_2$.

$\left(\frac{m}{n} \in Q_1 \text{ и } \frac{m}{n} = \frac{k}{l}\right) \Rightarrow m \otimes l = n \otimes k \Rightarrow m \cdot l = n \cdot k \Rightarrow \frac{m}{n} = \frac{k}{l}, \frac{m}{n} \in Q_2$

Итак, из того, что $\frac{m}{n} = \frac{k}{l}$, следует, что $\varphi\left(\frac{m}{n}\right) = \varphi\left(\frac{k}{l}\right)$, а значит, φ отображение Q_1 в Q_2.

Покажем, что отображение $\varphi : Q_1 \overset{на}{\to} Q_2$ (сюръекция).

Пусть $\frac{m}{n} \in Q_2$, тогда по теореме1 получим, что $m, n \in Z$, где $n \neq 0$, откуда по аксиоме Q_{10}: $Z \subset Q_1$ получим, что $m, n \in Q_1$, где $n \neq 0$, но тогда по аксиоме Q_8 частное чисел $\frac{m}{n} \in Q_1$.

Итак, для любого $\varphi\left(\frac{m}{n}\right) = \frac{m}{n} \in Q_2$ существует прообраз $\frac{m}{n} \in Q_1$, а это значит, что φ отображение Q_1 на Q_2

Покажем, что отображение $\varphi : Q_1 \overset{в}{\to} Q_2$ – инъективное.

Для этого достаточно показать, что из равенства образов следует равенство прообразов.

Рассмотрим $s=(k\cdot m)\cdot(l\cdot n)=(k\cdot l)\cdot(m\cdot n)\in Q^{+}$.

Q^{+} положительная часть поля рациональных чисел, тогда Q можно упорядочить.

II. Упорядоченность единственна.

Следует показать, что если Q^{++} положительные числа из Q, то $Q^{+}\subset Q^{++}$.

$1=1^{2}\in Q^{++}\Rightarrow 1+1+...+1\in Q^{++}\Rightarrow N\subset Q^{++}$.

$\left(\frac{k}{l}\in Q^{+},\ kl\in N\right)\Rightarrow N\subset Q^{++}\Rightarrow k,l\in Q^{++}$

$((Q,+,\cdot)-\text{поле},k,l>0)\Rightarrow(l^{-1}>0)\Rightarrow(k,l^{-1}\in Q^{++})\Rightarrow(kl^{-1}\in Q^{++})$

$\left(\forall q=\frac{k}{l}\in Q^{+}\Rightarrow\frac{k}{l}\in Q^{++}\right)\Rightarrow(Q^{+}\subset Q^{++}).$

Следовательно, порядок однозначен.

III. Порядок Q есть продолжение порядка в кольце целых чисел.

$Z^{+}\subset Q^{+}\Rightarrow$(порядок поля рациональных чисел является продолжением порядка "$>$" в кольце целых чисел Z).

IV. Поле Q архимедовски упорядочено, т.е. $(\forall q_1,q_2\in Q\ q_1\in Q^{+})\Rightarrow(\exists n\in N|\ q_1\cdot n>q_2)$.

а) $(q_1\in Q^{+}\text{ и }q_2\le 0)\Rightarrow(1\cdot q_1>q_2)$

b) пусть $q_1=\frac{k}{l}>0,\ q_2=\frac{m}{n}>0,\ l,n>0$

$((k\cdot n),(m\cdot l)\in Z)\Rightarrow(s\in N|\ s\cdot(k\cdot n)>(m\cdot l))\Rightarrow$

$\Rightarrow(s\cdot(k\cdot l^{-1})>m\cdot n^{-1})\Rightarrow(sq_1>q_2)$.

3.Полнота системы аксиом поля рациональных чисел.

***Теорема* 3.** Любые два поля рациональных чисел изоморфны, т.е. система аксиом рациональных чисел полная (категоричная).

ПОЛЕ РАЦИОНАЛЬНЫХ ЧИСЕЛ.

1. Аксиоматическое определение поля рациональных чисел.

Определение. Алгебру $(Q,+,\cdot,0,Z)$ называют системой рациональных чисел, а элементы рациональными числами, если имеют место аксиомы:

$Q_1:\ \forall a,b,c\in Q\Rightarrow(a+b)+c=a+(b+c)$

$Q_2:\ \forall a,b\in Q\Rightarrow a+b=b+c$

$Q_3:\ \exists 0\in Q|\ \forall a\in Q\ a+0=0$

$Q_4:\ \forall a\in Q\ \exists a_1\in Q|\ a+a_1=0$

$Q_5:\ \forall a,b,c\in Q\Rightarrow(a\cdot b)\cdot c=a\cdot(b\cdot c)$

$Q_6:\ \forall a,b\in Q\Rightarrow a\cdot b=b\cdot a$

$Q_7:\ \forall a,b,c\in Q\Rightarrow(a+b)\cdot c=a\cdot c+b\cdot c$

$Q_8:\ \forall a,b\in Q,a\ne 0,\ \exists x\in Q|\ ax=b$

$Q_9:\ (Z,+,\cdot)$ – кольцо целых чисел

$Q_{10}:\ Z\subset Q$

$Q_{11}:$ (*аксиома минимальности*) любое непустое подмножество множества Q содержащее кольцо целых чисел, для элементов которого выполняется операция деления, кроме деления на ноль, совпадает с множеством Q, т.е.

$$\left.\begin{array}{l}\text{если }\varnothing\ne M\subseteq Q\\ 1)\ Z\subseteq M\\ 2)\ \forall a,b\in M,a\ne 0\Rightarrow\frac{b}{a}\in M\end{array}\right\}\Rightarrow M=Q$$

Из аксиом Q_1-Q_8 следует, что $(Q+,\cdot)$ поле.

