МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Алгебра и теория чисел

7. Методические указания для обучающихся по освоению дисциплины

Приступая к изучению учебной дисциплины, целесообразно ознакомиться с учебной программой дисциплины, электронный вариант которой размещён на сайте БФ ВГУ.

Это позволит обучающимся получить четкое представление о:

- перечне и содержании компетенций, на формирование которых направлена дисциплина;
- основных целях и задачах дисциплины;
- планируемых результатах, представленных в виде знаний, умений и навыков, которые должны быть сформированы в процессе изучения дисциплины;
- количестве часов, предусмотренных учебным планом на изучение дисциплины, форму промежуточной аттестации;
- количестве часов, отведенных на аудиторные занятия и на самостоятельную работу;
- формах аудиторных занятий и самостоятельной работы;
- структуре дисциплины, основных разделах и темах;
- системе оценивания учебных достижений;
- учебно-методическом и информационном обеспечении дисциплины.

Знание основных положений, отраженных в рабочей программе дисциплины, поможет обучающимся ориентироваться в изучаемом курсе, осознавать место и роль изучаемой дисциплины в подготовке будущего выпускника, строить свою работу в соответствии с требованиями, заложенными в программе.

Основными формами аудиторных занятий по дисциплине являются лекции и практические занятия, посещение которых обязательно для всех студентов (кроме студентов, обучающихся по индивидуальному плану).

Подготовка к практическим занятиям ведется на основе планов практических занятий. В ходе подготовки к практическим занятиям необходимо изучить в соответствии с вопросами для повторения конспекты лекций, основную литературу, ознакомиться с дополнительной литературой. Кроме того, следует повторить материал лекций, ответить на контрольные вопросы, изучить образцы решения задач, выполнить упражнения (если такие предусмотрены).

При подготовке к промежуточной аттестации необходимо повторить пройденный материал в соответствии с учебной программой, примерным перечнем вопросов, выносящихся на зачет. Рекомендуется использовать конспекты лекций и источники, перечисленные в списке литературы в рабочей программе дисциплины, а также ресурсы электронно-библиотечных систем.

8. Методические материалы для обучающихся по освоению теоретических вопросов дисциплины

Тема. Бинарные отношения

План

1. Отношения эквивалентности.

2. Отношения порядка. Упорядоченные множества.

3. Связь отношений эквивалентности с разбиениями множества.

1. Отношения эквивалентности. Отношения порядка

ОПРЕДЕЛЕНИЕ. *Декартовым произведением* множеств A и B называется множество, состоящее из всех упорядоченных пар элементов вида <a, b>, в которых первый элемент принадлежит первому множеству, а второй – второму.

Обозначение: $A \times B = \{\langle a, b\rangle / a \in A, b \in B\}$.

Если множества A и B совпадают, то декартово произведение называют также *декартовым квадратом* множества A: $A \times A = A^2$.

ОПРЕДЕЛЕНИЕ. *Бинарным отношением,* заданным на непустом множестве A, называется всякое подмножество декартова квадрата множества A.

Для обозначения бинарных отношений используют либо специальные значки, общепринятые, например: =, ≤ , ≥ , ∥ , ⊥ и т.д., либо буквы греческого алфавита: α, δ, σ, φ, ρ и т.д.

Если элементы *x* и *y* множества A находятся в некотором бинарном отношении *σ,* то это может обозначаться одним из следующих образов:

$<x, y> \in \sigma$, либо $x \sigma y$.

ОПРЕДЕЛЕНИЕ. Бинарное отношение ρ, заданное на непустом множестве A, называется:

- *рефлексивным,* если $(\forall a \in A)$ справедливо $<a, a> \in \rho$;
- *антирефлексивным,* если $(\forall a \in A)$ справедливо $<a, a> \notin \rho$;
- *симметричным,* если $(\forall a, b \in A)$ из того, что пара $<a, b> \in \rho$, следует, что пара $<b, a> \in \rho$;
- *транзитивным,* если для $(\forall a, b, c \in A)$, из того, что пара $<a, b> \in \rho$ и пара $<b, c> \in \rho$, следует, что пара $<a, c> \in \rho$;
- *антисимметричным,* если для любых различных элементов $a, b \in A$ из того, что $<a, b> \in \rho$ и $<b, a> \in \rho$ следует, что $a = b$;
- *асимметричным,* если $(\forall a, b \in A, a \neq b)$ условие $<a, b> \in \rho$ никогда не влечет за собой выполнение условия $<b, a> \in \rho$;
- *отношением эквивалентности,* если оно рефлексивно, симметрично и транзитивно одновременно;
- *отношением порядка,* если оно антисимметрично и транзитивно;

2. Отношения порядка. Упорядоченные множества.

Если при этом отношение *ρ* обладает свойством антирефлексивности, то оно называется отношением *строгого порядка,* если же *ρ* обладает свойством рефлексивности, то – отношением *нестрогого порядка.*

ОПРЕДЕЛЕНИЕ. Отношение порядка ρ, заданное на множестве A, называется *отношением линейного порядка,* если для любых двух элементов $a, b \in A$ выполняется одно и только одно из условий:

$a = b$ или $<a, b> \in \rho$ или $<b, a> \in \rho$.

Говорят также, что в этом случае отношение ρ обладает свойством *связности.*

Если бинарное отношение ρ задано на конечном множестве, то его наглядно можно изобразить с помощью *ориентированного графа.* При этом элементы самого множества изображаются точками на плоскости.

Если пара $<a, b> \in \rho$, то соответствующие точки соединяются ориентированным ребром от a к b.

Также можно построить *график* бинарного отношения. Для этого по осям абсцисс и ординат откладываются элементы множества, а на координатной плоскости строятся точки, координаты которых соответствуют элементам бинарного отношения.

Верно и обратное. Любой ориентированный граф, а также график можно рассматривать как граф или график бинарного отношения и определять по ним его свойства.

ПРИМЕР **1**. Пусть A = {1, 2, 4, 6}.

Тогда декартов квадрат множества A будет равен:

A×A = {<1, 1>; <2, 2>; <4, 4>; <6, 6>; <1, 2>; <2, 1>; <1, 4>; <4, 1>;
<1, 6>; <6, 1>; <2, 4>; <4, 2>; <2, 6>; <6, 2>; <4, 6>; <6, 2>}.

Следующее подмножество ρ множества A×A является, согласно определению, бинарным отношением, заданным на множестве A:

ρ = {<2, 2>; <4, 4>; <1, 2>; <2, 1>; <1, 4>; <6, 2>; <4, 6>}.

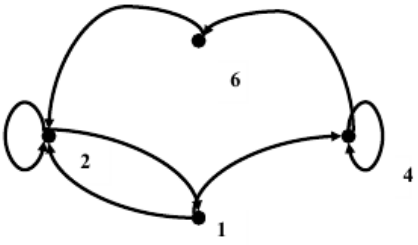
Данное отношение не обладает свойством рефлексивности, так как, например, пара <1, 1> ему не принадлежит.

С другой стороны, оно не обладает и свойством антирефлексивности, поскольку оно содержит пары <2, 2> и <4, 4>.

Отношение ρ не симметрично, хотя бы уже потому, что оно содержит пару <1, 4>, но не содержит пары <4, 1>. Однако, оно не будет также являться ни антисимметричным, ни асимметричным, поскольку ему одновременно принадлежат пары элементов <1, 2> и <2, 1>, причем $2 \neq 1$.

Отношение ρ не обладает также свойством транзитивности, так как, хотя пары <1, 4> и <4, 6> ему принадлежат, пара <1, 6> отношению ρ не принадлежит.

Построим граф и график этого бинарного отношения:



Граф отношения ρ

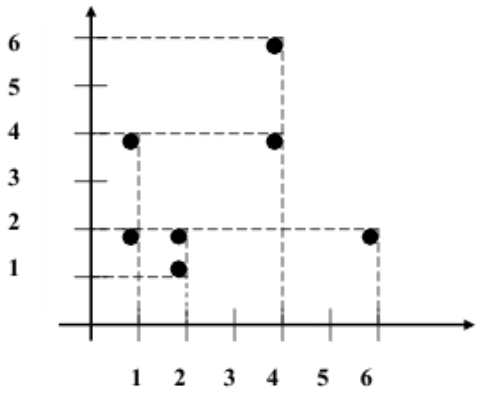


График отношения ρ

ЗАМЕЧАНИЯ. 1. Из определений следует, что ни одно бинарное отношение не может обладать одновременно свойствами рефлексивности и антирефлексивности или свойствами симметричности и антисимметричности (асимметричности). В то же время из примера следует, что некоторые бинарные отношения могут вообще не обладать ни одним из свойств соответствующей пары.

2. Примерами отношения эквивалентности могут служить:

- отношение равенства « = » на любом числовом множестве;
- отношение параллельности « ∥ » на множестве всех прямых плоскости;
- отношение ρ на множестве всех слов русского алфавита, если два слова *u* и *v* находятся в отношении ρ тогда и только тогда, когда они начинаются с одной и той же буквы, поскольку каждое из этих отношений, очевидно, обладает свойствами рефлексивности, симметричности и транзитивности.

3. Примерами отношения порядка могут служить:

- отношения сравнения по величине « < » и « > » на множестве целых чисел;
- отношение делимости нацело « **:** » на множестве натуральных чисел.

При этом первые два отношения есть отношения строгого линейного порядка, поскольку они обладают свойством антирефлексивности и связности (ни одно целое число не может быть строго больше или меньше самого себя и из двух различных целых чисел одно обязательно больше либо меньше другого), а последнее – нестрогого нелинейного порядка, так как оно, напротив, рефлексивно и несвязно (каждое натуральное число делится само на себя и для двух различных натуральных чисел не обязательно одно делится на другое нацело).

3. Связь отношений эквивалентности с разбиениями множества

ОПРЕДЕЛЕНИЕ. Говорят, что набор подмножеств множества A образует *разбиение* этого множества, если выполняются следующие условия:

1) хотя бы одно из подмножеств непусто,

2) никакие два подмножества не пересекаются,

3) объединение всех подмножеств совпадает с множеством A.

Подмножества называются в этом случае *классами разбиения.*

Множество $\bar{A}$, элементами которого являются классы данного разбиения, называют *фактор-множеством* множества A по данному разбиению.

Существует самая тесная связь между разбиениями некоторого множества и отношениями эквивалентности, которые можно на данном множестве построить.

ТЕОРЕМА. *По каждому отношению эквивалентности, заданному на множестве A, можно построить некоторое разбиение этого множества. И обратно, каждому разбиению множества A соответствует некоторое отношение эквивалентности.*

ЗАМЕЧАНИЯ

1. Следствием этой теоремы, которое имеет практическое значение, является тот факт, что существует взаимно-однозначное соответствие между множеством всех различных разбиений множества A и множеством всех различных отношений эквивалентности, которые можно задать на этом множестве. Таким образом, различных отношений эквивалентности на данном множестве будет ровно «столько», «сколько» различных разбиений этого множества можно построить.

2. Пусть дано разбиение множества A и соответствующее ему отношение эквивалентности ρ. Тогда фактор-множество по данному разбиению называют также фактор-множеством по отношению эквивалентности *ρ* и обозначают A/ρ .

ПРИМЕР **2**.

1. Пусть дано множество A = {a, b, c, d} и отношение эквивалентности на нем:

$$\rho = \{<a, a>; <d, d>; <a, d>; <d, a>; <c, c>; <b, b>\}.$$

Чтобы построить по отношению ρ разбиение этого множества, достаточно в один класс разбиения поместить те и только те элементы множества A, которые находятся в отношении ρ:

$$A = \{a, d\}; A = \{c\}; A = \{b\}.$$

2. Пусть дано множество A = {a, b, c, d}, на котором задано разбиение:

$$A = \{a\}; A = \{b, c\}; A = \{d\}.$$

Чтобы построить по данному разбиению соответствующее ему отношение эквивалентности, достаточно отнести к этому отношению те и только те пары элементов, которые принадлежат одному классу разбиения: ρ = {<a, a>; <b, b>; <c, c>; <.b, c>; <c, b>; <d, d>}.

ПРИМЕР **3.** Зададим на множестве Z отношение ≡ по следующему правилу:

$$b \equiv a \pmod m \Rightarrow b - a = m \cdot q,\ q, m \in Z,\ m > (1).$$

Говорят, что *a сравнимо с b по модулю m*.

Очевидно, что это отношение есть отношение эквивалентности, так как оно рефлексивно, симметрично и транзитивно. Также очевидно, что числа a и b сравнимы по mod m тогда и только тогда, когда они дают при делении на m одинаковые остатки.

Классами разбиения по данному отношению ≡ являются множества вида:

$$\{a+m\cdot q \mid q \text{ - целое}\} = \{\ldots,-3m+a, -2m+a, -m+a, a, m+a, 2m+a, 3m+a,\ldots\},$$

которые обозначаются через a+mZ или просто $\bar{a}$ и называются *классами вычетов* или просто *вычетами*.

Фактор-множество Z/ ≡ обозначается обычно через Z_m и называется *множеством вычетов или множеством целых чисел по модулю m*.

ЗАМЕЧАНИЕ. Каждый класс разбиения по отношению ≡ содержит бесконечно много элементов. Само множество классов эквивалентности содержит ровно *m*

элементов. Обычно из каждого класса эквивалентности выбирают представителя – неотрицательное число, которое при делении на *m* дает остаток r, где $0 \le r < m$.

3. Понятие и свойства бинарной алгебраической операции

Отображения или *функции*

ОПРЕДЕЛЕНИЕ. Бинарное отношение f, заданное на паре множеств A и B, называется *отображением* или *функцией* из A в B, если выполняются условия:

1) для любого элемента $a \in A$ найдется такой элемент $b \in B$, что пара $<a, b> \in f$;

2) для любого элемента $a \in A$ и любых элементов $b, c \in B$ из того, что пары $<a, b>$ и $<a, c>$ одновременно принадлежат отношению f, следует, что $b = c$.

Если пара $<a, b>$ принадлежит отношению f, то первый элемент пары называют *прообразом* второго, а второй – *образом* первого.

ЗАМЕЧАНИЕ. Учитывая последнее, определение короче можно сформулировать следующим образом:

Бинарное отношение f, заданное на паре множеств A и B, называется *отображением* или *функцией* из A в B, если каждый элемент множества A имеет *единственный* образ в множестве B.

Обозначение. Если f есть отображение из A в B и пара $<a, b> \in f$, то это записывают как $f(a) = b$.

ОПРЕДЕЛЕНИЕ. Отображение f из A в B называется *инъективным (или инъекцией)*, если для любых элементов $a, b \in A$ выполняется условие:

$$f(a) = f(b) \Rightarrow a = b.$$

Отображение f из A в B называется *сюръективным (или сюръекцией, или отображением «на»)*, если для всякого элемента $b \in B$ найдется такой элемент $a \in A$, для которого $f(a) = b$ (каждый образ имеет прообраз в множестве A).

Отображение f из A на B называется *биективным (или биекцией или взаимно-однозначным*, если оно инъективно и сюръективно одновременно.

ПРИМЕР **1**.

1. Пусть $f = \{<x, y> \in R^{+} \times R \,/\, x = y^2\}$. Данное отношение отображением не является, так как не выполнено второе условие из определения 8. Например, для $x = 4$ имеем $y = \sqrt{4} = 2$ и $y_1 = -\sqrt{4} = -2$. Таким образом, пары $<4, 2>$ и $<4, -2>$ одновременно принадлежат отношению f, хотя $2 \neq -2$.

2. Пусть $f = \{<x, y> \in R \times R \,/\, x^2 = y\}$. Очевидно, что в этом случае каждое действительное число x имеет единственный образ в множестве R, и потому f является отображением.

Однако из того, что $f(2) = f(-2) = 4$, не следует, что $2 = -2$, потому f не инъективно.

Кроме того, если $y < 0$, то нельзя найти ни одного элемента $x \in R$, для которого выполнялось бы равенство $x^2 = y$. Следовательно, отображение f не сюръективно.

3. Пусть $f = \{<x, y> \in R \times R \,/\, y = 2x\}$. Очевидно, что в этом случае f также является отображением. Более того, так как для любых действительных чисел x и x_1:

$$f(x) = f(x_1) \Leftrightarrow 2x = 2x_1 \Leftrightarrow x = x_1,$$

то отображение f инъективно, а так как для любого действительного числа y существует такое число $x = \frac{y}{2}$, что:

$$f(x) = f\left(\frac{y}{2}\right) = 2 * \frac{y}{2} = y,$$

то отображение f сюръективно. Следовательно, f является биекцией.

ОПРЕДЕЛЕНИЕ. Пусть f - отображение из множества X в множество Y:

$$f = \{<x, y> \,/\, x \in X, y \in Y\}.$$

Соответствие f^{-1} = {<y, x> / где <x, y> $\in$ f} называется *обратным* к отображению f.

ТЕОРЕМА. Соответствие f^{-1}, обратное к отображению f, само является отображением тогда и только тогда, когда отображение f биективно.

Тема. Алгебраические системы

План

1. Понятие и свойства бинарной алгебраической операции.

2. Структуры с одной бинарной операцией. Группы. Простейшие свойства групп.

3. Нормальные делители. Конечные группы.

4. Структуры с двумя бинарными операциями. Кольца и поля. Простейшие свойства колец и полей.

1. Понятие и свойства бинарной алгебраической операции.

ОПРЕДЕЛЕНИЕ. *Бинарной алгебраической операцией*, заданной на множестве A, называется отображение f: A × A → A, которое каждой паре элементов из множества *A* ставит в соответствие некоторый элемент этого же множества:

$$(\forall a,b \in A)\ (\exists c \in A)\ f\text{: } <a, b> \to c$$

Обозначение: a f b = c. Для обозначения бинарных операций обычно используют не буквы, а специальные значки: « +», « * »,«-», « : », « ◦ » и т.д.

ЗАМЕЧАНИЕ

Подобное определение можно сформулировать для n-арной алгебраической операции при любом конечном натуральном n. Однако в абстрактной алгебре наиболее часто, кроме бинарной, используют понятия унарной и нульарной операций.

ОПРЕДЕЛЕНИЕ. *Унарной алгебраической операцией*, заданной на множестве A, называется отображение f: A → A, которое каждому элементу множества A ставит в соответствие некоторый элемент этого же множества:

$$(\forall a \in A)\ (\exists c \in A)\text{: } f(a) = c.$$

Нульарной алгебраической операцией, заданной на множестве A, называется выделение в этом множестве некоторого фиксированного элемента.

ОПРЕДЕЛЕНИЕ. Операция « * », заданная на непустом множестве A, называется:

- *ассоциативной,* если:

$$(\forall a, b, c \in A)\ a * (b * c) = (a * b) * c;$$

- *коммутативной,* если:

$$(\forall a, b \in A)\ a * b = b * a.$$

ОПРЕДЕЛЕНИЕ. Говорят, что операция « * », заданная на непустом множестве A, обладает:

- *левым [правым] нейтральным элементом,* если:

$$(\exists e \in A)\ (\forall a \in A)\ \ e * a = a\ [a * e = a];$$

- *двусторонним нейтральным элементом (*или просто *нейтральным),* если она обладает и левым и правым нейтральным элементами, причем эти элементы совпадают:

$$(\exists e \in A)(\forall a \in A)\ \ e * a = a * e = a.$$

ОПРЕДЕЛЕНИЕ

Операция « * », заданная на непустом множестве A, называется:

- *обратимой слева [справа],* если:

$$(\forall a \in A)\ (\exists b \in A)\ b * a = e,\ [a * b = e],$$

где *e* – левый [правый] нейтральный элемент множества *A* по операции « * ».

- *двусторонне обратимой* (или просто *обратимой*), если она обратима и справа и слева:

$$(\forall a \in A)\ (\exists b \in A)\ a * b = b * a = e,$$

где *e* – нейтральный элемент множества A по операции *« * ».*

- *сократимой слева [справа],* если:

$$(\forall a, b, c \in A)\ (c * a = c * b \Rightarrow a = b).$$
$$[a * c = b * c \Rightarrow a = b].$$

- *сократимой,* если она сократима и слева и справа.

ОПРЕДЕЛЕНИЕ. Пусть на множестве A заданы две бинарные алгебраические операции - «* » и « ◦ ».

Операция « ◦ » называется *дистрибутивной слева [справа]* относительно операции « * », если:

$$(\forall a, b, c \in A)\ c \circ (a * b) = (c \circ a) * (c \circ b)$$
$$[(a * b) \circ c = (a \circ c) * (b \circ c)].$$

Операция « ◦ » называется *дистрибутивной* относительно операции « * », если она дистрибутивна относительно данной операции и слева и справа.

ЗАМЕЧАНИЯ

1. При проверке свойств бинарной операции, заданной на некотором множестве, прежде всего необходимо проверить, является ли данная операция алгебраической на данном множестве. Так, например, операция вычитания не является алгебраической на множестве N натуральных чисел, так как для случая, когда a < b, результат этой операции a – b < 0 и, следовательно, не принадлежит множеству N.

2. Очевидно, что не все свойства операций независимы друг от друга. Так, если по данной операции в данном множестве нет нейтрального элемента, то не имеет смысла говорить и об обратимости этой операции.

3. Если операция « * » коммутативна на множестве A, то любое из свойств, которое выполняется для нее слева или справа, очевидно, будет выполняться и с другой стороны.

2. Структуры с одной бинарной операцией. Группы. Простейшие свойства групп.

группы играют в современной абстрактной алгебре настолько важную роль и их приложения имеют настолько широкий спектр, что изучение различных классов групп, групповых конструкций и их свойств выросло в самостоятельную научную теорию – теорию групп. Поэтому в алгебре чаще используются несколько отличные от приведенного выше определения группы через так называемые групповые аксиомы.

ОПРЕДЕЛЕНИЕ 1. *Группой* называется алгебраическая структура $\mathbf{G} = < G, *, ^{-1}, e >$, где $G \neq \varnothing$ - основное множество структуры, на котором заданы:

- одна бинарная алгебраическая операция « * »;
- одна унарная алгебраическая операция $^{-1}$;
- одна нульарная алгебраическая операция – выделение нейтрального элемента *e*,

удовлетворяющие следующим аксиомам:

1) операция « * » ассоциативна: $(\forall a, b, c \in G)\ a*(b*c) = (a*b)*c$;

2) по данной операции существует нейтральный элемент:

$$(\exists e \in G)\ (\forall a \in G)\quad e*a = a*e = a;$$

3) операция « * » обратима на м G*:*

$$(\forall a \in G)\ (\exists b \in G)\quad a*b = b*a = e.$$

ОПРЕДЕЛЕНИЕ 2. *Группой* называется алгебраическая структура $\mathbf{G} = < G, * >$, где G – непустое основное множество структуры, « * » - бинарная алгебраическая операция, заданная на G, причем выполняются следующие аксиомы:

1) операция *« * »* ассоциативна: $(\forall a, b, c \in G)\ a*(b*c) = (a*b)*c$;

2) $(\forall a, b \in G)\ (\exists x, y \in G)\quad a*x = b$ и $y*a = b$ (т.е. в группе разрешимы уравнения такого вида).

ТЕОРЕМА. Определения 1 и 2 группы эквивалентны, то есть, если алгебраическая структура с одной бинарной операцией является группой в смысле определения 1, то она является группой и в смысле определения 2, и обратно.

ЗАМЕЧАНИЯ

1. Так как в определении группы отсутствует требование коммутативности бинарной операции, то в определении 1 необходимо требовать существования решения обоих уравнений, поскольку из разрешимости уравнения a*x = b в этом случае не следует разрешимость уравнения y*a = b и наоборот. Если же операция в группе коммутативна, то группу называют *абелевой.*

2. Чаще всего операцию в группе обозначают символами « + » или « $\bullet$ » и называют *сложением* и *умножением* соответственно. В первом случае группа называется *аддитивной,* нейтральный элемент – *нулем,* обратный элемент – *противоположным* и обозначаются они как 0 и -a. Во втором случае группу называют *мультипликативной.*

3. *Натуральной степенью* элемента g мультипликативной группы

< G, $\bullet$ > называется элемент $g^n = g \bullet g \bullet \ldots \bullet g$ (n раз), $n \in N$;

Степенью с отрицательным показателем называется элемент

$$g^{-n} = g^{-1} \bullet g^{-1} \bullet \ldots \bullet g^{-1} \text{ (n раз)}, n \in N.$$

4. Если группа конечна, то число ее элементов называется *порядком* группы. В противном случае группа называется группой *бесконечного порядка.*

Обозначение: порядок группы G обозначается как $|G|$.

5. Часто группа обозначается одной буквой G без указания операции.

ПРИМЕРЫ

1**.** Аддитивными абелевыми группами являются, например, структуры:

$$< Z, + >, < Q,, + >, < R, + >,$$

где Z, Q и R - множества целых, рациональных и действительных чисел соответственно.

2. Примерами мультипликативных абелевых групп могут служить структуры: $< Q^*, \bullet >$, $< R^*, \bullet >$, где Q^* и R^* - множества всех ненулевых рациональных и действительных чисел соответственно.

3. Примером некоммутативной группы может служить множество всех квадратных невырожденных матриц порядка *n* по операции матричного умножения.

4. Наибольший теоретический и прикладной интерес представляет группа симметрий правильного n-угольника, называемая *диэдрической группой Dn* или *группой диэдра.*

Элементами Dn являются, во-первых, n поворотов вокруг центра многоугольника на углы $\varphi_k = k \cdot \frac{2\pi}{n}$, где k = 0, 1, ..., (n - 1), во-вторых, n осевых симметрий. Осями симметрии служат: в случае четного n - n/2 диагоналей, соединяющих противоположные вершины, и (n/2) прямых, соединяющих середины противоположных сторон; в случае нечетного n - n высот многоугольника (рис. 3). Других симметрий у многоугольника нет.

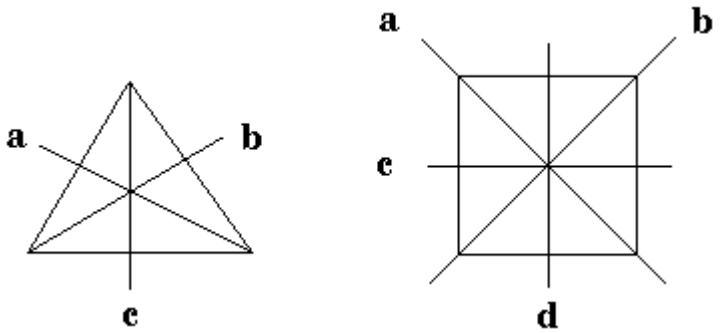


Рис. 3. Оси симметрий правильных многоугольников

Используя группы симметрий, Е. С. Федоров в 1890 году решил задачу классификации правильных пространственных систем точек, являющуюся одной из основных задач кристаллографии. Существует всего 17 плоских федоровских групп, они были найдены непосредственно; пространственных федоровских групп - 230, и

только теория групп позволила провести их исчерпывающую классификацию. Это был исторически первый случай применения теории групп непосредственно в естествознании.

Следующая теорема выражает простейшие свойства групп.

ТЕОРЕМА. Во всякой группе < G, ·> выполняются следующие свойства:

1) В G существует и притом единственный нейтральный элемент.

2) Для всякого элемента a группы G существует и притом единственный обратный элемент a^{-1}.

3) Для любых элементов a и b группы G справедливы равенства:

$$(a^{-1})^{-1} = a \text{ и } (a\cdot b)^{-1} = b^{-1}\cdot a^{-1}.$$

4) В группе < G, ·> нет делителей нуля.

5) В группе G уравнения a*x = b и y*a = b однозначно разрешимы для любых элементов a и b.

6) Во всякой группе операция двусторонне сократима.

ОПРЕДЕЛЕНИЕ. Подмножество H группы < G, ·> называется ее *подгруппой*, если оно само является группой относительно операции «·», определенной в группе G.

ТЕОРЕМА (*критерий подгруппы*). Подмножество H группы < G, ·> является ее подгруппой тогда и только тогда, когда выполняется условие:

$$(\forall\, a, b \in H)\quad a\cdot b^{-1} \in H.$$

ЗАМЕЧАНИЕ. Говорят, что подмножество H группы < G, ·> является ее подгруппой, если оно *замкнуто* относительно операции, определенной в группе G, и относительно операции взятия обратного элемента.

ПРИМЕРЫ.

1. Подгруппами всякой группы < G, · > являются сама эта группа и единичная подгруппа E, состоящая только из одного нейтрального элемента группы G : E = { e }. Эти подгруппы называются *несобственными.* Всякая подгруппа группы *G,* отличная от этих двух, называется *собственной.*

2. Множество всех четных чисел является подгруппой аддитивной группы всех целых чисел < Z, + >, так как для любых четных чисел a и b число a + (-b) является четным.

3. Множество {-1, 1} образует подгруппу мультипликативной группы всех ненулевых действительных чисел < R, · >.

4**.** Совокупность <g> = $\{g^n / n \in Z\}$ степеней элемента g группы G является подгруппой в G.

Отметим некоторые простейшие свойства подгрупп.

СВОЙСТВО **1.** Пересечение произвольной совокупности подгрупп группы *G* само будет подгруппой этой группы.

СВОЙСТВО **2.** Объединение двух подгрупп группы G будет являться подгруппой в том и только в том случае, когда одна из них содержится в другой.

ОПРЕДЕЛЕНИЕ. Подгруппа <g> = $\{g^n / n \in Z\}$ группы G называется *циклической подгруппой, порожденной элементом g.*

ЗАМЕЧАНИЕ. Если в группе принята аддитивная форма записи операции, то степени элемента g группы G называются *кратными* и обозначаются ng, ($n \in Z$).

ТЕОРЕМА **2.** Подгруппа <g> группы G конечна в том и только в том случае, когда

$$(\exists\, n \in N)\ g^n = e.$$

ЗАМЕЧАНИЕ. Если n – минимальное число со свойством $g^n = e$, то оно называется *порядком элемента g.* Если же $(\forall\, n \in N)\ g^n \neq e$, то все степени элемента g будут различны между собой, и подгруппу <g> называют *бесконечной циклической,* и сам элемент g – *элементом бесконечного порядка.*

3. Нормальные делители. Конечные группы.

ОПРЕДЕЛЕНИЕ. Пусть H – подгруппа группы < G, $\bullet$ >, g – произвольный элемент группы G. Множество $H \bullet g$ [$g \bullet H$] всех элементов группы G, которые представимы в виде $h \bullet g$ [$g \bullet h$], где h пробегает множество элементов подгруппы H, т. е.

$$H \bullet g = \{h \bullet g / h \in H\}$$

$$[\ g \bullet H = \{g \bullet h / h \in H\}\ ]$$

называется *правым [левым] смежным классом* группы G по подгруппе H.

ТЕОРЕМА. Пусть дана группа < G, $\bullet$ >, в ней подгруппа H и g – произвольный элемент из G. Тогда выполняются следующие свойства:

1) если элемент a принадлежит правому смежному классу $H \bullet g$, то

$$H \bullet a = H \bullet g,$$

т.е. всякий правый смежный класс группы G по подгруппе H задается любым из своих элементов, который называется *представителем класса* $H \bullet g$;

2) два любых смежных класса группы G по подгруппе H либо не пересекаются, либо совпадают;

3) одним из правых смежных классов группы G по подгруппе H является сама подгруппа H, и других подгрупп среди правых смежных классов группы G по подгруппе H нет;

4) объединение всех правых смежных классов группы G по подгруппе H совпадает с самой группой G.

СЛЕДСТВИЕ.

Множество всех правых классов группы G по подгруппе H образует разбиение этой группы, которое называют *правосторонним разложением* группы G по подгруппе H:

$$G = h_1 \bullet g \cup h_2 \bullet g \cup \ldots \cup h_{\grave{o}} \bullet g \quad (h_i \in H).$$

ЗАМЕЧАНИЯ

1. Аналогичные свойства можно сформулировать и для левых смежных классов. Соответствующее разбиение называют *левосторонним разложением* группы G по подгруппе *H.* Эти оба разложения состоят из одного и того же числа смежных классов. Если это число конечно, то оно называется *индексом* подгруппы H в группе G.

2. Пусть G – конечная группа порядка n, H – ее подгруппа порядка n и индекса k. Тогда из следствия предыдущей теоремы получаем равенство: $n = m \bullet k$.

ТЕОРЕМА *Лагранжа.*

1. Порядок и индекс любой подгруппы конечной группы являются делителями порядка самой группы.

2. Порядок любого элемента конечной группы является делителем порядка группы.

ОПРЕДЕЛЕНИЕ. Подгруппа H группы G называется *нормальной подгруппой* или *нормальным делителем* группы G, если для любого элемента $g \in G$ левый и правый смежные классы по подгруппе H совпадают:

$$(\forall\ g \in G)\ \ H \bullet g = g \bullet H.$$

В этом случае говорят просто о *разложении группы G по нормальному делителю H.* Обозначение: $H \nabla G$.

ЗАМЕЧАНИЕ. Нетрудно проверить, что пересечение любого числа нормальных делителей группы < G, $\bullet$ > само является нормальным делителем этой группы.

ПРИМЕР **1**

В абелевой группе всякая подгруппа является нормальным делителем, поэтому, например, подгруппа всех четных чисел будет нормальным делителем аддитивной группы всех целых чисел < Z, + >.

ОПРЕДЕЛЕНИЕ. Элементы x и y группы G называются *сопряженными в G,* если:

$$(\exists\ g \in G)\ \ y = g^{-1} \bullet x \bullet g.$$

ТЕОРЕМА (*Критерий нормального делителя)*

Подгруппа H группы G тогда и только тогда будет нормальным делителем в < G, • >, когда H вместе со всяким своим элементом будет содержать и все элементы, сопряженные с ним в G.

ТЕОРЕМА. Пусть H – нормальная подгруппа группы < G, • >. Множество всех различных смежных классов группы G по подгруппе H с операцией умножения:

$$(H \bullet g_1) \bullet (H \bullet g_2) = H \bullet (g_1 \bullet g_2)$$

образует группу, которая называется *фактор-группой группы G по подгруппе H* и обозначается:

$$G / H = \{H \bullet g / g \in G\}.$$

Гомоморфизмы и изоморфизмы групп

ОПРЕДЕЛЕНИЕ. Отображение группы *< G, • >* на группу <S, * > называется *гомоморфизмом групп,* если выполняется условие:

$$(\forall a, b \in G) \quad f(a \bullet b) = f(a) * f(b). \quad (1)$$

Сами группы называются при этом *гомоморфными.* Также говорят, что группа <S, * > есть *гомоморфный образ* группы < G, • >.

Обозначение: G ~ S.

ЗАМЕЧАНИЕ. Условие (1) из определения 1 называют также *требованием сохранения групповой операции.* Словами оно читается так: образ произведения элементов группы < G, • > равен произведению их образов в группе <S, * >.

Поэтому в правой части равенства (1) стоит знак операции « • » группы G, а в левой – знак операции « * » группы S.

ОПРЕДЕЛЕНИЕ. Гомоморфизм *f* групп G и S называется *изоморфизмом*, если отображение *f* биективно.

Сами группы называются при этом *изоморфными,* а группа *<S, * > - изоморфным образом* группы < G, • >. Обозначение: $G \cong S$.

Отметим некоторые свойства изоморфизмов групп.

СВОЙСТВО **1.** При изоморфизме групп нейтральный элемент переходит в нейтральный.

СВОЙСТВО **2.** При изоморфизме групп обратный элемент переходит в обратный:

$$(\forall a \in G) \; f(a^{-1}) = [f(a)]^{-1}.$$

СВОЙСТВО **3.** При изоморфизме групп сохраняется свойство коммутативности операции.

СВОЙСТВО **4.** Изоморфный образ группы является группой.

ПРИМЕР **1.** Аддитивная группа всех целых чисел изоморфна своей подгруппе, состоящей из четных чисел, так как отображение $\varphi: Z \to 2Z$ такое, что:

$$(\forall x \in Z) \quad \varphi(x) = 2x,$$

является изоморфизмом групп, так как очевидно, что φ - биективно и $(\forall x, y \in Z)$ $\varphi(x + y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y)$.

ПРИМЕР **2.** Аддитивная группа всех действительных чисел изоморфна мультипликативной группе всех положительных действительных чисел:

$$<R, + > \cong <R^+, \bullet >,$$

так как отображение $\varphi: R \to R^+$, при котором:

$$(\forall x \in R) \quad \varphi(x) = e^x$$

является биекцией, поскольку:

$$(\forall x, y \in R) \quad \varphi(x) = \varphi(y) <=> e^x = e^y <=> x = y,$$

$$(\forall r \in R^+) \; (\exists x \in R): \varphi(x) = y, \text{ а именно, } x = \ln y, \text{ т.к. } \varphi(\ln y) = e^{\ln y} = y$$

и сохраняет групповую операцию:

$$(\forall x, y \in R) \; \varphi(x + y) = e^{x+y} = e^x \bullet e^y = \varphi(x) \bullet \varphi(y).$$

ТЕОРЕМА *(о гомоморфизме групп).* Если $\varphi: K \to S$ есть гомоморфизм группы G на группу S, то фактор-группа G / Ker φ изоморфна группе S.

При этом изоморфизм χ: S $\to$ G / Ker φ можно выбрать таким образом, что для всех x $\in$ G ,будет выполняться равенство $\chi(\varphi(x)) = \pi(x)$, где π - естественный гомоморфизм G на G / Ker φ .

4. Структуры с двумя бинарными операциями. Кольца и поля. Простейшие свойства колец и полей.

ОПРЕДЕЛЕНИЕ. 1. Непустое множество A с заданными на нем бинарными операциями « $\circ$ » и « * » называется *полукольцом* < A, *, $\circ$ >, если:

1) < A, * > - абелева полугруппа, т.е., операция « * » ассоциативна, коммутативна и обладает нейтральным элементом;

2) < A, $\circ$ > - группоид;

3) операция « $\circ$ » связана с операцией « * » левым и правым законами дистрибутивности, т.е.

$$(\forall a, b, c \in A)\ c \circ (a * b) = (c \circ a) * (c \circ b)$$
$$\text{и} \quad (a * b) \circ c = (a \circ c) * (b \circ c).$$

2. Полукольцо < *A, *, $\circ$ >* называется *кольцом*, если:

1) *< A, * >* - абелева группа, т.е. операция *« * »* ассоциативна, коммутативна, обладает нейтральным элементом и обратима;

2) *< A, $\circ$ >* - группоид;

3) операция *« $\circ$ »* связана с операцией *« * »* левым и правым законами дистрибутивности, т.е.,

$$(\forall\ a, b, c \in A)\ c \circ (a * b) = (c \circ a) * (c \circ b)$$
$$(a * b) \circ c = (a \circ c) * (b \circ c).$$

3. Кольцо < A, *, $\circ$ > называется *полем*, если:

1) < A, * > - абелева группа, т.е. операция « * » ассоциативна, коммутативна, обладает нейтральным элементом и обратима;

2) < A /{0}, $\circ$ > -- абелева группа, т.е. операция « $\circ$ » ассоциативна, коммутативна, обладает нейтральным элементом и обратима;

3) операция « $\circ$ » связана с операцией « * » левым и правым законами дистрибутивности, т.е.

$$(\forall a, b, c \in A)\ c \circ (a * b) = (c \circ a) * (c \circ b)$$
$$(a * b) \circ c = (a \circ c) * (b \circ c).$$

ЗАМЕЧАНИЯ

1. Вообще, если на некотором непустом множестве A заданы две бинарные алгебраические операции « * » и « $\circ$ », то говорят, что задана *алгебраическая структура* < A, *, $\circ$ > *с двумя бинарными операциями.*

2. Так как по определению операция « * » коммутативна *в любом кольце*, то *коммутативным кольцом* называется такое кольцо, в котором коммутативна вторая операция *« $\circ$ ».* Обычно операцию « $\circ$ » называют *умножением,* а операцию « * » - *сложением* независимо от их природы. Аналогично, если речь идет об *ассоциативном кольце,* то этим свойством обладает операция умножения « $\circ$ ». Если по операции умножения в кольце существует нейтральный элемент, то кольцо называют *кольцом с единицей.*

ОПРЕДЕЛЕНИЕ. 1. Пусть на множестве A с элементом 0 задана операция «$\circ$».

Элемент x $\in$ A называется *левым [правым] делителем нуля*, если:

1) x $\neq$ 0;

2) ($\exists$a$\in$A) a $\neq$ 0 и x $\circ$ a = 0 [a $\circ$ x = 0].

Если элемент x $\in$ A является и левым и правым делителем нуля, то его называют *двусторонним* (или просто) *делителем нуля.*

2. Ассоциативно-коммутативное кольцо без делителей нуля называется *областью целостности.*

ПРИМЕР **2.** 1. Множество N натуральных чисел по операции обычного умножения образует абелев моноид < N, $\bullet$ >.

Множество N по операции обычного сложения также образует абелев моноид < N, + >, так как:

$$(\forall a, b \in N) \quad a + b \in N;$$
$$(\forall a, b, c \in N) \quad a + (b + c) = (a + b) + c;$$
$$(\forall a, b \in N) \quad a + b = b + a;$$
$$(\forall a \in N) \quad a + 0 = 0 + a = a;$$

однако операция сложения не обратима на N, так как, например, для числа 2 не существует обратного (противоположного) элемента в множестве N.

Так как $(\forall a, b, c \in N) \quad c\cdot(a + b) = c\cdot a + c\cdot b$, то умножение на N дистрибутивно относительно сложения.

Из сказанного следует, что структура < N, +, • > образует ассоциативно-коммутативное полукольцо с единицей.

2. Очевидно также, что умножение на множестве Z всех целых чисел обладает такими же свойствами, как и сложение, кроме свойства обратимости, поскольку для всякого целого числа a, за исключением 1 и -1, обратный элемент a^{-1} не является целым числом. Поэтому структура < Z, · > образует абелеву полугруппу. Кроме того, очевидно, что в множестве Z нет делителей нуля. Следовательно, структура < Z, +, · > является областью целостности.

3. Нетрудно проверить, что на множестве всех действительных чисел сложение и умножение обладают свойствами ассоциативности, коммутативности, в качестве нейтральных элементов выступают 0 и 1 соответственно, обе операции обратимы и умножение дистрибутивно относительно сложения. Следовательно, < R, +, · > по операциям сложения и умножения образует поле.

Рассмотрим еще один пример, который будет иметь особое значение в дальнейшем.

ПРИМЕР **3.** На множестве Z_m определим операции сложения и умножения вычетов по правилам:

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

Нетрудно проверить, что эти операции на множестве Z_m всегда выполнимы и однозначно определены, то есть результат выполнения операции не зависит от выбора представителя класса вычетов. В получающейся таким образом алгебре < Z_m, +, • > выполняются все аксиомы коммутативного кольца с единицей. Кольцо <Z_m, +, • > называется *кольцом классов вычетов* или просто *кольцом вычетов по модулю m*.

Справедливы следующие утверждения, которые будут нам полезны в дальнейшем.

ТЕОРЕМА. Элемент a кольца Z_m имеет обратный тогда и только тогда, когда

НОД(a, m) = 1.

ТЕОРЕМА

Кольцо вычетов < Z_m, +, · > тогда и только тогда является полем, когда m – простое число.

Гомоморфизмы и изоморфизмы колец и полей

СВОЙСТВО **1.** Всякая аддитивная абелева группа <G, + > может служить аддитивной группой кольца <G, + , • >, где умножение *« • »* определено следующим образом:

$$(\forall a, b \in G) \; a \bullet b = 0.$$

СВОЙСТВО **2.** В любом кольце выполняются все свойства аддитивной группы.

СВОЙСТВО **3.** Во всяком кольце <K, + , • > умножение дистрибутивно слева и справа относительно вычитания:

$$(\forall a, b, c \in K) \; c \bullet (a – b) = c \bullet a - c \bullet b \text{ и}$$
$$(a – b) \bullet c = a \bullet c - b \bullet c.$$

СВОЙСТВО **4**

Во всяком кольце <K, + , • > любое произведение, в котором хотя бы один из сомножителей равен нулю, само равно нулю, то есть:

$$(\forall\ a \in K)\ a \bullet 0 = 0 \bullet a = 0.$$

ЗАМЕЧАНИЕ. Обращение последнего свойства, вообще говоря, неверно. А именно, существуют кольца, например, кольцо квадратных матриц порядка *n*, в которых из равенства нулю произведения a •b = 0 не следует равенство нулю сомножителей. То есть, существуют кольца с *делителями нуля.*

ОПРЕДЕЛЕНИЕ. *Подкольцом* кольца К называется всякое подмножество К′ этого кольца, которое само является кольцом относительно операций, определенных в К.

ТЕОРЕМА *(критерий подкольца)*

Подмножество К′ кольца <K, + , • > будет его подкольцом тогда и только тогда, когда выполнены условия:

1) $(\forall\ a, b \in K')\ a + (-b) \in K'$, т.е., < К′ , + > - подгруппа аддитивной группы кольца*;*

2) $(\forall\ a, b \in K')\ \ a \bullet b \in K'$.

СВОЙСТВО **5.** Так как всякое поле является кольцом, то все свойства колец справедливы и для полей.

ОПРЕДЕЛЕНИЕ. Пусть дано кольцо <K, + , • >. Рассмотрим множество P всех таких упорядоченных пар элементов кольца K, у которых второй элемент не равен нулю:

$$P = \{<a, b>/\ a, b \in K, b \neq 0\}.$$

Будем обозначать такие пары в виде дробей $\frac{a}{b}$ и называть их частными кольца <K, + , • >. Зададим на множестве всех частных кольца операции « + » и «•» следующим образом:

$$(\forall\ a, b, c, d \in K)\quad \frac{a}{b} + \frac{c}{d} = \frac{a \bullet d + c \bullet b}{b \bullet d},\ b \neq 0,\ d \neq 0;$$

$$(\forall\ a, b, c, d \in K)\quad \frac{a}{b} \bullet \frac{c}{d} = \frac{a \bullet c}{b \bullet d},\ b \neq 0,\ d \neq 0.$$

ОПРЕДЕЛЕНИЕ. Два частных будем называть равными, если выполняется равенство:

$$\frac{a}{b} = \frac{c}{d} \iff a \bullet d = b \bullet c.$$

Множество всех равных между собой частных поля K будем объединять в один класс и в качестве представителя этого класса обычно рассматривается несократимая дробь, которая в данном классе единственна.

Нетрудно проверить, что операции заданы корректно, то есть результат их выполнения не зависит от выбора представителя класса. Поэтому в дальнейшем будем отождествлять весь класс равных между собой частных кольца с его несократимым представителем.

Следующие свойства множества всех частных кольца K показывают, что по заданным операциям это множество образует поле, которое называется *полем частных кольца K.*

СВОЙСТВО **6.** Операции сложения и умножения на множестве всех частных кольца K обладают свойствами ассоциативности и коммутативности. Умножение связано со сложением левым и правым законами дистрибутивности.

СВОЙСТВО **7.** По операции « + » существует нейтральный элемент, в качестве которого выступает класс дробей с числителем, равным нулю, и произвольным знаменателем.

Для элемента $\frac{a}{b}$ противоположным является элемент $\frac{-a}{b}$.

СВОЙСТВО **8.** По операции « $\bullet$ » существует нейтральный элемент, в качестве которого выступает класс дробей с числителем, равным знаменателю. Для всякого ненулевого элемента $\frac{a}{b}$ обратным является элемент $\frac{b}{a}$.

СВОЙСТВО **9.** Единица поля не равна нулю поля, следовательно, во всяком поле имеется по крайней мере два различных элемента – 0 и 1.

СВОЙСТВО **10.** Никакое поле не содержит делителей нуля.

ОПРЕДЕЛЕНИЕ. Пусть <K, + , $\bullet$ > и <S, $*$, °> - два кольца. Отображение φ: K $\rightarrow$ S называется *гомоморфизмом колец,* если выполняются условия:

1) ($\forall$ a, b $\in$ K) φ(a + b) = φ(a) $*$ φ(b);

2) ($\forall$ a, b $\in$ K) φ(a $\bullet$ b) = φ(a) ° φ(b).

Гомоморфизм φ колец K и S называется *изоморфизмом,* если отображение φ биективно.

ОПРЕДЕЛЕНИЕ. *Ядром гомоморфизма* колец K и S называется множество всех элементов кольца K, которые отображаются в нуль кольца S:

$$\mathrm{Ker}\ \varphi = \{x \mid x \in K, \varphi(x) = 0_S\}.$$

Тема. Теория делимости в кольце целых чисел

План

1. Деление целых чисел с остатком.

2. НОД и НОК целых чисел. Алгоритм Евклида. Каноническое представление целых чисел.

1. Деление целых чисел с остатком

ОПРЕДЕЛЕНИЕ. Говорят, что целое число a *делится* на целое число b ≠ 0, если найдется такое целое число c, что a = b·c.

Число a называется *кратным числа b,* число b – *делителем числа a,* число c – *частным от деления a на b.*

ЗАМЕЧАНИЕ. Отношение делимости, как видно из определения, вводится через обратную операцию – умножение целых чисел. Однако, если рассматривать деление как бинарную операцию, которая паре целых чисел <a, b>, b ≠ 0, ставит в соответствие число a : b, которое, вообще говоря, не обязательно является целым, то операция деления на множестве Z будет *частичной операцией.*

Отметим основные свойства отношения делимости в кольце Z.

СВОЙСТВО **1.** Пусть a и b – целые числа, не равные 0. Если одновременно выполняются условия: a : b и b : a, то a = $\pm$ b.

Если a : b, то a : -b и - a : b. Целое число 0 делится на любое другое целое число.

СВОЙСТВО **2.** Если для целых чисел a, b и c ≠ 0 выполняются условия:

a : b и a : c, то a : (b $\pm$ c).

ЗАМЕЧАНИЕ. Обратное утверждение в общем случае неверно, то есть, если для целых чисел a, b и c выполняется делимость a : (b $\pm$ c), то отсюда не следует, что число a делится на каждое из слагаемых. Например, 12 : (5 + 7), но при этом 12 не делится ни на 5, ни на 7.

СВОЙСТВО **3.** Отношение делимости на множестве Z \ {0} рефлексивно и транзитивно, так как:

($\forall$ a $\in$ Z \ {0}) a : $\pm$ a и

($\forall$ a, b, c $\in$ Z \ {0}) (a : b и b : c => b : c).

Очевидно, что на множестве Z^+ отношение делимости будет также антисимметрично, так как:

$$(\forall\ a, b \in Z^{+})\ (a : b \text{ и } b : a \Rightarrow a = b).$$

Поэтому на множестве всех положительных целых чисел отношение делимости является отношением нестрогого порядка.

СВОЙСТВО **4.** Если для целых a и $b \neq 0$, a : b, то для любого целого c: ac : b.

СВОЙСТВО **5.** Если каждое из двух целых чисел a и b делится на число $c \neq 0$, то: $(\forall\ n, m \in Z)\ (na \pm mb) : c$.

ОПРЕДЕЛЕНИЕ. Говорят, что целое число *a делится с остатком* на целое число $b \neq 0$, если существуют такие целые числа p и q, что выполняются условия:

$$a = bq + r,\ 0 \le r < |\ b\ |\ (*).$$

Число q называется *неполным частным*, а число r – *остатком* от деления a на b.

Из определения, вообще говоря, нельзя сделать выводов о том, всегда ли существует такая пара целых чисел q и r и однозначно ли они определены для данных a и b. Ответ на эти вопросы дает соответствующая теорема.

ТЕОРЕМА *(о делении целых чисел с остатком).* Для всяких целых чисел a и b, где $b \neq 0$, деление с остатком всегда выполнимо и однозначно определено.

Иными словами, для всяких целых чисел a и b, где $b \neq 0$, всегда существует и притом единственная пара целых чисел q и r, удовлетворяющих условию (*).

ЗАМЕЧАНИЕ. Если заданы числа a и q или a и r, то другую пару чисел из условия (*) можно подобрать не одним способом.

СВОЙСТВО **1.** Числа a и b дают одинаковые остатки при делении на некоторое целое число m тогда и только тогда, когда разность (a – b) делится на m нацело.

Пусть m – некоторое целое число, $m \neq 0$, $m \neq 1$. Рассмотрим на множестве Z бинарное отношение ρ :

$(\forall\ a, b \in Z)$ $\langle a, b\rangle \in \rho \iff$ числа a и b при делении на m дают одинаковые остатки.

Тогда справедливо следующее свойство.

СВОЙСТВО **2.** Отношение ρ на множестве целых чисел является отношением эквивалентности. Оно разбивает все множество Z на классы эквивалентности, в каждый из которых попадают те и только те целые числа, которые при делении на m дают один и тот же остаток r. Так как различными остатками при делении на m могут быть числа 0, 1, 2, … m – 1, то существует ровно m различных классов разбиения по данному отношению ρ:

$$K_r = \{a \in Z / a = xq + r,\ x, q \in Z\}.$$

Любое целое число, принадлежащее классу K_r, называют его *представителем.*

Обозначим множество вех классов разбиения по отношению эквивалентности ρ через Z / ρ :

$$Z / \rho = \{K_0, K_1, \ldots, K_{\hat{e}}, \ldots, K_{m-1}\}$$

и зададим на этом множестве операции сложения и умножения классов:

$$K_r + K_s = K_{r+s};$$

$$K_r \cdot K_s = K_{rs}, \text{ где } r, s \in \{0, 1, \ldots, m\text{-}1\}.$$

Нетрудно проверить, что операции определены корректно и результат их выполнения не зависит от выбора представителя класса. Тогда можно сформулировать следующие свойства.

СВОЙСТВО **3.** Операция сложения на множестве Z / ρ ассоциативна и коммутативна. Нейтральным элементом является класс K_0, противоположным элементом для класса K_r является класс K_s, где s – наименьшее целое положительное число со свойством: сумма (r + s) делится на m нацело.

СВОЙСТВО **4.** Операция умножения на множестве Z/ρ ассоциативна, коммутативна и обладает единицей, которой является класс K_1.

СВОЙСТВО **5.** Умножение классов связано со сложением законами дистрибутивности:

$$K_r \cdot (K_s + K_t) = K_r \cdot K_{s+t} = K_{r(s+t)} = K_{rs+rt} = K_{rs} + K_{rt} = K_r \cdot K_s + K_r \cdot K_t .$$

СВОЙСТВО **6**

Из свойств 4 – 6 следует, что множество Z / ρ по операциям сложения и умножения классов образует кольцо, которое называется *кольцом классов вычетов по модулю m*.

ЗАМЕЧАНИЕ. Можно показать, что фактор-кольцо кольца Z из примера 2 параграфа 2.6 вида Z / mZ будет изоморфно кольцу классов вычетов по модулю m. Поэтому кольца вида Z / mZ также называют кольцами классов вычетов по модулю m.

2. НОД и НОК целых чисел. Алгоритм Евклида. Каноническое представление целых чисел

НОД и НОК целых чисел

ОПРЕДЕЛЕНИЕ. Целое число d ≠ 0 называется *общим делителем* целых чисел a и b, если каждое из этих чисел делится на число d.

Общий делитель чисел a и b называется их *наибольшим общим делителем*, если он делится на любой другой их общий делитель.

Обозначение: d = НОД (a, b) или d = (a, b).

Отметим некоторые свойства НОД целых чисел, которые будут важны в дальнейшем.

СВОЙСТВО **1.** Если d = НОД (a, b) и d_1 = НОД (a, b), то $d_1 = \pm d$.

СВОЙСТВО **2.** Если число a делится на число b ≠ 0 нацело, то НОД (a, b) = b.

СВОЙСТВО **3.** Пусть d_1 = НОД (a, b), d = НОД (d_1, c), тогда d = НОД (a, b, c).

СВОЙСТВО **4.** Если число a делится на число b с остатком, то есть

$$a = bq + r,\ 0 \le r < |b|,$$ то НОД (a, b) = НОД (b, r).

ЗАМЕЧАНИЯ

1. Первое свойство означает, что НОД двух целых чисел определен с точностью до знака. Обычно принято проводить рассуждения с положительным значением НОД целых чисел.

2. Третье свойство фактически утверждает, что операция нахождения НОД целых чисел ассоциативна, так как:

НОД (НОД (a, b), c) = НОД (a, (НОД (b, c)) = НОД (a, b, c).

Это означает, что вычислять НОД нескольких целых чисел можно в произвольном порядке.

ОПРЕДЕЛЕНИЕ. Целое число h называется *общим кратным* ненулевых целых чисел a и b, если h делится на каждое из этих чисел.

Общее кратное целых чисел a и b называется их *наименьшим общим кратным*, если на него делится любое другое их общее кратное. Обозначение: h = НОК (a, b) или h = [a, b].

Отметим некоторые свойства НОК целых чисел, которые схожи со свойствами наибольшего общего делителя.

СВОЙСТВО **1.** Если h = НОК (a, b) и h_1 = НОК (a, b), то $h_1 = \pm h$.

СВОЙСТВО **2.** Если число a делится на число b ≠ 0 нацело, то НОК (a, b) = a.

СВОЙСТВО **3.** Пусть h_1 = НОК (a, b) и h = НОК (h_1, c), тогда h = НОК (a, b, c).

ЗАМЕЧАНИЯ

1. Первое свойство означает, что НОК двух целых чисел определено с точностью до знака.

2. Третье свойство утверждает ассоциативность операции нахождения НОК целых чисел: НОК нескольких целых чисел можно вычислять в произвольном порядке.

НОК (НОК (a, b), c) = НОК (a, (НОК (b, c)) = НОК (a, b, c).

Алгоритм Евклида. Теорема Ламе

Заметим, что из определения и свойств наибольшего общего делителя и

наименьшего общего кратного целых чисел не следует, что НОД и НОК двух чисел всегда существуют. Их существование нужно доказывать отдельно.

Пусть a, b ≠ 0 – целые числа. Построим для них так называемую *последовательность Евклида,* выполняя последовательно деление с остатком.

1) Если a делится на b нацело, то последовательность Евклида имеет вид: *a, b*.

2) Пусть $a > b$ и a не делится на b нацело. Тогда, выполняя деление a на b с остатком, получим:

$$a = bq_0 + r_0,\ 0 \le r_0 < |b|.$$

Затем делим число b на полученный остаток r_0:

$$b = r_0 q_1 + r_1,\ 0 \le r_1 < r_0.$$

Снова делим теперь уже r_0 на остаток r_1:

$$r_0 = r_1 q_2 + r_2,\ 0 \le r_2 < r_1.$$

Продолжаем процесс деления с остатком до тех пор, пока на некотором шаге не получим остаток, равный нулю:

$$r_{n-2} = r_{n-1} q_n + r_n,\ 0 \le r_n < r_{n-1},$$

$$r_{n-1} = r_n q_{n+1} + 0.$$

Последовательность, полученная в ходе этих операций:

$$a > b > r_0 > r_1 > \ldots > r_{n-1} > r_n > r_{n+1} = 0 \quad (**),$$

и будет последовательностью Евклида для случая 2).

Последовательность (**) обязательно оборвется на нуле через конечное число шагов, так как она является строго убывающей последовательностью натуральных чисел (начиная с r_0). Множество натуральных чисел ограничено снизу нулем, поэтому последовательность (**) не может убывать бесконечно.

Алгоритм построения последовательности Евклида называется *алгоритмом Евклида,* который используется при доказательстве существования НОД двух целых чисел.

ТЕОРЕМА *(о существовании НОД целых чисел).* Пусть a и b ≠ 0 – целые числа. Алгоритм Евклида доставляет НОД чисел a и b, который равен последнему не равному нулю остатку в последовательности Евклида (**):

$$\text{НОД}(a, b) = r_n.$$

ТЕОРЕМА *(о существовании НОК целых чисел).* Пусть a и b – не равные нулю целые числа. Тогда справедливо соотношение:

$$\text{НОК}(a, b) = \frac{ab}{\text{НОД}(a,b)} \quad (***).$$

ЗАМЕЧАНИЕ. В связи с использованием алгоритма Евклида возникает вопрос: сколько шагов необходимо выполнить для вычисления НОД? Ответ на этот вопрос дает теорема, доказанная французским математиком, физиком и инженером Габриэлем Ламе (1795-1870).

ТЕОРЕМА *(Ламе).* Пусть a и b - натуральные числа. Число шагов в алгоритме Евклида для чисел a и b не превосходит 5k, где k - число десятичных цифр меньшего из чисел a и b.

ТЕОРЕМА. Пусть d = НОД (a, b). Тогда существуют такие целые числа x и y, что d линейно выражается через сами числа a и b:

$$d = xa+yb,\ x, y \in Z. \quad (1)$$

Алгоритм, позволяющий вычислять числа x и y, удовлетворяющие равенству (1) для данных чисел a и b и их наибольшего общего делителя d, получил название *расширенного алгоритма Евклида,* который заключается в следующем.

Из каждого равенства, которые получаются при построении последовательности Евклида, выразим остаток и подставим его в следующее равенство, пока не дойдем до НОД чисел a и b. В последнем равенстве приведем подобные слагаемые при этих

числах. Полученные коэффициенты и будут численными значениями x и y:

$$r_0 = a - bq_0,\ r_1 = b - r_0 q_1,\ \Rightarrow r_1 = b - (a - bq_0)\, q_1, \text{ и т.д.}$$

ОПРЕДЕЛЕНИЕ. Натуральное число p называется *простым*, если оно не имеет других делителей, кроме себя и единицы. Если же число имеет делители, отличные от себя и единицы, то оно называется *составным.*

ПРИМЕР 1. Числа 2, 3, 19, 31 являются простыми, а числа 6, 222, 18, 864 – составными.

ЗАМЕЧАНИЕ. Единица, очевидно, не является ни простым, ни составным числом. Можно сказать, что множество всех натуральных чисел разбивается на три непересекающихся класса: класс простых чисел, класс составных чисел и класс, содержащий только единицу.

СВОЙСТВО **1.** Всякое составное число a имеет хотя бы один простой делитель p, не превосходящий $\sqrt{a}$: $p \le \sqrt{a}$.

СВОЙСТВО **2.** Если произведение двух целых чисел делится на простое число *p*, то хотя бы один из сомножителей делится на это число:

$$ab : p \Rightarrow a : p \text{ или } b : p.$$

СВОЙСТВО **3.** Если p и q – простые числа и p : q, то p = q.

Простые числа играют особую роль среди всех натуральных, и даже целых чисел, которая выражается следующей теоремой.

ТЕОРЕМА *(основная теорема арифметики).* Всякое натуральное число может быть представлено в виде произведения простых сомножителей единственным образом с точностью до порядка следования сомножителей.

ЗАМЕЧАНИЯ

1. Теорема справедлива и для целых чисел, так как всякое целое число a можно представить в виде:

$$a = \varepsilon_a |a| \text{ – где } \varepsilon_a \text{ - знак, } a|a| \text{ - натуральное число.}$$

2. Если в разложении целого числа *a* на простые множители собрать вместе в виде степени одинаковые простые числа, то полученное разложение называется *канонической формой записи числа* a*:*

$$a = \varepsilon_a\ p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \qquad (2)$$

где $p_1, p_2, \ldots, p_k$ - различные простые множители.

Основная теорема арифметики также может использоваться для нахождения НОД и НОК целых чисел по следующим правилам, которые следуют из определения и свойств делимости и свойств простых чисел.

ПРАВИЛО **1.** Чтобы найти НОД двух (или нескольких) целых чисел, нужно в их каноническом разложении на простые множители выбрать все множители, которые входят в разложения каждого из чисел, причем в наименьшей степени, и перемножить их.

ПРАВИЛО **2.** Чтобы найти НОК двух (или нескольких) целых чисел, нужно в их каноническом разложении на простые множители выбрать все множители, которые входят в разложение хотя бы одного из чисел, причем в наибольшей степени, и перемножить их.

Основной факт, который был установлен о множестве простых чисел, выражается следующей теоремой.

ТЕОРЕМА. Множество простых чисел бесконечно.

ОПРЕДЕЛЕНИЕ. Два целых числа a и b называются *взаимно-простыми*, если они не имеют других общих делителей кроме единицы.

СВОЙСТВО **4.** Числа a и b взаимно-просты тогда и только тогда, когда их НОД равен единице: НОД *(a, b) = 1.*

СВОЙСТВО **5.** Если числа a и b взаимно-просты, то существуют такие целые

числа x и y, что: ax + by = 1.

СВОЙСТВО **6.** Если числа a и b взаимно-просты, то НОК(a, b) = ab.

Тема. Векторное пространство. Подпространство. Сумма и прямая сумма подпространств

План

1. Определение и свойства линейного (векторного) пространства.

2. Подпространства линейного пространства

3. Линейная оболочка системы векторов.

4. Суммы линейных пространств.

5. Изоморфизм линейных пространств.

1. Определение и свойства линейного пространства

Определение. Пусть L есть некоторое непустое множество и P – числовое поле. В L определено действие, называемое *сложением*, согласно которому каждой паре элементов u, v ∈ L сопоставляется третий элемент из L, обозначаемый через u + v. Также определено действие *умножения элементов из L на числа из P*, согласно которому каждой паре, состоящей из элемента u ∈ L и числа λ ∈ P, сопоставлен элемент из L, обозначаемый через λu.

Если при этом выполнены следующие семь аксиом, то множество L, рассматриваемое вместе с указанными двумя операциями, называется линейным пространством над полем P.

Коммутативность сложения:

∀ u, v ∈ L u + v = v + u.

2) Ассоциативность сложения:

∀ u, v, w ∈ L (u + v) + w = u + (v + w).

Обратимость сложения:

∀ u, v ∈ L всегда найдется такой x ∈ L, что u + x = v

(при этом элемент x называется разностью между v и u и обозначается: x = v - u).

Ассоциативность умножения на числа из P:

∀ u ∈ L ∀ λ, μ ∈ P λ(μu) = (λμ)u.

Свойство дистрибутивности относительно сложения чисел из P:

∀ u ∈ L ∀ λ, μ ∈ P (λ + μ)u = λu + μu.

Свойство дистрибутивности относительно сложения элементов из L:

∀ u, v ∈ L ∀ λ ∈ P λ(u + v) = λu + λv.

Свойство единичного множителя:

для числа 1 ∈ P и ∀ u ∈ L выполнено 1u = u.

Элементы любого линейного пространства будем называть *векторами.*

Примеры.

1. Координатное векторное пространство.

Рассмотрим декартово произведение множества вещественных чисел $V^{(n)} = \underbrace{R \times R \times ... \times R}_{n\ раз}$, на котором введены действия сложения и умножения на элемент из R по следующим правилам:

∀ x , y ∈ V(n) если x = (x1, x2, …, xn) и y = (y1, y2, …, yn), то

1) x + y = (x1 + y1, x2 + y2, …, xn + yn),

2) ∀ α ∈ R αx = (αx1, αx2, …, αxn).

Напомним, что множество V(n) называют n-мерным координатным векторным пространством, а его элементы называют n-мерными векторами или n-векторами.

2. Множество Mm×n всех матриц размерности m×n над полем R.

Введем на множестве Mm×n действия сложения и умножения на элемент из R по следующим правилам:

∀ A, B ∈ Mm×n если A = (aij)m×n и B = (bij)m×n, то

1) $A + B = (a_{ij} + b_{ij})_{m\times n}$,

2) $\forall\ \alpha \in R\quad \alpha A = (\alpha a_{ij})_{m\times n}$.

3. Множество FR всех многочленов произвольной степени от одной переменной над полем R.

Введем на множестве FR действия сложения и умножения на элемент из R по следующим правилам: $\forall\ f(x), g(x) \in FR\ \ \forall\ \alpha \in R$

1) $\forall\ x \in C\quad (f + g)(x) = f(x) + g(x)$,

2) $\forall\ x \in C\quad (\alpha f)(x) = \alpha(f(x))$.

Следствия из аксиом линейного пространства

Свойство 1.

В произвольном линейном пространстве L существует единственный элемент θ, такой, что $u + \theta = u$ при любом $u \in L$. Элемент θ называется нулевым элементом в L. При необходимости в записи нулевого элемента указывается линейное пространство, относительно которого проводятся рассуждения: $\theta = \theta_L$.

Доказательство: Покажем существование нулевого элемента θ. Для произвольного элемента $u\in L$ по аксиоме 3) линейного пространства (для случая $v = u$) существует элемент $y\in L$, такой, что $u + y = u$. Рассмотрим произвольный элемент $w\in L$. По той же аксиоме 3) имеем: $u + t = w$ для некоторого $t\in L$. Тогда, используя аксиомы 1) и 2) из определения линейного пространства, получаем:

$w + y = (u + t) + y = (t + u) + y = t + (u + y) = t + u = u + t = w$.

Таким образом, существует элемент $y\in L$, такой, что $u + y = u$ при любом $u \in L$. Обозначим $\theta = y$.

Проверим единственность θ. Пусть в пространстве L существуют два нулевых элемента θ_1 и θ_2, тогда сумма $\theta_1 + \theta_2$ равна, с одной стороны, элементу θ_1 (если в качестве нулевого считать θ_2), а, с другой стороны, равна θ_2 (если в качестве нулевого считать θ_1), т.е. $\theta_1 = \theta_2$.

Свойство 2.

Для всякого $u \in L$ существует в L единственный элемент, называемый противоположным к u и обозначаемый –u, такой что $u + (-u) = \theta$. По отношению к –u элемент u является противоположным, т.е. $u = -(-u)$.

Доказательство: существование такого элемента –u следует из аксиомы 3) линейного пространства (для случая $v = \theta$). Проверим единственность –u. Пусть для $u \in L$ существуют два противоположных элемента w_1 и w_2, тогда $u + w_1 = u + w_2 = \theta$ и, следовательно, $w_1 = w_1+\theta = w_1+(u+w_2) = (w_1+u)+w_2 = (u+w_1)+w_2 = \theta+w_2 = w_2$. Т.е. противоположный элемент для элемента u существует единственный.

Свойство 3.

$0u = \theta$ для любого $u \in L$.

Доказательство: заметим, что для произвольного u выполнено $0u+0u = (0+0)u = 0u$. Тогда $\theta = 0u+(-(0u)) = (0u+0u)+(-(0u)) = 0u+(0u+(-(0u)) = 0u+\theta = 0u$.

Свойство 4.

$\lambda\theta = \theta$ для любого $\lambda \in P$.

Доказательство: рассмотрим произвольный элемент $u \in L$. По свойству 3) имеем $0u = \theta$, тогда для любого $\lambda \in P\ \ \lambda\theta = \lambda(0u) = (\lambda 0)u = 0u = \theta$.

Свойство 5.

Если $\lambda u = \theta$ ($u \in L$, $\lambda \in P$), то $\lambda = 0$ или $u = \theta$.

Доказательство: если $\lambda = 0$, то заключение выполнено. Пусть $\lambda \neq 0$, тогда $\frac{1}{\lambda}(\lambda u) = \frac{1}{\lambda}\theta$, откуда по аксиоме 4 и свойству 4) получаем $(\frac{1}{\lambda}\lambda)u = \theta$, а значит, $u = \theta$.

Свойство 6.

$(-1)u = -u$ при любом $u \in L$.

Доказательство: Нужно показать, что элемент $(-1)u$ является противоположным к элементу u. Действительно, $(-1)u + u = ((-1) + 1)u = 0u = \theta$, что и требовалось доказать.

Свойство 7.

$-(\alpha x) = (-\alpha)\, x = \alpha(-x)$ при любых $u \in L$, $\alpha \in P$.

2. Подпространства линейного пространства

Определение. Пусть L – линейное пространство над полем P. Непустое подмножество L' пространства L называется *подпространством пространства L*, если выполнены следующие условия:

$\forall\, u, v \in L' \quad u + v \in L'$,

$\forall\, u \in L' \ \forall\, \lambda \in P \quad \lambda u \in L'$,

т.е. L' замкнуто относительно сложения и относительно умножения на число.

Свойства подпространств

Свойство 1.

Непустое подмножество N линейного пространства L над полем P является подпространством пространства L тогда и только тогда, когда N является линейным пространством над полем P.

Доказательство: Достаточность следует из определения линейного пространства.

Необходимость. Пусть N – подпространство пространства L; значит, на N определены сложение и умножение на число из поля P. Нужно проверить выполнение на N семи аксиом линейного пространства. Аксиомы 1), 2), 4), 5), 6), 7) очевидно выполняются вследствие включения $N \subset L$. Кроме того, для любых $u, v \in N$ найдется такой $x \in N$, что $u + x = v$ (в качестве x рассмотрим $x = v + (-1)u$. Из замкнутости N относительно умножения на число из поля P и относительно сложения получаем, что, действительно, $x \in N$).

Свойство 2.

Пересечение любой совокупности подпространств линейного пространства L является подпространством L.

Примеры.

1) В любом линейном пространстве L само пространство L является своим подпространством, и подмножество, состоящее из одного нулевого элемента $\{\theta\}$, также является подпространством L. Эти два подпространства называются тривиальными, или несобственными. Подпространства линейного пространства L, отличные от самого L и от $\{\theta\}$, называются собственными.

2) В координатном векторном пространстве $V(3) = \{(a1, a2, a3) \mid ai \in R,\ i = 1 \div 3\}$ над полем R множество $L' = \{(a1, a2, 0) \mid ai \in R,\ i = 1 \div 2\}$ является подпространством. Действительно, $\forall\, x, y \in L'$ если $x = (x1, x2, 0)$ и $y = (y1, y2, 0)$, то $x + y = (x1+y1, x2+y2, 0) \in L'$ и $\forall \alpha \in R\ \alpha x = (\alpha x1, \alpha x2, 0) \in L'$.

3) В пространстве $Mn\times n$ всех матриц размерности $n\times n$ над полем R множество всех верхних треугольных матриц размерности $n\times n$ над полем R является подпространством. (Проверьте!)

4) В пространстве FR всех полиномов произвольной степени от одной переменной над полем R множества $Lk' = \{f(x) \in FR \mid \deg f(x) \le k$, где $k \in N\}$ являются подпространствами FR. (Проверьте!)

3. Линейная оболочка

Определение. Пусть L – линейное пространство над полем P и M – непустое подмножество L. *Линейной оболочкой множества M*, или подпространством, натянутым на множество M, называется множество, обозначаемое [M], являющееся пересечением всех подпространств пространства L, содержащих M.

Замечание. [M] является наименьшим по включению подпространством пространства L, содержащим M, т.е. любое подпространство пространства L,

содержащее M, содержит и [M]. Действительно, по второму свойству подпространств [M] является подпространством пространства L, и $M \subset [M]$ по определению линейной оболочки. Кроме того, если какое-либо подпространство L' пространства L содержит множество M, то L' – это одно из подпространств, пересечением которых является [M], а значит, по определению пересечения $[M] \subset L'$.

Теорема (***о строении линейной оболочки***)

Пусть M – непустое подмножество линейного пространства L над полем P. Тогда $[M] = \{\lambda_1 u_1+\lambda_2 u_2+\ldots+\lambda_k u_k \mid \lambda_i \in P, u_i \in M, k \in N\}$.

4. Суммы линейных пространств

Определение. Пусть L1, L2 – подпространства линейного пространства L над полем P. *Суммой подпространств* L1 и L2 называется множество $L1+L2 = \{z = x+y \mid x \in L1, y \in L2\}$. Если пересечение подпространств L1 и L2 состоит только из нулевого элемента θ, то сумма L1 и L2 называется прямой и обозначается $L1 \oplus L2$.

Предложение 1. Сумма подпространств линейного пространства L над полем P является линейным подпространством L.

Теорема 1. Пусть L – конечномерное линейное пространство над полем P и L1, L2 – подпространства L. Тогда

$$\dim (L1+L2) = \dim L1 + \dim L2 - \dim (L1 \cap L2).$$

Доказательство: Пусть $z_1, z_2, \ldots, z_d$ – базис $L1 \cap L2$, дополним $z_1, z_2, \ldots, z_d$ до базиса L1: $z_1, z_2, \ldots, z_d, u_1, \ldots, u_p$ и до базиса L2: $z_1, z_2, \ldots, z_d, v_1, \ldots, v_q$ (это можно сделать согласно теореме 1.1.9). Докажем, что элементы $z_1, z_2, \ldots, z_d, u_1, \ldots, u_p, v_1, \ldots, v_q$ образуют базис L1+L2.

1) Покажем, что любой элемент из L1+L2 линейно выражается через $z_1, z_2, \ldots, z_d, u_1, \ldots, u_p, v_1, \ldots, v_q$. Пусть $w \in L1+L2$, тогда $w = x+y$, где $x \in L1$, $y \in L2$. Но элемент x линейно выражается через базис $z_1, z_2, \ldots, z_d, u_1, \ldots, u_p$ подпространства L1:

$x = \gamma_1 z_1+\gamma_2 z_2+\ldots+\gamma_d z_d+\gamma_{d+1} u_1+\ldots+\gamma_{d+p} u_p$ $(\gamma_i \in P, i=1 \div (d+p))$, а элемент y линейно выражается через базис $z_1, z_2, \ldots, z_d, v_1, \ldots, v_q$ подпространства L2:

$y = \mu_1 z_1+\mu_2 z_2+\ldots+\mu_d z_d+\mu_{d+1} v_1+\ldots+\mu_{d+q} v_q$ $(\mu_i \in P, i=1 \div (d+q))$.

Тогда получаем, что w линейно выражается через $z_1, z_2, \ldots, z_d, u_1, \ldots, u_p, v_1, \ldots, v_q$.

2) Покажем, что элементы $z_1, z_2, \ldots, z_d, u_1, \ldots, u_p, v_1, \ldots, v_q$ линейно независимые. Предположим противное, пусть существуют такие числа $\alpha_i, \beta_j, \gamma_k \in P$, среди которых есть отличные от нуля, что выполняется равенство

$$\alpha_1 z_1+\alpha_2 z_2+\ldots+\alpha_d z_d+\beta_1 u_1+\ldots+\beta_p u_p+\gamma_1 v_1+\ldots+\gamma_q v_q = \theta$$

$(i=1 \div d, j=1 \div p, k=1 \div q)$. Все β_j $(j=1 \div p)$ не могут одновременно равняться нулю, т.к. тогда бы элементы $z_1, z_2, \ldots, z_d, v_1, \ldots, v_q$ были линейно зависимыми, что невозможно, поскольку они образуют базис подпространства L2. Аналогично все γ_k $(k=1 \div q)$ не могут одновременно равняться нулю. Значит, существует $\beta_j' \neq 0$ и существует $\gamma_k' \neq 0$.

Тогда получаем

$\alpha_1 z_1+\alpha_2 z_2+\ldots+\alpha_d z_d+\beta_1 u_1+\ldots+\beta_p u_p = (-\gamma_1)v_1 +\ldots+(-\gamma_q)v_q$.

Но элемент $\alpha_1 z_1+\alpha_2 z_2+\ldots+\alpha_d z_d+\beta_1 u_1+\ldots+\beta_p u_p$ принадлежит подпространству L1, а элемент $(-\gamma_1)v_1+\ldots+(-\gamma_q)v_q$ принадлежит подпространству L2. Таким образом, мы имеем элемент, принадлежащий одновременно L1 и L2, т.е. принадлежащий пересечению $L1 \cap L2$. Значит, этот элемент линейно выражается через базис $L1 \cap L2$:

$(-\gamma_1)v_1+ \ldots+(-\gamma_q)v_q = \delta_1 z_1+\delta_2 z_2+ \ldots+\delta_d z_d$

для некоторых $\delta_1, \delta_2, \ldots, \delta_d \in P$. Откуда получаем

$\delta_1 z_1+\delta_2 z_2+\ldots+\delta_d z_d+\gamma_1 v_1+\ldots+\gamma_q v_q = \theta$ $(\gamma_k' \neq 0)$,

т.е. элементы z1, z2, …, zd, v1, …, vq линейно зависимые, что невозможно. Полученное противоречие означает, что наше предположение неверно, и элементы z1, z2, …, zd, u1, …, up, v1, …, vq являются линейно независимыми.

Следствие. Размерность прямой суммы подпространств равна сумме размерностей этих подпространств.

Пример. Рассмотрим в пространстве V(3) подпространства $L1 = \{(a1, a2, 0) \mid ai \in R,\ i = 1, 2\}$ и $L2 = \{(0, b2, b3) \mid bi \in R,\ i = 2, 3\}$ (см. пример 1.2.2). $L1 \cap L2 = \{(0, d, 0) \mid d \in R\}$. dim L1 = 2, dim L2 = 2, dim (L1∩L2) = 1. Тогда dim (L1+L2) = 3.

Замечание. Если {e1, e2, …, en} – базис линейного пространства L над полем P, то L можно рассматривать как прямую сумму подпространств $[ei] = \{\lambda ei \mid \forall \lambda \in P\}$, т.е. $L = [e1] \oplus [e2] \oplus \ldots \oplus [en]$.

Теорема 2. Пусть L1, L2 – подпространства линейного пространства L над полем P. Тогда L представимо в виде прямой суммы подпространств L1 и L2 тогда и только тогда, когда любой вектор $w \in L$ представим в виде $w = v1+v2$ (где $vi \in Li$, i=1, 2) единственным образом.

Доказательство: *Необходимость*. Пусть $L = L1 \oplus L2$, тогда $L1 \cap L2 = \{\theta\}$. Предположим, что существует элемент $w \in L$, который представим в виде суммы элементов из L1 и L2 двумя способами: $w = x1+y1$ и $w = x2+y2$ (где $xi \in L1$, $yi \in L2$, i=1, 2). Тогда $x1+y1 = x2+y2$ и $x1–x2 = y2–y1$, левая часть полученного равенства принадлежит подпространству L1, а правая – подпространству L2. Но $L1 \cap L2 = \{\theta\}$, следовательно, $x1–x2 = \theta$ и $y2–y1 = \theta$, а значит, x1=x2 и y2=y1.

Достаточность. Пусть любой элемент $w \in L$ представим в виде $w = v1+v2$ (где $vi \in Li$, i=1, 2) единственным образом, и $L1 \cap L2 \neq \{\theta\}$. Тогда существует элемент $v \in L1 \cap L2$, $v \neq \theta$. Но тогда получаем два различных представления v: $v = v + \theta$ ($v \in L1$, $\theta \in L2$) и $v = \theta + v$ ($\theta \in L1$, $v \in L2$), что противоречит условию.

Изоморфизм линейных пространств

Определение1. Пусть L1, L2 – линейные пространства над полем P. Отображение $\varphi: L1 \to L2$ называется *изоморфизмом линейных пространств*, если выполняются следующие условия:

1) φ – биекция,
2) $\forall\ u, v \in L1$ $\varphi(u+v) = \varphi(u)+\varphi(v)$,
3) $\forall\ u \in L1\ \forall\ \lambda \in P$ $\varphi(\lambda u) = \lambda\varphi(u)$.

Определение. Пусть L1, L2 – линейные пространства над полем P. L1 и L2 называются изоморфными пространствами, если существует изоморфизм из L1 в L2. Обозначается: $L1 \approx L2$ или $L1 \cong L2$.

Свойства изоморфизма

Свойство 1.

Отношение $\approx$ “быть изоморфными” на множестве линейных пространств над полем P есть отношение эквивалентности.

Замечание. Из свойства 1 следует, что множество всех линейных пространств над некоторым полем P разбивается на классы изоморфных линейных пространств.

Свойство 2.

Изоморфизм линейных пространств L1 и L2 отображает нулевой элемент $\theta1$ линейного пространства L1 в нулевой элемент $\theta2$ пространства L2.

Свойство 3.

При изоморфизме линейных пространств образы линейно независимых элементов являются линейно независимыми элементами.

Свойство 4.

Если элементы u1, …, un образуют базис линейного пространства L1 и $\varphi: L1 \to L2$ – изоморфизм, то элементы φ(u1), …, φ(un) образуют базис линейного пространства L2.

Тема. Линейная зависимость и независимость систем векторов. Базис и размерность

План

1. Линейная зависимость и независимость систем векторов.

2. Свойства линейной зависимости.

3. Базис множества векторов линейного пространства.

4. Теорема о базисе. Координаты вектора в заданном базисе.

1. Линейная зависимость и независимость систем векторов

Определение. Говорят, что вектор v линейного пространства L над полем P ***линейно выражается*** через векторы $u_1, u_2, \ldots, u_m \in L$, если существуют такие числа $\lambda_1, \lambda_2, \ldots, \lambda_m \in P$, что

$$v = \lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_m u_m.$$

Выражение, стоящее в правой части, называют *линейной комбинацией* векторов u1, $u_1, u_2, \ldots, u_m$.

Векторы $u_1, u_2, \ldots, u_m$ называются ***линейно зависимыми***, если существуют такие числа $\alpha_1, \alpha_2, \ldots, \alpha_m \in P$, среди которых есть отличные от нуля, что

$$\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m = \theta.$$

Если векторы $u_1, u_2, \ldots, u_m$ не являются линейно зависимыми между собой, то они называются ***линейно независимыми***. Это означает, что соотношение

$$\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m = \theta$$

выполняется **только** при $\alpha_1 = \alpha_2 = \ldots = \alpha_m = 0$.

Теорема 1. Если векторы $u_1, u_2, \ldots, u_m \in$ L ($m \geq 2$) линейно зависимы, то хотя бы один из них выражается линейно через другие. Если же эти элементы линейно независимы, то ни один из них не может быть выражен линейно через другие.

Доказательство.

1. Предположим, что $u_1, u_2, \ldots, u_m$ между собой линейно зависимы. Это означает, что найдутся такие числа $\alpha_1, \alpha_2, \ldots, \alpha_m \in P$, среди которых есть отличные от нуля, что

$\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m = \theta$.

Пусть α_k отличен от нуля. Тогда

$$u_k = \left(-\frac{\alpha_1}{\alpha_k}\right)u_1 + \ldots + \left(-\frac{\alpha_{k-1}}{\alpha_k}\right)u_{k-1} + \left(-\frac{\alpha_{k+1}}{\alpha_k}\right)u_{k+1} + \ldots + \left(-\frac{\alpha_m}{\alpha_k}\right)u_m .$$

2. Теперь предположим, что $u_1, u_2, \ldots, u_m$ между собой линейно независимы. Линейное выражение одного из них через другие в этом случае невозможно, так как из равенства

$$u_k = \beta_1 u_1 + \ldots + \beta_{k-1} u_{k-1} + \beta_{k+1} u_{k+1} + \ldots + \beta_m u_m ,$$

очевидно, получилась бы линейная зависимость:

$$\beta_1 u_1 + \ldots + \beta_{k-1} u_{k-1} + (-1)u_k + \beta_{k+1} u_{k+1} + \ldots + \beta_m u_m = \theta$$

(коэффициент при u_k отличен от нуля).

2. Свойства линейной зависимости

Свойство 1. Система, состоящая из одного элемента u, будет линейно зависимой тогда и только тогда, когда u является нулевым элементом: $u = \theta$.

Свойство 2. Если вектор v линейно выражается через векторы $u_1, u_2, \ldots, u_m$:

$$v = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m ,$$

то, добавляя произвольные векторы $w_1, w_2, \ldots, w_k$ к исходной совокупности элементов, получаем совокупность векторов $u_1, u_2, \ldots, u_m$, $w_1, w_2, \ldots, w_k$, через которые v тоже линейно выражается.

Свойство 3. Пусть каждый из элементов $u_1, u_2, \ldots, u_m$ линейно выражается через элементы $v_1, v_2, \ldots, v_k$, а каждый из них в свою очередь линейно выражается через элементы $w_1, w_2, \ldots, w_n$. Тогда каждый из элементов $u_1, u_2, \ldots, u_m$ линейно выражается через $w_1, w_2, \ldots, w_n$.

Свойство 4. Пусть элементы $u_1, u_2, \ldots, u_m$ между собой линейно независимы. Если для какого-нибудь элемента v векторы $v, u_1, u_2, \ldots, u_m$ линейно зависимы, то v линейно выражается через $u_1, u_2, \ldots, u_m$.

Теорема *(четыре достаточных условия линейной зависимости).*

1) Если среди векторов $u_1, u_2, \ldots, u_m \in L$ есть нулевой вектор, то векторы $u_1, u_2, \ldots, u_m$ линейно зависимы.

2) Если часть векторов $u_1, u_2, \ldots, u_m \in L$ линейно зависима, то и все векторы системы $u_1, u_2, \ldots, u_m$ между собой линейно зависимы.

3) Если каждый из векторов $u_1, u_2, \ldots, u_m \in L$ может быть выражен линейно через векторы $v_1, v_2, \ldots, v_k \in L$, число которых k меньше m, то $u_1, u_2, \ldots, u_m$ линейно зависимы.

4) Если каждый из элементов $u_1, u_2, \ldots, u_m \in L$ может быть выражен линейно через элементы $v_1, v_2, \ldots, v_m$, которые между собой линейно зависимы, то и $u_1, u_2, \ldots, u_m$ линейно зависимы.

Доказательство.

Пусть m > k и

$$u_1 = \alpha_{11}v_1 + \alpha_{12}v_2 + \ldots + \alpha_{1k}v_k,$$
$$u_2 = \alpha_{21}v_1 + \alpha_{22}v_2 + \ldots + \alpha_{2k}v_k,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..$$
$$u_m = \alpha_{m1}v_1 + \alpha_{m2}v_2 + \ldots + \alpha_{mk}v_k.$$

Умножим эти равенства соответственно на $\lambda_1, \lambda_2, \ldots, \lambda_m$ и сложим их. При этом в качестве $\lambda_1, \lambda_2, \ldots, \lambda_m$ возьмем ненулевое решение следующей системы линейных уравнений:

$$\alpha_{11}\lambda_1 + \alpha_{21}\lambda_2 + \ldots + \alpha_{m1}\lambda_m = 0,$$
$$\alpha_{12}\lambda_1 + \alpha_{22}v_2 + \ldots + \alpha_{m2}\lambda_m = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..$$
$$\alpha_{1k}\lambda_1 + \alpha_{2k}\lambda_2 + \ldots + \alpha_{mk}\lambda_m = 0$$

(так как m > k, то ненулевое решение существует согласно следствию 3.3.).

При таком выборе чисел λ_i ($i=1\div m$) мы получаем равенство:

$$\lambda_1u_1 + \lambda_2u_2 + \ldots + \lambda_mu_m = 0v_1 + 0v_2 + \ldots + 0v_k = \theta.$$

4. Если векторы $v_1, v_2, \ldots, v_m$ линейно зависимы, то по теореме 5.3 один из них, пусть для определенности v_m, выражается линейно через остальные

$$v_m = \lambda_1v_1 + \lambda_2v_2 + \ldots + \lambda_{m-1}v_{m-1}.$$

В линейное выражение векторов $u_1, u_2, \ldots, u_m$ через $v_1, v_2, \ldots, v_m$ подставим вместо v_m сумму $\lambda_1v_1 + \lambda_2v_2 + \ldots + \lambda_{m-1}v_{m-1}$. Сгруппировав слагаемые с одинаковыми v_i, получим систему линейных выражений векторов $u_1, u_2, \ldots, u_m$ через $v_1, v_2, \ldots, v_{m-1}$. Так как $m > m - 1$, то согласно предыдущему пункту отсюда вытекает линейная зависимость $u_1, u_2, \ldots, u_m$.

3. Базис множества векторов линейного пространства

Определение. Векторы $u_1, u_2, \ldots, u_r$ из подмножества M линейного пространства L называются *базисом* множества M, если выполняются следующие условия:

1) Векторы $u_1, u_2, \ldots, u_r$ линейно независимы между собой.

2) Всякий вектор из M может быть линейно выражен через $u_1, u_2, \ldots, u_r$.

Пример. Покажем, что в координатном векторном пространстве $V^{(n)}$, рассмотренном нами в примере 4.3, один из базисов образуют векторы $e_1=(1, 0, \ldots, 0)$, $e_2=(0, 1, \ldots, 0)$, …, $e_n=(0, 0, \ldots, 1)$. Этот базис называется *главным*.

Действительно, пусть $\lambda_1e_1+\lambda_2e_2+\ldots+\lambda_ne_n=\theta$. Согласно правилам действий с векторами в пространстве $V^{(n)}$ это означает $(\lambda_1, \lambda_2, \ldots, \lambda_n)=(0, 0, \ldots, 0)$, т.е. $\lambda_1=\lambda_2=\ldots=\lambda_n=0$. Далее, пусть $x=(x_1, x_2, \ldots, x_n)\in V^{(n)}$. Тогда для чисел $x_1, x_2, \ldots, x_n \in \boldsymbol{R}$ имеет место $x_1e_1+x_2e_2+\ldots+x_ne_n=x$.

В частности, в векторном пространстве $V^{(2)}$ (вектора на плоскости) базис образуют вектора $e_1 = (1, 0)$ и $e_2 = (0, 1)$. В векторном пространстве $V^{(3)}$ (вектора в пространстве) базис образует вектора $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ и $e_3 = (0, 0, 1)$.

Следует иметь в виду, что в произвольном линейном пространстве не каждое множество имеет базис.

Пример. Покажем, что в линейном пространстве всех бесконечных последовательностей чисел из поля P (множество с бесконечными последовательностями чисел также является линейным пространством аналогично n-мерному координатному пространству) не существует базиса.

Действительно, предположим, что элементы $u_1, u_2, \ldots, u_n$ этого линейного пространства образуют базис. Тогда (n + 1) элементов

$$\begin{aligned} v_1 &= (1,0,0,...), \\ v_2 &= (0,1,0,...), \\ &... \\ v_n &= (\underbrace{0,0,...,0,1}_{n},0,...), \\ v_{n+1} &= (\underbrace{0,0,...,0,1}_{n+1},0,...) \end{aligned} \quad ,$$

выражающихся линейно через $u_1, u_2, \ldots, u_n$, должны были бы быть согласно 3-ому условию линейной зависимости линейно зависимыми между собой. Однако, если хотя бы одно из чисел $\alpha_i \in P$ отлично от нуля, то

$$\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_i v_i + \ldots + \alpha_{n+1} v_{n+1} = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_{n+1}, 0, 0, \ldots) \neq$$
$$\neq (0, 0, \ldots, 0, \ldots) = \theta.$$

Заметим, что если в линейном пространстве L базис существует, то их может быть бесконечно много. Вышесказанное иллюстрирует следующая теорема.

Теорема о базисе. Координаты вектора в заданном базисе

Теорема (*о базисах*). Если подмножество M линейного пространства L имеет базисы, то они обладают следующими свойствами:

1. Все базисы M состоят из одного и того же количества векторов.
2. Всякие линейно независимые между собой векторы из M могут быть включены в некоторый базис совокупности M.
3. Всякие линейно независимые между собой элементы из M в количестве, равном числу элементов в базисе, сами образуют базис M.

Доказательство.

1. Пусть системы векторов $u_1, u_2, \ldots, u_r$ и $v_1, v_2, \ldots, v_s$ являются базисами совокупности M. Соотношение $r<s$ невозможно, так как в противном случае по третьему достаточному условию линейной зависимости векторы $v_1, v_2, \ldots, v_s$ должны быть линейно зависимы, как выражающиеся через r (где $r<s$) векторов. Аналогично невозможно $s<r$. Значит, $r=s$.

2. Пусть $u_1, u_2, \ldots, u_k$ – произвольные линейно независимые векторы из M. (Такие совокупности существуют, например: совокупность, состоящая из одного ненулевого вектора.) Будем добавлять векторы $u_{k+1}, u_{k+2}, \ldots, u_m$ так, чтобы векторы совокупности $u_1, u_2, \ldots, u_k, u_{k+1}, u_{k+2}, \ldots, u_m$ оставались линейно независимыми. Длина такой последовательности ограничена (она не может превышать количества элементов в базисе M). Поэтому среди таких последовательностей найдутся имеющие максимальную длину, т.е. максимальные линейно независимые системы или базисы.

3. Пусть каждый базис совокупности M состоит из r векторов и $v_1, v_2, \ldots, v_r$ – линейно независимые элементы из M. Из второго условия теоремы следует, что систему $v_1, v_2, \ldots, v_r$ можно дополнить до базиса: $v_1, v_2, \ldots, v_r, v_{r+1}, \ldots, v_m$. Но по первому условию случай $m>r$ невозможен, т.е. $m=r$. А значит, $v_1, v_2, \ldots, v_r$ – базис M.

Определение. Если подмножество M линейного пространства L обладает базисом, то количество элементов в базисе называется *рангом* M и обозначается rang M.

Если M содержит единственный элемент θ, то ранг M считается равным нулю.

Определение. Если линейное пространство L само обладает рангом (т.е. существуют базисы всего линейного пространства L), то L называется *конечномерным*, а его ранг – *размерностью* L. В соответствии с термином «размерность» употребляют обозначение: dim L = rang L.

Если линейное пространство не имеет ранга, то его называют *бесконечномерным* и говорят, что его размерность бесконечна.

Замечание. Если элемент подмножества линейного пространства линейно выражается через линейно независимые элементы этого подмножества, то такое выражение единственное.

Действительно, предположим противное. Пусть в подмножестве M линейного пространства L над полем P векторы $u_1, u_2, \ldots, u_m$ линейно независимы и некоторый вектор $v \in M$ линейно выражается через $u_1, u_2, \ldots, u_m$ двумя разными способами:

$$v = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m, \quad (1)$$
$$v = \beta_1 u_1 + \beta_2 u_2 + \ldots + \beta_m u_m, \quad (2)$$

где $\alpha_1, \alpha_2, \ldots, \alpha_m \in P$, $\beta_1, \beta_2, \ldots, \beta_m \in P$ и существует $i \in \{1,2,\ldots,m\}$: $\alpha_i \neq \beta_i$. Тогда, рассмотрев разность равенств (1) и (2), получаем

$$(\alpha_1-\beta_1)u_1 + (\alpha_2-\beta_2)u_2 + \ldots + (\alpha_m-\beta_m)u_m = \theta,$$

причем коэффициент $(\alpha_i-\beta_i)$ отличен от нуля. Следовательно, элементы $u_1, u_2, \ldots, u_m$ являются линейно зависимыми, что противоречит условию.

Следствие. Элемент подмножества линейного пространства линейно выражается через базис этого подмножества единственным образом.

Определение. Пусть элементы $u_1, u_2, \ldots, u_m$ образуют базис подмножества M линейного пространства L над полем P. *Координатами элемента* $v \in M$ ***в базисе*** $u_1, u_2, \ldots, u_m$ называются числа $\alpha_1, \alpha_2, \ldots, \alpha_m \in P$, с помощью которых v линейно выражается через $u_1, u_2, \ldots, u_m$, т.е. для которых выполняется равенство

$$v = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m.$$

Тема. Линейный оператор. Собственные векторы и собственные значения линейных операторов

План

1. Линейные операторы. Матрица линейного оператора в заданном базисе.
2. Матрицы линейного оператора в разных базисах.
3. Действия с линейными операторами.
4. Собственные векторы и собственные значения линейных операторов.
5. Ранг и дефект линейного оператора.

1. Линейные операторы. Матрица линейного оператора в заданном базисе

Определение. Пусть L – линейное пространство над полем P. ***Линейным оператором***, или ***линейным преобразованием***, пространства L называется отображение φ: $L \to L$, для которого выполняются следующие условия:

1) $\forall u, v \in L \quad \varphi(u+v) = \varphi(u)+\varphi(v)$,

2) $\forall u \in L \ \forall \lambda \in P \quad \varphi(\lambda u) = \lambda\varphi(u)$.

Пример. В координатном векторном пространстве V^2 над полем R преобразование симметрии относительно прямой $y=x$ является линейным оператором. Действительно, симметрия φ относительно прямой $y=x$ в пространстве V^2 действует по правилу: $\varphi((x, y)) = (y, x)$. Тогда для $\forall (x, y), (x', y') \in V^2$ $\varphi((x, y)+(x', y')) = \varphi((x+x', y+y')) = (y+y', x+x') = (y, x)+(y', x') = \varphi((x, y))+\varphi((x', y'))$ и $\varphi(\lambda(x, y)) = \varphi((\lambda x, \lambda y)) = (\lambda y, \lambda x)) = \lambda(y, x) = \lambda\varphi((x, y))$ для $\forall \lambda \in R$.

Предложение 1. Если в линейном пространстве L над полем P отображение $\varphi: L \to L$ является линейным оператором, то $\varphi(\theta) = \theta$, где θ – нейтральный элемент по сложению в L.

Доказательство: Используем свойство линейных пространств: $0u = \theta$ для любого $u \in L$ (см. §1). Имеем $\varphi(\theta) = \varphi(0u) = 0\varphi(u) = \theta$.

Теорема 1. Пусть в линейном пространстве L над полем P задан базис $U = \{u_1, \ldots, u_n\}$. Для произвольных элементов $v_1, \ldots, v_n \in L$ существует и единственный линейный оператор $\varphi: L \to L$, такой, что $v_1=\varphi(u_1), \ldots, v_n=\varphi(u_n)$.

Доказательство: Рассмотрим произвольный элемент $w \in L$, пусть $w = b_1u_1+b_2u_2+\ldots+b_nu_n$, где $b_i \in P,\ i=1 \div n$, тогда положим по определению $\varphi(w) = b_1v_1+b_2v_2+\ldots+b_nv_n$.

Проверим, что φ – линейный оператор. Пусть $w, v \in L$ и пусть $w = b_1u_1+b_2u_2+\ldots+b_nu_n$, $v = c_1u_1+c_2u_2+\ldots+c_nu_n$, где $b_i, c_i \in P,\ i=1 \div n$. Тогда L
$\varphi(w+v) = \varphi((b_1u_1+b_2u_2+\ldots+b_nu_n)+(c_1u_1+c_2u_2+\ldots+c_nu_n)) =$
$\varphi((b_1+c_1)u_1+(b_2+c_2)u_2+\ldots+(b_n+c_n)u_n) = (b_1+c_1)v_1+(b_2+c_2)v_2+\ldots+(b_n+c_n)v_n =$
$(b_1v_1+b_2v_2+\ldots+b_nv_n)+(c_1v_1+c_2v_2+\ldots+c_nv_n) = \varphi(b_1u_1+b_2u_2+\ldots+b_nu_n)+ \varphi(c_1u_1+c_2u_2+\ldots+c_nu_n) = \varphi(w)+\varphi(v)$. Равенство $\varphi(\lambda w) = \lambda\varphi(w)$ для $\forall \lambda \in P$ проверьте самостоятельно.

Покажем, что $v_i=\varphi(u_i)\ \ (i=1 \div n)$. Действительно, $u_1 = 1u_1+0u_2+\ldots+0u_n$, тогда $\varphi(u_1) = 1v_1+0v_2+\ldots+0v_n = v_1$ и аналогично для $u_2, \ldots, u_n$.

Таким образом, мы построили линейный оператор, описанный в условии теоремы. Докажем, что такой оператор единственный.

Предположим, что существует ещё линейный оператор $\psi: L \to L$, такой, что $v_1=\psi(u_1), \ldots, v_n=\psi(u_n)$. Покажем, что $\varphi = \psi$, т.е. $\forall w \in L$ $\varphi(w) = \psi(w)$.
$\psi(w) = \psi(b_1u_1+b_2u_2+\ldots+b_nu_n) = \psi(b_1u_1)+\psi(b_2u_2)+\ldots+\psi(b_nu_n) =$
$b_1\psi(u_1)+b_2\psi(u_2)+\ldots+b_n\psi(u_n) = b_1v_1+b_2v_2+\ldots+b_nv_n = \varphi(b_1u_1+b_2u_2+\ldots+b_nu_n) = \varphi(w)$.

Матрица линейного оператора

Определение. Пусть в линейном пространстве L над полем P задан базис $U = \{u_1, u_2, \ldots, u_n\}$ и задан линейный оператор $\varphi: L \to L$. Пусть элементы $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ линейно выражаются через базис U следующим образом:

$$\varphi(u_1) = \alpha_{11}u_1+\alpha_{12}u_2+\ldots+\alpha_{1n}u_n,$$
$$\varphi(u_2) = \alpha_{21}u_1+\alpha_{22}u_2+\ldots+\alpha_{2n}u_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\varphi(u_n) = \alpha_{n1}u_1+\alpha_{n2}u_2+\ldots+\alpha_{nn}u_n,$$

где $\alpha_{ij} \in P,\ i=1 \div n,\ j=1 \div n$. Тогда матрица линейного выражения образов $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ базисных элементов через этот базис $u_1, u_2, \ldots, u_n$

$$A_U(\varphi) = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn} \end{pmatrix}$$

называется ***матрицей линейного оператора*** φ в базисе U.

Найдем связь между координатами элемента линейного пространства и координатами его образа при преобразовании φ.

Теорема 2. Пусть в линейном пространстве L над полем P задан базис $U = \{u_1, \ldots, u_n\}$ и пусть $A_U(\varphi)$ – матрица линейного оператора $\varphi: L \to L$ в базисе U.

Тогда если $(c_1, c_2, \ldots, c_n)$ – координаты некоторого элемента $w \in L$ в базисе U, а $(b_1, b_2, \ldots, b_n)$ – координаты $\varphi(w)$ в базисе U, то выполняется равенство

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = A_U(\varphi) \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}.$$

Доказательство: Пусть матрица $A_U(\varphi)$ имеет вид $A_U(\varphi) = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn} \end{pmatrix}$. Тогда для $w = c_1u_1+c_2u_2+\ldots+c_nu_n$ (где $c_i \in P$, $i=1 \div n$) выполнено:
$\varphi(w) = \varphi(c_1u_1+c_2u_2+\ldots+c_nu_n) = c_1\varphi(u_1)+c_2\varphi(u_2)+\ldots+c_n\varphi(u_n) =$
$c_1(\alpha_{11}u_1+\alpha_{12}u_2+\ldots+\alpha_{1n}u_n)+c_2(\alpha_{21}u_1+\alpha_{22}u_2+\ldots+\alpha_{2n}u_n)+\ldots$
$+c_n(\alpha_{n1}u_1+\alpha_{n2}u_2+\ldots+\alpha_{nn}u_n) = (c_1\alpha_{11}+c_2\alpha_{21}+\ldots+c_n\alpha_{n1})u_1 +$
$(c_1\alpha_{12}+c_2\alpha_{22}+\ldots+c_n\alpha_{n2})u_2 + \ldots +(c_1\alpha_{1n}+c_2\alpha_{2n}+\ldots+c_n\alpha_{nn})u_n$. Поскольку через базис элемент пространства выражается единственным способом, мы имеем следующие равенства:

$$\begin{gathered} c_1\alpha_{11}+c_2\alpha_{21}+\ldots+c_n\alpha_{n1}=b_1, \\ c_1\alpha_{12}+c_2\alpha_{22}+\ldots+c_n\alpha_{n2}=b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c_1\alpha_{1n}+c_2\alpha_{2n}+\ldots+c_n\alpha_{nn}=b_n. \end{gathered}$$

Полученная система равенств эквивалентна матричному равенству $\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = A_U(\varphi) \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$, что и требовалось доказать.

Лемма 1. Пусть A, B – матрицы размерности $n \times n$ над полем P. Если для всех элементов $w=(c_1, c_2, \ldots c_n)$ $(c_i \in P,\ i=1 \div n)$ линейного пространства L над полем P выполняется равенство $A \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = B \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$, то $A=B$.