Из аксиом Q_1-Q_4 следует, что $(Q+,\cdot,0)$ аддитивная группа рациональных чисел.

***Теорема* 1**. Всякое рациональное число представимо в виде частного целых чисел, т.е.

$$\left(\forall q \in Q\ \exists k,l \in Z \middle|\ q = \frac{k}{l} = k \cdot l^{-1}, \text{ где } l \neq 0\right), \qquad (1)$$

$$\text{причём } \left(\frac{k}{l} = \frac{m}{n}\right) \Leftrightarrow \left(kn = ml, l \neq 0, m \neq 0\right). \qquad (2)$$

Доказательство.

1. Пусть $M = \left\{ q = \frac{k}{l} \middle|\ k,l \in Z, l \neq 0 \right\}$ множество рациональных чисел, удовлетворяющее условию (1) теоремы.

a) $\left(\left(\forall a \in Z\right) \Rightarrow \left(a = \frac{a}{1}\right) \Rightarrow \left(a \in M\right)\right) \Rightarrow \left(\left(\forall a \in Z\right) \Rightarrow \left(a \in M\right)\right) \Rightarrow Z \subset M$

b) пусть $q_1 = \frac{k}{l}, q_2 = \frac{m}{n} \in M$, тогда $k,l,m,n \in Z, l \neq 0, n \neq 0$ и пусть $q_1 \neq 0$. Найдём частное чисел q_2 и q_1:

$$\frac{q_2}{q_1} = q_2 \cdot q_1^{-1} = \left(m \cdot n^{-1}\right) \cdot \left(k \cdot l^{-1}\right)^{-1} = \left(m \cdot l\right) \cdot \left(n \cdot k\right)^{-1} = \frac{m \cdot l}{n \cdot k} \in M .$$

Таким образом, M непустое подмножество множества Q содержащее кольцо целых чисел, для элементов которого выполняется операция деления, кроме деления на ноль, следовательно, M совпадает с множеством Q. Но тогда элементы Q удовлетворяют условию (1) теоремы.

Аналогично показывается выполнимость условия (2).

Доказать самостоятельно.

Следствие.

$$\left(\left(\forall q = \frac{k}{l} \in Q, s \in Z, s \neq 0\right) \Rightarrow \left(\frac{k}{l} = \frac{k \cdot s}{l \cdot s}\right) \Rightarrow l \cdot \left(k \cdot s\right) = k \cdot \left(l \cdot s\right)\right)$$

Доказать самостоятельно.

Полученное следствие позволяет считать целое число в знаменателе дроби положительным, так как, если знаменатель дроби отрицательное число, то умножив числитель и знаменатель на (–1) получим дробь равную данной с положительным знаменателем.

2.Упорядоченность поля рациональных чисел.

***Теорема* 2.** Поле рациональных чисел можно упорядочить, причем единственным образом, этот порядок является архимедовским и является продолжением порядка кольца целых чисел.

Доказательство.

I. Чтобы упорядочить Q необходимо показать, что в Q существует Q^+, такое что $Q^+ = \left\{ q = \frac{k}{l} \in Q \middle|\ k,l \in N \right\}$.

1) $\left(q = \frac{k}{l} = \frac{m}{n}\right) \Rightarrow \left(kn = ml\right) \Rightarrow \left(\left(k \cdot n\right) \cdot \left(l \cdot n\right) = \left(m \cdot l\right) \cdot \left(l \cdot n\right)\right) \Rightarrow$

$\Rightarrow \left(\left(k \cdot l\right) \cdot n^2 = \left(m \cdot n\right) \cdot l^2\right)$

Из последнего равенства следует, что произведения $k \cdot l$ и $m \cdot n$ одного знака.

2) рациональное число $q = \frac{k}{l}\left(l \neq 0, l,k \in Z\right)$ должно удовлетворять одному из трех условий:

1. $q = 0$, если $k = 0$;
2. $q \in Q^+$, если $k \cdot l \in N$;
3 $-q \in Q^+$, если $\left(-k \cdot l\right) \in N$;

3) $\left(q_1,q_2 \in Q^+\right) \Rightarrow \left(q_1 \cdot q_2 \in Q^+ \text{и } q_1 + q_2 \in Q^+\right)$

$$\left(q_1,q_2 \in Q^+\right) \Rightarrow \left(q_1 = \frac{k}{l}, q_2 = \frac{m}{n} \in Q^+\right) \Rightarrow \left(k,l,m,n \in N\right) \Rightarrow$$

$$\Rightarrow q_1 + q_2 = \frac{k}{l} + \frac{m}{n} = \frac{kn + ml}{ln}$$

Рассмотрим $d = \left(kn + ml\right)\left(ln\right) = \left(kl\right)n^2 + \left(mn\right)l^2$, тогда $d \in N$, а значит, $q_1 + q_2 \in Q^+$.

$$\left(q_1,q_2 \in Q^+\right) \Rightarrow \left(q_1 = \frac{k}{l}, q_2 = \frac{m}{n} \in Q^+\right) \Rightarrow \left(k,l,m,n \in N\right) \Rightarrow$$

$$\Rightarrow q_1 \cdot q_2 = \frac{k}{l} \cdot \frac{m}{n} = \frac{k \cdot m}{l \cdot n}$$