Доказательство: Пусть $A = (a_{ij})_{n \times n}$ и $B = (b_{ij})_{n \times n}$, тогда, рассмотрев в качестве w элемент $(1,0,0,\ldots,0)$, получаем равенство $A \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = B \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, откуда имеем $a_{i1} = b_{i1}$ для всех $i=1 \div n$. Аналогично, рассматривая в качестве w элементы $(0,1,0,\ldots,0)$, …, $(0,0,0,\ldots,1)$, получим $a_{i2} = b_{i2}$, …, $a_{in} = b_{in}$ для всех $i=1 \div n$, т.е. $A=B$.

2. Матрицы линейного оператора в разных базисах

Теорема 3. Пусть в линейном пространстве L над полем P заданы два базиса $U = \{u_1, \ldots, u_n\}$ и $V = \{v_1, \ldots, v_n\}$, и пусть S – матрица перехода от базиса U к базису V. Пусть линейный оператор φ: $L \to L$ в базисе U имеет матрицу $A_U(\varphi)$, а в базисе V – матрицу $A_V(\varphi)$. Тогда

$$A_V(\varphi) = S^{-1}A_U(\varphi)S.$$

Доказательство: Рассмотрим произвольный элемент $w \in L$. Пусть $w = b_1u_1+b_2u_2+\ldots+b_nu_n$ и $w = c_1v_1+c_2v_2+\ldots+c_nv_n$ $(b_i, c_i \in P, \ i=1\div n)$, и пусть $\varphi(w) = \beta_1u_1+\beta_2u_2+\ldots+\beta_nu_n$ и $\varphi(w) = \gamma_1v_1+\gamma_2v_2+\ldots+\gamma_nv_n$ $(\beta_i, \gamma_i \in P, \ i=1\div n)$.

Тогда по теореме 1.5.4 получаем:

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = S \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix},$$

а по следствию 1.5.5 получаем:

$$S^{-1} \cdot \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix}.$$

По теореме 1.6.7 имеем:

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix} = A_V(\varphi) \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = A_U(\varphi) \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Далее:

$$S^{-1}A_U(\varphi) \cdot S \cdot \begin{pmatrix} c_1 \\ \tilde{n}_2 \\ \vdots \\ \tilde{n}_n \end{pmatrix} = S^{-1}A_U(\varphi) \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = S^{-1} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix}.$$

Следовательно,

$$S^{-1}A_U(\varphi) \cdot S \cdot \begin{pmatrix} c_1 \\ \tilde{n}_2 \\ \vdots \\ \tilde{n}_n \end{pmatrix} = A_V(\varphi) \cdot \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}.$$

Поскольку полученное равенство выполняется для произвольного $w \in L$, т.е. для произвольной матрицы $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$, то по лемме 1.6.8 имеем равенство

$$S^{-1}A_U(\varphi)S = A_V(\varphi),$$

что и требовалось доказать.

3. Действия с линейными операторами

Определим на множестве всех линейных операторов пространства L над полем P действия сложение, умножение на число из поля P и композицию. Пусть φ, ψ – линейные операторы пространства L и $\lambda \in P$, тогда

1) $\boldsymbol{\varphi+\psi}$: $L \to L$ по правилу $\forall u \in L \ \ (\varphi+\psi)(u) = \varphi(u)+\psi(u)$,

2) $\boldsymbol{\lambda\varphi}$: $L \to L$ по правилу $\forall u \in L \ \ (\lambda\varphi)(u) = \lambda\varphi(u)$,

3) $\boldsymbol{\varphi\circ\psi}$: $L \to L$ по правилу $\forall u \in L \ \ (\varphi\circ\psi)(u) = \varphi(\psi(u))$.

Проверим, что $\varphi+\psi$ является линейным оператором пространства L. Действительно, $\forall u, v \in L \quad (\varphi+\psi)(u+v) = \varphi(u+v)+\psi(u+v) = \varphi(u)+\varphi(v)+\psi(u)+\psi(v) =$

$\varphi(u)+\psi(u)+\varphi(v)+\psi(v) = (\varphi+\psi)(u)+(\varphi+\psi)(v)$ и $\forall u \in L \ \forall \lambda \in P \ (\varphi+\psi)(\lambda u) = \varphi(\lambda u)+\psi(\lambda u) = \lambda\varphi(u)+\lambda\psi(u) = \lambda(\varphi(u)+\psi(u)) = \lambda(\varphi+\psi)(u)$.

Теорема 4. Пусть в линейном пространстве L над полем P задан базис $U = \{u_1, \ldots, u_n\}$, и пусть линейные операторы $\varphi: L \to L$ и $\psi: L \to L$ в базисе U имеют матрицы $A_U(\varphi)$ и $A_U(\psi)$ соответственно. Тогда имеют место соотношения:

1. $A_U(\varphi+\psi) = A_U(\varphi)+A_U(\psi)$,
2. $A_U(\lambda\varphi) = \lambda A_U(\varphi) \quad (\lambda \in P)$,
3. $A_U(\varphi\circ\psi) = A_U(\varphi)\cdot A_U(\psi)$.

4. Собственные векторы и собственные значения линейных операторов

Заметим, что если $A = (a_{ij})_{n\times n}$ – матрица над полем P, то определитель $|A - \lambda E|$ (где E – единичная матрица размерности $n\times n$) является многочленом над полем P относительно переменной λ, принимающей значения из P.

Опрееление. Пусть $A = (a_{ij})_{n\times n}$ – матрица над полем P и $\lambda \in P$. Многочлен $f(\lambda) = |A - \lambda E|$ называется ***характеристическим многочленом*** матрицы A, а корни данного многочлена называются ***характеристическими числами*** матрицы A.

Предложение 2. Если для матриц A и B выполняется равенство $B = Q^{-1}AQ$, где Q – некоторая матрица, то A и B обладают одинаковыми характеристическими числами.

Доказательство: Составим характеристический многочлен матрицы B: $|B - \lambda E| = |Q^{-1}AQ - \lambda E| = |Q^{-1}AQ - \lambda EQ^{-1}Q| = |Q^{-1}AQ - \lambda Q^{-1}EQ| =$
$|Q^{-1}AQ - Q^{-1}\lambda EQ| = |Q^{-1}(A - \lambda E)Q| = |Q^{-1}||A - \lambda E||Q| = |A - \lambda E|/|Q^{-1}||Q| =$
$|A - \lambda E|/|E| = |A - \lambda E|$.

Замечание. Т.к. для матриц произвольного линейного оператора φ в различных базисах выполняется равенство $A_V(\varphi) = S^{-1}A_U(\varphi)S$ (теорема 1.6.9.), то из предложения 1.7.2. получаем, что все матрицы линейного оператора имеют один и тот же характеристический многочлен и один и тот же набор характеристических чисел. Поэтому характеристический многочлен матрицы линейного оператора можно назвать ***характеристическим многочленом линейного оператора***, а характеристические числа матрицы линейного оператора можно назвать ***характеристическими числами линейного оператора***.

Определение. Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор. Элемент $w \in L$ называется ***собственным вектором*** оператора φ, если $w \neq \theta$ и существует $\lambda \in P$, такое, что $\varphi(w) = \lambda w$. При этом λ называется ***собственным значением*** оператора φ, соответствующим вектору w.

Предложение 3. Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор. Если w – собственный вектор оператора φ и λ – собственное значение φ, соответствующее вектору w, то для любого $\mu \in P \ (\mu \neq 0)$ вектор μw является собственным вектором оператора φ, и соответствующее ему собственное значение равно λ.

Доказательство: Пусть $\varphi(w) = \lambda w$. Рассмотрим $\varphi(\mu w) = \mu\varphi(w) = \mu(\lambda w) = (\mu\lambda)w = (\lambda\mu)w = \lambda(\mu w)$.

Теорема 5. Собственными значениями линейного оператора являются его характеристически числа, и только они.

Доказательство: Пусть L – линейное пространство над полем P и пусть линейный оператор $\varphi: L \to L$ в базисе $U = \{u_1, \ldots, u_n\}$ имеет матрицу $A_U(\varphi) = (a_{ij})_{n\times n}$.

Пусть w – собственный вектор φ и λ – собственное значение φ, т.е. $\varphi(w) = \lambda w$ ($\lambda \in P$) и $w \neq \theta$. Пусть $w = b_1u_1+b_2u_2+\ldots+b_nu_n$, $(b_i \in P, \ i=1\div n)$. По теореме 1.6.7.

$\varphi(w) = A_U(\varphi)\cdot\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$, значит, $\lambda\cdot\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = A_U(\varphi)\cdot\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$. Запишем последнее равенство в виде системы равенств $\begin{cases} a_{11}b_1 + a_{12}b_2 + \ldots + a_{1n}b_n = \lambda b_1 \\ a_{21}b_1 + a_{22}b_2 + \ldots + a_{2n}b_n = \lambda b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}b_1 + a_{n2}b_2 + \ldots + a_{nn}b_n = \lambda b_n \end{cases}$, откуда получаем $\begin{cases} (a_{11}-\lambda)b_1 + a_{12}b_2 + \ldots + a_{1n}b_n = 0 \\ a_{21}b_1 + (a_{22}-\lambda)b_2 + \ldots + a_{2n}b_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}b_1 + a_{n2}b_2 + \ldots + (a_{nn}-\lambda)b_n = 0 \end{cases}$. Тогда вектор $(b_1, b_2, \ldots, b_n)$ является решением однородной системы линейных уравнений $\begin{cases} (a_{11}-\lambda)x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + (a_{22}-\lambda)x_2 + \ldots + a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + (a_{nn}-\lambda)x_n = 0 \end{cases}$ (*). Поскольку $w \neq \theta$, то существует $b_i \neq 0$ $(i=1\div n)$, а значит, система (*) имеет ненулевое решение, тогда определитель матрицы системы (*) равен нулю (в противном случае по теореме Крамера существовало бы только одно решение (нулевое)). Таким образом, $\begin{vmatrix} a_{11}-\lambda & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22}-\lambda & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn}-\lambda \end{vmatrix} = \left|A_{U(\varphi)} - \lambda E\right| = 0$, т.е. λ – характеристическое число φ.

Пусть теперь λ – характеристическое число оператора φ, значит, $\left|A-\lambda E\right| = \begin{vmatrix} a_{11}-\lambda & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22}-\lambda & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn}-\lambda \end{vmatrix} = 0$. Тогда система линейных уравнений $\begin{cases} (a_{11}-\lambda)x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + (a_{22}-\lambda)x_2 + \ldots + a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + (a_{nn}-\lambda)x_n = 0 \end{cases}$ имеет ненулевое решение, пусть этим решением является вектор $(c_1, c_2, \ldots, c_n)$. Тогда $\begin{cases} a_{11}\tilde{n}_1 + a_{12}\tilde{n}_2 + \ldots + a_{1n}\tilde{n}_n = \lambda\tilde{n}_1 \\ a_{21}\tilde{n}_1 + a_{22}\tilde{n}_2 + \ldots + a_{2n}\tilde{n}_n = \lambda\tilde{n}_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}\tilde{n}_1 + a_{n2}\tilde{n}_2 + \ldots + a_{nn}\tilde{n}_n = \lambda\tilde{n}_n \end{cases}$, т.е. $A_U(\varphi)\cdot\begin{pmatrix} \tilde{n}_1 \\ \tilde{n}_2 \\ \vdots \\ \tilde{n}_n \end{pmatrix} = \begin{pmatrix} \lambda\tilde{n}_1 \\ \lambda\tilde{n}_2 \\ \vdots \\ \lambda\tilde{n}_n \end{pmatrix} = \lambda\cdot\begin{pmatrix} \tilde{n}_1 \\ \tilde{n}_2 \\ \vdots \\ \tilde{n}_n \end{pmatrix}$, откуда получаем $\varphi((c_1, c_2, \ldots, c_n)) = \lambda(c_1, c_2, \ldots, c_n)$. Значит,

вектор $(c_1, c_2, \ldots, c_n)$ – собственный вектор линейного оператора φ, а λ – собственное значение оператора φ.

Замечание. Из теоремы 1.7.6 следует, что для нахождения собственных векторов $w = (b_1, b_2, \ldots, b_n)$ линейного оператора нужно найти характеристические числа λ этого оператора, а затем найти w, решив уравнение $A_U(\varphi)\cdot\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} \lambda b_1 \\ \lambda b_2 \\ \vdots \\ \lambda b_n \end{pmatrix}$, где $A_U(\varphi)$ – матрица оператора в некотором базисе U.

Теорема 6. Собственные векторы линейного оператора, соответствующие попарно различным собственным значениям, линейно независимы.

Теорема 7. Если матрица линейного оператора φ является диагональной в некотором базисе V, то все элементы базиса V являются собственными векторами оператора φ, а диагональ матрицы составлена из соответствующих этим векторам собственных значений оператора.

Доказательство: Пусть L – линейное пространство над полем P и $V = \{v_1, v_2, \ldots, v_n\}$ – базис L, в котором матрица линейного оператора $\varphi: L \to L$ диагональная: $A_V(\varphi) = \begin{pmatrix} \alpha_{11} & 0 & \cdots & 0 \\ 0 & \alpha_{22} & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \alpha_{nn} \end{pmatrix}$, $\alpha_{ii} \in P$, $i=1 \div n$. Поскольку в базисе $V = \{v_1, v_2, \ldots, v_n\}$ мы имеем $v_1 = (1, 0, 0, \ldots, 0)$, $v_2 = (0, 1, 0, \ldots, 0)$, …, $v_n = (0, 0, 0, \ldots, 1)$, то, учитывая определение 1.6.5 матрицы линейного оператора, получаем:

$$\varphi(v_1) = \alpha_{11} v_1 + 0v_2 + \ldots + 0v_n,$$
$$\varphi(v_2) = 0v_1 + \alpha_{22} v_2 + \ldots + 0v_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\varphi(v_n) = 0v_1 + 0v_2 + \ldots + \alpha_{nn} v_n.$$

То есть $\varphi(v_1)=\alpha_{11} v_1$, $\varphi(v_2)=\alpha_{22} v_2$, …, $\varphi(v_n)=\alpha_{nn} v_n$. А значит, элементы $v_1, v_2, \ldots, v_n$ являются собственными векторами линейного оператора φ, и они соответствуют собственным значениям $\alpha_{11}, \alpha_{22}, \ldots, \alpha_{nn}$ этого оператора.

5. Ранг и дефект линейного оператора

Определение. Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор. ***Ядром линейного оператора*** φ называется множество (обозначаемое ***Ker φ***) элементов пространства L, образом которых является нулевой элемент θ, *т.е.*

$$Ker\,\varphi = \{u \in L \mid \varphi(u) = \theta\}.$$

Определение. Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор. ***Образом линейного оператора*** φ называется множество (обозначаемое ***Im φ***) элементов пространства L, имеющих прообразы при преобразовании φ, т.е.

$$Im\,\varphi = \{u \in L \mid \exists\, v \in L\ \varphi(v) = u\}.$$

Предложение 4. Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор. Множества $Ker\,\varphi$ и $Im\,\varphi$ являются подпространствами пространства L.

Предложение5. Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор.

1) φ является инъективным отображением тогда и только тогда, когда $Ker\,\varphi = \{\theta\}$.

2) φ является сюръективным отображением тогда и только тогда, когда $Im\,\varphi = L$.

Определение. Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор. Размерность подпространства $Ker\,\varphi$ (обозначается ***dim Ker φ***) называется ***дефектом оператора*** φ. Размерность подпространства $Im\,\varphi$ (обозначается ***dim Im φ***) называется ***рангом оператора*** φ.

Теорема 8. Ранг линейного оператора равен рангу матрицы этого оператора.

Доказательство: Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор. Пусть $U = \{u_1, u_2, \ldots, u_n\}$ – базис пространства L.

Покажем сначала, что $Im\,\varphi = [\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)]$.

Рассмотрим произвольный элемент $w \in Im\,\varphi$, тогда $w = \varphi(u)$, $u \in L$. Пусть $u = b_1u_1+b_2u_2+\ldots+b_nu_n$ $(b_i \in P,\ i=1 \div n)$, тогда $w = \varphi(u) = b_1\varphi(u_1)+b_2\varphi(u_2)+\ldots+b_n\varphi(u_n) \in [\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)]$ (см. теорему 1.2.5). Значит, $Im\,\varphi \subset [\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)]$. С другой стороны, согласно предложению 1.8.4, $Im\,\varphi$ является подпространством пространства L, тогда, поскольку $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n) \in Im\,\varphi$, то $[\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)] \subset Im\,\varphi$. Итак, $Im\,\varphi = [\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)]$.

Следовательно, по теореме 1.2.7 получаем: $dim\,Im\,\varphi = rang\{\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)\}$.

Пусть

$$\varphi(u_1) = \alpha_{11}u_1+\alpha_{12}u_2+\ldots+\alpha_{1n}u_n,$$
$$\varphi(u_2) = \alpha_{21}u_1+\alpha_{22}u_2+\ldots+\alpha_{2n}u_n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\varphi(u_n) = \alpha_{n1}u_1+\alpha_{n2}u_2+\ldots+\alpha_{nn}u_n,$$

где $\alpha_{ij} \in P$, $i=1 \div n$, $j=1 \div n$. Тогда $rang\{\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)\} = rang\begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn} \end{pmatrix}$, но $\begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn} \end{pmatrix} = A_U(\varphi)$. Значит, $dim\,Im\,\varphi = rang A_U(\varphi)$.

Теорема 9. Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор. Тогда

$$dim\,Ker\,\varphi + dim\,Im\,\varphi = dim\,L.$$

Доказательство: Обозначим $dim\,Ker\,\varphi = d$, $dim\,Im\,\varphi = r$, $dim\,L = n$ и докажем, что $n = d+r$. Рассмотрим базис подпространства $Im\,\varphi$: $v_1, v_2, \ldots, v_r$. Тогда по определению $Im\,\varphi$ существуют элементы $u_1, u_2, \ldots, u_r \in L$, такие, что $v_i = \varphi(u_i)$ $(i=1 \div r)$. Покажем, что $u_1, u_2, \ldots, u_r$ линейно независимы. Действительно, рассмотрим равенство $\alpha_1u_1+\alpha_2u_2+\ldots+\alpha_ru_r = \theta$ $(\alpha_i \in P,\ i=1 \div r)$, тогда $\varphi(\alpha_1u_1+\alpha_2u_2+\ldots+\alpha_ru_r) = \varphi(\theta) = \theta$, а значит, $\alpha_1\varphi(u_1)+\alpha_2\varphi(u_2)+\ldots+\alpha_r\varphi(u_r) = \theta$, т.е. $\alpha_1v_1+\alpha_2v_2+\ldots+\alpha_rv_r = \theta$. Но $v_1, v_2, \ldots, v_r$ линейно независимы (как базис $Im\,\varphi$), следовательно, $\alpha_1=\alpha_2=\ldots=\alpha_r=0$, т.е. $u_1, u_2, \ldots, u_r$ линейно независимы.

Далее, рассмотрим $N = [u_1, u_2, \ldots, u_r]$, заметим, что $dim\,N = r$ (см. замечание 1.2.8). Докажем, что $L = N \oplus Ker\,\varphi$ (см. определение 1.3.1).

1) Проверим, что $N \cap Ker\,\varphi = \{\theta\}$. Пусть $w \in N \cap Ker\,\varphi$, тогда (поскольку $w \in N$) $w = \beta_1u_1+\beta_2u_2+\ldots+\beta_ru_r$. Из того, что $w \in Ker\,\varphi$, получаем $\varphi(w) = \theta$. Значит, $\varphi(\beta_1u_1+\beta_2u_2+\ldots+\beta_ru_r) = \varphi(\theta)$, тогда, как было показано выше, имеем $\beta_1v_1+\beta_2v_2+\ldots+\beta_rv_r = \theta$ и $\beta_1=\beta_2=\ldots=\beta_r=0$. Отсюда $w = 0u_1+0u_2+\ldots+0u_r = \theta$.

2) Проверим, что каждый элемент w пространства L может быть представлен в виде $w = w_1+w_2$, где $w_1 \in N$, $w_2 \in Ker\,\varphi$.

Рассмотрим $\varphi(w) \in Im\,\varphi$, тогда $\varphi(w) = \alpha_1v_1+\alpha_2v_2+\ldots+\alpha_rv_r$ $(\alpha_i \in P,\ i=1 \div r)$. Обозначим $w_1 = \alpha_1u_1+\alpha_2u_2+\ldots+\alpha_ru_r$, очевидно $w_1 \in N$. Обозначим $w_2 = w - w_1$. Покажем, что $w_2 \in Ker\,\varphi$. Действительно, $\varphi(w_2) = \varphi(w - w_1) = \varphi(w) - \varphi(w_1) = (\alpha_1v_1+\alpha_2v_2+\ldots+\alpha_rv_r) -$

$\varphi(\alpha_1 u_1+\alpha_2 u_2+\ldots+\alpha_r u_r) = (\alpha_1 v_1+\alpha_2 v_2+\ldots+\alpha_r v_r) - (\alpha_1\varphi(u_1)+\alpha_2\varphi(u_2)+\ldots+\alpha_r\varphi(u_r)) = (\alpha_1 v_1+\alpha_2 v_2+\ldots+\alpha_r v_r) - (\alpha_1 v_1+\alpha_2 v_2+\ldots+\alpha_r v_r) = \theta$, значит, $w_2 \in Ker\,\varphi$. А тогда $w = w_1+w_2$, где $w_1 \in N$, $w_2 \in Ker\,\varphi$.

Итак, $L = N \oplus Ker\,\varphi$. Тогда по следствию 1.3.4 имеем $n = r+d$, что и требовалось доказать.

Определение. Линейный оператор φ линейного пространства L над полем P называется ***невырожденным оператором***, если φ – биективное отображение. В противном случае φ называется ***вырожденным оператором***.

Теорема 10. Пусть L – линейное пространство над полем P и $\varphi: L \to L$ – линейный оператор. Следующие условия эквивалентны:

1) φ – невырожденный оператор,
2) $Ker\,\varphi = \{\theta\}$,
3) $dim\ Im\,\varphi = dim\ L$,
4) $rang\ A_U(\varphi) = dim\ L$, где U – некоторый базис L.
5) $|A_U(\varphi)| \neq 0$.

Тема. Кольцо многочленов от одной переменной

План

1. Основные понятия и определения. Построение кольца многочленов от одной переменной над областью целостности.

2. Деление многочленов с остатком. Деление многочлена на двучлен. Корни многочлена. Кратные корни.

3. НОД и НОК многочленов. Алгоритм Евклида и теорема Ламе для многочленов.

4. Производная многочлена. Отделение кратных множителей многочлена.

1. Основные понятия и определения. Построение кольца многочленов от одной переменной над областью целостности

ОПРЕДЕЛЕНИЕ

Пусть P – некоторое поле. *Многочленом от одной переменной над полем P* будем называть формальную сумму вида:

f(x) = $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, где $a_i \in P$, $i \in \{0, 1, \ldots, n\}$, $n \in N$. (1)

Числа a_i называют *коэффициентами* многочлена f(x). Если $a_n \neq 0$, то число n называют *степенью многочлена f(x)*, a_n - *старшим коэффициентом,* a_0 *– свободным членом многочлена f(x).* Одночлен $a_n x^n$ называется в этом случае *старшим членом.*

Если старший коэффициент многочлена равен единице, то многочлен называется *нормированным*.

ЗАМЕЧАНИЯ

1. Всякий элемент поля P будем считать многочленом нулевой степени, многочлен произвольной степени с нулевыми коэффициентами – нулевым многочленом, единицу поля P – единичным многочленом и обозначать их $\vartheta(x)$ и E(x) соответственно.

Не следует путать многочлен *нулевой степени* с *нулевым* многочленом!

2. Вместо записи (1) иногда будем использовать запись:

f(x) = $\sum_{i=0}^{n} a_i x^i$ (1)

На множестве всех многочленов от одной переменной над полем P можно задать операции сложения и умножения многочленов по следующим правилам. Пусть f(x) – многочлен вида (1) и g(x) = $b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$, где

$b_j \in P$, $j \in \{0, 1, \ldots, m\}$, $m \in N$ – многочлен вида (2).

ОПРЕДЕЛЕНИЕ

Суммой многочленов f(x) и g(x) назовем многочлен h(x) вида:

h(x) = $c_k x^k + c_{k-1}x^{k-1} + ... + c_1 x + c_{0,}$,

где $c_i = a_i + b_i$, $i \in \{0, 1, \ldots, k\}$, $k = \max\{n, m\}$. (3)

ЗАМЕЧАНИЕ

Для удобства в многочлене меньшей степени будем представлять недостающие степени в виде одночленов с нулевыми коэффициентами, т.е., если $f(x) = \sum_{i=1}^{6} a_i x^i$, $g(x) = \sum_{j=1}^{4} b_j x^j$, то представим g(x) в виде: $g(x) = 0x^6 + 0x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0$.

ОПРЕДЕЛЕНИЕ

Произведением многочленов f(x) и g(x) будем называть многочлен h(x) вида: $h(x) = (\sum_{i=0}^{n} a_i x^i) \bullet (\sum_{j=0}^{m} b_j x^j) = \sum_{k=0}^{n+m} c_k x^k$, где $c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + ... + a_k b_0$.

Иными словами, чтобы найти произведение двух многочленов, нужно каждый одночлен первого сомножителя умножить на каждый одночлен второго и затем привести подобные слагаемые.

ЗАМЕЧАНИЕ

Так как мы рассматриваем многочлены над полем, а в поле нет делителей нуля, то старший член произведения двух многочленов всегда будет равен произведению их старших членов. В общем же случае это не так. Если коэффициенты взяты из произвольного кольца, то может оказаться, что произведение двух старших ненулевых коэффициентов, тем не менее, равно нулю.

Нетрудно проверить, что сложение и умножение многочленов над полем обладают свойствами коммутативности и ассоциативности, умножение дистрибутивно относительно сложения, нейтральным элементом по сложению является нулевой многочлен ϑ(x), а элементом, противоположным многочлену f(x), – многочлен, коэффициенты которого есть числа, противоположные (в поле P) коэффициентам данного многочлена. Поэтому справедлива теорема.

ТЕОРЕМА

Множество всех многочленов от одной переменой над полем P по заданным операциям сложения и умножения многочленов образует кольцо, которое называется *кольцом многочленов от одной переменной* и обозначается P[x].

ЗАМЕЧАНИЕ

Из предыдущего замечания следует, что кольцо P[x] над полем P является областью целостности.

ОПРЕДЕЛЕНИЕ

Число x_0 называется *корнем многочлена* f(x), если: $f(x_0) = \sum_{i=0}^{n} a_i x_0^i = 0$

ЗАМЕЧАНИЕ

Если подставить в выражение (1) вместо переменой x некоторое число α из поля P и произвести необходимые действия, то полученное в результате число называется значением многочлена f(x) при $x = \alpha$.

Учитывая это, корень многочлена можно определить как число, на котором многочлен принимает значение, равное нулю.

В кольце многочленов P[x] над полем P можно задать частичную операцию – деление многочленов, подобно тому, как это было сделано в кольце целых чисел.

ОПРЕДЕЛЕНИЕ

Говорят, что многочлен f(x) вида (1) *делится* на многочлен g(x) вида (2), если найдется такой многочлен h(x) над полем P, что $f(x) = g(x) \cdot h(x)$.

Деление многочленов удобно производить «уголком».

ПРИМЕР **1**

$x^4 - x^3 + 0x^2 + x - 1 \mid \underline{x^3 + 0x^2 + 0x + 1}$

$\underline{x^4 + 0x^3 + 0x^2 + x} \qquad x - 1$

$\underline{- x^3 - 1}$

$\underline{- x^3 - 1}$

0

Здесь f(x) = $x^4 - x^3 + 0x^2 + x - 1$, g(x) = $x^3 + 1$, h(x) = $x - 1$. Нулевые коэффициенты в записи многочленов появились для удобства вычисления.

Отметим некоторые простейшие свойства делимости многочленов, аналогичные свойствам делимости целых чисел.

СВОЙСТВО **1**

Если одновременно выполняется делимость многочлена f(x) на g(x) и обратно, то многочлены отличаются только на множитель нулевой степени или, иными словами, просто на числовой множитель c: f(x) = c g(x).

Многочлены f(x) и g(x) называются в этом случае *ассоциированными.*

Очевидно, что среди многочленов, ассоциированных с данным ненулевым многочленом, имеется ровно один нормированный многочлен.

СВОЙСТВО **2**

Если многочлен f(x) делится на каждый из двух многочленов g(x) и h(x), то он делится и на их произведение.

СВОЙСТВО **3**

Отношение делимости многочленов в кольце P[x] рефлексивно и транзитивно.

СВОЙСТВО **4**

Если многочлен f(x) делится на ненулевой многочлен g(x), то и любой многочлен, ассоциированный с f(x), будет делиться на g(x).

СВОЙСТВО **5**

Если каждый из двух многочленов f(x) и g(x) делится на ненулевой многочлен h(x), то и любая их линейная комбинация делится на h(x).

2. Деление многочленов с остатком. Деление многочлена на двучлен. Корни многочлена. Кратные корни.

ОПРЕДЕЛЕНИЕ. Пусть P – некоторое поле. *Многочленом от одной переменной над полем P* будем называть формальную сумму вида:

f(x) = $a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$, где $a_i \in$ P, i ∈ {0, 1, …, n}, n ∈ N. (1)

Числа a_i называют *коэффициентами* многочлена f(x). Если $a_n \neq 0$, то число n называют *степенью многочлена f(x)*, a_n - *старшим коэффициентом,* a_0 - *свободным членом многочлена f(x).* Одночлен $a_n x^n$ называется в этом случае *старшим членом.*

Если старший коэффициент многочлена равен единице, то многочлен называется *нормированным*.

ЗАМЕЧАНИЯ

1. Всякий элемент поля P будем считать многочленом нулевой степени, многочлен произвольной степени с нулевыми коэффициентами – нулевым многочленом, единицу поля P – единичным многочленом и обозначать их ϑ(x) и E(x) соответственно.

Не следует путать многочлен *нулевой степени* с *нулевым* многочленом!

2. Вместо записи (1) иногда будем использовать запись: f(x) = $\sum_{i=0}^{n} a_i x^i$ (2)

На множестве всех многочленов от одной переменной над полем P можно

задать операции сложения и умножения многочленов по следующим правилам. Пусть f(x) – многочлен вида (1) и g(x) = $b_m x^m + b_{m-1} x^{m-1} + ... + b_1 x + b_0$, где $b_j \in P$, $j \in \{0, 1, \ldots, m\}$, $m \in N$ – многочлен вида (2).

ОПРЕДЕЛЕНИЕ. *Суммой* многочленов f(x) и g(x) назовем многочлен h(x) вида: h(x) = $c_k x^k + c_{k-1} x^{k-1} + ... + c_1 x + c_{0,}$, где $c_i = a_i + b_i$, $i \in \{0, 1, \ldots, k\}$, $k = \max\{n, m\}$. (3)

ЗАМЕЧАНИЕ. Для удобства в многочлене меньшей степени будем представлять недостающие степени в виде одночленов с нулевыми коэффициентами, т.е., если f(x) = $\sum_{i=1}^{6} a_i x^i$, g(x) = $\sum_{j=1}^{4} b_j x^j$, то представим g(x) в виде: g(x) = $0x^6 + 0x^5 + b_4 x^4 + b_3 x^3 + b_2 x^2 + b_1 x + b_0$.

ОПРЕДЕЛЕНИЕ. *Произведением* многочленов f(x) и g(x) будем называть многочлен h(x) вида: h(x) = $(\sum_{i=0}^{n} a_i x^i) \bullet (\sum_{j=0}^{m} b_j x^j)$ = $\sum_{k=0}^{n+m} c_k x^k$, где $c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + ... + a_k b_0$.

Иными словами, чтобы найти произведение двух многочленов, нужно каждый одночлен первого сомножителя умножить на каждый одночлен второго и затем привести подобные слагаемые.

ЗАМЕЧАНИЕ. Так как мы рассматриваем многочлены над полем, а в поле нет делителей нуля, то старший член произведения двух многочленов всегда будет равен произведению их старших членов. В общем же случае это не так. Если коэффициенты взяты из произвольного кольца, то может оказаться, что произведение двух старших ненулевых коэффициентов, тем не менее, равно нулю.

Нетрудно проверить, что сложение и умножение многочленов над полем обладают свойствами коммутативности и ассоциативности, умножение дистрибутивно относительно сложения, нейтральным элементом по сложению является нулевой многочлен ϑ(x), а элементом, противоположным многочлену f(x), – многочлен, коэффициенты которого есть числа, противоположные (в поле P) коэффициентам данного многочлена. Поэтому справедлива теорема.

ТЕОРЕМА. Множество всех многочленов от одной переменой над полем P по заданным операциям сложения и умножения многочленов образует кольцо, которое называется *кольцом многочленов от одной переменной* и обозначается P[x].

ЗАМЕЧАНИЕ. Из предыдущего замечания следует, что кольцо P[x] над полем P является областью целостности.

ОПРЕДЕЛЕНИЕ. Число x_0 называется *корнем многочлена* f(x), если: $f(x_0) = \sum_{i=0}^{n} a_i x_0^i = 0$.

ЗАМЕЧАНИЕ. Если подставить в выражение (1) вместо переменой x некоторое число α из поля P и произвести необходимые действия, то полученное в результате число называется значением многочлена f(x) при x = α.

Учитывая это, корень многочлена можно определить как число, на котором многочлен принимает значение, равное нулю.

3. НОД и НОК многочленов. Алгоритм Евклида и теорема Ламе для многочленов.

В кольце многочленов P[x] над полем P можно задать частичную операцию – деление многочленов, подобно тому, как это было сделано в кольце целых чисел.

ОПРЕДЕЛЕНИЕ. Говорят, что многочлен f(x) вида (1) *делится* на многочлен g(x) вида (2), если найдется такой многочлен h(x) над полем P, что f(x) = g(x)·h(x).

Нулевые коэффициенты в записи многочленов появились для удобства вычисления.

Отметим некоторые простейшие свойства делимости многочленов, аналогичные свойствам делимости целых чисел.

СВОЙСТВО **1.** Если одновременно выполняется делимость многочлена f(x) на g(x) и обратно, то многочлены отличаются только на множитель нулевой степени или, иными словами, просто на числовой множитель c: f(x) = c g(x).

Многочлены f(x) и g(x) называются в этом случае *ассоциированными.*

Очевидно, что среди многочленов, ассоциированных с данным ненулевым многочленом, имеется ровно один нормированный многочлен.

СВОЙСТВО **2.** Если многочлен f(x) делится на каждый из двух многочленов g(x) и h(x), то он делится и на их произведение.

СВОЙСТВО **3.** Отношение делимости многочленов в кольце P[x] рефлексивно и транзитивно.

СВОЙСТВО **4.** Если многочлен f(x) делится на ненулевой многочлен g(x), то и любой многочлен, ассоциированный с f(x), будет делиться на g(x).

СВОЙСТВО **5.** Если каждый из двух многочленов f(x) и g(x) делится на ненулевой многочлен h(x), то и любая их линейная комбинация делится на h(x).

ОПРЕДЕЛЕНИЕ. Говорят, что многочлен f(x) *делится с остатком* на ненулевой многочлен g(x), если найдется такая пара многочленов q(x) и r(x), для которых выполняется равенство:

f(x) = g(x)·q(x) + r(x), причем степень r(x) < степени g(x) или r(x) = ϑ(x) (1)

В кольце многочленов, также как и в кольце целых чисел, можно доказать теорему о делении с остатком.

ТЕОРЕМА *(о делении с остатком).* Для всякой пары многочленов f(x) и g(x), где g(x) - ненулевой многочлен, существует и притом единственная пара многочленов q(x) и r(x), которые удовлетворяют условиям (1).

Рассмотрим более подробно частный случая деления многочленов: деление многочлена на двучлен, так как он дает некоторые интересные и полезные на практике результаты.

ТЕОРЕМА. Остаток от деления многочлена f(x) на двучлен x – c равен значению многочлена f(x) при x = c: f(x) = (x – c)·q(x) + f(c).

Пусть многочлен f(x) записан в следующем виде:

$$f(x) = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_{n,}(a_0 \neq 0) \qquad (1).$$

Представим его в виде:

$$f(x) = (x - c)\cdot(b_0x^{n-1} + b_1x^{n-2} + ... + b_{n-2}x + b_{n-1}) + r \quad (2)$$

Раскрывая мысленно скобки в правой части равенства и приравнивая коэффициенты при одинаковых степенях в равенствах (1) и (2), получим:

$$\begin{aligned} b_0 &= a_0, \\ b_1 &= a_1 + cb_0, \\ b_2 &= a_2 + cb_1, \\ &\cdots\cdots\cdots\cdots \\ b_k &= a_k + cb_{k-1}, \\ &\cdots\cdots\cdots\cdots \\ b_{n-1} &= a_{n-1} + cb_{n-2}, \\ r &= a_n + cb_{n-1}. \end{aligned} \qquad (3)$$

Вычисления (3) обычно записывают в виде таблицы и называют *схемой Горнера:*

	a_0	a_1	…	a_k	…	a_n
$x = c$	b_0	$b_1 = a_1 + cb_0$	…	$b_k = a_k + cb_{k-1}$	…	$r = a_n + cb_{n-1}$

Очевидно, что r = f(c), коэффициенты b_i есть коэффициенты частного *q(x)* от

деления f(x) на x – c.

Схему Горнера удобно использовать также для разложения многочлена f(x) по степеням разности x – c.

ТЕОРЕМА. Для любого числа *c* из поля P многочлен f(x) вида (1) степени n всегда можно представить и притом единственным образом в виде:

$$f(x)=b_0+b_1\cdot(x-c)+b_2\cdot(x-c)^2+...+b_n\cdot(x-c)^n,(b_n\neq 0)\ .\quad (4)$$

Представление в виде (4) и называется *разложением f(x) по степеням разности x – c*.

Используя формулу Тейлора и схему Горнера, можно также находить значения производных различных порядков для многочлена f(x) в точке x = c.

ТЕОРЕМА. В разложении (4) многочлена f(x) по степеням разности x – c, коэффициенты b_k определяются следующим образом:

$$b_k = \frac{f^{(k)}(c)}{k!},\ (k\in\{0,1,2,\ldots,n\})\quad (5).$$

Корни многочлена

Учитывая понятие кратности корня, можно сформулировать следующие утверждения о числе корней многочлена f(x).

ЛЕММА

Всякий ненулевой многочлен может быть представлен в виде:

$$f(x)=(x-x_1)^{k_1}\cdot(x-x_2)^{k_2}\cdot...\cdot(x-x_m)^{k_m}\cdot g(x)\quad (1).$$

где $x_1,x_2,...,x_m$ - различные числа, а $g(x)$ - многочлен, не имеющий корней.

ЛЕММА. Если многочлен f(x) представлен в виде (1), то $x_1,x_2,...,x_m$ - это все его корни, причем кратность корня x_i равна k_i.

ТЕОРЕМА. Сумма кратностей всех корней ненулевого многочлена f(x) не превосходит его степени, причем равенство имеет место тогда и только тогда, когда многочлен можно представить в виде произведения множителей первой степени.

Существуют равенства, выражающие связь корней многочлена с его коэффициентами. Пусть многочлен f(x) = $a_0x^n+a_1x^{n-1}+...+a_{n-1}x+a_{n,}(a_0\neq 0)$ имеет корни $x_1,x_2,\ldots,x_n$, причем они не обязательно различны. Тогда справедливы равенства:

$$\begin{aligned}
&a_1=-a_0\cdot(x_1+x_2+...+x_n),\\
&a_2=a_0\cdot(x_1x_2+x_1x_3+...+x_{n-1}x_n),\\
&.....\\
&a_n=(-1)^n\cdot a_0\cdot x_1x_2...x_n.
\end{aligned}\quad (6)$$

Равенства (6) называются *формулами Виета,* выражающими коэффициенты многочлена f(x) через его корни и старший коэффициент.

Определение и простейшие свойства наибольшего общего делителя и наименьшего общего кратного многочленов аналогичны простейшим свойствам наибольшего общего делителя и наименьшего общего кратного целых чисел (сформулировать самостоятельно).

Остановимся на некоторых особенностях, присущих НОД и НОК многочленов.

ЗАМЕЧАНИЕ. НОД целых чисел, как известно, определен однозначно с точностью до знака. НОД многочленов определен однозначно с точностью до множителя нулевой степени, поскольку очевидно, что если d(x) = НОД (f(x), g(x)), то и любой ассоциированный с d(x) многочлен также будет являться НОД (f(x), g(x)).

Поскольку в кольце многочленов над полем выполнимо деление с остатком, то доказать существование НОД многочленов также можно с помощью алгоритма

Евклида.

ТЕОРЕМА. Для всяких двух многочленов f(x) и g(x) существует их НОД, который равен последнему ненулевому остатку в последовательности Евклида.

ЗАМЕЧАНИЕ. Из предыдущего замечания следует, что для удобства вычислений при нахождении НОД двух многочленов можно домножать остатки, делимые или делители, которые получаются в процессе последовательных делений на любое ненулевое число.

ЗАМЕЧАНИЕ. В кольце многочленов над полем также выполняется расширенный алгоритм Евклида, который позволяет вычислить такие многочлены *u(x)* и *v(x)*, которые удовлетворяют равенству: НОД (f(x), g(x)) = u(x)·f(x) + v(x)·g(x) (7)

ОПРЕДЕЛЕНИЕ. Многочлены f(x) и g(x) называются *взаимно простыми*, если они не имеют других общих делителей кроме многочленов нулевой степени, или, иначе говоря, кроме постоянных из поля *P.*

Многочлены $f_1(x), f_2(x),..., f_k(x)$ называются *взаимно простыми в совокупности*, если они попарно взаимно просты.

СВОЙСТВО **1.** Многочлены f(x) и g(x), заданные над полем P взаимно просты тогда и только тогда, когда найдутся такие многочлены u(x) и v(x), для которых:

$$u(x)\cdot f(x) + v(x)\cdot g(x) = 1 \qquad (8)$$

СВОЙСТВО **2.** Многочлен g(x) тогда и только тогда взаимно прост с произведением многочленов $f_1(x)\cdot f_2(x)\cdot ...\cdot f_k(x)$, когда он взаимно прост с каждым из сомножителей.

СВОЙСТВО **3.** Если произведение многочленов $f_1(x)\cdot f_2(x)$ делится на многочлен g(x), причем $f_1(x)$ и g(x) взаимно просты, то $f_2(x)$ делится на g(x).

СВОЙСТВО **4.** Если многочлены $f_1(x)\cdot f_2(x)\cdot ...\cdot f_k(x)$ попарно взаимно просты и многочлен f(x) делится на каждый из них, то он делится и на их произведение.

СВОЙСТВО **5.** Многочлены $f_1(x)\cdot f_2(x)\cdot ...\cdot f_k(x)$ взаимно просты тогда и только тогда, когда у них нет корня, общего для всех.

Разложение многочленов на неприводимые множители

ОПРЕДЕЛЕНИЕ. Многочлен p(x) называется *неприводимым над полем P*, если он не раскладывается в произведение двух многочленов положительной степени над эти полем.

ЗАМЕЧАНИЕ. Когда речь идет о неприводимых многочленах, то важно, над каким полем они рассматриваются, так как один и тот же многочлен может быть неприводим над одним полем и приводим над другим. Например, многочлен f(x) = x^2-3 неприводим над полем рациональных чисел, но приводим над полем действительных чисел, так как f(x) = $(x-\sqrt{3})\cdot(x+\sqrt{3})$ - его разложение в произведение двух многочленов первой степени с действительными коэффициентами.

Отметим свойства неприводимых многочленов, которые выполняются над любым полем P.

СВОЙСТВО **1.** Любой многочлен первый степени неприводим над любым полем.

СВОЙСТВО **2.** Всякий многочлен степени ≥ 2, имеющий корень в поле P, приводим над этим полем.

ЗАМЕЧАНИЕ. Обратное не всегда верно, например, многочлен f(x) = $x^2+2x+1=(x+1)^2$ приводим над полем действительных чисел, хотя не имеет в нем корней.

СВОЙСТВО **3.** Если многочлен *f(x)* ненулевой степени над полем P является делителем неприводимого многочлена *p(x)* над этим же полем, то *f(x)* ассоциирован с *p(x)*: *f(x) = c p(x).*

СВОЙСТВО **4.** Пусть f(x) – произвольный многочлен над полем P и p(x) – неприводимый многочлен над этим же полем. Либо f(x) делится на p(x), либо они взаимно просты.

СВОЙСТВО **5.** Если произведение многочленов $f_1(x)\cdot f_2(x)\cdot ...\cdot f_k(x)$ над полем P делится на неприводимый над P многочлен p(x), то хотя бы один из сомножителей делится на p(x).

Из предыдущих параграфов видно, что теория делимости многочленов имеет глубокое сходство с теорией делимости целых чисел. Роль, аналогичную роли простых чисел, играют неприводимые многочлены, что подтверждается следующей теоремой.

ТЕОРЕМА. Каждый многочлен ненулевой степени над полем P может быть представлен и притом единственным образом (с точностью до порядка следования множителей) в виде произведения многочленов, неприводимых над P:

$$f(x)=\alpha\cdot p_1(x)\cdot p_2(x)\cdot ...\cdot p_n(x)\ , \qquad (9)$$

где $\alpha\neq 0\in P$, $p_i(x)$, $i\in\{1, 2, \ldots, n\}$ - неприводимые над P многочлены со старшими коэффициентами, равными единице.

ЗАМЕЧАНИЯ

1. Если в разложении (1) собрать вместе одинаковые множители (если таковые имеются) в виде степени, то оно примет вид:

$$f(x) = \alpha\cdot p_1^{k_1}(x)\cdot p_2^{k_2}(x)\cdot ...\cdot p_m^{k_m}(x)\ ,\ k_i\in N,\ i\in\{1, 2, \ldots, m\},\ (10)$$

где все неприводимые множители уже различны между собой.

2. Очевидно, что если для многочленов f(x) и g(x) известны их разложения на неприводимые множители (или такие разложения легко получить), то, как и в случае целых чисел, они могут быть использованы для нахождения НОД и НОК этих многочленов. (Опишите эти алгоритмы самостоятельно).

3. Если говорить об аналогии между кольцом целых чисел и кольцом многочленов от одной переменной, то не следует забывать и о понятии идеала. Например. очевидно, что совокупность всех многочленов кольца P[x], имеющих α своим корнем, будет являться идеалом, причем главным. Порождается этот идеал многочленом наименьшей положительной степени из всех многочленов данной совокупности.

4. Производная многочлена. Отделение кратных множителей многочлена.

ОПРЕДЕЛЕНИЕ. Для многочлена $f(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ будем называть его *производной* f'(x) формальное выражение вида:

$$f'(x) = na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + 2a_2x + a_1 \qquad (11)$$

ЗАМЕЧАНИЯ

1. Говоря о формальном выражении, мы имеем ввиду, что определение производной многочлена как некоторой функции связано с понятием предела, которое может оказаться неприменимым к элементам произвольного поля P. Поэтому выражение na_n нужно понимать как:

$$\underbrace{a_n + a_n + ... + a_n}_{n\ раз} = \underbrace{(1+1+...+1)}_{n\ раз}\cdot a_n\ . \qquad (12)$$

Если в поле P для любого натурального числа k :

$$\underbrace{1+1+...+1}_{k\ раз}\neq 0\ ,$$

то соответствующие коэффициенты в выражении (3) не равны нулю и f'(x) можно также считать многочленом над полем P степени n - 1. Поле P со свойством (4) называют *полем нулевой характеристики.*

2. Нетрудно проверить, что для производных многочленов, определенных таким образом, выполняются основные свойства производных функций, а именно:

- числовой множитель можно выносить за знак производной;
- производная суммы многочленов равна сумме их производных;
- производная произведения двух многочленов находится по формуле: (f(x)·g(x))' =

f’(x)·g(x) + g’(x)·f(x).

ОПРЕДЕЛЕНИЕ. Производная от производной многочлена f(x) называется его *второй производной* и обозначается как f”(x).

Аналогично определяется и производная k – го порядка $f^{(k)}(x)$.

Найти разложение многочлена f(x) в произведение неприводимых над полем P множителей в общем случае не так просто, как разложение целого числа на простые множители. В этом существенную помощь может оказать введенное понятие производной.

ТЕОРЕМА. Пусть P – поле нулевой характеристики, p(x) – неприводимый делитель многочлена f(x) над P кратности k. В этом случае p(x) будет неприводимым делителем производной многочлена f(x) кратности (k – 1).

В частности, если k = 1, то f’(x) не делится на p(x).

СЛЕДСТВИЕ. Если x_0 - корень кратности k многочлена f(x), то он будет корнем кратности (k – 1) для его производной.

Решим задачу разложения многочлена f(x) на неприводимые множители с помощью последней теоремы.

Пусть разложение f(x) над полем P имеет вид (10). Тогда многочлены $p_1(x), p_2(x),..., p_m(x)$ являются неприводимыми делителями производной f’(x) кратности k_1 -1, k_2 - 1,…, k_{ii} - 1 соответственно.

Отсюда следует, что d(x) = НОД (f(x), f’(x)) имеет вид:

$$d(x)= b \cdot p_1^{k_1-1}(x) \cdot ... \cdot p_m^{k_m-1}(x) \text{ ,(} b \neq 0 \in P). \quad (13)$$

Получили, что неприводимые множители d(x) = НОД (f(x), f’(x)) – это в точности кратные неприводимые множители f(x). Для нахождения d(x) можно использовать алгоритм Евклида.

Процедура отыскания НОД (f(x), f’(x)) получила название *отделения кратных неприводимых множителей многочлена f(x)*.

Тема. Многочлены от нескольких переменных

План

1. Построение кольца многочленов от нескольких переменных над областью целостности. Степень многочлена от нескольких переменных.

2. Симметрические многочлены от нескольких переменных и их свойства.

3. Основная теорема о симметрических многочленах.

1. Построение кольца многочленов от нескольких переменных над областью целостности. Степень многочлена от нескольких переменных.

ОПРЕДЕЛЕНИЕ

Одночленом от n переменных $x_1, x_2,..., x_n$ над полем P называется произведение вида: $a \cdot x_1^{k_1} x_2^{k_2} ... x_n^{k_n}$, где a ∈ P – коэффициент одночлена, $k_1, k_2,..., k_n \in N$ (1).

ОПРЕДЕЛЕНИЕ

Многочленом от n переменных $x_1, x_2,..., x_n$ над полем P называется формальная сумма одночленов вида (1):

$$f(x_1, x_2,..., x_n) = \sum_i a_i \cdot x_1^{k_1} x_2^{k_2} ... x_n^{k_n}, \quad (2)$$

где суммирование идет по всем различным одночленам (которые не являются подобными слагаемыми).

ПРИМЕР **1** $f(x_1, x_2, x_3) = 2x_2^3 x_3 + 3x_1^2 x_2^2 x_3^3 - x_1^3 x_2$

На множестве всех многочленов от n переменных $x_1, x_2,..., x_n$ над полем P можно задать естественным образом операции сложения и умножения многочленов по

аналогии с соответствующими операциями на множестве всех многочленов от одной переменной.

Нетрудно проверить, что все свойства операций сложения и умножения многочленов, которые выполняются для многочленов от одной переменной, выполняются и для многочленов от нескольких переменных. Следовательно, мы имеем право говорить о *кольце многочленов от n переменных* $x_1, x_2, ..., x_n$ *над полем P*, которое принято обозначать как: P[$x_1, x_2, ..., x_n$].

Понятие степени многочлена от нескольких переменных сложнее, чем в случае одной переменной. В многочлене из примера 1, первый и последний одночлены имеют по совокупности переменных одинаковую степень. Поэтому вводятся следующие понятия.

ОПРЕДЕЛЕНИЕ

Степенью ненулевого одночлена (1) многочлена *f*($x_1, x_2, ..., x_n$) *по совокупности переменных* называется число $k_1 + k_2 + ... + k_n$, равное суме показателей степенней, с которыми переменные $x_1, x_2, ..., x_n$ входят в произведение (1).

Степенью ненулевого многочлена *f*($x_1, x_2, ..., x_n$) *по совокупности переменных* называется максимальная из степеней его членов.

Степенью ненулевого многочлена *f*($x_1, x_2, ..., x_n$) *по переменной* x_i называется максимальная из степеней, с которой данная переменная водит в какой-либо из одночленов многочлена *f*($x_1, x_2, ..., x_n$).

ПРИМЕР **2.** Для многочлена *f*(x_1, x_2, x_3) $= 2x_2^3x_3 + 3x_1^2x_2^2x_3^3 - x_1^3x_2$ из примера 1:

- степень по переменной x_1 равна 3, по переменной x_2 равна 3, по переменной x_3 - также 3;
- степень этого многочлена по совокупности переменных равна 7.

ОПРЕДЕЛЕНИЕ

Многочлен называется *однородным по степени m,* если все его одночлены имеют степень, равную m.

Те члены многочлена *f*($x_1, x_2, ..., x_n$), которые имеют одинаковые степени по совокупности переменных, называются его *однородными компонентами.*

Уже из этого определения видно, что определить степень многочлена от n переменных как максимальную из степеней его одночленов, нельзя, поскольку таких одночленов может быть несколько.

Чтобы определить степень многочлена от нескольких переменных, вводят понятие *лексикографического упорядочения* ненулевых одночленов.

ОПРЕДЕЛЕНИЕ. Одночлен u = $a \cdot x_1^{k_1} x_2^{k_2} ... x_n^{k_n}$ считается *старше* одночлена v = $b \cdot x_1^{m_1} x_2^{m_2} ... x_n^{m_n}$ *в смысле лексикографического порядка*, если найдется такой индекс i ∈ {1, 2, …,n}, что: $k_1 = m_1, ..., k_{i-1} = m_{i-1}$, *но*.....$k_i > m_i$.

В этом случае пишут: $u \succ v$.

ПРИМЕР **3**

Расположить одночлены многочлена

$f(x_1, x_2, x_3) = x_2^4 + x_1x_2x_3 + 3x_1x_2^2 - x_2x_3 + 2x_2x_3^2$

в порядке лексикографического убывания:

$f(x_1, x_2, x_3) = 3x_1x_2^2 + x_1x_2x_3 + x_2^4 + 2x_2x_3^2 - x_2x_3$.

ОПРЕДЕЛЕНИЕ. Одночлен многочлена от нескольких переменных, который старше

всех остальных его одночленов в смысле лексикографического порядка, называется *старшим членом многочлена* $f(x_1, x_2, \ldots, x_n)$.

ЗАМЕЧАНИЯ

1. Очевидно, что отношение лексикографического порядка рефлексивно, симметрично и транзитивно, то есть является отношением эквивалентности.

2. Если $u \succ v$ и w – ненулевой одночлен, то $u \cdot w \succ v \cdot w$.

3. Если $u \succ v$ и $w \succ t$, то $u \cdot w \succ v \cdot t$.

Из свойств отношения лексикографического порядка, приведенных в замечании следует справедливость следующих теорем.

ТЕОРЕМА 1

Старший член произведения двух ненулевых многочленов от n переменных над полем P равен произведению их старших членов.

ТЕОРЕМА 2

Кольцо многочленов от n переменных над полем P является областью целостности.

2. Симметрические многочлены от нескольких переменных и их свойства

ОПРЕДЕЛЕНИЕ. Многочлен f (x,y) называют симметрическим, если он не изменяется при замене x на y,а y на x.

Многочлен $x^2y + xy^2$ - симметрический. Напротив многочлен $x^3 - 3y^2$ не является симметрическим: при замене x на y, а y на x он превращается в многочлен $y^3 - 3x^2$, который не совпадает с первоначальным.

Приведем примеры симметрических многочленов. Как известно из арифметики, сумма двух чисел не меняется при перестановке слагаемых, т.е.

$x + y = y + x$ для любых чисел x и y. Это равенство показывает, что многочлен $x + y$ является симметрическим.

Точно так же из закона коммутативности умножения $xy = yx$

Следует, что произведение xy является симметрическим многочленом.

Рассмотренные примеры симметрических многочленов являются самыми простыми. Их называют элементарными симметрическими многочленами от x и y. Для них используется специальное обозначение:

$\sigma_1 = x + y$, $\sigma_2 = xy$

Кроме σ_1 и σ_2,часто встречатюся так называемые степенные суммы, т.е. многочлены $x^2 + y^2, x^3 + y^3, \ldots, x^n + y^n, \ldots$ Принято обозначать многочлен $x^n + y^n$ через s_n. Таким образом,

$$s_1 = x + y,$$

$s_2 = x^2 + y^2,$

$s_3 = x^3 + y^3,$

$s_4 = x^4 + y^4,$

…….

Существует простой прием, позволяющий получать симметрические многочлены. Возьмем любой (вообще говоря, не симметрический) многочлен от $\sigma 1$ и $\sigma 2$ и подставим в него вместо $\sigma 1$ и $\sigma 2$ их выражения через x и y. Ясно, что при этом мы получим симметрический многочлен от x и y

Если взять любой многочлен от $\sigma 1$ и $\sigma 2$ и подставить в него вместо $\sigma 1$ и $\sigma 2$ их выражение $\sigma 1 = x+y$, $\sigma 2 = xy$, то получится симметрический многочлен f (x, y).

ТЕОРЕМА. Любой симметрический многочлен от x и y можно представить в виде многочлена от σ1=x + y и σ 2 =xy.

Доказательство: Сначала докажем теорему не для любых симметрических многочленов, а лишь для степенных сумм. Иными словами, мы установим, что каждую степенную сумму sn=xn+yn можно представить в виде многочлена от σ_1 и σ_2.

С этой целью умножим обе части равенства

sk-1= xk-1 + yк-1 на σ1= x+y.

Получим:

σ1sk-1=(x+ y)(xк-1+yк-1)=xк+ xyk-1+x к-1y+yk= xк + yk + xy (xk-2 + yk-2) =

= sk + σk+σ2sk-2

Таким образом,

sk=σ1sk-1-σ2sk-2 (1)

Докажем равенство (1) методом математической индукции.

При к=1 s1=x+y=σ_1 формула верна. Предположим, что она верна при k=n-1 т.е. sn выражается через σ_1 и σ_2, проверим выполнимость формулы при k=n sn=σ1sn-1-σ2sn-2 , по предположению sn-1,sn-2 выражаются через σ_1 и σ_2, следовательно и sn выражаются через σ_1 и σ_2.Условия теоремы математической индукции выполняются, значит sk=σ1sk-1-σ2sk-2 верна для любого k.

Любой симметрический многочлен от x и y содержит (после приведения подобных членов) слагаемые двух видов.

Во-первых, могут встречаться одночлены, в которые x и y входят в одинаковых степенях, т.е. одночлены вида axkyk. Ясно, что axkyk = a (xy)k= aσk2, т. е. одночлены этого вида непосредственно выражаются через σ_2.

Во-вторых, могут встретиться одночлены, имеющие разные степени относительно x и y, т. е, одночлены вида bxkyl, где k.$\neq$l. Ясно, что вместе с одночленом bxkyl симметрический многочлен содержит также и одночлен bxlyk получаемый из bxkyl перестановкой букв x и y. Другими словами, в симметрический многочлен входит двучлен вида b(xkyl + xlyk)

Предполагая для определенности l>k, можно переписать этот двучлен следующим образом: b(xkyl + xlyk)=bxkyk(yl-k+xl-k)=bσk2sl-k.. А т. к. по доказанному степенная сумма sl-k представляется в виде многочлена отσ1 и σ2, то и рассматриваемый двучлен выражается через σ1 и σ2.

Итак, каждый симметрический многочлен представляется в виде суммы одночлена вида axkyk и двучлена вида $b(x^k y^l + x^l y^k)$, каждый из которых выражается через σ1 и σ2 . Следовательно, любой симметрический многочлен представляется в виде многочлена от σ1 и σ2. Теорема полностью доказана.[6, с. 9-13]

Симметрические многочлены от трех переменных

Мы рассмотрели симметрические многочлены от двух переменных x, y, т. е. многочлены, которые не меняются при перестановке местами x и y. В многочлене от трех переменных x, y, z таких перестановок можно сделать не одну, а три: можно поменять местами x и y или x и z, или, наконец, y и z.

ОПРЕДЕЛЕНИЕ. Многочлен f (x, y, z) называется симметрическим, если при любой перестановке переменных он остается неизменным [1, с. 47].

Условие симметричности многочлена f (x, y, z) записывается следующим образом:

f (x, y, z)=f(y, x, z)=f(z, y, x)=f(x, z, y).

Из коммутативности сложения вытекает, что симметричным является многочлен x+y+z, а из коммутативности умножения следует симметричность многочлена xyz.

Симметричны и степенные суммы, т. е. многочлены, вида

$s_k = x^k + y^k + z^k$.

Вот еще примеры симметрического многочлена от трех переменных:

xy +yz+xz,

$x^3 + y^3 + z^3 - 3xyz$,

$(x + y)(x + z)(y + z)$,

$x(y^4 + z^4) + y(x^4 + z^4) + z(x^4 + y^4)$

Напротив, многочлен x2z + y2z не является симметрическим. Правда, при перестановке переменных x и y он не меняется: x2z + y2x = y2z + x2z.Но перестановка переменных x и z меняет вид этого многочлена – он переходит в многочлен $z^2x + y^2x \neq x^2z + y^2z$

Наиболее простыми являются симметрические многочлены $x + y + z$, $xy + xz + yz$, xyz.

Их называют элементарными симметрическими многочленами от трех переменных x,y,z и обозначают через $\sigma_1, \sigma_2, \sigma_3$:

$\sigma_1 = x + y + z$

$\sigma_2 = xy + xz + yz$

$\sigma_3 = xyz$.

Заметим, что многочлен σ_1 - многочлен первой степени, σ_2 - второй степени и σ_3 - многочлен третий степени.

Как и в случае двух переменных, можно построить симметрические многочлены от трех переменных. Возьмем любой многочлен от переменных, $\sigma_1, \sigma_2, \sigma_3$ и заменим в нем σ_1 на x+y+z, σ_2-на xy+xz+yz и σ_3- на xyz. В результате мы получим многочлен, симметрично зависящий от x, y, z.

ТЕОРЕМА. Любой симметрический многочлен от x, y, z можно представить в виде многочлена от $\sigma_1 = x + y + z$, $\sigma_2 = xy + xz + yz$, $\sigma_3 = xyz$.

Доказательство основной теоремы о симметрических многочленах от трех переменных несколько сложнее, чем для случая двух переменных, поэтому опустим его. (Приложение 3).

многочлена от m переменных. Свойства симметрических многочленов. Основная теорема о симметрических многочленах

Определение. Многочлен от m переменных называется симметрическим многочленом, если он не изменяется при любой перестановке переменных.

ПРИМЕР. Многочлен f(x1,x2,x3)=x12+x22+x32 является симметрическим т.к. f(x2,x1,x3)=x23+x13+x33= f(x3,x2,x1)= f(x1,x2,x3)

Многочлен g(x1,x2,x3)=3x13+x23+3x33 симметрическим не является т.к. g(x2,x1,x3)=3x23+x13+3x33 ≠ g(x1,x2,x3)

ПРИМЕР. Многочлен x12+…+xm2+x1+x2+…+xm переходит в себя при любой подстановке элементов x1,…,xm.

ОПРЕДЕЛЕНИЕ. Элементарными симметрическими многочленами от x1,…,xm называются многочлены[19, с. 496]

σ1=x1+x2+…+xm;

σ2=x1x2+x1x3+…+xm-1xm;

σ3=x1x2 x3+…+xm-2xm-1xm;

……

σm=x1x2…xm.

Элементарные симметрические многочлены получаются, если рассмотреть многочлена φ=(z-x1)(z-x2)…(z-xm), который равен многочлену

zm-(x1+x2+…+xm)zm-1+(x1x2+…+xm-1xm)zm-2+…+(-1)mx 1...xm.

Таким образом, φ=zm-σ1zm-1+σ2zm-2-…+(-1)mσm.

Свойства симметрических многочленов

1. Сумма, разность, произведение симметрических многочленов является симметрическим многочленом, т.е. множество симметрических многочленов является кольцом.

2. Всякий симметрический многочлен можно представить в виде суммы однородных многочленов.

3. Если одночлен axnα1 xnα2…xnαn входит в симметрический многочлен, то в этот симметрический многочлен входят и одночлены, полученные из данного любой перестановкой переменных.

4. Показатели степеней переменных в высшем члене симметрического многочлена образуют не возрастающую последовательность.

5. Пусть ax1k1x2k2…xmkm- высший член ненулевого симметрического многочлена f(x1,…,xm) ∈K[x1,…,xm].Тогда высшие члены многочленов f(x1,…,xm) и aσ1k1-k2σ2k2-k3…σmkm совпадают.

6. Убывающая цепочка ненулевых симметрических многочленов кольца многочленов K[x1,…,xm] не может быть бесконечной.

3. Основная теорема о симметрических многочленах

ТЕОРЕМА. Всякий симметрический многочлен из кольца многочленов K[x1,…,xm] можно представить в виде многочлена над K от элементарных симметрических многочленов .

Доказательство. Пусть многочлена f(x1,…,xm) -не нулевой симметрический многочлен над K и a0x1k1x2k2…xmkm -его высший член. Многочлен (1) f1= f- a0σk1-k2…σmkm -симметрический, как разность симметрических многочленов, причем, по свойству 50, f > f1. Пусть a1x1l1 …xm lm - высший член многочлена f1. Аналогично, многочлен (2) f2= f1- a1σ l1- l2…σm lm является симметрическим, причем f1> f2 и т.д. В результате получается убывающая цепочка симметрических многочленов f> f1> f2> …..По свойству 60, эта цепочка не может быть бесконечной. Предположим, что она обрывается на (s+1)-м шаге, т.е. (s+1) fs+1= fs- asσn1-n2…σmnm =0. Складывая почленно равенства (1),(2),…,(s+1), получим

f= a0σk1-k2…σmkm + a1σ l1- l2…σm lm + …+ asσn1-n2…σmnm .

Это равенство дает искомое представление симметрического многочлена f в виде многочлена над K от элементарных симметрических многочленов σ1,…,σm.

СЛЕДСТВИЕ. Пусть φ = zm+a1zm-1+…+am- многочлен над числовым кольцом K и φ = (z-c1)(z-c2)…(z-cm), где c1,…,cm∈C. Если f(x1,…,xm)- симметрический многочлен от x1,…,xm с коэффициентами из K, то f(c1,…,cm)∈ K.

Доказательство: Из равенства

(z-c1)(z-c2)… (z-cm) = zm+a1zm-1+ a2zm-2+…+am

вытекают следующие формулы (формулы Виета), выражающие связь между корнями и коэффициентами многочлена:

c1+…+cm= -a1;

c1c2+…+cm-1cm= a2;

…….

c1c2…cm= (-1)mam.

Эти равенства можно записать в виде

σ1(c1,…,cm) = -a1;

σ2(c1,…,cm) = a2;

…….. (1)

σm (c1,…,cm) = (-1)mam. ;

В силу основной теоремы о симметрических многочленах симметрический многочлен f из K[x1,…,xm] можно представить в виде многочлена g от элементарных симметрических многочленов σ1,…,σm с коэффициентами из K, т.е.

f(x1,…,xm)= g(σ1(x1,…,xm),…,σm(x1,…,xm)). (2)

Полагая в равенстве (2) x1=c1,…,xm=cm и учитывая равенства (1), получим

f(c1,…,cm)= g(-a1, a2,…, (-1)mam) (3)

Кроме того, g∈ K[x1,…,xm] и a1,…,am∈ K, следовательно, f(c1,…,cm) ∈ K.

Тема. Многочлены над полем действительных и комплексных чисел

План

1. Лемма о непрерывности многочлена с комплексными коэффициентами. Лемма о модуле старшего члена многочлена с комплексными коэффициентами.

2. Теорема о существовании корня многочлена с комплексными коэффициентами (основная теорема алгебры).

3. Разложение многочлена с комплексными коэффициентами в произведение линейных множителей.

1. Лемма о непрерывности многочлена с комплексными коэффициентами. Лемма о модуле старшего члена многочлена с комплексными коэффициентами.

Впервые доказанная в 1799 г. великим немецким математиком Гауссом, эта теорема известна как «основная теорема алгебры».

ТЕОРЕМА. Всякий многочлен положительной степени с комплексными коэффициентами имеет корень в поле комплексных чисел.

Сформулируем две леммы, которые потребуются для доказательства теоремы.

Пусть $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \quad a_i \in C, \quad n \geq 1$ (1) –

многочлен с комплексными коэффициентами.

ЛЕММА 1. Существует такое положительное число А, что для всех $x_0 \in C$, удовлетворяющих неравенству $|x_0 > A|$, выполняется неравенство $|f(x_0)| > |f(0)|$.

ЛЕММА 2. (*Даламбера).* Если многочлен $f(x)$ не обращается в нуль в точке $x_0 \in C$, то для любого $\varepsilon > 0$ существует такое $u \in C$, что $|u| < \varepsilon$ и $|f(x_0 + u)| < |f(x_0)|$.

2. Теорема о существовании корня многочлена с комплексными коэффициентами (основная теорема алгебры)

Доказательство основной теоремы.

Пусть А – число, определенное по лемме 1. Возьмем на комплексной плоскости замкнутый круг К радиусом А с центром в начале координат. По лемме вне этого круга многочлен $f(x)$ принимает значения по модулю большие, чем $|f(0)|$. (Отсюда, в частности, следует, что этот многочлен может обращаться в 0 только внутри круга К).

Рассмотрим функцию $\psi(u,v) = |f(u+iv)|$ от двух действительных переменных *u, v.* (Здесь переменная *x* как комплексная переменная представлена в алгебраической форме с выделением действительной и мнимой частей). Если подставить в выражение (1) для $f(x)$ вместо $x = u + iv$, вместо комплексных коэффициентов их представление в алгебраической форме $a_j = b_j + ic_j$, выполнить все действия и сгруппировать слагаемые с мнимой единицей и без нее, то получим, что эта функция представима в виде суммы двух функций (многочленов с действительными коэффициентами): $\psi(u,v) = \psi_1(u,v) + i\psi_2(u,v)$.

Так как модуль комплексного числа $z = a + bi$ находится по формуле: $|z| = |a + bi| = \sqrt{a^2 + b^2}$, то получаем, что $\psi(u,v) = \sqrt{\psi_1(u,v)^2 + \psi_2(u,v)^2}$.

Т.к. многочлены ψ_1 и ψ_2 непрерывны как функции, то и функция ψ непрерывна и определена на всей комплексной плоскости.

Известно, что всякая функция действительных переменных, определенная и непрерывная внутри некоторого замкнутого ограниченного множества, достигает минимума в некоторой точке этого множества. Отсюда следует, что для функции ψ в круге К существует точка $x_0 = u_0 + iv_0$, в которой эта функция достигает минимума. Тогда по определению точки минимума, для всех $x_1 \in K$, $|f(x_0)| \le |f(x_1)|$. (2)

Т.к. $0 \in$К, то, в частности, $|f(x_0)| \le |f(0)|$.

Согласно построению круга К, значения многочлена $f(x)$ вне этого круга по модулю больше, чем $|f(0)|$, и тем более, больше, чем $|f(x_0)|$:

$$|f(x_0)| \le |f(0)| < |f(x)|.$$

Следовательно, неравенство (2) выполняется для всех точек комплексной плоскости. Отсюда, учитывая лемму Даламбера, получаем, что $f(x)$ должен обращаться в 0 в точке x_0, следовательно, x_0 – корень $f(x)$. Теорема доказана.

Следствием этой теоремы является гораздо более сильное утверждение о том, что всякий многочлен степени *n* с комплексными коэффициентами имеет в поле комплексных чисел ровно *n* корней (с учетом кратностей).

Напомним, что комплексное число $\overline{z} = a - bi$ называется ***комплексно сопряженным*** к числу $z = a + bi$ и обозначается $\overline{z}$.

Теорема 1. Если комплексное число x_0 является корнем многочлена с действительными коэффициентами, то сопряженное число $\overline{x_0}$ также является корнем этого многочлена.

Доказательство. Пусть $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \quad a_i \in R, \quad n \ge 1$ – многочлен с действительными коэффициентами и x_0 – его корень, т.е. $f(x_0) = x_0^n + a_1 x_0^{n-1} + \cdots + a_{n-1} x_0 + a_n = 0$.

Для вычисления $f(\overline{x_0})$ воспользуемся свойствами комплексного сопряжения: $\overline{z_1} + \overline{z_2} = \overline{z_1 + z_2}, \quad \overline{z_1} \cdot \overline{z_2} = \overline{z_1 \cdot z_2}$, а также тем, что действительное число совпадает со своим сопряженным:

$$f(\overline{x_0}) = \overline{x_{01}^n} + a_1 \overline{x_0^{n-1}} + \cdots + a_{n-1} \overline{x_0} + a_n = \overline{x_0^n} + \overline{a_1} \cdot \overline{x_0^{n-1}} + \cdots + \overline{a_{n-1}} \cdot \overline{x_0} + \overline{a_n} =$$
$$= \overline{x_0^n} + \overline{a_1 \cdot x_0^{n-1}} + \cdots + \overline{a_{n-1} \cdot x_0} + \overline{a_n} = \overline{f(x_0)} = \overline{0} = 0.$$

Т.е. $\overline{x_0}$ также есть корень $f(x)$.

3. Разложение многочлена с комплексными коэффициентами в произведение линейных множителей

ОПРЕДЕЛЕНИЕ. Многочлен $f(x)$ называется ***неприводимым*** над некоторым полем, если он не раскладывается в произведение двух многочленов меньшей степени над этим же полем.

ТЕОРЕМА 2. В кольце многочленов над полем действительных чисел неприводимы только многочлены первой степени и многочлены второй степени, не имеющие действительных корней.

Доказательство. Пусть $f(x)$ – многочлен степени $n \geq 3$ над полем действительных чисел и x_0 – какой-нибудь его комплексный корень. Если этот корень – действительное число, то $f(x)$ по теорем Безу делится на двучлен $x - x_0$ над полем R, и, следовательно, приводим.

Пусть x_0 – мнимый корень, тогда по теореме 1, $\overline{x_0}$ также является его корнем. Тогда над полем комплексных чисел $f(x)$ делится на произведение $(x-x_0)\cdot(x-\overline{x_0}) = x^2 - (x_0+\overline{x_0})\cdot x + x\cdot\overline{x_0}$. Так как $x+\underline{x_0}$ u $x\cdot\overline{x_0}$ – действительные числа, то $f(x)$ делится на квадратный трехчлен с действительными коэффициентами.

Следовательно, над полем R всякий многочлен степени, большей 2, приводим. Из многочленов 2–й степени неприводимы только те, которые не имеют действительных корней. Теорема доказана.

Тема. Многочлены над полем рациональных чисел и алгебраические числа

План

1. Понятие расширения поля. Алгебраические и трансцендентные числа.

2. Минимальный многочлен алгебраического числа и его свойства.

3. Простое и составное алгебраические расширения.

1. Понятие расширения поля. Алгебраические и трансцендентные числа

ОПРЕДЕЛЕНИЕ. Пусть К и Р – некоторые поля, причем поле К содержится в поле Р: К $\subset$ Р. Тогда К называется *подполем* поля Р, а Р – *надполем* или *расширением* поля К.

Пусть Р есть расширение поля К и α – произвольный элемент поля Р. Очевидно, что существуют поля, которые содержат и поле К, и элемент α. Например, одним из таких полей является само поле Р.

Тогда справедливо УТВЕРЖДЕНИЕ:

Пересечение всех полей, содержащих поле К и элемент α, само является полем, содержащим К и α, которое обозначается как К(α): К $\subseteq$ К(α) $\subseteq$ Р. Очевидно также, что К(α) – наименьшее среди всех подполей поля Р, содержащих поле К и элемент α одновременно.

ЗАМЕЧАНИЕ. Иногда говорят, что элемент α *присоединен* к полю К.

Расширение Р поля К может быть получено присоединением любого конечного (и даже бесконечного) числа элементов $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$.

Если расширение получено присоединением одного элемента, то оно называется *простым*.

Так как К(α) – поле, то наряду с элементами поля К и самим элементом α оно, очевидно, содержит всевозможные элементы, получаемые при их сложении, вычитании, умножении и делении.

ТЕОРЕМА. Поле К(α) состоит из рациональных комбинаций элементов из К с элементами, представляющими степени и кратные элемента α.

Пусть дано простое расширение поля К элементом α: К(α).

Тогда оно содержит кольцо всех многочленов от α вида:

$$a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n + \ldots, a_k \in K \quad (14)$$

Запишем выражение (1) в виде суммы

$$\sum a_k\alpha^k = f(\alpha) \qquad (15)$$

и сравним его с элементами кольца многочленов Ω от одной переменной над тем же полем К – К[x]:

$$f(x) = a_0 + a_1x + a_2x^2 + .. + a_nx^n = \sum a_k x^k \qquad (16)$$

Тогда нетрудно проверить, что отображение φ: К[x] $\to \Omega$, заданное следующим образом:

$$\varphi: \sum a_k x^k \to \sum a_k \alpha^k \qquad (17)$$

является гомоморфизмом колец.

ЗАМЕЧАНИЯ

1. Из (4) и теоремы о гомоморфизме следует, что кольцо Ω изоморфно фактор-кольцу К[x] / Ker φ, причем ядро гомоморфизма состоит из всех таких многочленов f(x) $\in$ К[x], которые при гомоморфизме φ отображаются в нуль кольца Ω: $\varphi(f(x)) = f(\alpha) = 0_{\Omega}$, т.е., оно состоит из таких многочленов, для которых α является корнем. Очевидно, что Ker φ есть идеал в кольце К[x].

Поскольку в кольцах многочленов над полем нет делителей нуля, то идеал Ker φ является простым, т.е. не содержащим собственных идеалов. Он не может быть единичным идеалом, который при гомоморфизме переходит также в единичный идеал, а не в нулевой. Так как в кольце многочленов над полем каждый идеал является главным, то остаются только две возможности.

2. Ker φ = (g(x)), где g(x) – неприводимый над К многочлен. В силу простоты идеала (g(x)), g(x) – многочлен наименьшей степени со свойством g(α) = 0. В этом случае $\Omega \cong$ К[x] / (g(x)).

Кольцо классов вычетов К[x]/(g(x)) является полем (поскольку идеал простой); изоморфное ему кольцо Ω также будет полем, которое в данном случае и является простым расширением кольца К[x].

3. Ker φ = {0}, тогда в кольце К[x] не существует других многочленов, кроме нуля, которые отображались бы в нуль кольца Ω. В этом случае φ является изоморфизмом колец.

4. В случае 2, когда элемент α удовлетворяет некоторому алгебраическому уравнению g(α) = 0 над К, сам элемент α называется *алгебраическим над полем К*, а поле К(α) – *простым алгебраическим расширением* поля К.

В случае 3, когда из равенства f(α) = 0 следует, что f(x) =0, элемент α называется *трансцендентным над* К, а само поле К(α) – *простым трансцендентным расширением* поля К. Очевидно, что во втором случае не существует многочлена с коэффициентами из К, корнем которого являлось бы число α.

Вообще говоря, к понятию алгебраических и трансцендентных чисел подходят обычно следующим образом.

ОПРЕДЕЛЕНИЕ. Число α называется *алгебраическим над полем* Р, если оно является корнем какого-либо многочлена с коэффициентами из этого поля. В противном случае число α называется *трансцендентным над полем* Р.

ЗАМЕЧАНИЕ. Пусть α есть число, алгебраическое над полем Р. Если К есть подполе поля Р, то α может уже и не быть алгебраическим над этим полем. Например, число $\alpha = \pi$ будет алгебраическим над полем действительных чисел, так как оно есть корень многочлена f(x) = x - π, но не будет алгебраическим над полем рациональных чисел.

2. Минимальный многочлен алгебраического числа и его свойства

ОПРЕДЕЛЕНИЕ. Поле Р называется *конечным расширением поля* К, если любой элемент w $\in$ Р является линейной комбинацией конечного числа элементов $u_1, u_2, ..., u_n$ с коэффициентами из поля К: $w = a_1u_1 + a_2u_2 + ... + a_nu_n$.

ЗАМЕЧАНИЕ. Очевидно, что поле Р можно рассматривать как конечномерное векторное пространство над К. Базисом этого пространства является максимальная

линейно независимая подсистема элементов в системе $u_1, u_2, ..., u_n$. Число элементов базиса, т.е. размерность пространства P над K, называется *степенью расширения* P над K и обозначается через [P : K].

Пусть P – простое алгебраическое расширение поля K с помощью элемента α, степень которого над K равна n.

Тогда элементы $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ (18) образуют базис поля P = K(α), т.е. K(α) имеет конечную степень n над K.

Пусть поле L – промежуточное между полями K и P, т.е., K $\subseteq$ L $\subseteq$ P. Тогда справедлива теорема.

ТЕОРЕМА (*о степенях*). Если P конечно над K, то и L конечно над K, а P конечно над L. Обратно, если L конечно над K, а P конечно над L, то P конечно над K, причем

$$[P : K] = [P : L] \cdot [L : K]. \quad (19)$$

ЗАМЕЧАНИЕ. Вторую часть этой теоремы называют также *свойством транзитивности* конечных расширений.

СЛЕДСТВИЕ **1.** Если K $\subseteq$ L $\subseteq$ P и [P : K] = [L : K], то P = L.

СЛЕДСТВИЕ **2.** Если K $\subseteq$ L $\subseteq$ P и [P : L] = [P : K], то L = K.

СЛЕДСТВИЕ **3.** Если K $\subseteq$ L $\subseteq$ P, то степень [L : K] является делителем степени [P : K].

Установим взаимосвязь между расширениями конечной степени и алгебраичностью числа над полем.

ТЕОРЕМА. Число α является алгебраическим над полем P тогда и только тогда, когда векторное пространство P(α) конечномерно над полем P. При этом степень числа α над P равна размерности этого пространства.

СЛЕДСТВИЕ. Пусть K – некоторое кольцо, содержащее поле P. Если пространство K конечномерно над P, то всякое число из кольца *K* алгебраично над P.

ТЕОРЕМА. Совокупность всех чисел, алгебраических над данным полем P, является полем, которое называется *полем алгебраических чисел.*

ОПРЕДЕЛЕНИЕ. Поле называется *алгебраически замкнутым,* если любой многочлен положительной степени с коэффициентами из этого поля имеет корни в этом поле.

Так как любой многочлен с комплексными коэффициентами имеет корень в поле комплексных чисел, то поле C является алгебраически замкнутым.

ТЕОРЕМА. Всякое конечное расширение числового поля является простым алгебраическим расширением этого поля.

Эта теорема означает, что если поле $P(\alpha_1, \alpha_2, ..., \alpha_n)$ есть конечное расширение числового поля P, то можно подобрать такое число γ, что $P(\alpha_1, \alpha_2, ..., \alpha_n)$ =P(γ).

ОПРЕДЕЛЕНИЕ. Расширение *P* поля K *называется алгебраическим над K*, если каждый элемент из P является алгебраическим над K.

Между конечными и алгебраическими расширениями полей существует тесная взаимосвязь.

ТЕОРЕМА. Каждое конечное расширение поля P алгебраично и получается из P присоединением конечного числа алгебраических элементов.

ЗАМЕЧАНИЕ. Эта теорема позволяет говорить о «конечных алгебраических расширениях» вместо «конечных расширений».

Справедлива и обратная

ТЕОРЕМА. Каждое расширение поля P, которое получается присоединением конечного множества алгебраических чисел к полю P, конечно (и, следовательно, алгебраично).

Для решения некоторых задач полезна следующая

ТЕОРЕМА. Если элемент α алгебраичен над полем P, которое является алгебраическим расширением поля K, то α алгебраичен и над полем K.

Среди всех конечных алгебраических расширений особую роль играют так называемые *поля разложения многочлена* f(x).

ОПРЕДЕЛЕНИЕ. *Полем разложения многочлена* f(x), заданного над полем P, называется поле, полученное присоединением к P всех корней уравнения f(x)=0.

ЗАМЕЧАНИЕ. Речь в определении идет о полях $P(\alpha_1,\alpha_2,...,\alpha_n)$, в которых многочлен f(x) из кольца P[x] полностью разлагается на линейные множители: $f(x)=(x-\alpha_1)\cdot(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n)$ и которые получаются присоединением к P корней α_i этих линейных множителей.

В теории полей доказывается

ТЕОРЕМА. Для каждого многочлена f(x) из кольца многочленов P[x] существует некоторое поле разложения.

Тема. Важнейшие функции в теории чисел

План

1. Функции $\lfloor x\rfloor$, $\{x\}$, $\bmod$. и их свойства.

2. Мультипликативные функции

3. Функция Эйлера.

1. Функции $\lfloor x\rfloor$, $\{x\}$ и их свойства

ОПРЕДЕЛЕНИЕ

Пусть x - произвольное действительное число. Тогда:

$\lfloor x\rfloor$ равно наибольшему целому числу, не превосходящему x (читается функция «пол»);

$\lceil x\rceil$ равно наименьшему целому числу, большему или равному x (читается функция «потолок»).

Таким образом, $\begin{array}{l}\lfloor x\rfloor=a,\quad a\in Z,\quad a\le x,\quad a-наибольшее;\\ \lceil x\rceil=b,\quad b\in Z,\quad b\ge x,\quad b-наименьшее.\end{array}$

Отметим некоторые свойства этих функций.

СВОЙСТВО 1

$$\lfloor x\rfloor=x=\lceil x\rceil \quad\Leftrightarrow\quad x\in Z.$$

СВОЙСТВО 2

$$Если\quad x\notin Z,\quad то\quad \lceil x\rceil-\lfloor x\rfloor=1.$$

СВОЙСТВО 3

$$(\forall x\in R)\,(x-1<\lfloor x\rfloor\le x\le\lceil x\rceil<x+1.$$

СВОЙСТВО 4

$$\lfloor -x\rfloor=-\lceil x\rceil\quad и\quad \lceil -x\rceil=-\lfloor x\rfloor.$$

СВОЙСТВО 5

$$(\forall x\in R)\,(\forall n\in Z):$$
$$a)\,\lfloor x\rfloor=n\quad\Leftrightarrow\quad n\le x\le n+1;$$
$$b)\,\lfloor x\rfloor=n\quad\Leftrightarrow\quad x-1<n\le x;$$
$$c)\,\lceil x\rceil=n\quad\Leftrightarrow\quad n-1<x\le n;$$
$$d)\,\lceil x\rceil=n\quad\Leftrightarrow\quad x\le n<x+1.$$

СВОЙСТВО 6

$$(\forall x\in R)\,(\forall n\in Z)\,(\lfloor x+n\rfloor=\lfloor x\rfloor+n\quad и$$
$$\lceil x+n\rceil=\lceil x\rceil+n,$$

то есть целочисленное слагаемое можно выносить и вносить за скобки функций «пол» и «потолок».

СВОЙСТВО 7

$$(\forall x \in R)\ (\forall n \in Z):$$
$$a)\ x < n \quad \Leftrightarrow \quad \lfloor x \rfloor < n;$$
$$b)\ n < x \quad \Leftrightarrow \quad n < \lceil x \rceil;$$
$$c)\ x \le n \quad \Leftrightarrow \quad \lceil x \rceil \le n;$$
$$d)\ n \le x \quad \Leftrightarrow \quad n \le \lfloor x \rfloor.$$

Эти неравенства позволяют вставлять или опускать скобки функций «пол» и «потолок».

СВОЙСТВО 8

$$(\forall x \in R)$$
$$\lceil \lfloor x \rfloor \rceil = \lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor;$$
$$\lfloor \lceil x \rceil \rfloor = \lceil \lceil x \rceil \rceil = \lceil x \rceil.$$

ОПРЕДЕЛЕНИЕ. Разность между числом x и функцией $\lfloor x \rfloor$ называется *дробной частью* числа x и обозначается

$$\{x\} = x - \lfloor x \rfloor.$$

СВОЙСТВО 9. Пусть $f(x)$ - некоторая непрерывная, монотонно возрастающая функция, такая, что если $f(x)$ - целое число, то x - тоже целое число. Тогда:

$$\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor \quad (1);$$
$$\lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil \quad (2).$$

Доказательство.

Если $x = \lceil x \rceil$, то равенство (2) очевидно. Пусть $x \neq \lceil x \rceil$, тогда из определения функции «потолок» следует, что $x < \lceil x \rceil$. Так как $f(x)$ - возрастающая функция, то $f(x) < f(\lceil x \rceil)$ u $\lceil f(x) \rceil \le \lceil f(\lceil x \rceil) \rceil$, поскольку функции «потолок» невозрастающая.

Действительно, если бы выполнялось неравенство $\lceil f(x) \rceil < \lceil f(\lceil x \rceil) \rceil$, то должно найтись такое число y, для которого:

$$x \le y < \lceil x \rceil \quad u \quad f(y) = \lceil f(x) \rceil,$$

что следует из непрерывности функции $f(x)$. По свойству этой функции, y должно быть целым числом. Но по определению функции $\lceil x \rceil$, между числами x и $\lceil x \rceil$ не может найтись целого числа, отличного от $\lceil x \rceil$. Полученное противоречие доказывает равенство (2).

Равенство (1) доказывается аналогично.

Следствием этого свойства является следующее свойство.

СВОЙСТВО 10

$$(\forall x \in R)\,(\forall m \in Z)\,(\forall n \in N)$$

$$\left\lfloor \frac{x+m}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + m}{n} \right\rfloor \quad (1);$$

$$\left\lceil \frac{x+m}{n} \right\rceil = \left\lceil \frac{\lceil x \rceil + m}{n} \right\rceil \quad (2).$$

СВОЙСТВО 11. Пусть α и β - произвольные действительные числа. Количество заключенных между ними целых чисел равно:

$$a)\ на\quad [\alpha,\beta]:\quad \lfloor \beta \rfloor - \lceil \alpha \rceil + 1,\quad \alpha \le \beta;$$

$$b)\ на\quad [\alpha,\beta):\quad \lceil \beta \rceil - \lceil \alpha \rceil,\quad \alpha \le \beta;$$

$$c)\ на\quad (\alpha,\beta]:\quad \lfloor \beta \rfloor - \lfloor \alpha \rfloor,\quad \alpha \le \beta;$$

$$d)\ на\quad (\alpha,\beta):\quad \lceil \beta \rceil - \lfloor \alpha \rfloor,\quad \alpha < \beta.$$

Функция mod и ее свойства

Если m, n - целые числа, то частное от деления n на m равно значению функции «пол» от рационального числа $\frac{n}{m}$, то есть, равно $\left\lfloor \frac{n}{m} \right\rfloor$. Используя запись деления с остатком:

$$n = \left\lfloor \frac{n}{m} \right\rfloor \cdot q + r,$$

где r есть остаток от деления. Для обозначения остатка используют специальную функцию $r = n \bmod m$. Читается как «r есть остаток от деления n на m»:

$$n = \left\lfloor \frac{n}{m} \right\rfloor \cdot m + n \bmod m \qquad (1).$$

Из (1) следует, что $n \bmod m = n - \left\lfloor \frac{n}{m} \right\rfloor \cdot m \qquad (2).$

В выражении (2) можно считать n и m любыми действительными числами, $m \neq 0$.

Пример.

$$5 \bmod 3 = 5 - 3 \cdot \left\lfloor \frac{5}{3} \right\rfloor = 5 - 3 \cdot 1 = 2;$$

$$5 \bmod (-3) = 5 - (-3) \cdot \left\lfloor \frac{5}{-3} \right\rfloor = 5 + 3 \cdot (-2) = -1;$$

$$-5 \bmod 3 = -5 - 3 \cdot \left\lfloor \frac{-5}{3} \right\rfloor = -5 - 3 \cdot (-2) = 1;$$

$$-5 \bmod (-3) = -5 - (-3) \cdot \left\lfloor \frac{-5}{-3} \right\rfloor = -5 + 3 \cdot 1 = -2.$$

Отметим некоторые свойства функции $\bmod$.

СВОЙСТВО 1

$$(\forall x, y \in R)$$

$$0 \le x \bmod y < y, \quad если \quad y > 0;$$

$$y < x \bmod y \le 0, \quad если \quad y < 0.$$

СВОЙСТВО 2

$$(\forall x \in R)\ (x = \lfloor x \rfloor + \{x\} = \lfloor x \rfloor + x \bmod 1.$$

СВОЙСТВО 3

$$(\forall x \in R)\ (\forall y \ne 0 \in R)\ (\forall C = const, C \ne 0)$$

$$C \cdot (x \bmod y) = (Cx) \bmod (Cy).$$

Доказательство.

$$C \cdot (x \bmod y) \overset{def}{=} C \cdot \left(x - y \cdot \left\lfloor \frac{x}{y} \right\rfloor \right) = Cx - Cy \cdot \left\lfloor \frac{Cx}{Cy} \right\rfloor = (Cx) \bmod (Cy).$$

СВОЙСТВО 4

$$(\forall n \in Z)\ (\forall m \in N)$$

$$n = \left\lfloor \frac{n}{m} \right\rfloor + \left\lfloor \frac{n-1}{m} \right\rfloor + \cdots + \left\lfloor \frac{n-(m-1)}{m} \right\rfloor \quad и$$

$$n = \left\lfloor \frac{n}{m} \right\rfloor + \left\lfloor \frac{n+1}{m} \right\rfloor + \cdots + \left\lfloor \frac{n+m-1}{m} \right\rfloor.$$

СВОЙСТВО 5

$$(\forall x \in R)\ (\forall m \in N)$$

$$\lfloor mx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{m} \right\rfloor + \cdots + \left\lfloor x + \frac{m-1}{m} \right\rfloor.$$

2. Мультипликативные функции

Функция Θ(a) называется мультипликативной, если:

- она определена для $\forall\ a \in Z_+$, и при этом $\exists$a1:Θ(a1)≠0;
- $\forall\ a_1, a_2 \in Z_+$: (a1,a2)=1 $\Rightarrow$ Θ(a1·a2)=Θ(a1)·Θ(a2).

Пример. Степенная функция a^s – мультипликативная функция.

Свойства мультипликативных функций:

1. Если Θ(a) – мультипликативная функция, то Θ(1)=1.

Доказательство:

По определению мультипликативной функции, найдется a1: Θ(a1)≠0.

Тогда Θ(a1)=Θ(a1·1)=Θ(a1) · Θ(1). Отсюда Θ(1)=1.

2. Если Θ – мультипликативная функция, то для попарно простых чисел a1,a2,…,ak выполняется Θ(a1·a2·…·ak)= Θ(a1)·Θ(a2)·…·Θ(ak).

В частности, $\Theta\left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}\right) = \Theta\left(p_1^{\alpha_1}\right) \cdot \Theta\left(p_2^{\alpha_2}\right) \cdot \ldots \cdot \Theta\left(p_k^{\alpha_k}\right)$.

(Доказательство очевидным образом следует из 2-го условия на мультипликативную функцию.)

Если функции Θ1, Θ2, … ,Θk – мультипликативные, то их произведение Θ=Θ1·Θ2·…·Θk – также мультипликативная функция.

Если Θ(a) – мультипликативная функция, $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ – каноническое разложение a, то, обозначив знаком $\sum_{d \setminus a}$ сумму по всем делителям числа a, имеем

$$\sum_{d \setminus a} \Theta(d) = \left(1 + \Theta(p_1) + \Theta\left(p_1^2\right) + \ldots + \Theta\left(p_1^{\alpha_1}\right)\right) \cdot \ldots \cdot \left(1 + \Theta(p_k) + \ldots + \Theta\left(p_k^{\alpha_k}\right)\right)$$

(Доказываем, раскрывая скобки в правой части).

3. Функция Эйлера

Функция Эйлера φ(a) есть количество чисел ряда 0, 1, …, a–1, взаимно простых с a ($a \in Z_+$).

φ(1)=1, φ(2)=1, φ(3)=2, φ(4)=2, φ(5)=4, φ(6)=2 и т. д.

Свойства функции Эйлера:

1) φ(1)=1;

Доказательство следует из определения.

2) φ(p)=p–1, где p – простое;

Доказательство:

Действительно если p – простое, в ряду чисел 0, 1, …, p–1 не является взаимно простым с p только «0». Остальные p–1 чисел являются взаимно простыми с p в силу его простоты. Воспользовавшись определением функции Эйлера, получим искомое.

3)φ(pα)=pα–1(p–1) , где p – простое;

Доказательство:

Рассмотрим ряд чисел 0, 1, … , p, … , 2p, … , 3p, … , p2, … ,(p+1)p, …

В этом ряду не взаимно простыми с pα являются только те числа, которые кратны p, то есть числа 0, p, 2p, …, (pα–1–1)p. Таких чисел будет pα–1. Всего же чисел в этом ряду будет pα.

Таким образом, количество чисел в рассматриваемом ряду, взаимно простых с pα будет pα–pα–1= pα–1(p–1). Итак, φ(pα)=pα–1(p–1).

4)φ(a) – мультипликативная функция.

Доказательство:

Действительно, по определению функции Эйлера, она задана для всех положительных чисел, и согласно свойству №1 функции Эйлера, φ(1)=1.

Покажем, что φ(p1p2)=φ(p1)φ(p2), если p1, p2 – простые числа.

Действительно, в ряду чисел 0, 1, … , p1p2—1 ровно p2 чисел являются кратными p1 и ровно p1 чисел будут кратны p2. Причем, в силу взаимной простоты p1 и p2, это будут разные числа, и только число «0» кратно и p1, и p2. Таким образом, чисел, кратных p1 или p2 будет p1+p2—1. Тогда чисел, взаимно простых и с p1, и с p2 будет ровно p1p2—p1—p2+1=p1(p2—1)—(p 2—1) =(p1—1)(p2—1)= φ(p1)φ(p2).

Покажем теперь, что для взаимно простых чисел a1 и a2 справедливо φ(a1a2)=φ(a1)φ(a2).

Действительно, в ряду чисел 0, 1, … , a1a2—1 ровно a1a2—φ(a1)a2 чисел будут не взаимно простыми с a1 и a1a2—φ(a2)a1 чисел – не взаимно простыми с a2.

В то же время в ряду чисел 0, 1, … , a1—1 ровно a1— φ(a1) чисел не будут являться взаимно простыми с a1, в ряду чисел 0, 1, … , a2—1 ровно a2— φ(a2) чисел не будут являться взаимно простыми с a2. То есть среди чисел 0, 1, … , a1a2—1 не взаимно простыми одновременно и с a1 , и с a2 будут являться (a1—φ(a1))(a2—φ(a2)) чисел.

Таким образом, общее количество взаимно простых с a1a2 среди натуральных чисел, меньших a1a2, есть

a1a2—(a1a2—φ(a1)a2+ a1a2—φ(a2)a1—(a1—φ(a1))(a2—φ(a2)))=

= a1a2— (a1a2—φ(a1)a2— φ(a2)a1+ φ(a1)a2+ φ(a2)a1— φ(a1)φ(a2))= φ(a1)φ(a2).

Итак, доказали, что функция Эйлера – мультипликативная.

†

Пример. Вычислим φ(28350322).

Решение.

Для того, чтобы вычислить значение функции Эйлера, необходимо найти каноническое разложение аргумента.

28350322=2·14175161=2·7·2025023=2·72·289289=2·73·41327=

=2·73·11·3757=2·73·11·13·289=2·73·11·13·172.

φ(28350322)= φ(2·73·11·13·172)= φ(2) · φ(73)· φ(11)· φ(13)· φ(172)=

=1·72·6·10·12·17·16=9596160.
Ответ: φ(28 350 322)=9 596 160.

Тема. Отношение сравнений по модулю m. Полные и приведенные системы вычетов

План

1. Сравнения в кольце чисел.
2. Основные теоремы о сравнениях.
3. Полная и приведённая системы вычетов по модулю.

1. Сравнения в кольце целых чисел

Понятие сравнения было введено впервые Гауссом. Несмотря на свою кажущуюся простоту, это понятие очень важно и имеет много приложений.

Возьмем произвольное фиксированное натуральное число m и будем рассматривать остатки при делении на m различных целых чисел. При рассмотрении свойств этих остатков и произведении операций над ними удобно ввести понятие так называемого сравнения по модулю.

Определение. Целые числа a и b называются сравнимыми по модулю m, если разность $a-b$ делится на m, т.е. если $m|a-b$.

Таким образом, сравнение представляет собой соотношение между тремя числами a, b и m, причем m, играющее роль своего рода эталона сравнения, мы называем «модулем». Для краткости будем это соотношение между a, b и m записывать:

$$a \equiv b(mod\ m)$$

a и b будем называть соответственно левой и правой частями сравнения. Число m, стоящее под знаком модуля, будем всегда считать положительным, т.е. запись $mod\ m$ будет означать, что $m \geq 1$.

Если разность $a-b$ не делится на m, то мы будем записывать:

$a \not\equiv b(mod\ m)$.

Согласно определению, $a \equiv 0(mod\ m)$ означает, что a делится на m.

Примеры.

1. $m=3;\ 8 \equiv 5(mod\ 3)$, так как $8-5=3$ и 3 делится на 3.
2. $m=5;\ 12 \equiv 2(mod\ 5)$, так как $12-2=10$ и 10 делится на 5.
3. $m=2;\ 3 \equiv 7(mod\ 2)$, так как $3-7=-2$ и -4 делится на 2.

2. Основные теоремы о сравнениях

Теорема 1 (признак сравнимости двух чисел по модулю m). Два целых числа a и b сравнимы по модулю m тогда и только тогда, когда a и b имеют одинаковые остатки при делении на m.

Доказательство. Пусть остатки при делении a и b на m равны, т.е.

$$a = mq_1 + r, \quad (1.1)$$
$$b = mq_2 + r, \quad (1.2)$$

где $0 \leq r \leq m$.

Вычтем (1.2) из (1.1); получим $a-b=m(q_1-q_2)$,т.е. $a-b \vdots m$ или $a \equiv b(mod\ m)$.

Обратно, пусть $a \equiv b(mod\ m)$, это означает, что $a - b \vdots m$ или

$$a - b = mt, t \in Z. \quad (1.3)$$

Разделим b на m; получим $b = mq + r, 0 \leq r < m$. Подставив $b = mq + r$ в (1.3), будем иметь $a = m(q + t) + r$, т.е. при делении a на m получается тот же остаток, что и при делении b на m.

Пример 1. Определим, сравнимы ли числа 13 и 49 по модулю 6.

Решение. При делении 13 и 49 на 6 получаются одинаковые остатки $r_1 = r_2 = 1$. Следовательно, $13 \equiv 49(mod\ 6)$.

Определение. Два или несколько чисел, дающие при делении на m одинаковые остатки, называются равноостаточными или сравнимыми по модулю m.

Теорема 2. Отношение сравнимости рефлексивно: $a \equiv a(mod\ m)$.

Доказательство. a и a имеют одинаковые остатки при делении на m.

Теорема 3. Отношение сравнимости симметрично: если $a \equiv b(mod\ m)$, то $b \equiv a(mod\ m)$.

Доказательство. Если a и b имеют одинаковые остатки при делении на m, то остатки от деления b и a на m также равны.

Теорема 4. Отношение сравнимости транзитивно: если $a \equiv b(mod\ m)$, $b \equiv c(mod\ m)$, то $a \equiv c(mod\ m)$.

Доказательство. Если остатки от деления на m одинаковы у чисел a и b, а также у $чисел\ b$ и c, то a и c тоже имеют одинаковые остатки при делении на m.

Таким образом, отношение сравнимости есть отношение эквивалентности.

Теорема 5. Если $a \equiv b(mod\ m)$ и $k -$ произвольное целое число, то $ka \equiv kb(mod\ m)$.

Доказательство. Если $a \equiv b(mod\ m)$, то $m|a - b,\ m|k(a - b),\ m|ka - kb$, $ka \equiv kb(mod\ m)$.

Теорема 6. Если $ka \equiv kb(mod\ m)$ и$(k, m) = 1$, то $a \equiv b(mod\ m)$.

Доказательство. Если $ka \equiv kb(mod\ m)$, то $m\ |ka - kb,\ m\ |k(a - b)$, но тогда условие $(k, m) = 1$ дает $m\ |a - b$, т.е. $a \equiv b(mod\ m)$.

Теорема 7. Если $a \equiv b(mod\ m)$ и $k -$ произвольное натуральное число, то $ka \equiv kb(mod\ km)$.

Доказательство. Если $a \equiv b(mod\ m)$, то $m|\ a - b, km|\ ka - kb, ka \equiv kb(mod\ km)$.

Теорема 8. Если $ka \equiv kb(mod\ km)$, где k и $m -$ произвольные натуральные числа, то $a \equiv b(mod\ m)$.

Доказательство. Если $ka \equiv kb(mod\ km)$, то $km\ |ka - kb, km\ |k(a - b)$, $k -$ натуральное $(k \neq 0)$, тогда $m\ |a - b, a \equiv b(mod\ m)$.

Теорема 9. Если $a \equiv b(mod\ m),\ c \equiv d(mod\ m)$, то $a + c \equiv b + d(mod\ m)$ и $a - c \equiv b - d(mod\ m)$.

Доказательство. Если $a \equiv b(mod\, m)$ и $c \equiv d(mod\, m)$, то $m|a-b$ и $m|c-d$. Получим, что $m|(a-b) \pm (c-d),\ m|(a \pm c) - (b \pm d), a \pm c \equiv b \pm d(mod\, m)$.

Теорема 9'. Если $a_1 \equiv b_1(mod\, m), a_2 \equiv b_2(mod\, m), \dots, a_n \equiv b_n(mod\, m)$, то $a_1 + a_2 + \cdots + a_n \equiv b_1 + b_2 + \cdots + b_n(mod\, m)$.

Теорема 10. Если $a \equiv b(mod\, m)$ *и* $c \equiv d(mod\, m)$, то $ac \equiv bd(mod\, m)$.

Доказательство. Если $a \equiv b(mod\, m)$ и $c \equiv d(mod\, m)$, то $ac \equiv bc(mod\, m)$ и $bc \equiv bd(mod\, m)$. Тогда по транзитивности сравнений получим, что $ac \equiv bd(mod\, m)$.

Теорема 10'.

Если $a_1 \equiv b_1(mod\, m), a_2 \equiv b_2(mod\, m), \dots, a_n \equiv b_n(mod\, m)$, то $a_1 \dots a_n \equiv b_1 \dots b_n(mod\, m)$.

Доказательство. Последовательно применяя теорему 7, получим:

$a_1 a_2 a_3 \dots a_n \equiv b_1 a_2 a_3 \dots a_n \equiv b_1 b_2 a_3 \dots a_n \equiv \cdots \equiv b_1 b_2 b_3 \dots b_n(mod\, m)$.

Теорема 11. Если $a \equiv b(mod\, m)$, то при любом целом $n \geq 0$, $a^n \equiv b^n(mod\, m)$.

Доказательство. При $n = 0$ утверждение верно по теореме 2, а при $n \geq 1$ оно верно согласно теореме 10', если $a_1 = \cdots = a_n = a$ и $b_1 = \cdots = b_n = b$.

Переход от сравнений $a \equiv b(mod\, m), c \equiv d(mod\, m)$ к сравнениям

$a \pm c \equiv b \pm d(mod\, m), ac \equiv bd(mod\, m), a^n \equiv b^n(mod\, m)$

будем называть соответственно сложением (вычитанием), умножением, возведением в степень сравнений.

Так как из сравнения $c \equiv d(mod\, m)$ следует $d \equiv c(mod\, m)$, то из сравнений $a \equiv b(mod\, m)$ и $c \equiv d(mod\, m)$ следует также, что $a \pm d \equiv b \pm c(mod\, m)$ и $ad \equiv bc(mod\, m)$.

Теорема 12. Если $a \equiv b(mod\, m)$ и $f(x) = c_0 + c_1 x + \cdots + c_n x^n -$ произвольный многочлен с целыми коэффициентами, то $f(a) \equiv f(b)(mod\, m)$.

Доказательство. Если $a \equiv b(mod\, m)$, то, согласно теоремам 7 и 11, имеем:

$a^s \equiv b^s\,(mod\, m), c_s b^s\,(mod\, m)$ при $s = 0,1, \dots, n$.

По теореме 9', получаем $c_0 + c_1 a + \cdots + c_n a^n \equiv d_0 + c_1 b + \cdots + c_n b^n(mod\, m)$,

т.е. $f(a) \equiv f(b)(mod\, m)$.

Теорема 12'. Если $a_1 \equiv b_1(mod\, m), a_2 \equiv b_2(mod\, m), \dots, a_t \equiv b_t(mod\, m)$ и $f(x_1, \dots, x_t) -$ многочлен с целыми коэффициентами, то

$f(a_1, \dots, a_t) \equiv f(b_1, \dots, b_t)(mod\, m)$.

Теорема 13. Любое слагаемое левой или правой части сравнения можно перенести с противоположным знаком в другую часть.

Доказательство. Ввиду симметричности отношения сравнения достаточно рассмотреть случай, когда дано сравнение $a + b \equiv c(mod\, m)$. Складывая это сравнение со сравнением $-b \equiv -b(mod\, m)$, получаем $a \equiv c - b(mod\, m)$.

Следствие. В левой и правой частях сравнения можно добавлять или отбрасывать одно и то же слагаемое.

Теорема 14. В сравнении можно отбрасывать или добавлять слагаемые, делящиеся на модуль.

Доказательство. Если $a + c \equiv b(mod\, m)$ и $m|c$, т.е. $-c \equiv 0(mod\, m)$, то, складывая эти сравнения, получаем $a \equiv b(mod\, m)$. Аналогично из $a \equiv b(mod\, m)$ и $m|c$ получаем $a + c \equiv b(mod\, m)$.

Поскольку левую и правую части сравнения можно менять местами, утверждение верно и для слагаемых правой части.

Теорема 15. Если $a \equiv b(mod\, m)$ и $d|m$, то $a \equiv b(mod\, m)$.

Доказательство. Если $a \equiv b(mod\, m)$, то $m|a - b$. Из $d|m$, $m|a - b$ в силу транзитивности отношения делимости получаем $d|a - b$, $a \equiv b(mod\, m)$.

Теорема 16. Если $a \equiv b(mod\, m)$, то множество общих делителей a и m совпадает с множеством общих делителей b и m. В частности, $(a, m) = (b, m)$.

Доказательство. Если $a \equiv b(mod\, m)$, то $m|a - b$, $a - b = mq$, $b = a - mq$, любой общий делитель δ чисел a и m является общим делителем чисел b и m, и, наоборот, если $\delta|b$ и $\delta|m$, то $\delta|a$.

Поскольку пара a, m и пара b, m имеют одни и те же общие делители, то и $(a, m) = (b, m)$.

Теорема 17. Если $a \equiv b(mod\, m_1)$, $a \equiv b(mod\, m_1), \dots, a \equiv b(mod\, m_s)$, то $a \equiv b(mod\, m)$, где $m = [m_1, m_2, \dots, m_s]$.

Доказательство. Если $a \equiv b(mod\, m_1)$, $a \equiv b(mod\, m_1), \dots, a \equiv b(mod\, m_s)$, то $a \equiv b(mod\, m)$, то $m_1|a - b, m_2|a - b, \dots, m_s|a - b$ и, согласно свойствам наименьшего общего кратного, $m|a - b$.

3. Полная и приведённая системы вычетов

Определение. Числа $a_1, a_2, \dots, a_k$ образуют приведенную систему вычетов по модулю m, если они взаимно просты с m и любое целое число, взаимно простое с m, сравнимо с одним и только одним из этих чисел по модулю m.

Пример. Приведенная система вычетов по модулю 10: 1,3,7,9.

Лемма. Все приведенные системы вычетов по модулю m состоят из одного и того же количества чисел, которое обозначается $\varphi(m)$ — функция Эйлера.

Доказательство. Действительно, пусть есть две приведенные системы вычетов по модулю m, состоящие из разного количества чисел:

$a_1, a_2, \dots, a_k, \quad b_1, b_2, \dots, b_l \quad k > l.$

Тогда так как числа $b_1, b_2, \dots, b_l$ образуют приведенную систему вычетов по модулю m, то каждое из чисел $a_1, \dots, a_k$ сравнимо с одним и только одним из этих чисел. Поскольку $k > l$, то, по принципу Дирихле, по крайней мере два числа из $a_1, \dots, a_k$ будут сравнимы с каким-то числом b_j, а значит, будут сравнимы между собой по модулю m. А это противоречит тому, что $a_1, \dots, a_k$ — приведенная система вычетов по модулю m. Значит, $k = l$.

Докажем теперь, что $k = \varphi(m)$. В самом деле, числа, меньшие m и взаимно простые с m, образуют приведенную систему вычетов по модулю m.

Функция Эйлера

Функция Эйлера $\varphi(n)$ ставит в соответствие любому натуральному числу n количество натуральных чисел, меньших n и взаимно простых с n.

Общая формула для вычисления значения функции Эйлера от произвольного аргумента: если $n = p^k$, где p – простое число, $k \in N$, то

$$\varphi(n)=\varphi\left(p^k\right)=p^k-p^{k-1}=p^k\left(1-\frac{1}{p}\right).$$

Если p – простое число, то $\varphi(p)=p-1$.

Если $n=p_1^{k_1}p_2^{k_2}...p_m^{k_m}$ – каноническое разложение натурального числа n, то

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_m}\right)=\left(p_1^{k_1}-p_1^{k_1-1}\right)\left(p_2^{k_2}-p_2^{k_2-1}\right)...\left(p_m^{k_m}-p_m^{k_m-1}\right).$$

Теорема Эйлера. Если $(a,m)=1$, то $a^{\varphi(m)}\equiv 1(\mathrm{mod}\, m)$.

*Теорема Ферма***.** Если p – простое число и $(a,p)=1$, то $a^{p-1}\equiv 1(\mathrm{mod}\, p)$.

Тема. Сравнения с неизвестной

План

1. Сравнения первой степени с одной переменной.
2. Разные методы решения сравнений первой степени с одно переменной.
3. Сравнения высших степеней и методы их решения.
4. Системы сравнений.

1. Сравнения первой степени с одной переменной

Определение 1. Сравнением первой степени с одной переменной называется сравнение вида

$$ax \equiv b(mod\ m), \quad (2.1)$$

где $m \in N, a, b \in Z, a \vdots m.$

Будем говорить, что целое число c удовлетворяет сравнению (2.1), если $ax \equiv b(mod\ m)$ —верное сравнение.

Теорема 1. Если целое число c удовлетворяет сравнению (*), то и весь класс $\bar{c}$ по $mod\ m$ состоит из чисел, удовлетворяющих этому сравнению.

Определение 2. Решением сравнения (2.1) называется класс вычетов по $mod\ m$, которые при подстановке в сравнение обращают его в верное сравнение.

Число решений сравнения по $mod\ m -$ это число решений этого сравнения в какой-либо полной системе вычетов по модулю m.

Примеры.

1) $3x \equiv 2(mod\ m)$. Полная система наименьших неотрицательных вычетов по модулю 7: $\{0,1,2,3,4,5,6\}$ (так как классы вычетов будут $\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}$).

Если $x=0$, то $3\cdot 0-2=-2, -2 \vdots 7$, следовательно, $x=0$ не удовлетворяет сравнению.

Если $x=1$, то $3\cdot 1-2=1, 1 \vdots 7$, следовательно, $x=1$ не удовлетворяет сравнению.

Если $x=2$, то $3\cdot 2-2=4, 4 \vdots 7$, следовательно, $x=2$ не удовлетворяет сравнению.

Если $x=3$, то $3\cdot 3-2=7, 7 \vdots 7$, следовательно, $x=3$ удовлетворяет сравнению, а поэтому класс вычетов $\bar{3}$ по $\mathrm{mod}\ 7$ является решением сравнения.

Если $x=4$, то $3\cdot 4-2=10, 10 \vdots 7$, следовательно, $x=4$ не удовлетворяет сравнению.

Если $x=5$, то $3\cdot 5-2=13, 13 \vdots 7$, следовательно, $x=5$ не удовлетворяет сравнению.

Если $x = 6$, то $3 \cdot 6 - 2 = 16, 16 \vdots 7$, следовательно, $x = 6$ не удовлетворяет сравнению.

Таким образом, сравнение имеет одно решение $\overline{3} \bmod 7$ или, в другом виде, $x \equiv 3(mod\ 7)$.

Ответ: $x \equiv 3(mod\ 7)$.

2) $5x \equiv 3(mod\ 10)$.

Классы вычетов по mod 10: $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}$. Полная система наименьших по абсолютной величине вычетов по mod 10: {0, 1, 2, 3, 4, 5, -4, -3, -2, -1}. Проверим для каждого из этих чисел, будет ли выполнено условие $(5x - 3) \vdots 10$. Имеем:

$$x = 0, -3 \vdots 10 \quad x = 5, 22 \vdots 10$$
$$x = 1, 2 \vdots 10 \quad x = 6, 27 \vdots 10$$
$$x = 2, 7 \vdots 10 \quad x = 7, 32 \vdots 10$$
$$x = 3, 12 \vdots 10 \quad x = 8, 37 \vdots 10$$
$$x = 4, 17 \vdots 10 \quad x = 9, 42 \vdots 10$$

Получили, что ни одно из чисел, взятых из полной системы вычетов, не удовлетворяет сравнению, следовательно, данное сравнение не имеет решения.

Ответ: $\emptyset$.

Теорема 1. Пусть дано сравнение

$$ax \equiv b(mod\ m), \quad (2.4)$$

$НОД(a, m) = d, d > 1, b$ не $\vdots\ d$. Тогда сравнение (2.4) не имеет решения.

Рассмотрим сравнение:

$$ax \equiv b(mod\ m), \quad (2.7)$$

где $m \in N$, $a, b \in Z$, $a \vdots m$. Если $НОД(a, m) = d, d > 1$ и b не $\vdots\ d$, то сравнение не имеет решения.

Пусть теперь $b \vdots d$, тогда будем иметь: $a = da_1, a_1 \in Z$, $b = db_1, b_1 \in Z$, $m = dm_1, m_1 \in Z, НОД(a_1, m_1) = 1$.

Поэтому получим: $(da_1)x \equiv db_1(mod\ dm_1), НОД(a_1, m_1) = 1$. Так как по определению НОД число $d \in N$, то из последнего сравнения получим:

$a_1 x \equiv b_1(mod\ m_1)$, где $НОД(a_1, m_1) = 1$.

Таким образом, полагая в (1), что $НОД(a, m) = d, d > 1, b \vdots d$, мы пришли к сравнению такого же вида, но с условием: $НОД(a_1, m_1) = 1$. Исследуем этот случай.

Теорема. Пусть дано сравнение (2.7) и $НОД(a, m) = 1$. Тогда сравнение (2.7) имеет единственное решение.

Пример 1. $5x \equiv 2(mod\ 9)$. НОД (5,9) = 1, следовательно, сравнение имеет одно решение. Найдем его способом «подбора», то есть перебирая все числа из полной системы вычетов по *mod m*: {0, 1, 2, 3, 4, 5, 6, 7, 8} (*m = 9*).

$x = 0, \quad 5x - 2 = -2, \quad -2$ не $\vdots\ 9;$

$x = 1, \quad 3$ не $\vdots\ 9; \quad x = 2, \quad 8$ не $\vdots\ 9; \quad x = 3, \quad 13$ не $\vdots\ 9; \quad x = 4, \quad 18 \vdots 9;$

следовательно, $x = 4$ удовлетворяет сравнению, поэтому решением будет класс вычетов $\overline{4}$ по *mod m* или, по-другому, $x \equiv 4(mod\ m)$.

А так как данное сравнение имеет 1 решение, то остальные числа x: 5, 6, 7, 8 проверять уже не надо.

Ответ: $x \equiv 4(mod\ m)$.

Для нахождения решения сравнения первой степени с одной переменной (если оно есть) существует несколько способов:

1) подбора;
2) преобразования коэффициентов;
3) Эйлера (с помощью функции Эйлера);
4) цепных дробей.

Если модуль m является простым числом, то есть $ax \equiv b(mod\ p)$, число a не делится на p, то сравнение имеет единственное решение. Следовательно, множество классов вычетов $\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{p-1}\}$ образует поле по отношению сложения и умножения классов вычетов. Его обозначают через Z_p.

Пример 2. Вычислить остаток при делении $(3^{100} + 5^{100})^{100}$ на 15.

Решение. Сравнение $3^{100} \equiv x(mod\ 15)$ для применения теоремы Эйлера сократим на 3 (очевидно, $(x \vdots 3) : 3^{99} \equiv \frac{x}{3}(mod\ 5)$.

Так как $\varphi(5) = 4$, то по теореме Ферма показатель 99 можно уменьшить по модулю 4. Получаем, что из $99 \equiv 3\ (mod\ 4)$ следует:

$3^3 \equiv \frac{x}{3}(mod\ 5), \frac{x}{3} \equiv 27(mod\ 5) \equiv 2$.

Умножаем на 3 обе части сравнения и модуль: $x \equiv 6\ (mod\ 15)$, т.е.

$3^{100} = 6\ (mod\ 15)$.

Аналогично вычисляем $5^{100} = 10(mod\ 15)$. Отсюда почленным сложением сравнений найдем: $3^{100} + 5^{100} \equiv 6 + 10 = 16 \equiv 1\ (mod\ 15)$. Затем, возводя в 100-ю степень обе части сравнения, получаем $(3^{100} + 5^{100})^{100}\ x \equiv 1\ (mod\ 15)$.

Ответ: 1.

Пример 3. Разложить $322/159$ в цепную дробь. Проверить разложение, свернув цепную дробь последовательным вычислением подходящих дробей.

Решение. Найдём элементы цепной дроби как частные в алгоритме Евклида:

$$322/159 = 2 + \cfrac{1}{39 + \cfrac{1}{1 + \frac{1}{3}}}.$$

Сделаем сокращённую запись: $322/159 = (2; 39; 1; 3)$.

Пусть q_k обозначает $k-$ый элемент цепной дроби, $\delta_k -$ её k –ю подходящую дробь, $P_k -$ числитель, $Q_k -$ знаменатель $k-$й подходящей дроби. Будем вычислять подходящие дроби по рекуррентной формуле

$$\delta_k = \frac{q_k P_{k-1} + P_{k-2}}{q_k Q_{k-1} + Q_{k-2}},$$

используя схему:

q_i		2	39	1	3
P_i	1	2	79	81	322
Q_i	0	1	39	40	159

Как видно, последняя подходящая дробь совпадает с исходным числом.

Замечание. Непосредственное сворачивание конечной цепной дроби «снизу вверх» обычно громоздко:

$$2+\frac{1}{39+\frac{1}{1+\frac{1}{3}}}=2+\frac{1}{39+\frac{3}{4}}=2+\frac{4}{159}=\frac{322}{159}.$$

Метод преобразования коэффициентов

Теорема 1. Пусть дано сравнение:

$$ax \equiv b(mod\ m), \quad (2.8)$$

НОД$(a,m)=1, k\in Z$ и $(b+mk)\vdots a$. Тогда класс вычетов $\overline{x_0}=\overline{\left(\frac{b+mk}{a}\right)}$ по модулю *m* является решением сравнения (2.8).

Примеры.

1) $5x \equiv 2(mod\ 9).$

НОД$(5,9)=1$, поэтому сравнение имеет единственное решение.

$5x \equiv 2+9k(mod\ 9), k\in Z.$

Найдем такое целое число *k*, чтобы $2+9k$ делилось на 5. Например, $k=2:(2+9\cdot 2=20, 20:5)$. Тогда получим: $5x \equiv 2+9\cdot 2(mod\ 9)$, $5x \equiv 20(mod\ 9)$.

$x \equiv 4(mod\ 9)$

Проверка. $4\cdot 5-2=18$, 18 делится на 9, поэтому при подстановке в сравнение вместо переменной значения 4, получим верное сравнение, следовательно, число 4 удовлетворяет сравнению, поэтому класс целых чисел, содержащий число 4, является решением сравнения.

Ответ: $x \equiv 4(mod\ 9).$

2) $3x \equiv 2(mod\ 7)$

НОД$(3,7)=1$, следовательно, сравнение имеет одно решение.

$3x \equiv 2+7k(mod\ 7), k\in Z$ (при $k=1$ будет $2+7k=9,\ 9:3$)

$3x \equiv 2+7\cdot 1(mod\ 7)$, $3x \equiv 9(mod\ 7), x \equiv 3(mod\ 7).$

Ответ: $x \equiv 3(mod\ 7).$

Метод Эйлера

Получим метод решения сравнения

$$ax \equiv b(mod\ m), \quad (2.9)$$

с помощью функции Эйлера.

Теорема 1. Пусть дано сравнение (2.9), НОД$(a,m)=1$. Тогда класс вычетов

$\overline{x_0}=\overline{b\cdot a^{\varphi(m)-1}}$

по модулю *m* является решением сравнения (2.9), где $\varphi(m)$ – функция Эйлера.

Пример.

1) $3x \equiv 2(mod\ 5). a=3, b=2, m=5.$

НОД$(3,5) = 1$, следовательно, сравнение имеет одно решение, $x \equiv 2 \cdot 3^{\varphi(5)-1}(mod\ 5)$.

Преобразуем произведение $2 \cdot 3^{\varphi(5)-1}$. $5-$ простое число, то $\varphi(5) = 5 - 1 = 4$. Поэтому $2 \cdot 3^{\varphi(5)-1} = 2 \cdot 3^{4-1} = 2 \cdot 3^3 = 54$.

$x \equiv 54(mod\ 5)$, $x \equiv 4(mod\ 5), x \equiv -1(mod\ 5)$.

Ответ: $x \equiv -1(mod\ 5)$.

Сравнения высших степеней

Определение 1. Сравнением *n*-й степени с одной переменной называется сравнение вида

$$f(x) \equiv 0(mod\ m), \quad (3.1)$$

где $m \in N, f(x) -$ многочлен с целыми коэффициентами:

$$f(x) \equiv a_n x^n + \cdots + a_1 x + a_0, \quad (3.2)$$

причем, a_n не $\vdots\ m$.

Целое число c удовлетворяет сравнению (3.1), если сравнение $f(\mathrm{c}) \equiv 0(mod\ m)$ является верным сравнением.

Теорема 1. Пусть дано сравнение (3.1) и целое число c удовлетворяет сравнению (3.1). Тогда весь класс $\bar{c}$ по mod *m* состоит из чисел, удовлетворяющих сравнению (3.1).

Доказательство. Число c удовлетворяет сравнению (3.1), следовательно, $f(c) \equiv 0(mod\ m) -$ верное сравнение. Для любого $b \in \bar{c}$ всегда $b \equiv c(mod\ m)$. Но тогда по свойству сравнений $f(b) \equiv f(c)(mod\ m)$, поэтому по транзитивности получим, что $f(b) \equiv 0(mod\ m)$, отсюда следует, что число b удовлетворяет сравнению (3.1). А так как $b -$ произвольное из $\bar{c}$, то, следовательно, весь класс вычетов $\bar{c}$ по mod *m* состоит из чисел, удовлетворяющих сравнению (3.1). Теорема 1 доказана.

Определение 2. Решением сравнения (3.1) называется класс вычетов по модулю *m*, состоящий из чисел, удовлетворяющих сравнению (3.1).

Если класс $\bar{c}$ mod *m* является решением сравнения (3.1), то будем говорить, что класс $\bar{c}$ удовлетворяет сравнению (3.1). Числом решений сравнения (3.1) называется число классов вычетов по mod *m*, удовлетворяющих сравнению (3.1).

Задача нахождения чисел, удовлетворяющих сравнению (3.1), сводится к нахождению классов, удовлетворяющих уравнению $f(\bar{x}) = \bar{0}$.

Действительно:

- так как $f(c) \equiv 0(mod\ m)$ верно, то $\overline{f(c)} = \bar{0}$, но $\overline{f(c)} = f(\bar{c})$;
- обратно, если $f(\bar{c}) = \bar{0}$, то $\overline{f(c)} = \bar{0}$, следовательно, $f(c) \equiv 0(mod\ m)$.

Чтобы решить сравнение $f(x) \equiv 0(mod\ m)$, можно

1) взять любую полную систему вычетов по mod *m*:
$x_0, x_1, \ldots, x_{m-1}$, где $x_0 \in \bar{0}, x_1 \in \bar{1}, \ldots, x_{m-1} \in \overline{m-1}$;

2) вычислить $f(x_0), \ldots, f(x_{m-1})$;

3) взять те числа x_i, при которых сравнение $f(x_i) \equiv 0(mod\, m)$ является верным, то есть $f(x_i) : m$. Соответствующие классы $\overline{x_i}$, дадут все решения сравнения.

Удобнее брать полную систему наименьших по абсолютной величине вычетов по mod m. Если сравнение имеет несколько решений $\overline{c_1}, \dots, \overline{c_s}$, то эти решения можно записывать в виде $x \equiv c_1, \dots, c_s(mod\, m)$(то есть x принимает любые значения, сравнимые с одним из чисел $c_1, \dots, c_s$) вместо записи $x \equiv c_1(mod\, m), \dots, x \equiv c_s(mod\, m)$.

Примеры.

1) $x^3 - 2x + 6 \equiv 0$(mod 11).

$\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}$ классы вычетов по mod 11.

$x \equiv 5(mod\ 11) -$ решение сравнения

2) $x^4 + 2x^3 + 6 \equiv 0(mod\, 8)$.

$\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}$. Сравнение не имеет решения.

3) $x^4 - x^3 - x^2 + 5x - 2 \equiv 0(mod\, 6)$.

$\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, 2, -1;\ x \equiv 2(mod\, 6), x \equiv -1(mod\, 6) -$ решения сравнения.

Ответ: $x \equiv -1,2(mod\, 6)$

Задача нахождения решения сравнения $f(x) \equiv 0(mod\, m)$ проще, чем рассматриваемая в курсе алгебры задача нахождения решения уравнения $f(x) = 0$. Так как решая уравнение в некотором бесконечном множестве (R, C) нельзя перебрать все числа x. А решая сравнение $f(x) \equiv 0(mod\, m)$, ищем решение в конечном кольце Z_m классов вычетов по mod *m*. Следовательно, с помощью конечного числа операций можно найти все решения. Но надо заметить, что при больших *m* будут громоздкие вычисления, поэтому надо изучить способы, позволяющие определить число решений, а иногда и способы нахождения решения с помощью возможно меньшего числа операций.

Сравнения вида $f(x) \equiv g(x)(mod\, m)$

Рассмотрим сравнение с одной переменной вида

$$f(x) \equiv g(x)(mod\, m) \quad (3.3)$$

где $f(x)g(x) \in Z[x], m \in N$, коэффициенты при старшем члене $f(x)$ и $g(x)$ не делятся на m.

Определение 1. Решением сравнения (3.3) называется класс вычетов по *mod m*, состоящий из чисел, удовлетворяющих этому сравнению.

Теорема 1. Пусть $f(x)$ и $g(x)$ – многочлены с целыми коэффициентами и целое число a удовлетворяет сравнению (3.3). Тогда весь класс вычетов $\overline{a}$(*mod m)* состоит из чисел, удовлетворяющих этому сравнению.

Определение 2. Два сравнения

$$f_1(x) \equiv g_1(x)(mod\, m_1) \quad (3.4)$$

$$f_2(x) \equiv g_2(x)(mod\, m_2) \quad (3.5)$$

называются эквивалентными, если множество чисел, удовлетворяющих одному из них, совпадает с множеством чисел, удовлетворяющих другому сравнению.

Если $m_1 = m_2 = m$ и сравнения (3.4) и (3.5) имеют одни и те же решения, то получим два эквивалентных сравнения по $mod\, m$.

Эквивалентные сравнения могут иметь разную степень.

Пример. $2x+1 \equiv 0(mod\ 3), x^3-1 \equiv 0(mod\ 3)$.

Решение первого сравнения: $x \equiv 1(mod\ 3)$, решением второго сравнения тоже будет класс вычетов $x \equiv 1(mod\ 3)$. Следовательно, они эквивалентны. Но степени их различны (степень первого сравнения равна 1, степень второго – 3).

Теорема. Пусть дано сравнение

$$f(x) \equiv g(x)(mod\ m), \quad (3.6)$$

где $f(x), g(x) \in Z[x], m \in N$.

Тогда имеют место следующие утверждения:

1) Если к обеим частям сравнения (3.6) прибавить любой многочлен $t(x) \in Z[x]$ то получится сравнение, эквивалентное сравнению (3.6).

2) Если обе части сравнения (3.6) умножить на одно и то же целое число, взаимно простое с модулем, то получится сравнение, эквивалентное сравнению (3.6).

3) Если обе части сравнения и модуль умножить на одно и то же натуральное число k, то получится сравнение, эквивалентное сравнению (3.6).

Теорема 2. Пусть даны сравнения

$f(x) \equiv 0(mod\ m)$ и $g(x) \equiv 0(mod\ m)$, где $f(x) = a_n x^n + \cdots + a_0$, $g(x) = b_n x^n + \cdots + b_0$ и пусть $a_n \equiv b_n(mod\ m), \ldots, a_0 \equiv b_0(mod\ m)$.

Тогда сравнения эквивалентны.

Из доказанной теоремы, в частности, следует, что сравнение заменится эквивалентным, если отбросить (или добавить) слагаемое с коэффициентами, делящимися на модуль.

3. Сравнения по простому модулю с одним неизвестным

Переходя от сравнений 1-й степени к сравнениям более высоких степеней, целесообразно сначала рассмотреть тот случай, когда модуль – простое число. В этом случае имеется ряд весьма важных теорем, которые, вообще говоря, неверны для составных модулей. Вместе с тем теория сравнений по простому модулю является основой, на которой строится изучение сравнений по составному модулю.

Во всей этой главе буквой p будем обозначать модуль, представляющий собой простое число.

Теорема 1. Если $p \nmid c_0$, то сравнение

$$c_0 x^n + c_1 x^{n-1} + \cdots + c_n \equiv 0(mod\ p)$$

может быть заменено эквивалентным сравнением с коэффициентом при старшем члене, равном единице.

Пример 1. Заменить сравнение

$$27x^3 + 14x^2 - 10x + 13 \equiv 0(mod\ 59)$$

эквивалентным сравнением с коэффициентом при старшем члене, равным 1.

Решаем сравнение $27y_0 \equiv 1(mod\ 59)$ и находим $y_0 = 35$. Данное нам сравнение эквивалентно сравнению

$$x^3 + 14 \cdot 35x^2 - 10 \cdot 35x + 13 \cdot 35 \equiv 0(mod\ 59),$$

т.е. сравнению $x^3 + 18x^2 + 4x - 17 \equiv 0(mod\ 59)$.

Теорема 2. Если $f(x)$и $g(x)$ – многочлены с целыми коэффициентами, то сравнения по простому модулю

$$f(x) \equiv 0(mod\ p) \quad (3.15)$$

$$f(x) - (x^p - x)g(x) \equiv 0(mod\ p) \quad (3.16)$$

эквивалентны.

Теорема 3. Сравнение по простому модулю p, степень которого больше, чем этот модуль или равна ему, может быть заменено эквивалентным сравнением степени, меньшей p.

Пример 2. Сравнение $x^{16}+3x^8-5x^7-x^4+6x-2\equiv 0(mod\ 7)$ заменить эквивалентным сравнением степени, меньшей чем 7.

Решение. Мы получим эквивалентное сравнение, если заменим x^{16} на $x^{16-2\cdot 6}=x^4$, x^8 на x^2, x^7 на x. Таким образом, заданное сравнение эквивалентно сравнению

$$(x^4+3x^2-5x)-x^4+6x-2\equiv 0(mod\ 7),$$

т.е. сравнению $3x^2+x-2\equiv 0(mod\ 7)$.

Теорема 4. Если $f(x),\ g(x),\ h(x),\ r(x)$ – многочлены с целыми коэффициентами: $f(x)=g(x)h(x)+r(x)$, и все коэффициенты $r(x)$ делятся на простое число p, то любое решение сравнения

$$f(x)\equiv 0(mod\ p) \quad (3.17)$$

является решением, по крайней мере, одного из сравнений:

$$g(x)\equiv 0(mod\ p), h(x)\equiv 0(mod\ p). \quad (3.18)$$

Пример 3. В сравнении $x^4+18x^2+5\equiv 0(mod\ 31)$ левую часть можно представить в виде $(x^2-4)(x^2-9)+(31x^2-31)$, и мы находим все решения этого сравнения, решая сравнения: $x^2-4\equiv 0(mod\ 31)$, $x^2-9\equiv 0(mod\ 31)$, т.е. $x\equiv\pm 2(mod\ 31)$ и $x\equiv\pm 3(mod\ 31)$. Все эти четыре класса удовлетворяют нашему сравнению.

Для составных модулей эта теорема неверна. Например, сравнению

$$x^2+4x=x(x+4)\equiv 0(mod\ 12)$$

удовлетворяет класс $\overline{6}$, не являющийся решением ни одного из сравнений:

$$x\equiv 0(mod\ 12),\ x+4\equiv 0(mod\ 12).$$

Теорема 5. Сравнение степени n по простому модулю p с коэффициентом при старшем члене, не делящимся на p, может иметь не больше чем n решений.

Пример 4. $x_0=31$ удовлетворяет сравнению $11x^2\equiv 65(mod\ 103)$. Найти все решения этого сравнения.

Очевидно, что вместе с классом $\overline{31}$ этому сравнению удовлетворяет и класс $-\overline{31}$. Коэффициент при старшем члене 11 не делится на простой модуль 103, поэтому сравнение не может иметь больше двух решений.

Ответ. $x\equiv\pm 31(mod\ 103)$.

Для составных модулей эта теорема неверна. Сравнение степени n по составному модулю с коэффициентом при старшем члене, не делящемся на модуль или даже взаимно простом с модулем, может иметь больше чем n решений. Например, сравнение $x^2-3x+2\equiv 0(mod\ 6)$ имеет 4 решения: $\overline{1},\overline{2},\overline{4},\overline{5}$.

Теорема 6. Если сравнение степени n по простому модулю p имеет больше чем n решений, то все коэффициенты сравнения делятся на p.

Теорема 7. Пусть $f(x)=x^n+c_1x^{n-1}+\cdots+c_n$ – многочлен с целыми коэффициентами и свободным членом $c_n\not\equiv 0(mod\ p)$, где p – простое число, причем

$p \geq n$. Сравнение $f(x) \equiv 0(mod\ p)$ имеет n решений тогда и только тогда, когда все коэффициенты остатка от деления $x^{p-1} - 1$ на $f(x)$ кратны p.

Пример 5. Сравнению $x^3 \equiv 1(mod\ 13)$ удовлетворяют классы $\overline{1}$ и $\overline{3}$. Имеет ли это сравнение еще одно решение?

Делим $x^{12} - 1$ на $x^3 - 1$, находим: $x^{12} - 1 = (x^3 - 1)(x^9 + x^6 + x + 1)$,

так что $r(x) = 0$ и, следовательно, это сравнение имеет три решения.

4. Системы сравнений

Систему сравнений первой степени с одним и тем же неизвестным, но с разными модулями, запишем в общем виде так:

$$\begin{cases} a_1 x \equiv b_1 (mod\ m_1), \\ a_2 x \equiv b_2 (mod\ m_2), \\ \dots\dots\dots\dots\dots\dots \\ a_n x \equiv b_n (mod\ m_n), \end{cases} \quad (4.1)$$

Общий способ (способ последовательного решения) состоит в том, что сначала находится $x \equiv \alpha (mod\ m)$ из первого сравнения, где α – наименьший неотрицательный или абсолютно наименьший вычет по модулю m_1 и берется класс чисел

$$x \equiv m_1 t + \alpha, \quad (*')$$

удовлетворяющих первому сравнению.

Затем это значение x подставляется во второе сравнение, что дает

$$a_2(m_1 t + \alpha) \equiv b_2 (mod\ m_2),$$

откуда находится t опять в виде класса чисел и подставляется в равенство $(*')$.

В результате получается значение x в виде класса чисел, удовлетворяющих первым двум сравнениям системы. Дальше это значение x подставляется в третье сравнение системы, так же находится t_1, затем находится x и подставляется в четвертое сравнение системы и т.д.

Заметим, что можно идти и несколько иным путем: сначала решается каждое из сравнений системы и представляется в виде:

$$\begin{cases} x \equiv \alpha_1 (mod\ m_1), \\ x \equiv \alpha_2 (mod\ m_2), \\ \dots\dots\dots\dots\dots\dots \\ x \equiv \alpha_n (mod\ m_n), \end{cases} \quad (4.2)$$

а затем поступают описанным способом.

Если окажется, что хотя бы одно из сравнений системы (4.1) не имеет решения или сравнение относительно t_1 в описанном способе неразрешимо, то система (4.1) не имеет решения.

Если для сравнений $a_1 x \equiv b_1 (mod\ m_1)$ системы (4.1) $(a_i, m_i) = d_i$ и $d_i | b_i$ то, сокращая члены и модуль каждого сравнения на d_i получаем систему:

$$\begin{cases} \frac{a_1}{d_1}x \equiv \frac{b_1}{d_1}\left(mod\ \frac{m_1}{d_1}\right), \\ \frac{a_2}{d_2}x \equiv \frac{b_2}{d_2}\left(mod\ \frac{m_2}{d_2}\right), \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \frac{a_n}{d_n}x \equiv \frac{b_n}{d_n}\left(mod\ \frac{m_n}{d_n}\right), \end{cases} \quad (4.3)$$

эквивалентную (4.1).

Сравнения этой системы можно решить относительно x и свести решение системы (4.3) к решению системы:

$$\begin{cases} x \equiv \alpha_1\left(mod\ \frac{m_1}{d_1}\right), \\ x \equiv \alpha_2\left(mod\ \frac{m_2}{d_2}\right), \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ x \equiv \alpha_n\left(mod\ \frac{m_n}{d_n}\right), \end{cases} \quad (4.4)$$

Если в системе (4.2) модули $m_1, \dots, m_n$ попарно просты, то решение ее можно находить не указанным выше общим способом, а по формуле:

$$x_0 = \frac{M}{m_1}y_1\alpha_1 + \dots + \frac{M}{m_n}y_n\alpha_n,$$

где $M = [m_1, \dots, m_n]$ и $y_1, \dots, y_n$ есть решения сравнений:

$$\frac{M}{m_i}y_i \equiv 1(mod\ m_i).$$

Решением системы будет: $x \equiv x_0(mod\ M)$.

Этим способом можно решать и систему (4.4), если модули $\frac{m_1}{d_1}, \dots, \frac{m_n}{d_n}$ попарно просты.

Пример. Решить систему сравнений:

$$\begin{cases} x^2 + x + 7 \equiv 0(mod\ 9), \\ x^2 - x + 3 \equiv 0(mod\ 9). \end{cases}$$

Классы вычетов по $mod\ 9$: $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}$, при $x = -2$ имеем:

1) $(-2)^2 + 2 + 7 = 9,\ 9 : 9$, следовательно, $x = 2$ удовлетворяет первому сравнению системы,

2) $(-2)^2 + (-2) + 3 = 9,\ 9 : 9$, следовательно, $x = 2$ удовлетворяет второму сравнению системы.

Поэтому класс вычетов $x \equiv -2(mod\ 9)$ является решением системы. Можно записать этот класс иначе: прибавив к (-2) модуль 9, получим, что $x \equiv 7(mod\ 9)$.

Итак, данная система сравнений имеет решение $\bar{7}\ mod\ 9$.

Тема. Арифметические приложения теории сравнений

План

1. Арифметические действия и их свойства.

2. Проверка результатов арифметических действий.

1. Арифметические действия

К арифметическим действиям относятся:

– Сложение является начальным понятием, для которого невозможно дать строгое формальное определение. Тем не менее, чтобы придать этому действию некоторое разумное представление, мы скажем, что сложение – это операция нахождения суммы двух или нескольких чисел, где под суммой понимается общее количество единиц, содержащихся в рассматриваемых числах вместе. Эти числа называются слагаемыми. Например, 11 + 6 = 17. Здесь 11 и 6 – слагаемые, 17 – сумма. Если слагаемые поменять местами, то сумма не изменится: 11 + 6 = 17 и 6 + 11 = 17.

– Вычитание является действием, обратным к сложению, так как это операция нахождения одного из слагаемых по сумме и другому слагаемому. Вычесть из одного числа (уменьшаемого) другое (вычитаемое) - значит найти такое третье число (разность), которое при сложении с вычитаемым дает уменьшаемое: 17 – 6 = 11. Здесь 17 – уменьшаемое, 6 – вычитаемое, 11 – разность.

– Умножение. Умножить одно число n (множимое) на другое целое число m (множитель) – значит повторить множимое n в качестве слагаемого m раз. Результат умножения называется произведением. Запись операции умножения: n x m или n · m . Например, 12 x 4 = 12 + 12 + 12 + 12 = 48. Таким образом, 12 x 4 = 48 или 12 · 4 = 48. Здесь 12 – множимое, 4 – множитель, 48 – произведение. Если множимое n и множитель m поменять местами, то произведение не изменится. Например, 12 · 4 = 12 + 12 + 12 + 12 = 48 и соответственно, 4 · 12 = 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 4 = 48. Поэтому множимое и множитель часто называются сомножителями.

– Деление является действием, обратным к умножению, так как это операция нахождения одного из сомножителей по произведению и другому сомножителю: Разделить одно число (делимое) на другое (делитель) – значит найти такое третье число (частное), которое при умножении на делитель даёт делимое: 48 : 4 = 12. Здесь 48 – делимое, 4 – делитель, 12 – частное. Частное от деления одного целого числа на другое целое число может и не быть целым числом. Тогда это частное представляется в виде дроби. Если частное – целое число, то говорят, что эти числа делятся нацело. В противном случае мы выполняем деление с остатком. Пример: 23 не делится на 4, в этом случае мы можем записать: 23 = 5 · 4 + 3. Здесь 3 – остаток.

– Возведение в степень. Возвести число (основание степени) в целую степень (показатель степени) – значит повторить его сомножителем столько раз, каков показатель степени. Результат называется степенью. Запись возведения в степень:

3 5 = 3 · 3 · 3 · 3 · 3 = 243

Здесь 3 – основание степени, 5 – показатель степени, 243 – степень.

Вторая степень любого числа называется квадратом, третья – кубом. Первой степенью любого числа является само это число.

– Извлечение корня является действием, обратным к возведению в степень, так как это операция нахождения основания степени по степени и её показателю. Извлечь корень n-ой степени (n – показатель корня) из числа a (подкоренное число) – значит найти третье число, n-ая степень которого равна a . Результат называется корнем. Например:

$$\sqrt[5]{243} = 3$$

Сложение и вычитание, умножение и деление, возведение в степень и извлечение корня являются попарно взаимно-обратными операциями.

Про свойства арифметических операций сформулированы пять законов, которые считаются основными законами арифметики:

– Коммутативность: переместительный закон гласит, что от перемены мест слагаемых сумма не меняется. Аналогичный закон известен и для умножения, но он, конечно, говорит о множителях и произведении. Эти законы можно выразить в алгебраической форме с помощью буквенных обозначений:

$$a+b=b+a$$

$$a\cdot b=b\cdot a$$

– Ассоциативность: сочетательный закон сложения гласит, что складывая несколько слагаемых, можно группировать их в любом порядке. Аналогичный закон умножения говорит о перемножении множителей. Эти законы также можно выразить в алгебраической форме:

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

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

– Дистрибутивность: распределительный закон гласит: чтобы умножить сумму на число, можно умножить каждое слагаемое на это число и потом сложить полученные произведения. В алгебраической форме:

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

2. Проверка результатов арифметических действий

С помощью сравнений легко указать необходимые признаки правильности и достаточные признаки неправильности результатов выполнения арифметических действий сложения, вычитания и умножения целых чисел.

Теория сравнений дает следующий способ проверки арифметических действий.

Выбираем некоторый модуль т и заменяем большие числа a, b, c, . . . , над которыми нам надо производить действия (сложение, вычитание, умножение, возведение в степень), небольшими числами a', b', c', . . . , сравнимыми с ними по модулю т. Произведя действия над a, b, c мы точно такие же действия производим над a', b', c', ... Если действия произведены правильно, то результаты этих действий над a, b, c, ... и над a', b', c', ... должны быть сравнимы по модулю т.

Если $a\equiv a'(\mathrm{mod}\ m)$, $b\equiv b'(\mathrm{mod}\ m)$,…,

то $a+b+\ldots\equiv a'+b'+\ldots(\mathrm{mod}\ m)$, $a\cdot b\ldots\equiv a'\,b'\ldots(\mathrm{mod}\ m)$.

Для проверки соотношения $\frac{a}{b}=c$ представляем его в виде a=bc. Применение этого способа проверки, конечно, имеет смысл только тогда, когда нахождение таких чисел a', b', c', . . . может быть осуществлено легко и быстро. Для этого обычно в качестве модуля т выбирают т=9 или m=11. Каждое число, записанное в десятичной системе счисления, сравнимо с суммой его цифр по модулю 9, так что мы можем сформулировать следующий способ “проверки с помощью девятки”.

Для каждого числа вычисляется остаток от деления на 9 суммы цифр. Производя действия над числами, производят такие же действия над этими остатками. Результат рассматриваемых действий над этими остатками должен отличаться от суммы цифр искомого результата на число, кратное девяти.

Конечно, если ошибка такова, что разность между найденной и истинной величинами кратна 9, то она при этом способе проверки не будет замечена.

По модулю m = 11 каждое число, записанное в десятичной системе счисления, будет сравнимо с суммой цифр, взятых справа налево попеременно со знаками „плюс” и „минус”; поэтому мы можем сформулировать следующий способ „проверки с помощью одиннадцати”. Для каждого числа вычисляется остаток от деления на 11 суммы цифр, взятых попеременно справа налево со знаками „плюс” и „минус”. Результат рассматриваемых действий над этими остатками должен отличаться от суммы взятых попеременно со знаками „плюс” и „минус” справа налево цифр искомого результата на число, кратное 11. Если ошибка будет кратна 11, она не будет замечена при этом способе.

При сложных вычислениях имеет смысл проводить две проверки: одну с помощью модуля 9, а другую с помощью модуля 11. В этом случае ошибка не будет замечена только, если она кратна 99, что, конечно, бывает очень редко.

Примеры. Проверим правильность выполнения действий (с помощью 9 и 11):

1) $13547-9862=3685$
2) $8740297-561245=8179052$

Решение.

1) $13547\equiv 1+3+5+4+7\equiv 2(\text{mod } 9)$

$9862\equiv 9+8+6+2\equiv 7(\text{mod } 9)$

$3685\equiv 3+6+8+5\equiv 4(\text{mod } 9)$

$2-7\equiv 4(\text{mod } 9)$

$-5\equiv 4(\text{mod } 9)$

Сравнение подтверждает, но не гарантирует правильности выполнения действий.

$13547\equiv 7+(-4)+5+(-3)+1\equiv 6(\text{mod } 11)$

$9862\equiv 2+(-6)+8+(-9)\equiv 6(\text{mod } 11)$

$3685\equiv 5+(-8)+6+(-3)\equiv 0(\text{mod } 11)$

$6-6\equiv 0(\text{mod } 11)$

$0\equiv 0(\text{mod } 11)$

Проверка одиннадцатью подтверждает правильность получения результата.

2) $8740297\equiv 8+7+4+0+2+9+7\equiv 1(\text{mod } 9)$

$561245\equiv 5+6+1+2+4+5\equiv 5(\text{mod } 9)$

$8179052\equiv 8+1+7+9+0+5+2\equiv 5(\text{mod } 9)$

$1-5\equiv 5(\text{mod } 9)$

$-4\equiv 5(\text{mod } 9)$

Сравнение подтверждает, но не гарантирует правильности выполнения действий.

$8740297\equiv 7+(-9)+2+(-0)+4+(-7)+8\equiv 5(\text{mod } 11)$

$561245\equiv 5+(-4)+2+(-1)+6+(-5)\equiv 3(\text{mod } 11)$

$8179052\equiv 2+(-5)+0+(-9)+7+(-1)+8\equiv 2(\text{mod } 11)$

$5-3\equiv 2(\text{mod } 11)$

$2\equiv 2(\text{mod } 11)$

Проверка одиннадцатью подтверждает правильность получения результата.

Тема. Натуральные числа

План

1. Аксиоматическое задание системы натуральных чисел.

2. Теоремы о свойствах операций над натуральными числами.

3. Аксиоматика Пеано натуральных чисел и её свойства.

1. Аксиоматическое задание системы натуральных чисел

Определение. Натуральными числами назовем только следующие слова в алфавите цифр:

1) слово 0 есть натуральное число;

2) если слово w — натуральное число, то следующее за ним слово w' — тоже натуральное число;

3) других натуральных чисел нет.

Это определение по существу является ***правилом получения*** натуральных чисел.

Выпишем некоторые числа, получаемые согласно указанным правилам:

$$0,1,2,3,4,5,6,7,8,9,10,11,12,\ldots$$

Числа $0,1,2,3,4,5,6,7,8,9$ назовем ***однозначными.***

Теорема 1.

1. 0 не следует ни за каким натуральным числом.

2. Число $w' \neq w$.

3. Если $w = v$, то $w' = v'$.

Сформулируем ***принцип индукции*** для натуральных чисел. Пусть о некотором утверждении относительно натуральных чисел известно:

1) утверждение справедливо для числа 0;

2) если утверждение справедливо для числа w, то оно справедливо и для числа w'.

Тогда это утверждение справедливо для всех натуральных чисел.

Такой метод доказательства называют ***принципом*** или ***методом математической индукции***.

Замечание. Если п. 1 принципа математической индукции сформулировать так: «утверждение справедливо для числа 1», то очевидно, что утверждение справедливо для всех натуральных чисел, начиная с 1.

Теорема 2. Начальная цифра любого натурального числа, кроме нуля, отлична от нуля.

Теорема 3. Любое число, отличное от нуля, следует только за одним, числом, т. е. если $w' = v'$', то $w = v$ (или, если $w \neq v$, то $w' \neq v'$).

Сложение натуральных чисел

Определение Сложение двух чисел w, v (обозначаемое $w + v$) определяет число, называемое их ***суммой***, по следующему правилу:

1) $w + 0 = w;$;

2) $w + v' = (w + v)'$;

Найдем $w + 1 = (w + 0)' = w'$. Итак, $w' = w + 1$.

Теорема 4. Сложение натуральных чисел всегда выполнимо и однозначно определено.

Доказательство. Проведем доказательство индукцией по числу v при произвольном, но фиксированном числе w.

1. При $v = 0$ сумма $w + 0$ существует и однозначна: $w + 0 = w$.

2. Пусть сумма $w + v$ существует и однозначна, тогда в соответствии с. п. 2 определения существует и однозначна сумма $w + v'$.

Отсюда по принципу математической индукции следует справедливость теоремы для всех натуральных чисел.

Пример 1. Найти сумму $3 + 4$.

Решение.

$$1)\ 3 + 1 = 3' = 4;$$

$$2)\ 3 + 2 = 3 + 1' = (3 + 1)' = 4' = 5;$$

$$3)\ 3 + 3 = 3 + 2' = (3 + 2)' = 5' = 6;$$

$$4)\ 3 + 4 = 3 + 3' = (3 + 3)' = 6' = 7.$$

Каждый следующий шаг использует результат предыдущего шага.

2. Теоремы о свойствах операций над натуральными числами

Теорема 5 (*закон ассоциативности для сложения*). Для любых натуральных чисел w, v, u имеет место $(w + v) + u = w + (v + u)$.

Лемма 1. Для любого числа w справедливо $w+0=w$.

Доказательство.

1. При $w=0$ имеем $0+0=0,$ согласно п. 1 определения суммы натуральных чисел.

2. Предположим, что для $w=n$ лемма верна, т. е. $0+n'=(0+n)'=n'$.

3. Докажем лемму для $w=n'$. В самом деле:

$(0+n)'=n'$.

Первый знак равенства получаем, согласно п. 2 определения суммы, второй по предположению относительно n.

Согласно принципу математической индукции, отсюда следует, что лемма справедлива для любого w.

Лемма 2. Для любого w справедливо равенство: $1+w=w'$.

Доказательство (*проведем индукцией по числу* w).

1. Для $w=0$ лемма справедлива.
2. Предположим, что лемма справедлива для $w=n$.
3. Докажем лемму для $w=n'$, т. е. что $1+n'=(n')'$.

В самом деле, $1+n'=(1+n)'=(n')'$.

Второй знак равенства получаем по предположению индукции относительно $w=n$. Согласно принципу математической индукции, лемма доказана.

Теорема 6. (*закон коммутативности сложения*). Для любых натуральных чисел w,v имеет место $w+v=v+w$.

Доказательство.

Пусть w — произвольное фиксированное число.

1. Для $v=0$ теорема верна, т.к. $w+0=w$ и $0+w=w$. (см. лемму 1).
2. Предположим, что теорема верна для $v=n$.
3. Докажем ее для $v=n'$.
4. Имеем:
5. $$v+n'=(v+n)'=(n+v)'=1+(n+v)=(1+n)+v=n'+v.$$

Первый знак равенства получен согласно определению суммы, второй — согласно предположению индукции, третий и пятый — по лемме 2, четвертый — по свойству ассоциативности.

Итак, $v+n'=n'+v$.

Согласно принципу математической индукции, теорема доказана.

*Теорема 7.*Сумма $w+v\neq w$ при $v\neq 0$.

Лемма3. Для любых натуральных чисел $w,v\neq 0$ справедливо выражение:

$$w+v\neq 0.$$

Умножение натуральных чисел

Определение Умножение двух натуральных чисел w,v (обозначаемое $w\cdot v$) определяет число, называемое их ***произведением***, по следующему правилу:

$1)w\cdot 0=0;$

$2)w\cdot v'=w\cdot v+w.$;

Теорема 8. Умножение натуральных чисел всегда выполнимо и однозначно определено.

Лемма 4. Для любого натурального числа w справедливо равенство:

$$0\cdot w=0.$$

Лемма 5. Для любого натурального числа w имеет место равенство:

$$1 \cdot w = w.$$

Теорема 9. (*дистрибутивный закон*). Для любых натуральных чисел w, v, u имеет место равенство $(v + u) \cdot w = v \cdot w + u \cdot w.$

Следствие. Для любых натуральных чисел w, v справедливо равенство $v' \cdot w = v \cdot w + w.$

Теорема 10 (закон коммутативности умножения). Для любых натуральных чисел w, v имеет место равенство $v \cdot w = w \cdot v.$.

Доказательство.

1. Для $v = 0$ теорема верна, так как $v \cdot 0 = 0$ и $0 \cdot v = 0$.

2. Пусть теорема верна для $v = n$, т. е. $w \cdot n = n \cdot w$.

3. Докажем, что она верна для $v = n'$. В самом деле:

$$w \cdot n' = w \cdot n + w = n \cdot w + w = n' \cdot w.$$

Первое равенство следует из п. 2 определения произведения натуральных чисел, второе — по предположению индукции, третье — на основании следствия теоремы о дистрибутивности. По принципу математической индукции теорема справедлива для любых w и v.

Следствие. Справедливо равенство $w \cdot (v + u) = w \cdot v + w \cdot u.$

Теорема 11. (закон ассоциативности умножения). Для любых натуральных чисел *w*, *v*, *u* справедливо равенство $(w \cdot v) \cdot u = w \cdot (v \cdot u).$

Лемма 6.. Если $w \neq 0$ $v \neq 0$, то $w \cdot v \neq 0$

Сравнение натуральных чисел

Определение. Натуральное число w больше натурального числа v (пишут $w > v$), если существует такое натуральное число $u \neq 0$, что

$w = v + u.$

Если $w > v$, то говорят, что v меньше w, и обозначают $v < w$.

Лемма 7. Для любых натуральных чисел w и v справедливо одно и только одно из соотношений:

$$w > v,\ w = v, v < w\ -$$

закон монотонности сложения:

$$1)(w = v) \to (w + u = v + u);$$

$$2)(w > v) \to (w + u > v + u);$$

$$3)(w < v) \to (w + u < v + u).$$

Теорема 13 (закон монотонности умножения):

$$1)(w = v) \to (w \cdot u = v \cdot u);$$

$$2)((w > v) \wedge (u > 0)) \to (w \cdot u > v \cdot u);$$

$$3)((w < v) \wedge (u < 0)) \to (w + u > v + u).$$

Теорема 13 (*свойство Архимеда*). Для любых натуральных чисел w, $v \neq 0$ существует такое натуральное число n, что $n \cdot v > w.$

3. Аксиоматика Пеано натуральных чисел и её свойства

Множеством натуральных чисел мы будем называть любое множество A, на котором определена операция следования x' (элемент x' интерпретируется как элемент множества A, непосредственно следующий за элементом x) и выполняется ряд аксиом *(аксиомы Пеано).* Для простоты мы будем пока равенство $a = b$ понимать как совпадение элементов a и b (не описывать аксиоматически отношение равенства).

Аксиомы Пеано:

(П1) $\exists 1\ \forall b\ \ b' \neq 1$ (аксиома наличия наименьшего элемента);

(П2) $\forall a\ \forall b\ a = b \Leftrightarrow a' = b'$;

(П3) *(аксиома индукции).* Пусть B – подмножество множества A такое, что выполняются условия:

(а) $1 \in B$;

(б) $\forall a \in A\ \ a \in B \Rightarrow a' \in B.$

Тогда $B = A.$

Определим ***сложение*** двух натуральных чисел. Пусть $a \in A.$ Положим: $a + 1 = a'$; $a + x' = (a + x)'$ при $x \in A$ (*индуктивное определение*). Ввиду аксиомы индукции мы можем считать, что $a + b$ определено для всех $a, b \in A.$

Докажем *свойство коммутативности* натуральных чисел, т.е. что $a + b = b + a.$ Для этого нам понадобятся две леммы.

Лемма 1. $\forall a \in A\ a + 1 = 1 + a.$

Доказательство проведём индукцией по $a.$ При $a = 1$ утверждение очевидно. Пусть $x + 1 = 1 + x$; докажем, что $x' + 1 = 1 + x'$. Имеем: $x' + 1 = (x')' = (x + 1)' = (1 + x)' = 1 + x'.$

Лемма 2. $a' + b = a + b'$ для любых $a, b \in A.$

Доказательство. Индукция по $b.$ При $b = 1$ получаем: $a' + 1 = (a')' = (a + 1)' = a + 1'.$ Пусть $a' + x = a + x'$ при всех $a \in A$ и некотором $x.$ Докажем, что то же верно для $x'.$ Имеем: $a' + x' = (a' + x)' = (a + x')' = a + x'',$ что и требовалось.

Теорема 1. $a + b = b + a$ при всех $a, b \in A.$

Доказательство. Индукция по $b.$ При $b = 1$ утверждение следует из леммы 1. Пусть $a + x = x + a$ при всех $a \in A$ и некотором $x.$ Докажем, что то же верно для $x'.$ Имеем (с учётом предположения индукции и леммы 2): $a + x' = (a + x)' = (x + a)' = x + a' = x' + a.$ Теорема доказана.

Аналогично доказывается *закон ассоциативности*

$$(a + b) + c = a + (b + c).$$

На множестве A натуральных чисел можно определить ***отношение порядка***: $a < b \Leftrightarrow \exists c\ b = a + c;$ $a \leq b \Leftrightarrow (a < b) \vee (a = b)$ а также ***операцию умножения***: $a \cdot 1 = a,$ $a \cdot x' = a \cdot x + a.$ С помощью аксиом Пеано можно доказать *законы ассоциативности* $(ab)c = a(bc)$ и *коммутативности* $a \cdot b = b \cdot a$ *умножения*, а также *закон дистрибутивности* $(a + b) \cdot c = a \cdot c + b \cdot c.$ Доказываются также *свойства неравенств:* $a < b,\ b < c \Rightarrow a < c,$ $a < b \Rightarrow a + c < b + c$ и многие другие. Тем самым аксиомы Пеано позволяют построить строгую и стройную теорию натуральных чисел.

Заметим, что *любое множество* (независимо от его природы) мы называем множеством натуральных чисел, если оно удовлетворяет аксиомам Пеано. Образно говоря, если бы множество стульев удовлетворяло аксиомам Пеано, мы стулья называли бы натуральными числами. Не следует ли отсюда, что множество натуральных чисел не одно, а таких множеств огромное количество? Вообще говоря, следует, но не надо этого бояться. Ниже мы докажем, что любые два “множества натуральных чисел” (т.е. два множества *A* и *B*, удовлетворяющие аксиомам Пеано) изоморфны друг другу, т.е. существует взаимно однозначное соответствие $\varphi : A \to B,$ сохраняющее операцию следования: $\varphi(a') = \varphi(a)'.$ Значит, *множество натуральных чисел единственно с точностью до изоморфизма*. Для других аксиоматических систем ситуация может быть совсем иной. Например, *аксиомы группы* не определяют объект однозначно с точностью до изоморфизма. В самом деле, две неизоморфные группы удовлетворяют аксиомам группы (ассоциативность, наличие единицы, наличие обратного элемента).

Теорема 2. Любые два множества *A* и *B*, удовлетворяющие аксиомам (П1)–(П3), изоморфны друг другу.

Доказательство. Ввиду аксиомы (П1) в A есть наименьший элемент e, а в B – наименьший элемент f. Построим индуктивно отображение $\varphi: A \to B$. Положим $\varphi(e) = f$, $\varphi(e') = f'$ и вообще, если $\varphi(a) = b$, то положим $\varphi(a') = b'$. По аксиоме (П3) φ продолжается до всего A и $\varphi(A) = B$. По аксиоме (П2) φ взаимно однозначно. Равенство $\varphi(x') = \varphi(x)'$ следует из определения отображения φ.

Тема. Аксиоматическая теория целых и рациональных чисел

План

1. Аксиоматическое построение кольца целых чисел как расширения полукольца натуральных чисел.

2. Операции над целыми числами и их свойства. Свойства аксиоматической системы целых чисел.

3. Поле частных кольца. Модель поля рациональных чисел.

1. Аксиоматическое построение кольца целых чисел как расширения полукольца натуральных чисел

Определение. *Кольцом целых чисел* называется кольцо Z, обладающее свойствами:

$(Z1)$ Z содержит множество N натуральных чисел, т. е. в Z имеется подмножество N', изоморфное N.

$(Z2)$ Множество Z есть кольцо (всегда выполнимо вычитание — целевое требование).

$(Z3)$ Z — упорядоченное кольцо.

$(Z4)$ Z — минимальное кольцо, т. е. не содержит отличного от него подкольца, содержащего N (категоричность)·

Элементы кольца Z называются целыми числами. Перечисленные свойства можно рассматривать как *систему аксиом, определяющую кольцо целых чисел.*

Чтобы доказать непротиворечивость системы аксиом кольца Z, достаточно построить одну его модель

2. Операции над целыми числами и их свойства

Определение *Целым числом* назовем слово $z = \varepsilon n$, где n — натуральное число, $\varepsilon \in \{+,-\}$. Букву ε назовем *знаком целого числа* z, натуральное число n — *модулем* целого числа z.

Определение. Числа $(-0),(+0)$ считаются равными: $+0 = -0$.

2. Числа u и z равны тогда и только тогда, когда их знаки одинаковы и модули равны.

Определение *Суммой двух целых чисел* $z = \varepsilon n$ и $u = \varepsilon m$ называют целое число, которое вычисляют по следующему правилу:

1) если знаки слагаемых одинаковы, то знак суммы совпадает со знаком слагаемых и модуль суммы равен сумме модулей,

2) если знаки слагаемых различны, то знак суммы совпадает со знаком слагаемого с большим (или равным) модулем и модуль суммы равен разности большего и меньшего модулей, т. е.

Теорема 1. Сложение целых чисел всегда выполнимо и однозначно определено.

Теорема 2 (закон ассоциативности сложения целых чисел).

Для любых целых чисел $z = \varepsilon n,\ u = \gamma m,\ v = \eta k$ $(n,m,k \in N, \varepsilon,\gamma,\eta \in \{+,-\})$ имеет место равенство:

$$(z+u)+v = (\varepsilon n + \gamma m) + \eta k = \varepsilon n + (\gamma m + \eta k) = z + (u+v).$$

Определение *Разностью* двух целых чисел $z=\varepsilon n, u=\gamma m \ (n,m\in N, \varepsilon,\gamma\in\{+,-\})$ называется целое число, обозначаемое $z-u=\varepsilon n-\gamma m$ и удовлетворяющее условию:

$$(\varepsilon n-\gamma m)+\gamma m=\varepsilon n.$$

Теорема 3. Вычитание целых чисел всегда выполнимо и однозначно определено.

Умножение и деление целых чисел

Определение. *Произведением* целого числа $z=\varepsilon n$ на целое число $u=\gamma m$ называется такое целое число $v=\eta k$, что:

1) модуль произведения равен произведению модулей;

2) знак вычисляется по правилу знаков: если знаки сомножителей одинаковы, то знак произведения – «плюс», а если противоположны, то «минус».

Теорема 4 Умножение целых чисел выполнимо, однозначно определено и коммутативно.

Доказательство. Выполнимость умножения целых чисел следует из того, что оно сводится к умножению натуральных и нахождению знака, операции тоже выполнимой. Так как эти операции однозначны, то умножение однозначно.

Коммутативность произведения вытекает непосредственно из определения, потому что в нем нет указания на порядок сомножителей. Коммутативность также можно доказать, опираясь на коммутативность умножения натуральных чисел, поскольку умножение целых чисел сводится к умножению натуральных.

Теорема 5. Произведение целых чисел равно нулю тогда и только тогда, когда хотя бы один из сомножителей равен нулю.

Доказательство. В самом деле, из определения произведения целых чисел вытекает, что если сомножители не равны нулю, т. е. их модули не равны нулю, то произведение не равно нулю (по свойствам натуральных чисел). Если учесть, что хотя бы при одном сомножителе, равном нулю, произведение также равно нулю, то получим доказательство теоремы.

Лемма 1. Число $(+1)$ является единицей относительно умножения в множестве целых чисел. Для любого целого числа $z=\varepsilon n$ справедливо равенство:

$$z\cdot(-1)=(\varepsilon n)\cdot(-1)=-(\varepsilon n)=-z.$$

Теорема 6 (*закон ассоциативности умножения целых чисел).*

Для любых целых чисел $z=\varepsilon n,\ u=\gamma m,\ v=\eta k \ (n,m,k\in N, \varepsilon,\gamma,\eta\in\{+,-\})$ имеет место равенство:

$$z\cdot(u\cdot v)=\varepsilon n(\gamma m\cdot\eta k)=(\varepsilon n\cdot\gamma m)\cdot\eta k=(z\cdot u)\cdot v.$$

Теорема 7. Умножение целых чисел дистрибутивно относительно сложения.

Определение *Частным* двух целых чисел $z=\varepsilon n$ и $u=\gamma m\neq 0$ называется целое число $v=\eta k$, удовлетворяющее равенству:

$$z=\varepsilon n=u\cdot v=(\gamma m)\cdot(\eta k).$$

Очевидно, что знак частного – *«плюс»*, если знаки ε и γ одинаковы, «минус» – в противном случае

Упорядоченность множества целых чисел

Лемма 2. Разности $\varepsilon n-\gamma m$ и $\gamma m-\varepsilon n$ есть взаимно противоположные числа.

Введем отношения «больше» и «меньше» на множестве целых чисел.

Определение. Целое число $z=\varepsilon n$ называется ***большим (меньшим)*** целого числа $u=\gamma m$ тогда и только тогда, когда разность $z-u=\varepsilon n-\gamma m$ есть положительное (отрицательное) число.

Теорема 8. Множество целых чисел есть ***упорядоченное множество***. Это означает, что:

1) всякие два целых числа $z = \varepsilon n$, $u = \gamma m$ находятся в одном и только в одном их трёх отношений:

$$\varepsilon n > \gamma m, \text{ или } \varepsilon n < \gamma m, \text{ или } \varepsilon n = \gamma m;$$

2) если $\varepsilon n > \gamma m$ и $\gamma m > \eta k$, то $\varepsilon n > \eta k$.

Нетрудно доказать также, что на множестве целых чисел выполняются законы монотонности сложения и умножения.

Свойства аксиоматической системы целых чисел

Теорема 9. Множество целых чисел с определенными выше операциями сложения и умножения и отношением порядка > является кольцом целых чисел Z, удовлетворяющим аксиомам $(Z1)-(Z4)$.

Доказательство. Выполнимость аксиом $(Z1)-(Z3)$ следует из определения и доказанных свойств операций сложения и умножения целых чисел и отношения ">". Справедливость последней аксиомы следует из того, что всякое целое число можно представить как разность двух натуральных чисел.

3. Поле частных кольца. Модель поля рациональных чисел

Определение. Пусть дано кольцо $\langle K,+,\cdot\rangle$. Рассмотрим множество P всех таких упорядоченных пар элементов кольца K, у которых второй элемент не равен нулю:

$$P = \{\langle a,b\rangle | a,b \in K, b \neq 0.\}$$

Будем обозначать такие пары в виде дробей $\frac{a}{b}$ называть их *частными кольца* $\langle K,+,\cdot\rangle$.

Зададим на множестве всех частных кольца операции "+" и "·" следующим образом:

$$(\forall a,b,c,d \in K)\left(\frac{a}{b}+\frac{c}{d}=\frac{a\cdot d + c\cdot b}{b\cdot d},\ b\neq 0, d\neq 0\right);$$

$$(\forall a,b,c,d \in K)\left(\frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d},\ b\neq 0, d\neq 0\right).$$

Определение. Два частных будем называть ***равными,*** если выполняется равенство:

$$\frac{a}{b}=\frac{c}{d} \Leftrightarrow a\cdot d = b\cdot c.$$

Множество всех равных между собой частных кольца K будем объединять в один класс. В качестве представителя этого класса обычно рассматривается несократимая дробь, которая в данном классе единственна.

Нетрудно проверить, что операции заданы корректно, то есть результат их выполнения не зависит от выбора представителя класса. Поэтому в дальнейшем будем отождествлять весь класс равных между собой частных кольца с его несократимым представителем.

Следующие свойства множества всех частных кольца K показывают, что по заданным операциям это множество образует поле, которое называется ***полем частных кольца*** K***.***

Свойство 2. .Операции сложения и умножения на множестве всех частных кольца K обладают свойствами ассоциативности и коммутативности. Умножение связано со сложением левым и правым законами дистрибутивности.

Свойство 3. .По операции "+" существует нейтральный элемент, в качестве которого выступает класс дробей с числителем, равным нулю, и произвольным знаменателем.

Для элемента $\frac{a}{b}$ противоположным является элемент $\frac{-a}{b}$.

Свойство 4. По операции "·" существует нейтральный элемент, в качестве которого выступает класс дробей с числителем, равным знаменателю. Для всякого ненулевого элемента $\frac{a}{b}$ обратным является элемент $\frac{b}{a}$.

Свойство 5. .Единица поля не равна нулю поля, следовательно, во всяком поле имеется по крайней мере два различных элемента – 0 *и* 1.

Свойство 6..Никакое поле не содержит делителей нуля.

Как известно, в кольце целых чисел уравнение $ax = b$, $a \neq 0$ не всегда имеет решение. Возникает задача построения расширения кольца целых чисел, в котором операция деления была бы всегда выполнима.

Алгоритм построения модели поля рациональных чисел Q

В качестве такого расширения выступает поле рациональных чисел. Рассмотрим *алгоритм построения модели поля рациональных чисел* Q как поля, удовлетворяющего условиям:

1. Кольцо Z должно содержаться в поле Q, операции сожжения и умножения в Q должны быть продолжением соответствующих операций в Z.

2. В поле Q должна быть всегда выполнима операция деления (исключая деление на 0).

3. Поле Q должно быть минимальным расширением кольца Z в том смысле, что не должно существовать поле, содержащее кольцо Z и само содержащееся в поле Q и удовлетворяющее условиям 1–2.

Определение. Полем рациональных чисел Q назовем поле частных кольца целых чисел. Элементы поля Q назовем *рациональными числами.*

Замечание. Из определения следует, что любое рациональное число представимо в виде частного целых чисел.

1. Отождествим рациональное число $q = \frac{a}{1}$ с целым числом a. Тогда можно считать, что кольцо целых чисел изоморфно подкольцу всех рациональных чисел со знаменателем 1. Т.к. изоморфные структуры с точки зрения алгебры одинаковы, то будем считать, что само кольцо Z содержится в поле Q.

2. Согласно определению поля частных кольца K, в поле рациональных чисел всегда выполнима операция деления.

3. Допустим, существует поле Q', удовлетворяющее условиям 1–2, причем: $Z \subset Q' \subset Q$. Тогда каждый элемент поля Q' также представим в виде частного двух целых чисел. Построим соответствие между множествами Q и Q' по следующему правилу: элемент $q \in Q$ соответствует именно тому элементу $q' \in Q'$, который представляется в виде частного тех же целых чисел a, b, что и элемент q. Нетрудно показать, что это соответствие является изоморфизмом полей Q и Q'.

Отношение "<" на множестве Q вводится с помощью отношения "<" на множестве Z.

Определение Отношение "<" *на множестве* Q рациональных чисел вводится следующим образом:

$$\left(\forall \frac{a}{b}, \frac{c}{d} \in Q\right)\left(\frac{a}{b} < \frac{c}{d} \Leftrightarrow a \cdot d < b \cdot c,\ b, d \in N; a, b \in Z\right).$$

Непосредственной проверкой можно показать, что это отношение на множестве Q есть отношение строго порядка, продолжающее отношения порядка на множестве Z.

Теорема. Отношение "$<$" на множестве Q всех рациональных чисел обладает свойствами:

$$1)(\forall a, b, c \in Q)((a < b) \wedge (b < c) \rightarrow (a < c));$$
$$2)(\forall a, b \in Q)((a < b) \vee (b < a) \vee a = b);$$
$$3)(\forall a, b, c \in Q)((a < b) \rightarrow (a + c < b + c));$$
$$4)(\forall a, b, c \in Q)((a < b) \wedge (0 < c) \rightarrow (a \cdot c < b \cdot c)).$$

Тема. Действительные числа

План

1. Содержательная теория действительных чисел.

2. Другие подходы к построению системы действительных чисел.

1. Содержательная теория действительных чисел

Множество вещественных чисел имеет стандартное обозначение — R (от лат. realis – действительный.

Множество действительных чисел будем рассматривать как множество, на котором определены *операция сложения* $a+b$, *умножения* $a \cdot b$, *отношение порядка* $\leq$ и выполняются аксиомы:

(1) $\forall a\ \forall b\ \forall c\ \ (a+b)+c = a+(b+c);$

(2) $\exists 0\ \forall a\ \ a+0 = a;$

(3) $\forall a\ \exists b\ \ a+b = 0;$

(4) $\forall a\ \forall b\ \ a+b = b+a;$

(5) $\forall a\ \forall b\ \forall c\ \ (ab)c = a(bc);$

(6) $\exists 1\ \ (1 \neq 0\ \&\ \forall a\ \ a \cdot 1 = a);$

(7) $\forall a\ \exists b\ \ (a = 0 \vee ab = 1);$

(8) $\forall a\ \forall b\ \ ab = ba;$

(9) $\forall a\ \forall b\ \forall c\ \ (a+b)c = ac + bc;$

(10) $\forall a\ \ a \leq a;$

(11) $\forall a\ \forall b\ \forall c\ \ (a \leq b\ \&\ b \leq c \Rightarrow a \leq c);$

(12) $\forall a\ \forall b\ \ (a \leq b\ \&\ b \leq a \Rightarrow a = b);$

(13) $\forall a\ \forall b\ \ (a \leq b \vee b \leq a);$

(14) $\forall a\ \forall b\ \forall c\ \ (a \leq b \Rightarrow a + c \leq b + c);$

(15) $\forall a\ \forall b\ \forall c\ \ (a \leq b\ \&\ c \geq 0 \Rightarrow ac \leq bc);$

(16) (*аксиома Архимеда*). Каковы бы ни были действительные числа $a, b > 0$, существует натуральное число n такое, что $na > b$;

(17) (***аксиома непрерывности***). Если A, B – непустые подмножества множества действительных чисел и $a \leq b$ при всех $a \in A,\ \ b \in B,$ то существует действительное число c такое, что $A \leq c \leq B$ (т.е. $a \leq c \leq b$ при $a \in A,\ \ b \in B.$

Как видно, по форме построения аксиомы (16) и (17) отличаются от других аксиом. Правда, аксиому Архимеда можно переписать так: $\forall a\ \ \forall b\ \ (a, b > 0 \Rightarrow \exists n \in \square\ \ (na > b))$, а аксиома непрерывности переписывается так:

$$\forall A, B \subseteq \mathbf{R}\ \ (A, B \neq \varnothing\ \&\ A \leq B \Rightarrow \exists c\ A \leq c \leq B).$$

Но, в отличие от аксиом (1)–(15), не все кванторы имеют областью определения множество действительных чисел: в аксиоме Архимеда квантор действует на натуральные числа, а в аксиоме непрерывности – на подмножества. Мы будем говорить, что аксиомы (1)–(15) являются формулами *логики первого порядка*, а аксиомы (16), (17) таковыми не являются (точные определения будут даны в следующем разделе).

В курсе математического анализа доказывается, что аксиома непрерывности эквивалентна *принципу вложенных отрезков*, а также *теореме о существовании точной верхней грани непустого ограниченного множества*. Следовательно, аксиома (17) может быть заменена на одно из этих утверждений.

Отметим, что множество действительных чисел определяется аксиомами (1)–(17) однозначно с точностью до изоморфизма. Однако доказывать это утверждение мы не будем. Аксиом (1)–(16) для определения множества R недостаточно, так как этим аксиомам удовлетворяет также множество Q рациональных чисел. Кроме того, данное рассуждение показывает независимость аксиомы (17) от предыдущих аксиом.

2. Другие подходы к построению системы действительных чисел

Современная теория вещественных чисел была построена во второй половине XIX века, в первую очередь трудами Вейерштрасса, Дедекинда и Кантора. Они предложили различные, но эквивалентные подходы к теории этой важнейшей математической структуры и окончательно отделили это понятие от геометрии и механики.

При конструктивном определении понятия вещественного числа на основе известных математических объектов, которые принимают заданными, строят новые объекты, которые, в определённом смысле, отражают наше интуитивное понимание о понятии вещественного числа. Существенным отличием между вещественными числами и этими построенными объектами является то, что первые, в отличие от вторых, понимаются нами лишь интуитивно и пока не являются строго определённым математическим понятием.

Эти объекты и объявляют вещественными числами. Для них вводят основные арифметические операции, определяют отношение порядка и доказывают их свойства.

Исторически первыми строгими определениями вещественного числа были именно конструктивные определения.

Теория фундаментальных последовательностей Кантора

В данном подходе вещественное число рассматривается как предел последовательности рациональных чисел. Чтобы последовательность рациональных чисел сходилась, на неё накладывается условие Коши:

$$(\forall \varepsilon > 0)(\exists N(\varepsilon))((\forall n > N(\varepsilon)) \wedge (\forall m > 0)|a_{n+m} - a_n| < \varepsilon).$$

Смысл этого условия заключается в том, что члены последовательности, начиная с некоторого номера, будут лежать сколь угодно близко друг от друга. Последовательности, удовлетворяющие условию Коши, называются *фундаментальными*.

Вещественное число, определяемое фундаментальной последовательностью рациональных чисел $\{x_n\} = \left\{ x_n \in Q : \lim\limits_{n\to\infty} x_n = a_n \right\}$, обозначим a_n.

Два вещественных числа a_n и b_n, определённые соответственно фундаментальными последовательностями $\{x_n\}$ и $\{y_n\}$, называются *равными*, если

$$\lim_{n\to\infty} (a_n - b_n) = 0 \cdot$$

Если даны два вещественных числа a_n и b_n, то их *суммой* и *произведением* называются числа, определённые соответственно суммой и произведением последовательностей $\{x_n\}$ и $\{y_n\}$.

Отношение порядка на множестве вещественных чисел устанавливается посредством соглашения, в соответствии с которым число a_n по определению больше числа b_n, если

$$(\exists \varepsilon > 0)(\exists N)((\forall n > N)(a_n \geq b_n + \varepsilon))$$

Способ построения множества вещественных чисел с помощью фундаментальных последовательностей рациональных чисел является частным случаем конструкции пополнения произвольного метрического пространства. Как и в общем случае, полученное в результате пополнения множество вещественных чисел само уже является полным, то есть содержит пределы всех фундаментальных последовательностей своих элементов.

Теория бесконечных десятичных дробей

Вещественное число определяется как бесконечная десятичная дробь, то есть выражение вида $\alpha = \pm a_0, a_1 a_2 \ldots a_n \ldots$.

Бесконечная десятичная дробь интерпретируется как такое число, которое на числовой прямой лежит между рациональными точками вида q_1 и q_2, причём

$$(\forall \varepsilon > 0)((q_1 \leq \alpha \leq q_2) \wedge (q_2 - q_1 < \varepsilon)).$$

Сравнение вещественных чисел в форме бесконечных десятичных дробей производится поразрядно. Например, пусть даны два неотрицательных числа

$$\alpha = +a_0, a_1 a_2 \ldots a_n \ldots \ и \ \beta = +b_0, b_1 b_2 \ldots b_n \ldots$$

Если $a_0 < b_0$, то $\alpha < \beta$; если $a_0 > b_0$ то $\alpha > \beta$. В случае равенства переходят к сравнению следующего разряда. И так далее.

Арифметические операции над бесконечными десятичными дробями определяются как непрерывное продолжение соответствующих операций над рациональными числами. Например, суммой вещественных чисел $\alpha \ и \ \beta$ называется вещественное число $\alpha + \beta$, удовлетворяющее следующему условию:

$$(\forall a', a'', b', b'' \in Q)((a' \leq \alpha \leq a'') \wedge (b' \leq \beta \leq b'')) \Rightarrow (a' + b' \leq \alpha + \beta \leq a'' + b'')$$

Аналогично определяет операция умножения бесконечных десятичных дробей.

Теория сечений в области рациональных чисел

В подходе Дедекинда вещественные числа определяются с помощью сечений в множестве рациональных чисел.

Сечением в множестве рациональных чисел называется всякое разбиение совокупности всех рациональных чисел на два непустых класса – нижний и верхний, так что каждое число из нижнего класса строго меньше всякого числа из верхнего:

Если существует число q, которое является максимальным в нижнем классе, либо минимальным в верхнем классе, то это число *разделяет* множества верхних и нижних классов: числа нижнего и верхнего классов лежат по разные стороны от q. Говорят также, что рациональное число q *производит данное сечение* множества рациональных чисел.

Если же в нижнем классе сечения нет максимального элемента, а в верхнем – минимального, то не существует никакого рационального числа, которое разделяло бы эти множества.

В этом случае по определению полагают, что данное сечение определяет некоторое *иррациональное число* α, которое находится между нижним и верхним классами, и тем самым производит данное сечение. Иначе говоря, для всякого сечения, не производимого никаким рациональным числом, вводят новый объект – *иррациональное число*, которое по определению больше всякого числа из нижнего класса и меньше всякого числа из верхнего класса:

Объединение всех рациональных и всех иррациональных чисел называют *множеством вещественных чисел*, а его элементы — *вещественными числами*.

Арифметические операции над вещественными числами определяются как непрерывное продолжение соответствующих операций над рациональными числами.

Аксиоматический подход

Множество R называется *множеством вещественных чисел*, а его элементы – *вещественными числами*, если выполнены следующие условия, называемые *аксиомами* вещественных чисел:

Аксиомы поля

Аксиомы порядка

Между элементами R определено отношение $\leqslant$, то есть для любой упорядоченной пары элементов a,b из R установлено, выполняется соотношение $a \leqslant b$ или нет. При этом имеют место следующие свойства.

II_1. *Рефлексивность.* Для любого $a \in \mathbb{R}\ a \leqslant a$

II_2. *Антисимметричность.* Для любых $a, b \in \mathbb{R}$

$(a \leqslant b) \wedge (b \leqslant a) \Rightarrow (a = b)$

II_3. *Транзитивность.* Для любых $a, b, c \in \mathbb{R}$

$(a \leqslant b) \wedge (b \leqslant c) \Rightarrow (a \leqslant c)$

II_4. *Линейная упорядоченность.* Для любых $a, b \in \mathbb{R}$

$(a \leqslant b) \vee (b \leqslant a)$

II_5. *Связь сложения и порядка.* Для любых $a, b, c \in \mathbb{R}$

$(a \leqslant b) \Rightarrow (a + c \leqslant b + c)$

II_6. *Связь умножения и порядка.* Для любых $a, b \in \mathbb{R}$

$(0 \leqslant a) \wedge (0 \leqslant b) \Rightarrow (0 \leqslant a \cdot b)$

Аксиомы непрерывности

III_1. Каковы бы ни были непустые множества $A \subset \mathbb{R}$ и $B \subset \mathbb{R}$, такие что для любых двух элементов $a \in A$ и $b \in B$ выполняется неравенство $a \leqslant b$, существует такое число $\xi \in \mathbb{R}$, что для всех $a \in A$ и $b \in B$ имеет место соотношение

III_1.

$$a \leqslant \xi \leqslant b$$

Этих аксиом достаточно, чтобы строго вывести все известные свойства вещественных чисел.

Определение. Множеством вещественных чисел называется непрерывное упорядоченное поле.

Связь с рациональными числами

Очевидно, что на числовой прямой рациональные числа располагаются вперемешку с вещественными, причём множество вещественных чисел в известном смысле «плотнее» множества рациональных. Возникает закономерный вопрос, насколько часто на числовой прямой попадаются рациональные и вещественные числа и можно ли одни числа приблизить другими. Ответ на этот вопрос дают три леммы, основанные, в основном, на аксиоме Архимеда.

Лемма 1. Для любого вещественного числа и любого наперёд взятого положительного рационального расстояния найдётся пара рациональных чисел, отстоящих друг от друга менее, чем на это расстояние, таких что вещественное число лежит на отрезке между этими рациональными числами.

$$(\forall a \in R)(\forall \varepsilon \in Q^+)(\exists q_1, q_2 \in Q)((q_1 \le \alpha \le q_2) \wedge (q_2 - q_1 < \varepsilon))$$

Эта лемма говорит о том, что любое вещественное число можно с заданной точностью с двух сторон приблизить рациональными числами.

Лемма 2. Между любыми двумя различными вещественными числами содержится рациональное число.

$$\forall a, b \in \mathbb{R} :\ a < b\ \exists q \in \mathbb{Q} : a < q < b.$$

Очевидным следствием из этой леммы является тот факт, что между любыми двумя несовпадающими вещественными числами содержится целое бесконечное

множество рациональных. Кроме того, ещё более очевидно, что между любыми двумя различными рациональными числами содержится вещественное.

Лемма 3. Приближение вещественного числа рациональными, описанное в лемме 1, идентифицирует вещественное число единственным образом.

$$(\forall a,b \in R)(\forall \varepsilon \in Q^+)(\exists q_1, q_2 \in Q)((q_1 \le a \le q_2) \wedge ((q_1 \le b \le q_2))(q_2 - q_1 < \varepsilon))$$

Эти леммы, прежде всего, говорят о том, что множество вещественных чисел не такое «плотное» по сравнению с множеством рациональных чисел, как может показаться. Особенно ярко это иллюстрирует лемма 2. Все три леммы активно используются для доказательства различных теорем, связанных с операциями сложения и умножения вещественных чисел.

Теоретико-множественные свойства

Изначально вещественные числа были естественным обобщением рациональных, но у них впервые было обнаружено свойство несчётности, которое говорит о том, что множество вещественных чисел нельзя занумеровать, то есть не существует биекции между множествами вещественных и натуральных чисел. Чтобы показать несчётность всего множества вещественных чисел, достаточно показать несчётность интервала (0,1) .

Пусть все числа указанного промежутка уже занумерованы некоторым образом. Тогда их можно выписать в следующем виде:

$$x_1 = 0, a_{11}a_{12}\cdots a_{1m}\cdots$$
$$x_2 = 0, a_{21}a_{22}\cdots a_{2m}\cdots$$
$$\cdots$$
$$x_k = 0, a_{k1}a_{k2}\cdots a_{km}\cdots$$
$$\cdots$$

Очевидно, что все числа указанного вида действительно принадлежат рассматриваемому промежутку, если только в каждом числе не все цифры сразу являются 0 или 9.

Далее предлагается рассмотреть следующее число:

$$x = 0, d_1 d_2 \cdots d_m \cdots$$

Пусть каждая цифра этого числа удовлетворяет следующим трём свойствам:

- $d_i \neq 0$
- $d_i \neq 9$
- $d_i \neq a_{ii}$

Такое число действительно существует на указанном промежутке, так как оно является вещественным, не совпадает ни с нулём, ни с единицей, а десятичных цифр достаточно, чтобы третье свойство выполнялось. Кроме этого, данное число интересно тем фактом, что оно не совпадает ни с одним из чисел x_j, выписанных выше, ведь иначе j-я цифра числа x совпала бы с j-ой цифрой числа x_j. Пришли к противоречию, заключающемуся в том, что как бы числа рассматриваемого промежутка ни были занумерованы, всё равно найдётся число из этого же промежутка, которому не присвоен номер.

Это свидетельствует о том, что *множество вещественных чисел не является счётным.* Его мощность называется *мощностью континуума*.

Тема. Комплексные числа

План

1. Построение поля комплексных чисел.

2. Комплексное сопряжение и его свойства.

3. Тригонометрическая форма комплексного числа.

4. Нахождение значений корня n-й степени из комплексного числа. Первообразный корень n-й степени из единицы.

1. Построение поля комплексных чисел

Рассмотрим всевозможные упорядоченные пары действительных чисел: $\langle a,b\rangle \in R\times R$ и обозначим множество всех таких пар через C.

Определение. Множество $C=\{\langle a,b\rangle | a,b\in R\}$ назовем ***множеством комплексных чисел,*** а его элементы – ***комплексными числами***.

Определение. Два комплексных числа $\langle a,b\rangle$ и $\langle c,d\rangle$ называются ***равными***, если равны соответствующие элементы этих пар: $a=c,\ b=d.$

На множестве C зададим операции сложения и умножения следующим образом:

$$\langle a,b\rangle+\langle c,d\rangle=\langle a+b,c+d\rangle \qquad (1)$$

$$\langle a,b\rangle\cdot\langle c,d\rangle=\langle a\cdot c-b\cdot d,a\cdot d+b\cdot c\rangle \qquad (2).$$

Операции $(1)\,и\,(2)$ заданы корректно, так как они сводятся к сложению, умножению и вычитанию действительных чисел, которые всегда выполнимы и однозначно определены.

Непосредственной проверкой можно показать, что сложение и умножение комплексных чисел обладают следующими свойствами:

- коммутативность и ассоциативность;
- умножение дистрибутивно относительно сложения;
- нейтральным элементом по сложению является пара $\langle 0,0\rangle$; по умножению – пара $\langle 1,0\rangle$;
- для числа $\langle a,b\rangle$ противоположным элементом является число $\langle -a,-b\rangle$.

Из определения равенства комплексных чисел следует, что комплексное число $\langle a,b\rangle$ отлично от нуля тогда и только тогда, когда оба элемента этой пары не равны нулю одновременно, т.е. когда $a^2+b^2\neq 0.$ Выясним, всегда ли для ненулевого числа $\langle a,b\rangle$ существует в множестве C обратный элемент по операции умножения.

Пусть $\langle a,b\rangle\neq 0$, и пусть $\langle a,b\rangle\cdot\langle x,y\rangle=\langle 1,0\rangle.$ Решим это уравнение относительно $x\ и\ y$:

$$\langle a\cdot x-b\cdot y,a\cdot y+b\cdot x\rangle=\langle 1,0\rangle\Leftrightarrow$$

$$\begin{cases} a\cdot x-b\cdot y=1,\\ a\cdot y+b\cdot x=0 \end{cases}\Leftrightarrow\begin{cases} x=\dfrac{a}{a^2+b^2},\\ y=-\dfrac{b}{a^2+b^2}. \end{cases}$$

Таким образом, для ненулевого комплексного числа $\langle a,b\rangle$ обратным элементом будет число вида $<\frac{a}{a^2+b^2},-\frac{b}{a^2+b^2}>$.

Из перечисленных свойств операций "+" и "·" следует справедливость теоремы.

Теорема. Множество комплексных чисел C относительно заданных на нем операций "+" и "·" образует поле, которое называется ***полем комплексных чисел***.

Лемма. Подмножество C_R множества C, состоящее из элементов вида $\langle a,0\rangle$, изоморфно полю действительных чисел: $C_R\cong R.$

Замечания. 1**.** Так как изоморфные объекты с точки зрения своих алгебраических свойств одинаковы, то часто говорят не об изоморфном вложении, а том, что само поле действительных чисел содержится в поле комплексных чисел.

2. Будем отождествлять пары комплексных чисел, у которых второй элемент равен нулю, с первым элементом и называть ***действительными комплексными числами***: $\langle a,0\rangle \equiv a$.

В частности, $\langle 0,0\rangle \equiv 0; \langle 1,0\rangle \equiv 1; \langle -1,0\rangle \equiv -1.$

Теорема. В поле комплексных чисел разрешимо уравнение

$$z^2 = -1 \qquad (3).$$

Замечания. 1. Очевидно, решением уравнения (3) является комплексное число вида $\langle 0,1\rangle$, которое принято обозначать буквой i и называть ***мнимой единицей***: $i^2 = -1.$

2. Пары комплексных чисел, у которых первый элемент равен нулю будем называть *комплексными мнимыми числами.*

Теорема. Всякое комплексное число $\langle a,b\rangle$ можно представить в виде:

$$\langle a,b\rangle = \langle a,0\rangle + \langle b,0\rangle \cdot \langle 0,1\rangle \qquad (4).$$

Замечания.1. Учитывая замечания 1 и 2, запись (4) можно представить в виде:

$$z = \langle a,b\rangle = a + b \cdot i \qquad (5).$$

Запись комплексного числа z в виде (5) называют *алгебраической формой комплексного числа.*

2. Число a называют *действительной частью комплексного числа* z *,* а число b *– мнимой* и обозначают:

$$a = \mathrm{Re}\, z,\ b = \mathrm{Im}\, z.$$

Операции над комплексными числами в алгебраической форме

Сложение

$$(a + b \cdot i) + (c + d \cdot i) = (a + c) + (b + d) \cdot i \qquad (6)$$

Умножение

$$(a + b \cdot i) \cdot (c + d \cdot i) = (a \cdot c - b \cdot d) + (a \cdot d + b \cdot c) \cdot i \qquad (7)$$

Деление

$$\frac{a + bi}{c + di} = \frac{(a + bi) \cdot (c - di)}{c^2 + d^2} \qquad (8).$$

Свойство 1. В поле комплексных чисел нельзя задать отношение порядка δ так, чтобы оно обладало одновременно следующими тремя свойствами:

а) линейность, т.е.:

$$(\forall z,u \in C)((z = u) \vee (z \delta u) \vee (u \delta z));$$

б) монотонность относительно сложения, т.е.:

$$(\forall z,u,v \in C)((u \delta v) \to (u + z) \delta (v + z));$$

в) монотонность относительно умножения, т.е.:

$$(\forall z,u,v \in C)((u \delta v) \to (u \cdot z) \delta (v \cdot z)).$$

Замечания. Это свойство фактически означает, что в поле комплексных чисел отсутствует упорядоченность, так как на числовых множествах имеет смысл рассматривать отношение порядка только в том случае, когда оно обладает указанными тремя свойствами. Таким образом, два комплексных числа (если только они оба не принадлежат множеству действительных чисел) *не сравнимы между собой,* т.е. нельзя сказать, что одно из них больше другого.

2. Комплексное сопряжение и его свойства

Определение. Для комплексного числа $z = a + b \cdot i$ число $\bar{z} = a - b \cdot i$ называется *комплексно сопряженным числом.*

Свойство 2. Сумма и произведение комплексно сопряженных чисел есть числа действительные:

$$z+\bar{z}=(a+b\cdot i)+(a-b\cdot i)=2a\in R;$$
$$z\cdot\bar{z}=(a+b\cdot i)\cdot(a-b\cdot i)=a^2+b^2\in R.$$

Свойство 3. Комплексное число z сопряжено само с собой тогда и только тогда, когда оно является действительным числом:

$$\bar{z}=z\Leftrightarrow z\in R.$$

Свойство 4. Число, комплексно сопряженное с числом $\bar{z}$, совпадает с z:

$$\bar{\bar{z}}=z.$$

Замечание. Следующие свойства относятся к применению комплексного сопряжения к операциям над комплексными числами.

Свойство 5. Число, сопряженное сумме комплексных чисел, равно сумме чисел, сопряженных слагаемым:

$$\overline{z+z_1}=\bar{z}+\bar{z_1}.$$

Свойство 6. Число, сопряженное произведению комплексных чисел, равно произведению чисел, сопряженных сомножителям:

$$\overline{z\cdot z_1}=\bar{z}\cdot\bar{z_1}.$$

Свойство 7. Число, сопряженное частному двух комплексных чисел, равно частному чисел, сопряженных числителю и знаменателю:

$$\overline{\left(\frac{z}{z_1}\right)}=\frac{\bar{z}}{\bar{z_1}}.$$

Свойство 8. Число, сопряженное степени комплексного числа z, равно степени с тем же показателем от числа, сопряженного самому z:

$$\overline{(z^n)}=(\bar{z})^n.$$

Свойство 9. Отображение f, которое каждому комплексному числу ставит в соответствие число, ему сопряженное:

$$(\forall z\in C)\left(f:z\to\bar{z}\right),$$

является изоморфным отображением поля комплексных чисел на себя.

3. Тригонометрическая форма комплексного числа

Так как комплексные числа представляют собой упорядоченные пары действительных чисел, то очевидно, что существует взаимно-однозначное соответствие между множеством всех комплексных чисел и множеством всех точек плоскости R × R, заданных двумя действительными декартовыми координатами.

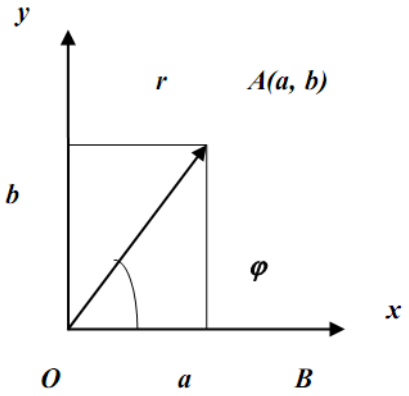


Рис. 1

Пусть комплексное *число* $z = a + b \cdot i$ изображено на плоскости точкой $A(a,b)$ (рисунок 1). Ось абсцисс, по которой откладывается число $a = \operatorname{Re} z$, называется *действительной осью*, а ось ординат, по которой откладывается число $b = \operatorname{Im} z$ – *мнимой осью.*

Как известно, точку на плоскости можно задать не только в декартовой системе координат, но и, например, в полярной (r,φ), где r – ***радиус-вектор*** точки A, φ – угол между радиус-вектором и положительным направлением оси абсцисс.

Связь между декартовыми и полярными координатами точки A можно получить из ΔABC по теореме Пифагора (рис.1).

$$r^2 = a^2 + b^2,\ r = \sqrt{a^2 + b^2},$$

$$\cos\varphi = \frac{a}{r}, \qquad (1)$$

$$\sin\varphi = \frac{b}{r}.$$

Выражая значения $a\ u\ b$ из равенств (1) и учитывая, что $z = a + b \cdot i$, получим:

$$z = r \cdot (\cos\varphi + i \cdot \sin\varphi) \qquad (2).$$

Определение Запись комплексного числа в виде (2) называется *тригонометрической формой комплексного числа*.

Для всякого комплексного числа $z \neq 0$ действительное число r, определенное первым из равенств (1), называется *модулем* комплексного числа z, а действительное число φ, определенное вторым и третьим равенствами, называется *аргументом* числа z:

$$r = |z|,\ \varphi = Arg\ z.$$

Замечания. 1. Для комплексного числа, равного нулю, модуль однозначно не определен. В качестве модуля может выступать любое действительное число.

2. Аргумент комплексного числа z определен однозначно с точностью до периода, т.е., с точностью до целого кратного 2π. Это означает, что если $\varphi = Arg\ z,\ то\ u\ \psi = \varphi + 2\pi k = Arg\ z.$

3. Комплексно сопряженные числа имеют одинаковые модули, аргументы их отличаются только знаком. Геометрически они представляют собой точки плоскости, симметричные относительно оси OX в декартовой системе координат.

Теорема 1. Всякое комплексное число можно представить в тригонометрической форме (2) и притом единственным образом (с учетом замечания 1).

Действия над комплексными числами в тригонометрической форме примут следующий вид.

Пусть z и z_1 – два комплексных числа, записанных в тригонометрической форме:

$$z = r \cdot (\cos\varphi + i \cdot \sin\varphi),\ z_1 = \rho \cdot (\cos\psi + i \cdot \sin\psi).$$

Теорема 2. Чтобы найти произведение двух комплексных чисел, записанных в тригонометрической форме, нужно их модули перемножить, а аргументы сложить:

$$z \cdot z_1 = r \cdot \rho \cdot (\cos(\varphi + \psi) + i \cdot \sin(\varphi + \psi)) \qquad (3).$$

Теорема3. Чтобы разделить комплексное число $z = r \cdot (\cos\varphi + i \cdot \sin\varphi)$

на ненулевое комплексное число $z_1 = \rho \cdot (\cos\psi + i \cdot \sin\psi)$, нужно модуль первого числа разделить на модуль второго, а из аргумента первого числа вычесть аргумент второго:

$$\frac{z}{z_1} = \frac{r}{\rho} \cdot [\cos(\varphi - \psi) + i \sin(\varphi - \psi)] \qquad (4).$$

Определение. Натуральная степень комплексного числа $z \neq 0$ определяется рекуррентно:

$$z^0 = 1,$$
$$z^{n+1} = z^n \cdot z,\ n \in N,$$

если z^n определено.

Теорема 4. Чтобы возвести комплексное число, записанное в тригонометрической форме, в степень с натуральным показателем, нужно модуль этого числа возвести в степень, а аргумент умножить на показатель степени:

$$z^n = r^n \cdot (\cos(n\varphi)) + i \cdot \sin(n\varphi) \qquad (5.)$$

Замечание. Равенство (5) получило также название ***формулы Муавра,*** по имени ученого, который ее обосновал.

Очевидно, что в ряде случаев, когда необходимо выполнить действия со степенями комплексных чисел, более рационально использовать именно тригонометрическую форму записи.

Тригонометрические и показательная функции в области комплексных чисел связаны между собой формулой

$$e^{i\varphi} = \cos\varphi + i \sin\varphi \qquad (6),$$

которая носит название *формулы Эйлера*. Обосновать ее можно с помощью теории степенных рядов. Эта теория будет изложена в курсе математического анализа.

Пусть комплексное число z в тригонометрической форме имеет вид:

$$z = r(\cos\varphi + i \sin\varphi)\ .$$

На основании формулы Эйлера выражение в скобках можно заменить на показательное выражение. В результате получим:

$$z = re^{i\varphi} \qquad (7).$$

Эта запись называется *показательной формой* комплексного числа. Так же, как и в тригонометрической форме, здесь

$$r = |z|,\ \varphi = Arg\ z.$$

4. Нахождение значений корня n-й степени из комплексного числа. Первообразный корень n-й степени из единицы

Определение Корнем n– ной степени из комплексного числа z называется такое комплексное число $u = \sqrt[n]{z}$, для которого выполняется равенство:

$$u^n = z.$$

В поле комплексных чисел справедлива следующая теорема.

Теорема 5. В поле комплексных чисел существует ровно n различных значений корня n– ной степени из любого ненулевого числа $z = r \cdot (\cos\varphi + i \cdot \sin\varphi)$ – $u_0, u_1, ..., u_{n-1}$, которые можно найти по формуле:

$$u_k = \sqrt[k]{r} \cdot (\cos\frac{\varphi + 2\pi k}{n} + i \sin\frac{\varphi + 2\pi k}{n}), n \in \{0,1,...,n-1\} \qquad (10.).$$

Замечания.1. Геометрически все значения корня n– ной степени из комплексного числа z расположены в вершинах правильного n– угольника, вписанного в окружность с центром в начале координат и радиусом, равным модулю числа z.

2. Особое значение имеют корни n– ной степени из единицы, для нахождения которых формула (6) модифицируется следующим образом:

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, n \in \{0,1,...,n-1\} \qquad (11).$$

и которые расположены в вершинах правильного n– угольника, вписанного в окружность с центром в начале координат единичного радиуса, причем одно из значений лежит на оси OX, а каждое следующее получается из предыдущего поворотом на угол, равный $\frac{2\pi}{n}$.

Определение Значение ε_k корня n– ной степени из единицы называется *первообразным корнем,* если все степени числа ε_k от нулевой до $(n-1)$-ой различны и исчерпывают все значения корня n – ной степени из единицы.

Теорема 6. Корни n – ной степени из единицы образуют мультипликативную абелеву группу.

Теорема 7. Если u_k – одно из значений корня n – ной степени из комплексного числа z, то все остальные его значения можно получить, умножая число u_k на различные степени первообразного корня из единицы.

Тема. Алгебры над полем действительных чисел

План

1. Ассоциативные алгебры.

2. Теорема Фробениуса.

3. Дуальные и двойные числа (ассоциативные алгебры над полем действительных чисел размерности 2).

1. Ассоциативные алгебры

Определение. Алгеброй *A* над полем *K* или *K*-алгеброй называется линейное пространство *A* над полем *K*, в котором определена бинарная операция умножения векторов, удовлетворяющая следующим аксиомам:

$1.\ a,b,c \in A\ a(b+c) = ab + ac$

$2.\ a,b,c \in A\ (b+c)a = ba + ca$

$3.\ a,b \in A,\ \alpha \in K\ \alpha(ab) = (\alpha a)b = a(\alpha b).$

Определение. Алгебра *A* над полем *K* называется ассоциативной, если

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

Определение. Алгебра *A* над полем *K* называется коммутативной, если

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

Определение. Алгебра *A* над полем *K* называется алгеброй с делением, если

$a,b \in A\ a \neq 0$ разрешимы уравнения $ax = b$ и $xa = b$

Определение. Рангом алгеброй *A* над полем *K* называется размерность линейного пространства *A* над полем *K* в случае его конечномерности.

Примеры:

1. $M_n(K)$ - алгебра квадратных матриц *n*-ого порядка над полем *K*, где $\dim[M_n(K):K] = n^2$.

2. C - алгебра над полем *R*, где $\dim[C:R] = 2$.

3. H - алгебра над полем C, где $\dim[H:C] = 2$.

Определение. Алгебры *A* и *B* над полем *K* называются изоморфными, если существует биективное отображение $\sigma: A \to B$,удовлетворяющее условиям:

$1.\ a,b \in A\ \sigma(a+b) = \sigma(a) + \sigma(b)$

$2.\ a,b \in A\ \sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$

$3.\ a \in A,\ \alpha \in K\ \sigma(\alpha a) = \alpha\sigma(a).$

Пример. Алгебра квадратных матриц *n*-ого порядка над полем *K* и линейное пространство линейных операторов *n*-мерного линейного пространства над полем *K* (каждому оператору можно поставить в соответствие его матрицу в некотором фиксированном базисе).

2. Теорема Фробениуса

Теорема Фробениуса. Единственными с точностью до изоморфизма конечномерными ассоциативными алгебрами с делением над полем действительных чисел являются алгебры R, C, H.

Доказательство.

Пусть A - конечномерная ассоциативная алгебра с делением над полем действительных чисел и $[A:R]=n$. Возможны случаи:

1. $n=1$. Тогда $A \cong R$.

2. $n>1$. Тогда в алгебре A есть хотя бы один элемент, который не является действительным числом. Обозначим этот элемент через u. В $R[x]$ существует неприводимый многочлен $m_u(x)$, корнем которого является u. Поскольку наивысшая степень неприводимого многочлена с действительными коэффициентами над полнм действительных чисел равна 2 и элемент $u \notin R$, а, значит, не может быть корнем ни непостоянного многочлена, ни многочлена первой степени, то $\deg m_u(x)=2$.

Пусть $m_u(x)=x^2+2px+q$. Так как $m_u(u)=0$, то $u^2+2pu+q=0$. Выделим полный квадрат в левой части. Получим $u^2+2pu+p^2=-q+p^2$. Поскольку многочлен $x^2+2px+q \in R_{[x]}$ неприводим, то $D/4 = p^2-q<0 \Rightarrow q-p^2>0$.

Рассмотрим число $i=\dfrac{u+p}{\sqrt{q-p^2}}$, причем $\left(\dfrac{u+p}{\sqrt{q-p^2}}\right)^2 = i^2 = -1$, $i \in A, i \notin R$. Тогда в алгебре A система $\{1,i\}$ является линейно независимой, а, значит, $A \cong C$ в случае $n=2$.

3. $n>3$. Тогда в алгебре A найдется еще один элемент $v \in A, v \notin R$ такой, что система $\{1,i,v\}$ линейно независима и v - корень подходящего неприводимого многочлена $m_v(x)=x^2+2rx+t$ второй степени. Аналогично пункту 2 формируется элемент $j_0=\dfrac{v+r}{\sqrt{t-r^2}}$, который также удовлетворяет условиям $j_0{}^2=-1$ и $j_0 \in A, j_0 \notin R$.

Поскольку $n>3$ система $\{1,i,j_0\}$ линейно независима.

Рассмотрим пару элементов $i+j_0$ и $i-j_0$. Оба элемента не принадлежат полю действительных чисел, а, значит, является корнями неприводимых над полем действительных чисел многочленов с действительными коэффициентами x^2-ax-b и x^2-cx-d соответственно. Тогда

$$\begin{cases}(i-j_0)^2-a(i-j_0)-b=0\\(i-j_0)^2-c(i-j_0)-d=0\end{cases}$$

$$\begin{cases}i^2+j_0^2+ij_0+j_0i-a(i-j_0)=b\\i^2+j_0^2-ij_0-j_0i-c(i-j_0)=d\end{cases}$$

Заменив i^2 и j_0^2 на -1 и сложив уравнения системы, получим

$$i(a+c)+j_0(a-c)+(4+b+d)=0.$$

Поскольку $\{1, i, j_0\}$ система линейно независима, то $a = b = 0$ и $4 + b + d = 0$. Возвращаясь к исходному соотношению, получим $i^2 + j_0^2 + ij_0 + j_0 i = b \Rightarrow ij_0 + j_0 i = b + 2$.

Введем число $t = \frac{1}{2}(b+2) \in R \Rightarrow ij_0 + j_0 i = 2t \in R$. Рассмотрим число

$$j_1 = j_0 + ti \Rightarrow (j_1)^2 = (j_0 + ti)^2 = j_0^2 + j_0 it + tij_0 + t^2 i^2 = -1 + t^2 + (j_0 i + ij_0)t = -1 + t^2 + 2t^2 = -1 + t^2$$

Зная, что $-1 + t^2 < 0$, введем число $j = \frac{j_1}{\sqrt{1 - t^2}}$. Поскольку $j^2 = -1$ система $\{1, i, j\}$ линейно независима.

Вычислим $ij + ji = \frac{ij_1 + j_1 i}{\sqrt{1-t^2}} = \frac{1}{\sqrt{1-t^2}}(ij_0 + j_0 i + i^2 t + i^2 t) = \frac{1}{\sqrt{1-t^2}}(2t - 2t) = 0$.

Таким образом получается, что нашлась линейно независимая система $\{1, i, j\}$ такая, что $i^2 = j^2 = -1$ и $ij + ji = 0$.

Обозначим через $k = ij$. Покажем, что система $\{1, i, j, k\}$ линейно независима. Поскольку ранее установлена линейная независимость $\{1, i, j\}$, то остается показать, что k линейно не выражается через $1, i, j$. Предположим, что $k = \alpha + \beta i + \gamma j$, где $\alpha, \beta, \gamma \in R$.

$ik = \alpha i - \beta + \gamma k$, так как $ik = i(ij) = i^2 j = -j$. Тогда

$$-j = \alpha i - \beta + \gamma k = \alpha i - \beta + (\alpha + \beta i + \gamma j) = (\alpha + \gamma\beta)i + \gamma^2 j - (\alpha\gamma - \beta) \Rightarrow$$

$$\Rightarrow (\alpha + \gamma\beta)i + (1 + \gamma^2) j + (\alpha\gamma - \beta) = 0, \text{ где } 1 + \gamma_2 \neq 0.$$

Последнее противоречит линейной независимости элементов $1, i, j$, следовательно, k линейно не выражается через $1, i, j$ и система $\{1, i, j, k\}$ линейно независима.

Нетрудно проверяется, что элементы $1, i, j, k$ относительно умножения образуют следующую таблицу:

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

Например, $jk = j(ij) = (ji)j = (-ij)j = -ij^2 = i$.

Таким образом, $A \cong H$ в случае $n = 4$.

4. $n > 4$. Тогда существует элемент $w \in A, w \notin R, w^2 = -1$.

Предположим, что w линейно не выражается через $1, i, j, k$, т.е. $1, i, j, k, w$ -

$$iw + wi = a_1$$

линейно независима. Пусть $jw + wj = b_1$.

$$kw + wk = c_1$$

Найдем произведение $wk = w(ij) = (wi)j = (a_1 - iw)j = a_1 j - i(wj) = a_1 j - i(b_1 - jw) =$

$$= a_1 j - ib_1 + i(jw) = a_1 j - b_{1i} + (ij)w = a_1 j - b_1 i + kw = a_1 j - b_1 i + (c_1 - wk) \Rightarrow$$

$$\Rightarrow 2wk = a_1 j - b_1 i + c_1.$$

Умножим последнее равенство на k. Получим $a_1 i + b_1 j + c_1 k + 2w = 0$, где $2w \neq 0$, что противоречит линейной независимости системы $\{1, i, j, k, w\}$. Следовательно, система $\{1, i, j, k, w\}$ линейно зависима.

Таким образом, n не может быть больше 4, а, значит, размерности всех конечномерных алгебр над полем действительных чисел совпадают с одним из чисел 1, 2, 4.

3. Дуальные и двойные числа (ассоциативные алгебры над полем действительных чисел размерности 2)

Опишем все ассоциативные алгебры над полем R размерности 2.

Нетрудно устанавливается, что множества $D_1 = \{a + bi_1 \mid a,b \in R, i_1 \in R, i_1^2 = 1\}$ и $D_0 = \{a + bi_0 \mid a,b \in R, i_0 \in R, i_0^2 = 0\}$ образуют ассоциативные алгебры, которые договоримся называть алгебрам двойных чисел и дуальных чисел соответственно.

Теорема. Любая коммутативная ассоциативная алгебра с единицей над полем действительных чисел R размерности 2 изоморфна одной из из алгебр C, D_1, D_0.

Доказательство:

Пусть $[A:R] = 2$, где A - коммутативная ассоциативная алгебра с единицей e. Рассмотрим $R_e = \{re \mid r \in R\}$. Нетрудно устанавливается, что R_e изоморфно полю R. Тогда, с точностью до изоморфизма, можно утверждать, что $R \leq A$ (R подполе поля A). Последнее означает, что в A найдется элемент $j \notin R, j \in A$ такой, что система $\{e, j\}$ образует базис алгебры A над полем R.

$j^2 \in A \Rightarrow j^2 = u + vj$ для некоторых $u, v \in R$. $j^2 = u + vj \Rightarrow j^2 - vj + v^2/4 = u + v^2/4 \Rightarrow$

$\Rightarrow (j - v/2)^2 = u + v^2/4$.

Возможны случаи:

1. $u + v^2/4 < 0$.

Существует положительное действительное число k такое, что

$$u + v^2/4 = -k^2 \Rightarrow (j - v/2)^2 = -k^2 \Rightarrow \frac{(j - v/2)^2}{k^2} = -1 \Rightarrow \left(\frac{j}{k} - \frac{v}{2k}\right)^2 = -1 \Rightarrow \frac{j}{k} - \frac{v}{2k} = i \Rightarrow j = \frac{v}{2} + ki$$

Тогда $\{e, i\}$ - система порождающих в A. Покажем, что $\{e, i\}$ - базис в A. Предположим, что $xe + yi = 0 \Rightarrow x + y\frac{j}{k} - y\frac{v}{2k} = 0 \Rightarrow x - y\frac{v}{2k} = 0 \wedge \frac{y}{k} = 0 \Rightarrow x = 0 \wedge y = 0$.

Таким образом $A = C$.

2. $u + v^2/4 = 0 \Rightarrow (j - v/2)^2 = 0 \Rightarrow j - v/2 = i_0$. Аналогично устанавливается, что $\{e, i_0\}$ - базис в A. Следовательно, $A = D_0$.

3. $u + v^2/4 > 0$.

Существует положительное действительное число m такое, что

$$u + v^2/4 = m^2 \Rightarrow (j - v/2)^2 = m^2 \Rightarrow \frac{(j - v/2)^2}{m^2} = 1 \Rightarrow \left(\frac{j}{m} - \frac{v}{2m}\right)^2 = 1 \Rightarrow \frac{j}{m} - \frac{v}{2m} = i_1 \Rightarrow j = \frac{v}{2} + mi_1$$

Тогда $\{e, i_1\}$ - система порождающих в A. Аналогично устанавливается, что $\{e, i_1\}$ - базис в A. Следовательно, $A = D_1$.

Замечание. Наличие единицы e позволяет включить R в A, а ассоциативность и коммутативность позволяют выполнять действия, указанные выше.

что и требовалось доказать.

Теорема. Алгебры D_1, D_0 не являются полями.

Доказательство

Предположим, что элемент $0 \neq i_0 \in D_0$ обратим. Тогда существует элемент $a + bi_0$ такой, что $(a+bi_0)i_0 = 1 \Rightarrow ai_0 = 1 \Rightarrow -1 + ai_0 = 0$. Последнее противоречит линейной независимости элементов $\{1, i_0\}$. Следовательно, предположение об обратимости элемента i_0 оказывается ложным, а, значит, D_0 не является полем.

Аналогично устанавливается необратимость элемента $1 + i_1 \in D_1$. Тогда D_1 также не является полем.

что и требовалось доказать.

Теорема. Алгебры D_1, D_0 существуют.

Замечание. Алгебры C, D_0 и D_1 являются подалгебрами алгебры $M_2(R)$.

9. Методические материалы для обучающихся по подготовке к практическим занятиям

Тема. Алгебраические системы

План

1. Отношения эквивалентности. Отношения порядка. Разбиения множества.

2. Понятие и свойства бинарной алгебраической операции.

3. Группы. Нормальные делители. Кольца и поля.

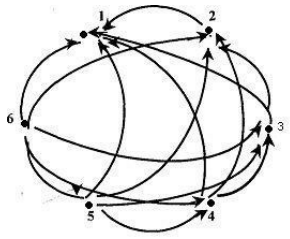
1. Отношения эквивалентности. Отношения порядка. Разбиения множества

Задание 1. Дано множество *A*={1;2;3;4;5;6}. На нем задано бинарное отношение ρ «больше», т. е. $< x, y > \in \rho \Leftrightarrow x > y$.

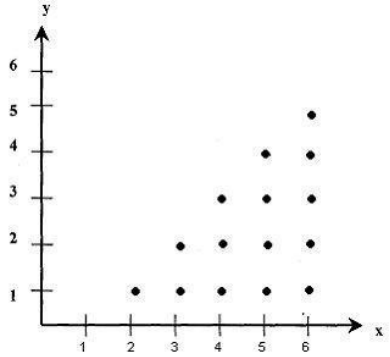
Построить граф и график этого отношения. Какими свойствами обладает это отношение?

Решение.

1) Граф указанного отношения:



2) График этого отношения:



3) Рефлексивность. Если бы это отношение было рефлексивным, $(\forall x \in A)\, x > x$, например, было бы верно 2 > 2 (ложь). Значит отношение «>» на *A* не является рефлексивным.

Симметричность. Если бы это отношение было симметричным на множестве *A*, то $(\forall x, y \in A)(x > y \Rightarrow y > x)$. Например, 3 > 2 => 2 > 3(ложь). Значит, отношение « > » на *A* не является симметричным.

Транзитивность. Если бы это отношение было транзитивным на множестве *A*, то $(\forall x, y, z \in A)(x > y \wedge y > z \Rightarrow x > z)$. Это утверждение истинно для любых натуральных чисел, т. е. и для чисел из *A*. Значит, отношение « > » на *A* является транзитивным.

Асимметричность: Ни для каких чисел *A* не может быть одновременно истинным

$$\begin{cases} x > y \\ y > x \end{cases},$$

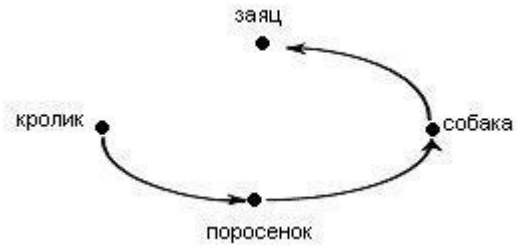
т.е. отношение «>» на *A* асимметрично. Отношение «>» на множестве *A* является отношением строгого порядка, т. к. оно асимметрично и транзитивно.

Т.к. отношение «>» на множестве *A* связное и является отношением строгого порядка, то оно есть отношение строгого линейного порядка.

Задание 2. Построить граф отношения «легче, чем» на множестве *A* = {кролик, заяц, собака, поросёнок}, если известно, что заяц тяжелее собаки, кролик легче поросёнка, а собака тяжелее поросёнка. Кто из животных самый легкий, кто – самый тяжелый.

Решение.

Строим граф указанного отношения:



Ответ: кролик – самый легкий, заяц – самый тяжелый.

На множестве людей Земли введено бинарное отношение «быть родственником по крови». Будет ли это отношение отношением эквивалентности?

Решение.

Задание 3. Обозначим через *A* множество людей Земли, а заданное отношение буквой ρ. Тогда $x\rho y$ <=> человек *x* является родственником человека *y*. Что бы отношение ρ было отношением эквивалентности, оно должно быть рефлексивным, симметричным, транзитивным.

Рефлексивность. Если бы ρ было рефлексивным, то было бы верно: $(\forall x \in A)\ x\rho x$, т. е. любой человек Земли является родственником самому себе (истина), т.е. отношение ρ на *A* рефлексивно.

Симметричность. Если бы ρ было симметрично. ($x\rho y$ => $y\rho x$), т. е. если бы человек *x* был родственником человека *y*, то *y* был бы родственником человека *x* (истина). Значит, отношение ρ на *A* симметрично.

Транзитивность. Если бы ρ было транзитивно на *A*, то если бы человек *x* был бы родственником человека *y*, а *y* был родственником человека *z*, то *x* был бы родственником *z*. Но это не обязательно. Например, человек *x* родственник для *y* по матери, а *y* – родственник для *z* по отцу. Тогда *x* и *y* могут не быть родственниками по крови. Значит, отношение ρ на *A* не является транзитивным.

Следовательно, отношение «быть родственником по крови» на множестве людей Земли не является отношением эквивалентности.

Задание 4. Сформулировать свойства отношения «больше в 2 раза», заданного на множестве натуральных чисел.

Решение.

«Больше в 2 раза» – это краткая запись отношения «число x больше числа y в 2 раза».

Это отношение антисимметрично, так как выполняется условие: из того, что число x больше числа y в 2 раза, следует, что число y не больше числа x в 2 раза.

Данное отношение не обладает свойством рефлексивности, потому что ни про одно число нельзя сказать, что оно больше самого себя в 2 раза.

Заданное отношение не транзитивно, так как из того, что число x больше числа y в 2 раза, а число y больше числа z в 2 раза, следует, что число x не может быть больше числа z в 2 раза.

Это отношение на множестве натуральных чисел свойством связности не обладает, так как существуют пары таких чисел x и y, что ни число x не больше числа y в два раза, ни число y не больше x в 2 раза. Например, это числа 7 и 3, 5 и 8 и др.

Задания

1. На множестве $A=\{1;5;7\}$ задано бинарное отношение $\rho=\{(1;1),(1;7),(5;1),(5;5),(7;5)\}$. 1) Найти $\rho^{-1};\overline{\rho};\overline{\rho}^{-1}$; 2) начертить граф и график бинарного отношения ρ.

2. На множестве задано бинарное отношение с помощью графика. Определить, какими свойствами оно обладает. Добавить одну точку так, чтобы бинарное отношение стало рефлексивным. Добавить две точки так, чтобы оно стало транзитивным.

3. На множестве натуральных чисел задано бинарное отношение ρ следующим образом: $x\rho y \Leftrightarrow |y-x|=12$. Определить, какими свойствами оно обладает.

4. Для следующего бинарного отношения, определённого на множестве натуральных чисел, найти область определения, область значений, указать свойства и нарисовать график: $x\rho y \Leftrightarrow x=3y$.

5. Указать свойства бинарного отношения ρ, если ρ - это отношение «работать на одной кафедре» во множестве преподавателей и сотрудников института.

6. Определить, является ли следующее бинарное отношение отображением. Если да, то является ли оно инъекцией, сюръекцией, биекцией? а) $\varphi=\{(x;y)\in R\times R \mid y=x^2\}$, б) $f=\{(x;y)\in N\times N \mid x-y=3\}$.

7. Выяснить, является ли данное отображение инъективным, сюръективным: $f:R\to R,\ x\to \log_2\left(x^2+\frac{1}{2}\right)$.

8. Дано множество $A=\{1;2;3;4\}$; $A_1=\{1;2\}, A_2=\{3\}, A_3=\{4\}$ - разбиение этого множества на классы. Построить по данному разбиению отношение эквивалентности.

9. Доказать, что $\sigma=\{(a;a);(b;b);(c;c);(d;d);(c;d);(d;c);(a;b);(b;a)\}$ является отношением эквивалентности и построить по нему разбиение множества $A=\{a,b,c,d\}$ на классы.

10. На множестве целых чисел задано бинарное отношение ρ следующим образом: $x\rho y \Leftrightarrow (x-y)\vdots 7$. Доказать, что ρ – отношение эквивалентности, и построить разбиение на классы по данному отношению эквивалентности.

11. Построить разбиение на классы по отношению равенства на множестве Z, предварительно убедившись, что оно является отношением эквивалентности.

12. M – множество городов планеты Земля, ρ – отношение «город x расположен в том же государстве, что и город y». Доказать, что ρ является отношением эквивалентности, и построить по нему разбиение множества M на классы.

13. Дано множество $A = \{a, b, c\}$. Сколько можно задать на нём разных отношений эквивалентности?

2. Понятие и свойства бинарной алгебраической операции

Задание 1. Примерами бинарных операций, заданных на числовых множествах, могут служить операции обычного сложения и умножения чисел, примерами унарных операций – взятие обратного и противоположного элементов, возведение в степень или извлечение корня, примерами нульарных операций - выделение нуля или единицы.

Задание 2. Множество N натуральных чисел по операции обычного умножения образует абелев моноид <N, • >.

Множество N по операции обычного сложения также образует абелев моноид <N, + >, так как:

$$(\forall a, b \in N) \quad a + b \in N;$$
$$(\forall a, b, c \in N) \quad a + (b + c) = (a + b) + c;$$
$$(\forall a, b \in N) \quad a + b = b + a;$$
$$(\forall a \in N) \quad a + 0 = 0 + a = a;$$

однако операция сложения не обратима на N, так как, например, для числа 2 не существует обратного (противоположного) элемента в множестве N.

Так как $(\forall a, b, c \in N) \quad c\cdot(a + b) = c\cdot a + c\cdot b$, то умножение на N дистрибутивно относительно сложения.

Из сказанного следует, что структура <N, +, • > образует ассоциативно-коммутативное полукольцо с единицей.

Задание 3.

1). Операция обычного сложения на множестве всех целых чисел Z*:*

- ассоциативна, т.к. $(\forall a, b, c \in Z) \quad a +(b + c) = (a + b) + c$;
- коммутативна, т.к. $(\forall a, b \in Z)\ a + b = b + a$;
- обладает двусторонним нейтральным элементом, роль которого играет целое число 0*:* $(\exists 0 \in Z)\ (\forall a \in Z) \quad a + 0 = 0 + a = a$;
- обратима, т.к. $(\forall a \in Z)\ (\exists - a \in Z) \quad -a + a = a + (-a) = 0$;
- двусторонне сократима, т.к. $(\forall a, b, c \in Z)\ (a + c = b + c \Rightarrow a = b)$.

2). Операция обычного умножения на множестве всех целых чисел *Z* дистрибутивна относительно операции сложения, так как:

$$(\forall a, b, c \in Z) \quad c(a + b) = ca + cb \text{ и}$$
$$(\forall a, b, c \in Z) \quad (a + b)c = ac + bc.$$

Задания

1. Выяснить, какими свойствами обладают следующие бинарные операции, заданные на указанных множествах:

2. $A = R, (\forall a, b \in R)\ a \circ b = \dfrac{a+b}{2}$;

3. $A = R^+, a \circ b = a^b$;

4. $A = N, a * b = \max\{a; b\}$.

5. Определить, какой алгебраической структурой является множество A по операции умножения, если: а) $A = \{2^n \mid n \in Z\}$, б) $A = \{x + y\sqrt{3} \mid x, y \in R\}$.

6. Являются ли алгебраическими следующие числовые операции:
   a. операция деления на множестве Q;
   b. операция деления на множестве Z;
   c. операция вычитания на множестве Z;
   d. операция вычитания на множестве N;

e. операция извлечения корня на множестве R;
f. операция извлечения корня на множестве A = {x∈R, x > 1};
g. операция извлечения корня на множестве A = {x∈R, x > 2}?

7. В группе из четырех подростков: Саши, Даши, Пети и Маши взаимоотношения определяются следующими условиями:

a. У Саши и Даши авторитет Даша.
b. У Саши и Маши авторитет Саша.
c. У Саши авторитет Саша.
d. У Даши и Маши авторитет Саша.
e. У Даши авторитет Даша.
f. У Маши авторитет Петя.
g. У Пети и Даши авторитет Петя.
h. У Пети и Маши авторитет Петя.
i. У Пети и Саши авторитет Саша.
j. У Пети авторитет Саша.

8. Можно ли утверждать, что на множестве из четырех человек задана бинарная алгебраическая операция? Каковы ее свойства?

9. Какую структуру образует множество A по операции «*»:

a. $A = R^+$; $x*y = \frac{x+y}{2}$.
b. A = Z; x*y = x + y – 1.
c. A = Q; $x*y = \sqrt{xy}$.
d. A = N; x*y = 1.
e. A = R; $x*y = xy^2$.
f. $A = \{a + b\sqrt{3} \mid a, b \in Q, a^2 + b^2 \neq 0\}$; операция «*» - операция обычного сложения чисел.
g. $A = \{a + b\sqrt{5} \mid a, b \in Q, a^2 + b^2 \neq 0\}$; операция «*» - операция обычного умножения чисел.
h. $A = \{\frac{a}{7^k} \mid a \in Z, k \in N\}$; операция «*» - операция обычного сложения чисел.
i. A = N; x*y = max{x, y}.
j. A = Z; x*y = |x – y|.

3. Группы. Нормальные делители. Кольца и поля

Задание 1. Аддитивная группа всех целых чисел изоморфна своей подгруппе, состоящей из четных чисел, так как отображение $\varphi: Z \to 2Z$ такое, что:

$$(\forall x \in Z) \quad \varphi(x) = 2x,$$

является изоморфизмом групп, так как очевидно, что φ - биективно и $(\forall x, y \in Z)$ $\varphi(x + y) = 2(x + y) = 2x + 2y = \varphi(x) + \varphi(y)$.

Задание 2. Аддитивная группа всех действительных чисел изоморфна мультипликативной группе всех положительных действительных чисел:

$$<R, +> \cong <R^+, \bullet>,$$

так как отображение $\varphi: R \to R^+$, при котором:

$$(\forall x \in R) \quad \varphi(x) = e^x$$

является биекцией, поскольку:

$$(\forall x, y \in R) \quad \varphi(x) = \varphi(y) <=> e^x = e^y <=> x = y,$$

$(\forall r \in R^+)$ $(\exists x \in R)$: $\varphi(x) = y$, а именно, $x = \ln y$, т.к. $\varphi(\ln y) = e^{\ln y} = y$

и сохраняет групповую операцию:

$$(\forall x, y \in R) \quad \varphi(x + y) = e^{x+y} = e^x \bullet e^y = \varphi(x) \bullet \varphi(y).$$

Задания

1. Выяснить, образует ли кольцо относительно обычных сложения и умножения множество натуральных чисел.

2. Выяснить, является ли $\langle M,+,\cdot\rangle$ кольцом, если $M=\{a+b\sqrt{3}\,|\,a,b\in Z\}$.

3. Определить, является ли $\langle Z,*,\circ\rangle$ кольцом, полем, если $(\forall a,b\in Z)$ $a*b=a+b+1,\ a\circ b=ab+a+b$.

4. Гомоморфны ли алгебры $\langle Z,+\rangle$ и $\langle 2Z,+\rangle$, если задано отображение $\varphi: Z\to 2Z$ по следующему правилу: $(\forall x\in Z)\,\varphi(x)=2x$? Является ли φ изоморфизмом?

5. Выяснить, является ли $\varphi:\langle Z^{+},+\rangle\to\langle Z,\cdot\rangle$ изоморфизмом, если $\varphi(x)=7x$.

6. Выяснить, является ли φ гомоморфизмом (изоморфизмом), если: $\varphi:\langle Z,*,\circ\rangle\to\langle Z,+,\cdot\rangle,\ \varphi(a)=a+5,\ a*b=a+b+5,\ a\circ b=ab+5a+5b+20$;

$\varphi:\langle Z,+,\cdot\rangle\to\langle Z,+,\cdot\rangle,\ \varphi(a)=0$.

7. Верно ли, что…а) множество с заданной на нём бинарной операцией – это группоид; б) моноид – это группоид, в котором существует нейтральный элемент; в) группа – это моноид, в котором для каждого элемента существует обратный?

8. Выяснить, какой алгебраической структурой является $\langle R\setminus\{0\},*\rangle$, если $a*b=5ab\ \ \forall a,b\in R\setminus\{0\}$.

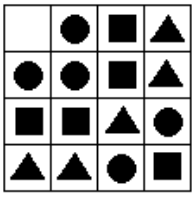
9. Определить, является ли $\langle A,+\rangle,\ A=\{12^{k}\,|\,k\in N\cup\{0\}\}$, подгруппой аддитивной группы целых чисел.

10. Определить, является ли $\langle M,+\rangle$ подгруппой аддитивной группы действительных чисел, если $M=\{a+b\sqrt{5}|a,b\in Q\}$.

11. Определить, будет ли мультипликативная алгебра положительных действительных чисел подгруппой аддитивной группы действительных чисел.

12. Составить кластер понятий по теме «Группа» и обосновать его.

13. (Задачао наследовании признака). Пусть имеется конечное множество *M* простейших существ, каждое из которых обладает одним из признаков *A, B, C*. Пусть, например, эти признаки характеризуют форму глаз: соответственно круглые, квадратные и треугольные. Известно, что в результате слияния двух существ *X* и *Y* получается одно новое существо *Z*. При этом наследование формы глаз осуществляется по закону «*» описанному таблицей на рисунке:

14. 

15. В результате эволюции существ остается одно существо. Доказать, что форма глаз оставшегося существа не зависит от того, в каком порядке сливаются существа.

16. К кубику Рубика применили последовательность поворотов. Доказать, что применяя ее несколько раз, можно привести кубик в начальное состояние.

17. Доказать, что множество всех наборов фиксированной длины *n,* составленных из 0 и 1, образует аддитивную группу по операции суммирования по модулю два. Что представляет собой элемент, противоположный произвольному элементу а этой группы?

18. Восстановить цепочку понятий между понятиями «отображение» и «изоморфизм групп», в которой каждое следующее понятие образуется из предыдущего через видовое отличие.

19. Построить левое и правое разбиения группы симметрий правильного треугольника на смежные классы: а) по подгруппе вращений этого треугольника; б) по подгруппе $A=\{R_0,a\}$, где *a* – одна из симметрий.

20. Построить левое и правое разложения мультипликативной группы действительных чисел на смежные классы по подгруппе $A=\{-1;1\}$.

21. Построить таблицу Кэли для группы симметрий квадрата.

22. Построить фактор-группу аддитивной группы целых чисел по ее подгруппе целых чисел, кратных пяти. Построить таблицу Кэли для этой группы и найти элемент, противоположный элементу 2+B.

23. Дано множество $F=\{f_1;\ f_2;\ f_3;\ f_4\}$, где $f_1(x)=x,\ f_2(x)=-x,\ f_3(x)=\frac{1}{x},\ \ f_4(x)=-\frac{1}{x}$. Выяснить, образует ли данное множество группу по операции композиции функций. Если да, то найти все подгруппы этой группы и построить разбиение на смежные классы по какой-либо подгруппе.

24. Определить, образует ли группу по операции умножения множество классов вычетов, взаимно простых с модулем m=8.

Тема. Теория делимости в кольце целых чисел

План

1. Деление целых чисел с остатком.

2. НОД и НОК целых чисел. Алгоритм Евклида.

1. Деление целых чисел с остатком.

Метод анализа остатков

Суть метода состоит в рассмотрении случаев различных остатков от деления на заданное число, что позволяет в конечном итоге решить поставленную задачу. В примерах этого пункта использовались следующие свойства остатков: остатки, полученные при делении двух натуральных чисел на некоторое натуральное число q, можно складывать (вычитать), перемножать при выполнении соответствующих действий над самими числами. Если при выполнении этих операций получится число, превышающее делитель q, то оно опять-таки заменяется остатком от деления на q.

Эти свойства остатков более наглядно формулируются на языке теории сравнений, основные положения которой будут рассмотрены позже.

Пример 1. Докажите, что квадраты натуральных чисел не дают остатка 2 при делении на 3.

Решение. Число n может давать при делении на 3 остатки $0,1,2$. Составим таблицу:

Остаток числа n при делении на 3	Остаток числа n^2 при делении на 3
0	0
1	1
2	1

Поясним заполнение третьей строки таблицы:

$$n=3q+2\Rightarrow n^2=(3q+2)^2=9q^2+12q+4=3(3q^2+4q+1)+1.$$

Пример 2. Существует ли такая степень двойки, из которой перестановкой можно получить другую степень двойки?

Решение. Пусть число $n=\overline{a_k a_{k-1}\ldots a_0}=2^m$ есть некоторая степень двойки. Вопрос заключается в следующем: если мы переставим цифры этого числа в произвольном порядке, можем ли при этом снова получить некоторую степень числа 2? (Например, $n=128=2^7$, но ни одна перестановка цифр числа 128 не является степенью двойки).

Воспользуемся следствием из признака делимости на 9: любые два числа, отличающиеся лишь порядком следования цифр, дают при делении на 9 одинаковые остатки, и рассмотрим, какие остатки при делении на 9 могут давать числа вида 2^m:

Степень числа 2	Остаток степени при делении на 9
2^1	2
2^2	4
2^3	8
2^4	7
2^5	5
2^6	1
2^7	2
2^8	4
…	…

Докажем, что последовательность остатков при делении на 9 степеней двойки $2,4,8,7,5,1$ периодична с периодом 6. Для этого рассмотрим разность $2^{m+6}-2^m=2^m\cdot 63$ – очевидно, она делится на 9, следовательно, через 6 шагов остатки будут повторяться.

Предположение. Допустим теперь, что две степени двойки отличаются только порядком следования цифр (количество цифр одинаково!). Тогда они дают при делении на 9 одинаковые остатки, что возможно лишь через 6 шагов (т.е. 6 раз умножаем число на 2). Тогда одна из степеней двойки будет больше другой по величине не менее чем в $2^6=64$ раза, и, следовательно, в ней должно быть большее количество цифр. Получили противоречие с предположением.

Ответ: Не существует такая степень двойки, из которой перестановкой можно получить другую степень двойки.

Пример 3. Пусть остаток от деления натурального числа m на 7 равен 3. Найти остаток от деления на 7 числа $3m^2+5m+1$.

Решение. Из условия следует, что число m имеет вид: $m=7k+3$.

Тогда $3m^2+5m+1=3(7k+3)^2+5(7k+3)+1=7(21k^2+23k+6)+1$.

Ответ: остаток от деления числа $3m^2+5m+1$ на 7 равен 1.

Пример 4. Доказать, что при любых целых x число $x(x^2+5)$ делится нацело на 6.

Решение. Разобьём множество всех целых x на 6 групп в зависимости от остатка при делении на 6, т.е. рассмотрим 6 случаев: $x=6n+q$, где $q\in\{0,1,2,3,4,5\}$.

1) Пусть целое число делится на 6 нацело, то есть $x=6n$, тогда $x(x^2+5)=6n\cdot(36n^2+5)\vdots 6$.

2) Пусть целое число при делении на 6 даёт остаток 1, то есть $x=6n+1$, тогда

$$x(x^2+5)=(6n+1)\cdot((6n+1)^2+5)=$$
$$=(6n+1)(36n^2+12n+6)=(6n+1)\cdot 6\cdot(6n^2+2n+1)\vdots 6.$$

3) Пусть целое число при делении на 6 даёт остаток 2, то есть $x = 6n + 2$, тогда
$x(x^2 + 5) = (6n + 2) \cdot ((6n + 2)^2 + 5) =$
$= (6n + 2)(36n^2 + 24n + 9) = 2 \cdot (3n + 1) \cdot 3 \cdot (12n^2 + 8n + 3) \vdots 6.$

4) Пусть целое число при делении на 6 даёт остаток 3, то есть $x = 6n + 3$, тогда
$x(x^2 + 5) = (6n + 3) \cdot ((6n + 3)^2 + 5) = (6n + 3)(36n^2 + 36n + 14) =$
$= 3 \cdot (2n + 1) \cdot 2 \cdot (18n^2 + 18n + 7) \vdots 6.$

5) Пусть целое число при делении на 6 даёт остаток 4, то есть $x = 6n + 4$, тогда
$x(x^2 + 5) = (6n + 4) \cdot ((6n + 4)^2 + 5) =$
$= (6n + 4)(36n^2 + 48n + 21) = 2 \cdot (3n + 2) \cdot 3 \cdot (12n^2 + 16n + 7) \vdots 6.$

6) Пусть целое число при делении на 6 даёт остаток 5, то есть $x = 6n + 5$, тогда
$x(x^2 + 5) = (6n + 5) \cdot ((6n + 5)^2 + 5) =$
$= (6n + 5)(36n^2 + 60n + 30) = (6n + 5) \cdot 6 \cdot (6n^2 + 10n + 5) \vdots 6.$

Так как других вариантов делимости на 6 целых чисел нет, то мы рассмотрели все целые числа x и доказали, что в каждом из шести случаев выражение $x(x^2 + 5)$ кратно 6.

Пример 5. Учительница принесла в класс счётные палочки. Дети раскладывали их в пакетики. Когда разложили по 2 палочки в каждый пакетик, то осталась 1 лишняя палочка. Затем разложили по 13 штук в пакетик, и тогда осталось 7 лишних палочек. Когда же палочки разложили по 9 штук в пакетик, то лишних не осталось. Сколько, самое меньшее, было счётных палочек?

Решение. Пусть всего было n счётных палочек. Тогда условия задачи приводят к системе

$$\begin{cases} n = 2l + 1 & (l = 0,1,2,\ldots), \\ n = 13k + 7 & (k = 0,1,2,\ldots), \\ n = 9m & (m \in N), \\ n_{\min} = ? \end{cases}$$

Таким образом, требуется найти наименьшее натуральное нечётное число n, делящееся на 9 и дающее при делении на 13 остаток 7. Заметим, что в силу нечётности $n = 13k + 7$ число k должно быть чётным, то есть $k = 2p$ $(p = 0,1,2,\ldots)$, причём меньшему n соответствует меньшее p, но тогда имеем
$n = 26p + 7 = 27p + 9 - (p + 2)$.

Поскольку числа n и $27p + 9$ делятся нацело на 9, то, следовательно, число $p + 2$ также должно быть кратно 9 (и при этом быть минимальным). Наименьшее целое неотрицательное p, для которого выполняются эти условия, равно 7, откуда находим $n = 26p + 7 = 26 \cdot 7 + 7 = 189$.

Ответ: Самое меньшее – 189 счётных палочек.

Пример 6. Сумма неполного частного и остатка, полученных при делении некоторого натурального числа на 100, равна сумме неполного частного и остатка, полученных при делении того же числа на 1995. Чему могут быть равны неполные частные?

Решение. Пусть n – натуральное число из условия задачи. Тогда:

$$\begin{matrix} n = 100q + r \\ n = 1995t + k \end{matrix},$$

где q,t – неполные частные, r,k – остатки при делении на 100 и 1995 соответственно. Тогда $100q+r=1995t+k$ и по условию $q+r=t+k$. Из этих двух равенств получаем:

$$99q+(q+r)=1994t+(t+k)\Rightarrow 99q=1994t.$$

Разложив числа 99 и 1994 на простые множители, получим: $3^2\cdot 11\cdot q=2\cdot 997\cdot t$. Так как числа 99 и 1994 взаимно простые, то из последнего равенства следует, что q должно быть кратно 1994, t – кратно 99.

Ответ: $q=1994m,\ t=99m,\ m\in N$.

Задания

1. На столе лежат книги, которые надо упаковать. Если их связать в одинаковые пачки по 4, по 5 или по 6 книг, то каждый раз останется одна лишняя книга, а если связать по 7 книг в пачку, то лишних книг не останется. Какое наименьшее количество книг может быть на столе?

2. Найдите наименьшее трёхзначное число, которое при делении на 2 даёт остаток 1, при делении на 3 даёт остаток 2, при делении на 5 даёт остаток 3 и которое записано тремя различными нечётными цифрами.

3. Найдите наименьшее трёхзначное натуральное число, которое при делении на 6 и на 11 даёт равные ненулевые остатки и у которого средняя цифра является средним арифметическим двух крайних цифр.

4. Найдите трехзначное натуральное число, большее 500, которое при делении на 4, на 5 и на 6 дает в остатке 2, и в записи которого есть только две различные цифры. В ответе укажите какое-нибудь одно такое число.

5. Найдите трехзначное натуральное число, большее 600, которое при делении на 4, на 5 и на 6 дает в остатке 3, и цифры которого расположены в порядке убывания слева направо. В ответе укажите какое-нибудь одно такое число.

6. Приведите пример трёхзначного натурального числа, большего 500, которое при делении на 8 и на 5 даёт равные ненулевые остатки и первая слева цифра которого является средним арифметическим двух других цифр. В ответе укажите ровно одно такое число.

7. Приведите пример трёхзначного натурального числа, большего 500, которое при делении на 3, 4 и на 5 даёт в остатке 2 и в записи которого есть только две различные цифры. В ответе укажите ровно одно такое число.

8. Приведите пример трёхзначного натурального числа, которое при делении на 3, на 5 и на 7 даёт в остатке 1, и цифры которого расположены в порядке убывания слева направо. В ответе укажите ровно одно такое число.

9. Приведите пример трёхзначного натурального числа, которое при делении на 3, на 5 и на 7 даёт в остатке 2, и в записи которого есть только две различные цифры. В ответе укажите ровно одно такое число.

10. Сумма неполного частного и остатка, полученных при делении натурального числа на 100, равна сумме неполного частного и остатка, полученных при делении того же натурального числа на 2007. Чему могут быть равны неполное частное и остаток?

11. Найдите такие цифры x и y, чтобы: $a)\overline{2x39y}:88;\ b)\overline{2x3y}:45;\ c)\overline{7x37y}$ давало от деления на 4 остаток 3, а от деления на 11 остаток 7.

12. Натуральное число при делении на 2001 и на 2002 даёт остаток 315. Каков остаток от деления этого числа на 58?

13. В арифметической прогрессии, состоящей из натуральных чисел, разность прогрессии взаимно проста с натуральным числом k. Докажите, что любые k

последовательных членов этой прогрессии дают все возможные остатки от деления на k, причём по одному разу.

14. Найдите наименьшее натуральное число, которое при делении на 6 даёт остаток 5, при делении на 7 – остаток 6, а при делении на 11 – остаток 10.

2. НОД и НОК целых чисел. Алгоритм Евклида

Задание 1. Найти с помощью расширенного алгоритма Евклида числа x и y для a=1250, b=675.

Решение.

Из примера 1 получили, что НОД (1250, 675) = 25.

Запишем шаги алгоритма Евклида в виде равенств:

$$a = 1250 = 675\cdot 1 + 575 = r_0,$$
$$b = 675 = 575\cdot 1 + 100 = r_1,$$
$$575 = 100\cdot 5 + 75 = r_2,$$
$$100 = 75\cdot 1 + 25 = d.$$

Выразим теперь из каждого равенства остаток и подставим его в последующее равенство

$$575 = a - b,$$
$$100 = b - 575 \Rightarrow 100 = b - (a - b),$$
$$75 = 575 - 100\cdot 5 \Rightarrow 75 = (a - b) - [b - (a - b)]\cdot 5,$$
$$d = 25 = 100 - 75 \Rightarrow d = [b - (a - b)] - \{(a - b) - [b - (a - b)]\cdot 5\}.$$

В последнем выражении приведем подобные при числах *a* и *b*:

$$d = b - a + b - \{a - b - [5b - 5a + 5b]\} =$$
$$= 2b - a - a + b + 5b - 5a + 5b =$$
$$= 13b - 7a.$$
$$НОД\ (1250, 675) = -7\cdot 1250 + 13\cdot 675 \Rightarrow x = -7,\ y = 13.$$

Задание 2. Простым или составным является число 1267?

Решение.

Пользуясь признаками делимости на 2, 3 и 5, можно утверждать, что ни на одно из этих простых чисел данное число не делится. Число 1267 также не делится на 11, 13, 17, 19, 23, 29, 31. Делимость на последующие простые числа, по свойству 1, проверять нет необходимости, так как $\sqrt{1267} > 37^2 = 1369$.

Поэтому число 1267 является простым.

Задание 3. Найти НОД и НОК чисел 1250 и 675 разложением на простые множители.

Решение.

Так как $1250 = 2\cdot 5^4$, а $675 = 3^3\cdot 5^2$, то

$$НОД\ (1250, 675) = 5^2 = 25;$$
$$НОК\ (1250, 675) = 2\cdot 3^3\cdot 5^4 = 33750.$$

Задание 4. Найти такие натуральные числа a и b, что $НОД(a,b) = 3$, $НОК(a,b) = 630$, и при этом сумма $a + b$ минимальна.

Решение.

Так как $НОД(a,b) = 3$, то существуют такие взаимно простые натуральные числа m,n, что $a = 3m$, $b = 3n$. Тогда задачу можно сформулировать в виде: «Найти такие натуральные m,n, что $НОД(m,n) = 1$, $НОК(m,n) = 210$, и при этом сумма $m + n$ минимальна».

Задача решается перебором. Заметим, что условия симметричны относительно m и n. Пусть, ради определённости, $m \le n$. Так как $210 = 2\cdot 3\cdot 5\cdot 7$, то возможны следующие случаи:

m	n	$m+n$
2	$3\cdot5\cdot7$	>70
3	$2\cdot5\cdot7$	>70
5	$2\cdot3\cdot7$	>40
7	$2\cdot3\cdot5$	37
$2\cdot3$	$5\cdot7$	41
$2\cdot5$	$3\cdot7$	31
$2\cdot7$	$3\cdot5$	29

Итак, сумма $m+n$ минимальна (и равна 29), если $m=14$, $n=15$. Им соответствуют $a=42$, $b=45$. С учётом симметрии получаем ответ.

Ответ: $(a;b)\in\{(42;45);(45;42)\}$.

Задание 5.. Найти все пары натуральных чисел, наименьшее общее кратное которых равно 78, а наибольший общий делитель равен 13.

Решение.

Пусть a и b – искомые числа. По условию $НОД(a,b)=13$, значит, по определению наибольшего общего делителя, $a=13a_1, b=13b_1$, где числа a_1 и b_1 взаимно простые. Так как $НОК(a,b)=78$ и $НОК(a,b)=\dfrac{a\cdot b}{НОД(a,b)}$, то

$$78=\frac{a\cdot b}{13}\Rightarrow a\cdot b=78\cdot13=6\cdot13^2.$$

С другой стороны, $a\cdot b=13a_1\cdot13b_1=13^2\cdot a_1\cdot b_1\Rightarrow6\cdot13^2=13^2\cdot a_1\cdot b_1\Rightarrow a_1\cdot b_1=6$. Осталось подобрать пары взаимно простых чисел, произведение которых равно 6 и вычислить для них a и b:

$$\begin{gathered}a_1=1,b_1=6\Rightarrow a=13,b=78\\ a_1=6,b_1=1\Rightarrow a=78,b=13\\ a_1=2,b_1=3\Rightarrow a=26,b=39\\ a_1=3,b_1=2\Rightarrow a=39,b=26\end{gathered}.$$

С учётом того, что условия симметричны относительно a и b, получаем ответ.

Ответ: $(a;b)\in\{(13;78);(26;39)\}$.

Задание 6. Докажите, что дробь $\dfrac{6n+7}{10n+12}$ несократима при любых натуральных n.

Решение.

Допустим, дробь сократима, тогда числитель и знаменатель должны иметь наибольший общий делитель – некоторое натуральное число d:

$$(6n+7):d,\ (10n+12):d.$$

Воспользуемся свойствами делимости натуральных чисел. Если два числа (выражения) делятся на некоторое натуральное число, то и любая линейная комбинация этих выражений делится на данное натуральное число:

$$[\alpha(6n+7)+\beta(10n+12)]:d.$$

Подберём коэффициенты α и β так, чтобы слагаемые с n взаимно уничтожились: например, $\alpha=-5$, $\beta=3$. Тогда

$$\begin{gathered}\alpha(6n+7)+\beta(10n+12)=-5(6n+7)+3(10n+12)=\\ =-30n-35+30n+36=-35+36=1.\end{gathered}$$

Получили, что $-1 \vdots d$. По свойствам делимости натуральных чисел $d = 1$, следовательно, НОД числителя и знаменателя исходной дроби равен единице. Следовательно, они взаимно просты и дробь несократима.

Задание 7. Интервалы движения городских автобусов по трём маршрутам, проходящим через общую остановку, составляют 15, 20 и 24 минуты соответственно. Сколько раз с 7.55 до 17.05 того же дня на этой остановке одновременно встречаются автобусы всех трёх маршрутов, если одна из таких встреч происходит в 12.35?

Решение.

Предположим, в некоторый момент времени все три автобуса встретились на остановке. Найдём, через сколько минут они вновь повстречаются на этой остановке. Это количество минут должно быть наименьшим общим кратным чисел 15, 20 и 24. Так как $15 = 3 \cdot 5$, $20 = 2^2 \cdot 5$, $24 = 2^3 \cdot 3$, то $НОК(15,20,24) = 120$.

Отсчитывая этот отрезок времени от 12.35, находим все моменты встреч, попадающие в заданный временной интервал с 7.55 до 17.05 – $8.35, 10.35, 12.35, 14.35, 16.35$ – всего 5 раз.

Ответ: 5 раз.

Задание 8.. Доказать, что $НОД(bc, ac, ab)$ делится на $НОД^2(a,b,c)$.

Решение.

Пусть $d = НОД(bc, ac, ab)$, $d_1 = НОД(a,b,c)$.

Тогда $a = d_1 \cdot a_1, b = d_1 \cdot b_1, c = d_1 \cdot c_1$. Отсюда получаем:

$bc = d_1 \cdot b_1 \cdot d_1 \cdot c_1 = d_1^2 \cdot b_1 \cdot c_1, ac = d_1 \cdot a_1 \cdot d_1 \cdot c_1 = d_1^2 \cdot a_1 \cdot c_1, bc = d_1 \cdot b_1 \cdot d_1 \cdot c_1 = d_1^2 \cdot b_1 \cdot c_1$.

Таким образом, d_1^2 есть общий делитель чисел bc, ac, ab, поэтому d делится на d_1^2.

Задание 9. Доказать, что $НОД(a,b) = НОД(5a+3b, 13a+8b)$.

Решение.

Пусть $d = НОД(a,b)$. По определению наибольшего общего делителя, a *и* b делятся на d, причём d делится на любой общий делитель этих чисел. Пусть $d_1 = НОД(5a+3b, 13a+8b)$, то есть $5a+3b$ *и* $13a+8b$ делятся на d_1, причём d_1 делится на любой общий делитель этих чисел.

По свойствам делимости, $5a+3b$ делится на d, $13a+8b$ делится на d, следовательно, d есть общий делитель этих чисел и, по вышесказанному, $d_1 \vdots d$ (1).

С другой стороны, по свойствам делимости $\alpha(5a+3b) + \beta(13a+8b)$ делится на d_1 при любых целых α *и* β. Возьмём сначала $\alpha = -13, \beta = 5$:

$$-13(5a+3b) + 5(13a+8b) \vdots d_1 \Leftrightarrow -65a - 39b + 65a + 40b = b \vdots d_1.$$

Возьмём теперь $\alpha = 8, \beta = -3$:

$$8(5a+3b) - 3(13a+8b) \vdots d_1 \Leftrightarrow 40a + 24b - 39a - 24b = a \vdots d_1.$$

Получили, что d_1 – общий делитель чисел a *и* b. Так как $d = НОД(a,b)$, то $d \vdots d_1$ (2). Из делимостей (1) и (2) следует, что $d_1 = d$ (считаем d *и* d_1 натуральными числами).

Задания

1. Дано $a = b + c$. а) $a \vdots d, b \vdots d$. Следует ли из этого, что $c \vdots d$? б) $a \vdots d$. Верно ли, что $b \vdots d$ и $c \vdots d$?
2. Дано $a \vdots b$. Выяснить, верно ли, что $(\forall n \in N)$ $a \vdots bn$.
3. Выполнить деление с остатком: 168 на 35; 168 на (-35); -168 на 35; -168 на (-35).

4. Найти делители и соответствующие им остатки, если: а)делимое 534, частное 26; б) делимое 741, частное (-14).

5. Доказать, что квадрат любого целого числа либо нацело делится на 3, либо дает в остатке 1.

6. Числа a, b, c при делении на 7 дают остатки 1, 4, 5 соответственно. Найти остаток от деления числа $a+b+c$ на 7.

7. Найти все числа, большие 25000, но меньшие 30000, у которых как при делении на 131, так и при делении на 1965 остаток равен 125.

8. Найти НОД и НОК чисел 531 и 93; -78 и 24.

9. Найти НОД(663, 731, 2516, 3655).

10. Решить в натуральных числах следующие системы уравнений:

а) $\begin{cases} x+y=180, \\ (x;y)=30; \end{cases}$ б) $\begin{cases} (x;y)=4, \\ x\cdot y=720; \end{cases}$ в) $\begin{cases} (a;b)=15, \\ [a;b]=420. \end{cases}$

11. Найти линейное представление НОД (90; 35) через эти числа.

12. Пусть a, b, c, d – различные цифры. Доказать, что число cdcdcdcd не делится на число aabb.`

13. Число при некоторой перестановке своих цифр удваивается. Доказать, что оно делится на 9.

14. Найти натуральные числа, дающие при делении на 2, 3, 4, 5 и 6 остаток 1 и, кроме того, делящиеся на 7.

15. Генерал построил солдат в колонну по 4, но при этом солдат Иванов остался лишним. Тогда генерал построил солдат в колонну по 5. И снова Иванов остался лишним. Когда же и в колонне по 6 Иванов оказался лишним, генерал посулил ему наряд вне очереди, после чего в колонне по 7 Иванов нашел себе место и никого лишнего не осталось. Сколько солдат могло быть у генерала?

16. Доказать, что если НОК(a, a+5)=НОК(b, b+5), где a и b – натуральные числа, то a = b.

17. Пусть d = НОД(1819, 3587). Найти d и целые числа x, y такие, что: 1819x+3587y=d .

Тема. Подпространство. Линейная зависимость и независимость систем векторов

Примеры решения задач

Пусть L есть некоторое непустое множество и P – числовое поле. В L определено действие, называемое *сложением*, согласно которому каждой паре элементов u, v ∈ L сопоставляется третий элемент из L, обозначаемый через u + v. Также определено действие *умножения элементов из L на числа из P*, согласно которому каждой паре, состоящей из элемента u ∈ L и числа λ ∈ P, сопоставлен элемент из L, обозначаемый через λu.

Если при этом выполнены следующие семь аксиом, то множество L, рассматриваемое вместе с указанными двумя операциями, называется линейным пространством над полем P.

Коммутативность сложения:

∀ u, v ∈ L u + v = v + u.

2) Ассоциативность сложения:

∀ u, v, w ∈ L (u + v) + w = u + (v + w).

Обратимость сложения:

∀ u, v ∈ L всегда найдется такой x ∈ L, что u + x = v

(при этом элемент x называется разностью между v и u и обозначается: x = v - u).

Ассоциативность умножения на числа из P:

∀ u ∈ L ∀ λ, μ ∈ P λ(μu) = (λμ)u.

Свойство дистрибутивности относительно сложения чисел из P:

$\forall u \in L \ \ \forall \lambda, \mu \in P \ \ (\lambda + \mu)u = \lambda u + \mu u.$

Свойство дистрибутивности относительно сложения элементов из L:

$\forall u, v \in L \ \ \forall \lambda \in P \ \ \lambda(u + v) = \lambda u + \lambda v.$

Свойство единичного множителя:

для числа $1 \in P$ и $\forall u \in L$ выполнено $1u = u$.

Элементы любого линейного пространства будем называть *векторами*

Пусть L – линейное пространство над полем P. Непустое подмножество L' пространства L называется *подпространством пространства L*, если выполнены следующие условия:

$\forall u, v \in L' \ \ u + v \in L'$,

$\forall u \in L' \ \ \forall \lambda \in P \ \ \lambda u \in L'$,

т.е. L' замкнуто относительно сложения и относительно умножения на число.

Говорят, что вектор v линейного пространства L над полем P ***линейно выражается*** через векторы $u_1, u_2, \ldots, u_m \in L$, если существуют такие числа $\lambda_1, \lambda_2, \ldots, \lambda_m \in P$, что

$$v = \lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_m u_m.$$

Выражение, стоящее в правой части, называют *линейной комбинацией* векторов u1, $u_1, u_2, \ldots, u_m$.

Векторы $u_1, u_2, \ldots, u_m$ называются ***линейно зависимыми***, если существуют такие числа $\alpha_1, \alpha_2, \ldots, \alpha_m \in P$, среди которых есть отличные от нуля, что

$$\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m = \theta.$$

Если векторы $u_1, u_2, \ldots, u_m$ не являются линейно зависимыми между собой, то они называются ***линейно независимыми***. Это означает, что соотношение

$$\alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_m u_m = \theta$$

выполняется **только** при $\alpha_1 = \alpha_2 = \ldots = \alpha_m = 0$.

Задача 1. Найти линейную комбинацию

$$3A_1 - 2A_2 + 8A_3$$

следующих векторов:

$$A_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 4 \end{pmatrix}, \quad A_2 = \begin{pmatrix} -1 \\ -3 \\ 4 \\ 5 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} -5 \\ 0 \\ 2 \\ 3 \end{pmatrix}.$$

Решение.

$$3A_1 - 2A_2 + 8A_3 = 3\begin{pmatrix} 1 \\ -1 \\ 0 \\ 4 \end{pmatrix} + (-2)\begin{pmatrix} -1 \\ -3 \\ 4 \\ 5 \end{pmatrix} + 8\begin{pmatrix} -5 \\ 0 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 \\ -3 \\ 0 \\ 12 \end{pmatrix} + \begin{pmatrix} 2 \\ 6 \\ -8 \\ -10 \end{pmatrix} + \begin{pmatrix} -40 \\ 0 \\ 16 \\ 24 \end{pmatrix} = \begin{pmatrix} -35 \\ 3 \\ 8 \\ 14 \end{pmatrix}.$$

Задача 2. Выяснить, является ли заданная система векторов линейно зависимой.

$$a_1 = \begin{pmatrix} -3 \\ 1 \\ 5 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 6 \\ -2 \\ 15 \end{pmatrix}.$$

Решение. Составим линейную комбинацию векторов и приравняем её к нулю:

$$\lambda a_1 + \mu a_2 = 0; \quad \lambda \begin{pmatrix} -3 \\ 1 \\ 5 \end{pmatrix} + \quad \mu \begin{pmatrix} 6 \\ -2 \\ 15 \end{pmatrix} = \Theta$$

$$\begin{pmatrix} -3\lambda + 6\mu \\ \lambda - 2\mu \\ 5\lambda + 15\mu \end{pmatrix} = \Theta = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \begin{cases} -3\lambda + 6\mu = 0, \\ \lambda - 2\mu = 0, \\ 5\lambda + 15\mu = 0 \end{cases}$$

Решая систему, получим:

$$\begin{cases} -3\lambda + 6\mu = 0, \\ \lambda - 2\mu = 0, \\ 5\lambda + 15\mu = 0 \end{cases} \Leftrightarrow \begin{cases} \lambda = 2\mu, \\ \lambda = -3\mu \end{cases} \Leftrightarrow \lambda = \mu = 0 .$$

Получили, сто равенство нулю линейной комбинации возможно только, если коэффициенты при векторах равны нулю. Следовательно, заданная система векторов линейно независима.

Задания

1. Решить векторное уравнение:

а) $A_1 + 2A_2 + 3A_3 + 4X = \Theta$

$$A_1 = \begin{pmatrix} 5 \\ -8 \\ -1 \\ 2 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 2 \\ -1 \\ 4 \\ -3 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} -3 \\ 2 \\ -5 \\ 7 \end{pmatrix}.$$

б) $3(A_1 - X) + 2(A_2 + X) = 5(A_3 + X)$

$$A_1 = \begin{pmatrix} 2 \\ 5 \\ 1 \\ 3 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 10 \\ 1 \\ 5 \\ 10 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} 4 \\ 1 \\ -1 \\ 1 \end{pmatrix}.$$

в) $2A_1 + 3A_2 - A_3 - 7X = A_4$

$$A_1 = \begin{pmatrix} -1 \\ 2 \\ -3 \\ 4 \end{pmatrix}, \quad A_2 = \begin{pmatrix} -1 \\ -1 \\ -1 \\ 5 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 2 \\ -5 \\ -1 \\ 3 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 2 \\ 1 \\ -2 \\ -1 \end{pmatrix}.$$

2. Выяснить, является ли заданная система векторов линейно зависимой:

а) $A_1 = \begin{pmatrix} 4 \\ -12 \\ 28 \end{pmatrix}, \quad A_2 = \begin{pmatrix} -7 \\ 21 \\ -49 \end{pmatrix}.$

б). $A_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 2 \\ 4 \\ 6 \\ 1 \end{pmatrix}.$

в). $A_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$, $A_2 = \begin{pmatrix} 2 \\ 5 \\ 7 \end{pmatrix}$, $A_3 = \begin{pmatrix} 3 \\ 7 \\ 10 \end{pmatrix}$.

3. Доказать, что в координатном векторном пространстве V(3) = {(a1, a2, a3)| ai ∈ R, i = 1 ÷ 3} над полем R множество всех векторов, у которых:

а) первая координата равна нулю;

б) вторая координата равна нулю;

в) третья координата равна нулю;

является подпространством.

4. Построить линейную оболочку системы векторов:

а). $A_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}$, $A_2 = \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \end{pmatrix}$, $A_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$, $A_4 = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$;

б). $A_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \end{pmatrix}$, $A_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}$, $A_3 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$, $A_4 = \begin{pmatrix} 1 \\ 3 \\ 0 \\ 1 \end{pmatrix}$;

в). $A_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$, $A_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \\ 4 \end{pmatrix}$, $A_3 = \begin{pmatrix} 1 \\ 3 \\ 1 \\ 3 \end{pmatrix}$, $A_4 = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 2 \end{pmatrix}$.

5. Выясните, образуют ли векторы $\vec{p}, \vec{q}, \vec{r}$ базис. Если образуют, то разложите вектор $\vec{x}$ по этому базису.

1. $\vec{p} = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}, \vec{q} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \vec{r} = \begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix}, \vec{x} = \begin{pmatrix} 3 \\ 1 \\ 3 \end{pmatrix}$.

2. $\vec{p} = \begin{pmatrix} 5 \\ 1 \\ 0 \end{pmatrix}, \vec{q} = \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}, \vec{r} = \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \vec{x} = \begin{pmatrix} 13 \\ 2 \\ 7 \end{pmatrix}$.

3. $\vec{p} = \begin{pmatrix} 4 \\ 1 \\ 1 \end{pmatrix}, \vec{q} = \begin{pmatrix} 2 \\ 0 \\ -3 \end{pmatrix}, \vec{r} = \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}, \vec{x} = \begin{pmatrix} -9 \\ 5 \\ 5 \end{pmatrix}$.

4. $\vec{p} = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, \vec{q} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \vec{r} = \begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix}, \vec{x} = \begin{pmatrix} 3 \\ -3 \\ 4 \end{pmatrix}$.

5. $\vec{p} = \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}, \vec{q} = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, \vec{r} = \begin{pmatrix} 2 \\ 0 \\ -1 \end{pmatrix}, \vec{x} = \begin{pmatrix} 3 \\ 1 \\ 8 \end{pmatrix}$.

Тема. Линейный оператор и его простейшие свойства. Матрица линейного оператора

Примеры решения задач

Пусть L – линейное пространство над полем P. Линейным оператором, или линейным преобразованием, пространства L называется отображение $\varphi: L \to L$, для которого выполняются следующие условия:

1) $\forall\, u, v \in L \quad \varphi(u+v) = \varphi(u)+\varphi(v)$,

2) $\forall\, u \in L\ \forall\, \lambda \in P \quad \varphi(\lambda u) = \lambda\varphi(u)$.

Пусть в линейном пространстве L над полем P задан базис $U = \{u_1, u_2, \ldots, u_n\}$ и задан линейный оператор $\varphi: L \to L$. Пусть элементы $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ линейно выражаются через базис U следующим образом:

$\varphi(u_1) = \alpha_{11}u_1+\alpha_{12}u_2+\ldots+\alpha_{1n}u_n$,

$\varphi(u_2) = \alpha_{21}u_1+\alpha_{22}u_2+\ldots+\alpha_{2n}u_n$,

……

$\varphi(u_n) = \alpha_{n1}u_1+\alpha_{n2}u_2+\ldots+\alpha_{nn}u_n$,

где $\alpha_{ij} \in P,\ i=1\div n,\ j=1\div n$. Тогда матрица линейного выражения образов $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ базисных элементов через этот базис $u_1, u_2, \ldots, u_n$

$$A_U(\varphi) = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn} \end{pmatrix}$$

называется ***матрицей линейного оператора*** φ в базисе U.

Задача 1. Доказать линейность, найти матрицу, область значений и ядро оператора проектирования на плоскость $y–z=0$.

Если $\mathbf{x} = \{x_1;\ x_2;\ x_3\}$, то

$$A\mathbf{x} = \left\{ x_1;\ \frac{1}{2}x_2 + \frac{1}{2}x_3;\ \frac{1}{2}x_2 + \frac{1}{2}x_3 \right\}.$$

Оператор является линейным, если

$A(\mathbf{x}+\mathbf{y}) = A\mathbf{x} + A\mathbf{y}$ и $A(\lambda\mathbf{x}) = \lambda(A\mathbf{x})$.

Проверяем

$$A(\mathbf{x}+\mathbf{y}) = \left(x_1 + y_1;\ \frac{1}{2}(x_2+y_2) + \frac{1}{2}(x_3+y_3);\ \frac{1}{2}(x_2+y_2) + \frac{1}{2}(x_3+y_3) \right) =$$

$$= \left(x_1 + y_1;\ \frac{1}{2}(x_2+x_3) + \frac{1}{2}(y_2+y_3);\ \frac{1}{2}(x_2+x_3) + \frac{1}{2}(y_2+y_3) \right) =$$

$$= A\mathbf{x} + A\mathbf{y}.$$

$$A(\lambda\mathbf{x}) = \left\{ \lambda x_1;\ \frac{1}{2}\lambda x_2 + \frac{1}{2}\lambda x_3;\ \frac{1}{2}\lambda x_2 + \frac{1}{2}\lambda x_3 \right\}.$$

$$\lambda(A\mathbf{x}) = \left\{ \lambda x_1;\ \lambda\left(\frac{1}{2}x_2 + \frac{1}{2}x_3\right);\ \lambda\left(\frac{1}{2}x_2 + \frac{1}{2}x_3\right) \right\} =$$

$$= \left\{ \lambda x_1;\ \frac{1}{2}\lambda x_2 + \frac{1}{2}\lambda x_3;\ \frac{1}{2}\lambda x_2 + \frac{1}{2}\lambda x_3 \right\} = A(\lambda\mathbf{x}).$$

Т.е. оператор A является линейным.

Его матрица:

$$\mathbf{A}=\begin{pmatrix}1 & 0 & 0\\ 0 & 1/2 & 1/2\\ 0 & 1/2 & 1/2\end{pmatrix}.$$

Область значений оператора – это множество всех векторов

$$\mathbf{y}=A\mathbf{x}=\left\{x_1;\quad \frac{1}{2}x_2+\frac{1}{2}x_3;\quad \frac{1}{2}x_2+\frac{1}{2}x_3\right\}.$$

Ядро линейного оператора – это множество всех векторов, которые A отображает в нуль-вектор:

$$\operatorname{Ker}A=\{0;\quad x_2;\quad -x_2\}.$$

Задания

Доказать линейность, найти матрицу, область значений и ядро операторов A, B и C:

1. $Ax=(6x_1-5x_2-4x_3,\quad -3x_1-2x_2-x_3,\quad x_2+2x_3),$
$Bx=(6-5x_2-4x_3,\quad 3x_1-2x_2-x_3,\quad x_2+2),$
$Cx=(x_3^4,\quad 3x_1-2x_2-x_3,\quad x_2+2x_3).$

2. $Ax=(5x_1-4x_2-3x_3,\quad 2x_1-x_2,\quad x_2+2),$
$Bx=(5x_1-4x_2-3x_3,\quad 0,\quad x_2^4+2x_3),$
$Cx=(5x_1-4x_2-3x_3,\quad 2x_1-x_2,\quad x_2+2x_3).$

3. $Ax=(4x_1-3x_2-2x_3,\quad x_1,\quad x_1+2x_2^4+3x_3),$
$Bx=(4x_1-3x_2-2x_3,\quad x_1,\quad x_1+2x_2+3x_3),$
$Cx=(4x_1-3x_2-2x_3,\quad x_1,\quad x_1+2x_2+3).$

.4. $Ax=(3x_1+2x_2+x_3,\quad x_3,\quad 2x_1-3x_2-4x_3),$
$Bx=(3x_1+2x_2+x_3,\quad 1,\quad 2x_1-3x_2-4),$
$Cx=(3x_1+2x_2+x_3,\quad x_3,\quad 2x_1^4-3x_2-4x_3).$

5. $Ax=(x_1,\quad x_1-2x_2-3,\quad 4x_1-5x_2-6),$
$Bx=(x_1,\quad x_1-2x_2-3x_3,\quad 4x_1^4-5x_2-6x_3),$
$Cx=(x_1,\quad x_1-2x_2-3x_3,\quad 4x_1-5x_2-6x_3).$

Тема. Связь между матрицами линейного оператора в разных базисах. Ранг и дефект линейного оператора

Примеры решения задач

Пусть L – линейное пространство над полем P. Линейным оператором, или линейным преобразованием, пространства L называется отображение $\varphi: L \to L$, для которого выполняются следующие условия:

1) $\forall\ u, v \in L \quad \varphi(u+v) = \varphi(u)+\varphi(v)$,

2) $\forall\ u \in L\ \forall\ \lambda \in P \quad \varphi(\lambda u) = \lambda\varphi(u)$.

Пусть в линейном пространстве L над полем P задан базис $U = \{u_1, u_2, \ldots, u_n\}$ и задан линейный оператор $\varphi: L \to L$. Пусть элементы $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ линейно выражаются через базис U следующим образом:

$\varphi(u_1) = \alpha_{11}u_1+\alpha_{12}u_2+\ldots+\alpha_{1n}u_n,$

$\varphi(u_2) = \alpha_{21}u_1+\alpha_{22}u_2+\ldots+\alpha_{2n}u_n,$

$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

$\varphi(u_n) = \alpha_{n1}u_1+\alpha_{n2}u_2+\ldots+\alpha_{nn}u_n,$

где $\alpha_{ij} \in P,\ i=1\div n,\ j=1\div n$. Тогда матрица линейного выражения образов $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ базисных элементов через этот базис $u_1, u_2, \ldots, u_n$

$$A_U(\varphi) = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn} \end{pmatrix}$$

называется ***матрицей линейного оператора*** φ в базисе U.

Общая постановка задачи

Найти матрицу некоторого оператора А в базисе $(\mathbf{e}_1';\ \mathbf{e}_2';\ \ldots;\ \mathbf{e}_n')$, где

$$\begin{cases} \mathbf{e}_1' = t_{11}\mathbf{e}_1 + t_{21}\mathbf{e}_2 + \ldots + t_{n1}\mathbf{e}_n, \\ \mathbf{e}_2' = t_{12}\mathbf{e}_1 + t_{22}\mathbf{e}_2 + \ldots + t_{n2}\mathbf{e}_n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \mathbf{e}_n' = t_{1n}\mathbf{e}_1 + t_{2n}\mathbf{e}_2 + \ldots + t_{nn}\mathbf{e}_n. \end{cases}$$

если в базисе его $(\mathbf{e}_1';\ \mathbf{e}_2';\ \ldots;\ \mathbf{e}_n')$ матрица имеет вид

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}.$$

План решения.

При переходе от базиса $(\mathbf{e}_1;\ \mathbf{e}_2;\ \ldots;\ \mathbf{e}_n)$ к базису $(\mathbf{e}_1';\ \mathbf{e}_2';\ \ldots;\ \mathbf{e}_n')$ матрица оператора преобразуется по формуле $\mathbf{A}' = \mathbf{T}^{-1}\mathbf{A}\mathbf{T}$, где Т – матрица перехода от базиса $(\mathbf{e}_1;\ \mathbf{e}_2;\ \ldots;\ \mathbf{e}_n)$ к базису $(\mathbf{e}_1';\ \mathbf{e}_2';\ \ldots;\ \mathbf{e}_n')$.

1. Выписываем матрицу перехода:

$$\mathbf{T} = \begin{pmatrix} t_{11} & t_{12} & \ldots & t_{1n} \\ t_{21} & t_{22} & \ldots & t_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ t_{n1} & t_{n2} & \ldots & t_{nn} \end{pmatrix}.$$

2. Находим обратную матрицу $\mathbf{T}^{-1}$.

3. Находим матрицу оператора А в базисе $(\mathbf{e}_1';\ \mathbf{e}_2';\ \ldots;\ \mathbf{e}_n')$ по формуле $\mathbf{A}' = \mathbf{T}^{-1}\mathbf{A}\mathbf{T}$.

Задача. 1. Найти матрицу в базисе $(e_1',\ e_2',\ e_3')$, где

$$e_1' = e_1 - e_2 + e_3,\ e_2' = -e_1 + e_2 - 2e_3,\ e_3' = -e_1 + 2e_2 + e_3,$$

если она задана в базисе $(e_1,\ e_2,\ e_3)$:

$$\begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix}.$$

2. Найти ранг и дефект оператора А.

Решение.

Матрица в базисе (e_1', e_2', e_3') находится по формуле $\mathbf{A'} = \mathbf{T}^{-1}\mathbf{A}\mathbf{T}$.
где

$$\mathbf{T} = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & 2 \\ 1 & -2 & 1 \end{pmatrix}.$$

Найдем обратную матрицу $\mathbf{T}^{-1}$.
Определитель:

$$|\mathbf{T}| = \begin{vmatrix} 1 & -1 & -1 \\ -1 & 1 & 2 \\ 1 & -2 & 1 \end{vmatrix} = 1-2-2+1+4-1=1.$$

Алгебраические дополнения:

$$A_{11} = \begin{vmatrix} 1 & 2 \\ -2 & 1 \end{vmatrix} = 5;\ A_{12} = -\begin{vmatrix} -1 & 2 \\ 1 & 1 \end{vmatrix} = 3;\ A_{13} = \begin{vmatrix} -1 & 1 \\ 1 & -2 \end{vmatrix} = 1;$$

$$A_{21} = -\begin{vmatrix} -1 & -1 \\ -2 & 1 \end{vmatrix} = 3;\ A_{22} = \begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2;\ A_{23} = -\begin{vmatrix} 1 & -1 \\ 1 & -2 \end{vmatrix} = 1;$$

$$A_{31} = \begin{vmatrix} -1 & -1 \\ 1 & 2 \end{vmatrix} = -1;\ A_{32} = -\begin{vmatrix} 1 & -1 \\ -1 & 2 \end{vmatrix} = -1;\ A_{33} = \begin{vmatrix} 1 & -1 \\ -1 & 1 \end{vmatrix} = 0.$$

Обратная матрица:

$$\mathbf{T}^{-1} = \begin{pmatrix} 5 & 3 & -1 \\ 3 & 2 & -1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Находим матрицу в новом базисе:

$$\mathbf{A'} = \begin{pmatrix} 5 & 3 & -1 \\ 3 & 2 & -1 \\ 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & 2 \\ 1 & -2 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 10+0+1 & 5+3-1 & 0-3-1 \\ 6+0+1 & 3+2-1 & 0-2-1 \\ 2+0+0 & 1+1+0 & 0-1+0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & 2 \\ 1 & -2 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 11 & 7 & -4 \\ 7 & 4 & -3 \\ 2 & 2 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & 2 \\ 1 & -2 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 11-7-4 & -11+7+8 & -11+14-4 \\ 7-4-3 & -7+4+6 & -7+8-3 \\ 2-2-1 & -2+2+2 & -2+4-1 \end{pmatrix} = \begin{pmatrix} 0 & 4 & -1 \\ 0 & 3 & -2 \\ -1 & 2 & 1 \end{pmatrix}$$

Т.е. матрица А в базисе (e_1', e_2', e_3') имеет вид:

$$\mathbf{A'} = \begin{pmatrix} 0 & 4 & -1 \\ 0 & 3 & -2 \\ -1 & 2 & 1 \end{pmatrix}.$$

Так как $\det A = \begin{vmatrix} 2 & 1 & 0 \\ 0 & 1 & -1 \\ -1 & 1 & 1 \end{vmatrix} = 111 \neq 0$, то $\operatorname{rang} A = 3 = \operatorname{rang} R^3$, то оператор А – невырожденный и его дефект равен нулю.

Задания

1. Найти матрицу оператора в базисе (e_1', e_2', e_3'), где

$$e_1' = e_1 - e_2 + e_3,\ e_2' = -e_1 + e_2 - 2e_3,\ e_3' = -e_1 + 2e_2 + e_3,$$

если она задана в базисе (e_1, e_2, e_3).

2. Найти ранг и дефект оператора.

1. $\begin{pmatrix} 1 & 0 & 2 \\ 3 & -1 & 0 \\ 1 & 1 & -2 \end{pmatrix}$.
2. $\begin{pmatrix} 2 & 1 & 0 \\ 3 & 0 & 4 \\ 1 & -1 & 2 \end{pmatrix}$.
3. $\begin{pmatrix} 0 & 2 & 3 \\ 4 & 1 & 0 \\ 2 & -1 & -2 \end{pmatrix}$.
4. $\begin{pmatrix} 1 & 2 & 0 \\ 3 & 0 & -1 \\ 2 & 1 & -1 \end{pmatrix}$.
5. $\begin{pmatrix} 2 & 0 & 1 \\ 3 & 0 & 2 \\ -1 & 1 & 2 \end{pmatrix}$.
6. $\begin{pmatrix} 0 & 3 & 2 \\ 2 & 1 & -1 \\ 0 & -1 & 2 \end{pmatrix}$.
7. $\begin{pmatrix} 1 & 3 & 0 \\ 2 & 1 & -1 \\ 0 & 2 & 1 \end{pmatrix}$.
8. $\begin{pmatrix} 2 & 1 & 2 \\ 3 & 0 & 2 \\ 1 & 0 & 1 \end{pmatrix}$.
9. $\begin{pmatrix} 0 & 1 & 2 \\ 4 & 0 & 1 \\ -1 & -2 & 1 \end{pmatrix}$.

Собственные векторы и собственные значения линейных операторов

Примеры решения задач

Пусть L – линейное пространство над полем P. Линейным оператором, или линейным преобразованием, пространства L называется отображение $\varphi: L \to L$, для которого выполняются следующие условия:

1) $\forall\ u, v \in L \quad \varphi(u+v) = \varphi(u)+\varphi(v)$,

2) $\forall\ u \in L\ \forall\ \lambda \in P \quad \varphi(\lambda u) = \lambda\varphi(u)$.

Пусть в линейном пространстве *L* над полем *P* задан базис $U = \{u_1, u_2, \ldots, u_n\}$ и задан линейный оператор $\varphi: L \to L$. Пусть элементы $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ линейно выражаются через базис *U* следующим образом:

$\varphi(u_1) = \alpha_{11}u_1+\alpha_{12}u_2+\ldots+\alpha_{1n}u_n$,

$\varphi(u_2) = \alpha_{21}u_1+\alpha_{22}u_2+\ldots+\alpha_{2n}u_n$,

……

$\varphi(u_n) = \alpha_{n1}u_1+\alpha_{n2}u_2+\ldots+\alpha_{nn}u_n$,

где $\alpha_{ij} \in P,\ i=1 \div n,\ j=1 \div n$. Тогда матрица линейного выражения образов $\varphi(u_1), \varphi(u_2), \ldots, \varphi(u_n)$ базисных элементов через этот базис $u_1, u_2, \ldots, u_n$

$$A_U(\varphi) = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdots & \alpha_{n1} \\ \alpha_{12} & \alpha_{22} & \cdots & \alpha_{n2} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{1n} & \alpha_{2n} & \cdots & \alpha_{nn} \end{pmatrix}$$

называется ***матрицей линейного оператора*** φ в базисе *U*.

Пусть *L* – линейное пространство над полем *P* и $\varphi: L \to L$ – линейный оператор. Элемент $w \in L$ называется ***собственным вектором*** оператора φ, если $w \neq \theta$ и существует $\lambda \in P$, такое, что $\varphi(w) = \lambda w$. При этом λ называется ***собственным значением*** оператора φ, соответствующим вектору *w*.

Пусть $A = (a_{ij})_{n\times n}$ – матрица над полем *P* и $\lambda \in P$. Многочлен $f(\lambda) = |A - \lambda E|$ называется ***характеристическим многочленом*** матрицы *A*, а корни данного многочлена называются ***характеристическими числами*** матрицы *A*.

Общая постановка задачи.

Найти собственные значения и собственные векторы оператора A, заданного в некотором базисе матрицей

$$\mathbf{A}=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{m} \end{pmatrix}.$$

План решения.

Собственные значения оператора A являются корнями его характеристического уравнения $\det(\mathbf{A}-\lambda\mathbf{E})=0$.

1. Составляем характеристическое уравнение и находим все его вещественные корни λ (среди которых могут быть и кратные).

2. Для каждого собственного значения λ находим собственные вектора. Для этого записываем однородную систему уравнений $(\mathbf{A}-\lambda_i\mathbf{E})X=0$ и находим ее общее решение.

3. Исходя из общих решений каждой из однородных систем, выписываем собственные векторы.

Задача. Найти собственные значения и собственные векторы оператора, заданного матрицей

$$\begin{pmatrix} 2 & 0 & -1 \\ 1 & 1 & -1 \\ -1 & 0 & 2 \end{pmatrix}$$

Решение.

$$\begin{pmatrix} 2 & 0 & -1 \\ 1 & 1 & -1 \\ -1 & 0 & 2 \end{pmatrix}.$$

Составляем характеристическое уравнение и находим его решение:

$$\begin{vmatrix} 2-\lambda & 0 & -1 \\ 1 & 1-\lambda & -1 \\ -1 & 0 & 2-\lambda \end{vmatrix}=0.$$

Собственные значения: $\lambda_{1,2}=1,\ \lambda_3=3$.

Найдем собственные векторы:

$$\lambda_{1,2}=1:\quad \begin{cases} x_1-x_3=0, \\ x_1-x_3=0, \\ -x_1+x_3=0; \end{cases} \Rightarrow \begin{cases} x_1=c_1, \\ x_2=c_2, \\ x_3=c_1. \end{cases}$$

$$\lambda_3=3:\quad \begin{cases} -x_1-x_3=0, \\ x_1-2x_2-x_3=0, \\ -x_1-x_3=0. \end{cases} \Rightarrow \begin{cases} x_1=c_1, \\ x_2=c_1, \\ x_3=-c_1. \end{cases}$$

Собственные векторы:

$$X_1=\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix};\quad X_2=\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix};\quad X_3=\begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}.$$

Задания

1. Найти собственные значения и собственные векторы оператора, заданного в некотором базисе матрицей

1. $A=\begin{pmatrix} 2 & -1 & 1 \\ -1 & 2 & -1 \\ 0 & 0 & 1 \end{pmatrix}$;
2. $A=\begin{pmatrix} 1 & 1 & 3 \\ 1 & 5 & 1 \\ 3 & 1 & 1 \end{pmatrix}$
3. $A=\begin{pmatrix} 2 & -1 & 2 \\ 5 & -3 & 3 \\ -1 & 0 & -2 \end{pmatrix}$.
4. $A=\begin{pmatrix} 0 & 1 & 0 \\ -4 & 4 & 0 \\ -2 & 1 & 2 \end{pmatrix}$.
5. $A=\begin{pmatrix} 4 & -5 & 2 \\ 5 & -7 & 3 \\ 6 & -9 & 4 \end{pmatrix}$.
6. $A=\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

2. Определить, является ли данный оператор вырожденным или невырожденным.

Тема. Кольцо многочленов от одной переменной

План

1. Деление многочленов с остатком. Деление многочлена на двучлен. Корни многочлена. Кратные корни.

2. НОД и НОК многочленов. Алгоритм Евклида и теорема Ламе для многочленов.

3. Производная многочлена. Отделение кратных множителей многочлена.

1. Деление с остатком. Деление многочлена на двучлен. Корни многочлена

Задание 1. Даны многочлены

$F_4(x)=6-5x+4x^2-3x^3+2x^4$,

$Q_2(x)=1-3x+x^2$.

Используя определение, найти $F_4(x)Q_2(x)$.

Решение.

Так как $\deg[F(x)Q(x)]=\deg F(x)+\deg Q(x)$, то степень произведения $\deg[F(x)Q(x)]=\deg T(x)=6$.

Ищем многочлен вида $T_6(x)=d_0+d_1x+d_2x^2+d_3x^3+d_4x^4+d_5x^5+d_6x^6$, где коэффициенты вычисляем по общей формуле $d_k=\sum_{i+j=k}a_ia_j\ \ (k=0,1,2,\ldots,6)$.

Подставляя данные $a_0=6$, $a_1=-5$, $a_2=4$, $a_3=-3$, $a_4=2$, $b_0=1$, $b_1=-3$ $b_2=1$ в эту формулу, получаем:

$d_0=a_0b_0=6$;

$d_1=a_0b_1+a_1b_0=-18-5=-23$;

$d_2=a_0b_2+a_1b_1+a_2b_0=6+(-5)\cdot(-3)+4\cdot1=25$;

$d_3=a_1b_2+a_2b_1+a_3b_0=(-5)\cdot1+4\cdot(-3)+(-3)\cdot1=-20$;

$d_4=a_2b_2+a_3b_1+a_4b_0=4\cdot1+(-3)\cdot(-3)+2\cdot1=15$;

$d_5=a_3b_2+a_4b_1=(-3)\cdot1+2\cdot(-3)=-9$;

$d_6=a_4b_2=2$.

Следовательно, искомый многочлен имеет вид $T_6(x)=6-23x+25x^2-20x^3+15x^4-9x^5+2x^6$. $\otimes$

Задание 2. Выполнить деление с остатком многочлена:

$F_4(x)=3x^4+4x^3+x^2-x-18$ на многочлен $G_2(x)=x^2+3x+2$.

Решение.

Воспользуемся общим алгоритмом согласно которому имеем деления многочленов с остатком:

1) $F_3^{(1)}(x)=F_4(x)-\frac{a_4}{b_2}x^{4-2}G_2(x)=3x^4+4x^3+x^2-x-18-$

$-3x^2\left(x^2+3x+2\right)=-5x^3-5x^2-x-18$;

2) $F_2^{(2)}(x)=F_3^{(1)}(x)-\frac{a_3^{(1)}}{b_2}x^{3-2}G_2(x)=-5x^3-5x^2-x-18+$

$+5x\left(x^2+3x+2\right)=10x^2+9x-18$;

3) $F_1^{(3)}(x)=F_2^{(2)}(x)-\frac{a_2^{(2)}}{b_2}x^{2-2}G_2(x)=10x^2+9x-18-$

$-10\left(x^2+3x+2\right)=-21x-38$.

Имеем:

$3x^4+4x^3+x^2-x-18=\left(x^2+3x+2\right)\left(3x^2-5x+10\right)-21x-38$.

Задание 3. Вычислить значение $F(c)$ многочлена $F(x)=x^4-8x^3+24x^2-50x+22$, если $c=2$.

Решение.

По теореме Безу значение многочлена $F(c)$ равно остатку от деления многочлена $F(x)$ на линейный двучлен $x-c$. Поэтому, деля многочлен $F(x)$ на $x-2$, получаем:

$$\begin{array}{l|l}
F(x)=x^4-8x^3+24x^2-50x+22 & \\
\underline{-\left(x^4-2x^3\right)} & \\
-6x^3+24x^2-50x+22 & \\
\underline{-\left(-6x^3+12x^2\right)} & \\
12x^2-50x+22 & \\
\underline{-\left(12x^2-24x\right)} & \\
-26x+22 & \\
\underline{-\left(-26x+52\right)} & \\
-30 &
\end{array}
\qquad
\begin{array}{l}
x-2 \\
\hline
x^3-6x^2+12x-26
\end{array}$$

Итак, $F(c)=-30$.

Задание 4. При каких условиях многочлен $F(x)$ делится на многочлен $G(x)$, если $F(x)=x^3+px+q$, $G(x)=x^2+mx-1$.

Решение.

Пусть для определённости, $F(x)\in C[x]$ и $G(x)\in C[x]$. Тогда по определению делимости многочленов имеем:

$F(x)\vdots G(x)\Leftrightarrow\left(\exists\Phi(x)\in C[x]\right):F(x)=G(x)\cdot\Phi(x)$.

Для нахождения многочлена $\Phi[x]$ производим деление «уголком»:

$$\begin{array}{l|l} F(x)=x^3+px+q & G(x)=x^2+mx-1 \\ \hline -\left(x^3+mx^2-x\right) & \hline \Phi(x)=x-m \\ \hline -mx^2+(p+1)x+q & \\ -\left(-mx^2-m^2x+m\right) & \\ \hline R(x)=\left(p+m^2+1\right)x+q-m & \end{array}$$

Чтобы выполнялось равенство $F(x)=G(x)\cdot\Phi(x)$, то есть

$F(x)=x^3+px+q=\left(x^2+mx-1\right)(x-m)$,

должно быть $R(x)=\left(p+m^2+1\right)x+q-m=0$, откуда, приравнивая коэффициенты к нулю, получаем искомые условия: $p=-1-m^2$, $q=m$.

Задание 5. Найти НОД$\left(F(x),G(x)\right)$, если $F(x)=x^4+4x^3-7x+2$, $G(x)=x^3+3x^2-4$.

Решение.

Используем общую схему алгоритма Евклида

1) Делим $F(x)$ на $G(x)$ с остатком:

$$\begin{array}{l|l} F(x)=x^4+4x^3-7x+2 & \\ \hline x^4+3x^3-4x & \hline G(x)=x^3+3x^2-4 \\ \hline x^3-3x+2 & Q_1=x+1 \\ x^3+3x^2-4 & \\ \hline R_1(x)=-3x^2-3x+6 & \end{array}$$

2) Делим $G(x)$ на $R_1(x)$ с остатком:

$$\begin{array}{l|l} G(x)=x^3+3x^2-4 & \\ \hline x^3+x^2-2x & \hline R_1(x)=-3x^2-3x+6 \\ \hline 2x^2+2x-4 & Q_2=-\frac{1}{3}x-\frac{2}{3} \\ 2x^2+2x-4 & \\ \hline 0 & \end{array}$$

Получаем наибольший общий делитель данных многочленов в виде $\left(F(x),G(x)\right)=R_1(x)=-3x^2-3x+6$, или по неоднозначности определения НОД $\left(F(x),G(x)\right)=x^2+x-2$.

Задание 6. Найти многочлен $F(x)=a_0+a_1x+a_2x^2$, если $F(1)=1, F(2)=2, F(3)=3$.

Решение.

Для нахождения многочлена требуется определить его коэффициенты a_0, a_1, a_2. Из условия задачи для коэффициентов имеем систему линейных алгебраических уравнений

$$\begin{cases} a_0+a_1+a_2=1, \\ a_0+2\,a_1+4\,a_2=2, \\ a_0+3\,a_1+9\,a_2=3. \end{cases}$$

Решаем СЛАУ методом Гаусса. Для этого совершаем ряд последовательных исключений.

1) Из первого уравнения $a_0=1-a_1-a_2$ подставляем во второе:

$$\begin{cases} a_0 + a_1 + a_2 = 1, \\ a_1 + 3\,a_2 = 1, \\ a_0 + 3\,a_1 + 9\,a_2 = 3. \end{cases}$$

2) Из второго уравнения $a_1 = 1 - 3a_2$ подставляя в третье:

$$\begin{cases} a_0 + a_1 + a_2 = 1, \\ a_1 + 3\,a_2 = 1, \\ 2\,a_2 = 0. \end{cases}$$

Двигаемся «обратным ходом» (находимся в поле действительных чисел):

3) из третьего уравнения находим $a_2 = 0$;

4) из второго уравнения находим $a_1 = 1$;

5) из первого уравнения находим $a_0 = 0$.

Составляем многочлен

$F(x) = a_0 + a_1 x + a_2 x^2 = x$.

Проверка очевидна. Искомый многочлен имеет вид $F(x) = x$.

Задание 7. Разложить многочлен $f(x) = x^3 + 1$ на неприводимые множители над полями R и C.

Решение.

$x^3 + 1 = (x+1)(x^2 + x + 1)$ (1) Над R: Многочлен $x^2 + x + 1$ не имеет действительных корней, следовательно (1) и есть разложение над полем R.

Над C: $x^2 + x + 1 = 0,\ D = -3 = 3i,\ i^2 = -1, \Rightarrow x_{1,2} = \dfrac{-1 \pm i\sqrt{3}}{2}$. Тогда искомое разложение на полем C будет иметь вид: $x^3 + 1 = (x+1)\left(x - \dfrac{-1 - i\sqrt{3}}{2}\right)\left(x + \dfrac{-1 - i\sqrt{3}}{2}\right)$.

Задание 8. Разделить с остатком многочлен f(x)=$x^3 - 4x^2 + 3x + 5$ на многочлен g(x)=$x^2 - 3x + 1$.

Решение.

$$\begin{array}{r|l} x^3 - 4x^2 + 3x + 5 & x^2 - 3x + 1 \\ \cline{2-2} x^3 - 3x^2 + x & x - 1 \\ \cline{1-1} -x^2 + 2x + 5 & \\ -x^2 + 3x - 1 & \\ \cline{1-1} -x + 6 & \end{array}$$

Ответ: $x^3 - 4x^2 + 3x + 5 = (x-1)(x^2 - 3x + 1) + (-x + 6)$.

Задание 9. Разделить многочлен f(x) = $x^3 + 2x - 5$ на двучлен x – 2 с помощью схемы Горнера.

Решение.

В данном случае c = 2.

	1	0	2	-5
c = 2	1	0 + 2·1 = 2	2 + 22 = 6	-5 + 2·6 = 7

Итак, $x^3 + 2x - 5 = (x-2)\cdot(x^2 + 2x + 6) + 7$, следовательно, значение многочлена f(x) при x = 2 равно, согласно теореме 1, семи: f(2) = 7.

Задание 10. Разложить многочлен f(x) = $x^3 + 2x - 5$ по степеням разности x – 2.

Решение.

По схеме Горнера выполним ряд последовательных делений с остатком на x – 2:

	1	0	2	-5
c = 2	1	0 + 2·1 = 2	2 + 2·2 = 6	-5 + 2·6 = 7
c = 2	1	4	14	
c = 2	1	6		
c = 2	1			

Таким образом, беря в качестве коэффициентов последние члены в каждой строке полученной схемы, можно записать:

$$x^3+2x-5 = (x-2)^3+6\cdot(x-2)^2+14\cdot(x-2)+7.$$

Задание 11. Найти значения производных многочлена f(x) = x^3+2x-5 при x = 2.

Решение.

Из схемы Горнера, построенной в примере 3, получаем:

$$b_0 = \frac{f(2)}{0!} = 7, \quad \Rightarrow \quad f(2) = 7\cdot 0! = 71 = 7,$$

$$b_1 = \frac{f'(2)}{1!} = 14, \quad \Rightarrow \quad f'(2) = 14\cdot 1! = 14,$$

$$b_2 = \frac{f''(2)}{2!} = 6, \quad \Rightarrow \quad f''(2) = 6\cdot 2! = 6\cdot 2 = 12,$$

$$b_3 = \frac{f^{(3)}(2)}{3!} = 1, \quad \Rightarrow \quad f^{(3)} = 1\cdot 3! = 1\cdot 6 = 6,$$

Так как все последующие коэффициенты b_4, b_5, …, b_k, равны нулю, то и значения всех производных данного многочлена, начиная с производной четвертого порядка, также будут равны нулю.

Задание 12. Разложить на множители многочлен над полем $\mathbb{Q}$

$$f(x) = x^4 - 15x^3 + 69x^2 - 72x - 108.$$

Решение.

Возможные целые корни — делители 108: $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 9, \pm 12, \pm 27, \pm 36, \pm 54, \pm 108$.

Пусть α— целый корень, $f(\alpha) = 0$.

$f(x) = (x-\alpha)g(x),$

$f(1) = 1 - 15 + 69 - 72 - 108 = -125,$

$f(1) = (1-\alpha)g(1),$

$f(1) \vdots (\alpha - 1).$

Из последней делимости следует, что корень нужно искать среди чисел 2; –4 и 6. Проверим их с помощью схемы Горнера:

	1	-15	69	-72	-108
2	1	-13	43	14	-80
-4	1	-19	119	590	$\neq 0$
6	1	-9	15	18	0
6	1	-3	-3	0	

Числа 2 и –4 не являются корнями многочлена, число 2 – является. Поэтому

$$f(x) = (x-6)^2(x^2-3x-3).$$

Задания

1. Записать в стандартном виде сумму и разность многочленов $f(x) = 2x^6 - 8x^3 + 3x^5 - 35x - 18 + 17x^2$ и $g(x) = 5x^5 - 2x^4 - 2x^6 + 10x^3 + 35x + 8$.

2. Записать в стандартном виде произведение многочленов $f(x) = 3x^4 - 2x^3 + 2x^2 + 7$ и $g(x) = 5x^3 + 4x - 5$.

3. Проверить, что в кольце $Z[x]$ многочлен $f(x)=6x^3+11x^2-13x+2$ делится на многочлен $g(x)=2x^2+5x-1$ (двумя способами).

4. Разделить с остатком $f(x)=x^4-4x^3+5x^2+x-1$ на $g(x)=x^2-2x-3$.

5. Найти многочлен $f(x)=a_0+a_1x+a_2x^2$, если $f(1)=1,\ f(2)=2,\ f(3)=3$.

6. Известны делимое $f(x)=2x^4+x^3+3x^2+1$, неполное частное $q(x)=2x^2+3x+2$ и остаток $r(x)=-4x-3$. Найти делитель $g(x)$.

7. Пусть $f(x)\in Z[x]$. При каких p,q многочлен $f(x)=x^4+px^2+q$ делится на $g(x)=x^2+x+1$?

8. Многочлен $P(x)$ делится без остатка на $(x-1)$ и $(x+1)$, а при делении на $(x+3)$ даёт в остатке 8. Найти остаток от деления $P(x)$ на x^3+3x^2-x-3.

9. Доказать, что при любом натуральном n и $a\in A$ (A – область целостности): а) $(x^n-a^n)\vdots(x-a)$; б) $(x^{2n}-a^{2n})\vdots(x+a)$.

10. Составить кубический многочлен, корнями которого являются числа 2, 4 и (-1), а старший коэффициент равен 4.

11. Пользуясь схемой Горнера, разделить с остатком многочлен $f(x)=x^6+4x^5-5x^4+3x^3-4x^2+2x-1$ на двучлен $(x-2)$.

12. Найти показатель кратности корня $x_0=-2$ для многочлена $f(x)=x^5+7x^4+16x^3+8x^2-16x-16$.

13. Разложить многочлен $f(x)=x^4-6x^3+12x^2-26x+37$ по степеням двучлена $(x-2)$.

14. Найти значение многочлена $f(x)=2x^5+7x^4-x^3+3x-2$ и всех его производных при $x=-3$ и разложить $f(x)$ по степеням двучлена $(x+3)$.

15. Вычислить значения многочлена $f(x)=x^4+5x^3-9x^2+7$ при $x=3{,}01$ и $x=2{,}98$.

2. Алгоритм Евклида для многочленов

Задание 1. Найти $НОД(f,g)$ для $f=x^2-1$ и $g=x+1$ над R.

Решение.

Многочлен f делится на все многочлены вида $\lambda(x^2-1)$, $\lambda\in R$, $(\lambda\neq 0)$, на все многочлены вида $\beta(x-1)$, $\beta\in R$, $(\beta\neq 0)$, на все многочлены вида $\gamma(x+1)$, $\gamma\in R$, $(\gamma\neq 0)$, на все многочлены вида μ, $\mu\in R$, $(\mu\neq 0)$. Многочлен g делится на все многочлены вида $\delta(x+1)$, $\delta\in R$, $(\delta\neq 0)$, и на все многочлены вида ω, $\omega\in R$, $(\omega\neq 0)$. Общими делителями многочленов f и g являются все многочлены вида $a(x+1)$, $a\in R$, $(a\neq 0)$ и все многочлены вида c, $c\in R$, $(c\neq 0)$. Среди них делятся на все общие делители многочленов f и g только многочлены вида $a(x+1)$, $a\in R$, $(a\neq 0)$. Значит, они и являются общими делителями многочленов f и g. Их бесконечно много. Среди них выделяется нормированный $НОД(f,g)=x+1$.

$НОД(f,g)$ можно найти с помощью алгоритма Евклида.

Пусть даны $f\neq\overline{0}$ и $g\neq\overline{0}$ и $\deg f\geq\deg g$.

1)Разделим f на g: $f=g\cdot q_1+r_1$, $\deg r_1<\deg g$,

2)Если $r_1\neq\overline{0}$, то разделим g на r_1: $g=r_1\cdot q_2+r_2$, $\deg r_2<\deg r_1$,

3)Если $r_2 \neq \bar{0}$, то разделим r_1 на r_2: $g_1 = r_2 \cdot q_3 + r_3$, $\deg r_3 < \deg r_2$, и т.д. до тех пор, пока в остатке не получится $\bar{0}$:

$$r_{k-2} = r_{k-1} \cdot q_k + r_k, \qquad \deg r_k < \deg r_{k-1}, \qquad r_k \neq \bar{0}.$$

$$r_{k-1} = r_k \cdot q_{k+1} + \bar{0}.$$

$$НОД(f, g) = r_k.$$

Заметим, что деление нужно производить «уголком».

Задание 2. Найти $НОД(f, g)$, если $f = 2x^3 - 3x^2 + x - 5$, $g = x^2 - 2x + 1$.

Решение.

1) $f = g \cdot q_1 + r_1$,
$q_1 = 2x + 1$, $r_1 = x - 6$

$$\begin{array}{r|l} 2x^3 - 3x^2 + x - 5 & x^2 - 2x + 1 \\ \hline \bar{}\,2x^3 - 4x^2 + 2x & 2x + 1 \\ \hline x^2 - x - 5 & \\ \bar{}\,x^2 - 2x + 1 & \\ \hline x - 6 & \end{array}$$

2) $g = r_1 \cdot q_2 + r_2$,
$q_2 = x + 4$, $r_2 = 25$

$$\begin{array}{r|l} x^2 - 2x + 1 & x - 6 \\ \hline \bar{}\,x^2 - 6x & x + 4 \\ \hline 4x + 1 & \\ \bar{}\,4x - 24 & \\ \hline 25 & \end{array}$$

3) $r_1 = r_2 \cdot q_3 + r_3$,
$q_3 = 1/25\,x - 6/25$, $r_3 = \bar{0}$

$$\begin{array}{r|l} x - 6 & 25 \\ \hline \bar{}\,x & 1/25\,x - 6/25 \\ \hline -6 & \\ -6 & \\ \hline 0 & \end{array}$$

Значит, $НОД(f, g) = 25$. Запишем нормированный $НОД(f, g)$: $d = 1$.

С помощью алгоритма Евклида для многочленов f и g всегда можно подобрать такие m_1 и m_2, что $f \cdot m_1 + g \cdot m_2 = НОД(f, g)$.

Задание 3. Для многочленов f и g подобрать такие многочлены m_1 и m_2, чтобы $f \cdot m_1 + g \cdot m_2 = НОД(f, g)$, если алгоритм Евклида для f и g состоит из двух строк.

Решение.

Пусть алгоритм Евклида для многочленов f и g состоит из двух строк:

$$f = g \cdot q_1 + r_1,$$
$$g = r_1 \cdot q_2 + \bar{0}.$$

Тогда $НОД(f, g) = r_1$.

Выделим r_1 из первой строки алгоритма: $r_1 = f - g \cdot q_1 = f \cdot 1 + g(-q_1)$. Тогда $m_1 = 1,\ m_2 = -q_1$.

Задание 4. Выделить кратные неприводимые множители многочлена

$$f = x^8 - x^6 - 2x^5 + 2x^3 + x^2 - 1 \in R[x].$$

Решение.

Дифференцируя f, получаем $f' = 8x^7 - 6x^5 - 10x^4 + 6x^2 + 2x$.

С помощью алгоритма Евклида находим

$$НОД(f, f') = x^4 - x^3 - x + 1 = (x^3 - 1)\cdot(x - 1) = (x^2 + x + 1)\cdot(x - 1)^2.$$

Отсюда следует, что кратными неприводимыми множителями многочлена f являются многочлены $p_1 = x^2 + x + 1$ (кратности 2) и $p_2 = x - 1$ (кратности 3).

Разделив f на $(x^2 + x + x)^2 (x - 1)^3$ получим $p_3 = x + 1$.

Итак, $f = (x^2 + x + 1)^2 (x - 1)^3 (x + 1)$.

Так как корни многочлена соответствуют его неприводимым множителям первой степени, то корни многочлена $НОД(f, f')$– это кратные корни многочлена f. Поэтому выделение кратных неприводимых множителей является в то же время выделением кратных корней многочлена f.

Задания

1. Найти НОД многочленов $f(x) = 3x^5 + 6x^4 + 3x^3 - x^2 - 2x - 1$ и $g(x) = x^4 - 2x^2 + 1$. (Ответ: $x^2 + 2x + 1$)
2. Найти линейное выражение НОД многочленов через сами эти многочлены: $f(x) = 2x^4 + 3x^3 - 3x^2 - 5x + 2$, $g(x) = 2x^3 + x^2 - x - 1$.
3. Разложить многочлен $f(x) = x^2 + \sqrt{2}$ на неприводимые множители над полем R; над полем C.
4. Разложить многочлены на неприводимые множители над полем действительных чисел: а) $a^5 - a^2 - a - 1$; б) $x^8 + x^4 - 2$; в) $y^{12} - 3y^6 + 1$.
5. Разложить многочлен $f(x) = x^4 + 1$ на неприводимые множители над полями C, R, Q.
6. Найти НОД многочлена $f(x) = (x + 1)\cdot(x^4 - 1)\cdot(x^3 - 1)$ и его производной.
7. Найти $НОД(f, g)$, если $f = (x - 1)^2 \cdot (x^2 - 1)^3$ и $g = (x + 1)^2 \times . \times (x - 2)$
8. Для многочленов f и g подобрать такие многочлены m_1 и m_2, чтобы $f \cdot m_1 + g \cdot m_2 = НОД(f, g)$, если алгоритм Евклида для f и g состоит из трех строк.
9. Выделить кратные неприводимые множители многочлена $f = x^8 - x^6 - 2x^5 + 2x^3 + x^2 - 1 \in R[x]$.
10. Отделить кратные множители многочлена $f(x) = x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4$.

Тема. Многочлены от нескольких переменных

План

1. Симметрические многочлены от нескольких переменных и их свойства.

2. Основная теорема о симметрических многочленах.

1. Симметрические многочлены от нескольких переменных и их свойства.

Теорема 1. Пусть σ_1 и σ_2 - два произвольных числа. Квадратное уравнение

$$z^2 - \sigma_1 z + \sigma_2 = 0 \qquad (*)$$

и система уравнений

$$\begin{cases} x + y = \sigma_1, \\ xy = \sigma_2 \end{cases} \qquad (**)$$

связанны друг с другом следующим образом: если z_1, z_2 корни квадратного уравнения $(*)$, то система имеет два решения

$$\begin{cases} x_1 = z_1, \\ y_1 = z_2; \end{cases} \quad \begin{cases} x_2 = z_2, \\ y_2 = z_1 \end{cases}$$

и других решений не имеет; обратно, если $x=a$, $y=b$ – решение системы $(**)$, то числа a и b является корнями уравнения $(*)$.

Доказательство. Если z_1 и z_2 - корни квадратного уравнения $(*)$, то по формулам Виета

$$z_1 + z_2 = \sigma_1,$$

$$z_1 z_2 = \sigma_2,$$

т.е. числа

$$\begin{cases} x_1 = z_1, \\ y_1 = z_1; \end{cases} \quad \begin{cases} x_2 = z_2, \\ y_2 = z_1 \end{cases}$$

является решениями системы $(**)$.

Пусть $x = a,\ y = b$ - решение системы $(**)$

$$a + b = \sigma_1,$$

$$ab = \sigma_2.$$

Тогда имеем:

$z^2 - \sigma_1 z + \sigma_2 = z^2 - (a+b)z + ab = (z-a)(z-b)$.

Но это означает, что числа a и b являются корнями квадратного уравнения $(*)$. Теорема доказана.

Система двух уравнений с двумя неизвестными, состоящая из несимметрических уравнений, может быть сведена к симметричной системе введением новых (вспомогательных) неизвестных. Например, если в системе

$$\begin{cases} x^3 - y^3 = 5 \\ xy^2 - x^2 y = 1 \end{cases}$$

заменить неизвестное y новым неизвестным $z=-y$ придем к системе

$$\begin{cases} x^3 + z^3 = 5 \\ xz^2 + x^2 z = 1 \end{cases}$$

левые части, которой симметрично зависят от x и y.

Иногда нужная подстановка имеет более сложный вид. Например, в системе:

$$\begin{cases} 3x - 2y = 5 \\ 81x^4 + 16y^4 = 6817 \end{cases}$$

замена $3x=u$, $-2y=v$, позволяет симметричную систему

$$\begin{cases} u + v = 5 \\ u^4 + v^4 = 6817 \end{cases}$$

Иногда, введением вспомогательных неизвестных можно свести уравнение с одним неизвестным к симметричной системе двух уравнений с двумя неизвестными.

Решение систем уравнений от трех переменных

Теорема 2. Пусть $\sigma_1, \sigma_2, \sigma_3$ - три произвольных числа. Кубическое уравнение $u^3 - \sigma_1 u^2 + \sigma_2 u - \sigma_3 = 0 \quad (*)$

и система уравнений $\begin{cases} x + y + z = \sigma_1, \\ xy + yz + xz = \sigma_2, \\ xyz = \sigma_3 \end{cases} \quad (**)$

связаны друг с другом следующим образом: если u_1, u_2, u_3 – корни кубического уравнения, то система уравнений $(**)$ имеет шесть решений

$$\begin{cases} x_1 = u_1, \\ y_1 = u_2, \\ z_1 = u_3; \end{cases} \quad \begin{cases} x_2 = u_1, \\ y_2 = u_3, \\ z_2 = u_2; \end{cases} \quad \begin{cases} x_3 = u_2, \\ y_3 = u_1, \\ z_3 = u_3; \end{cases} \quad \begin{cases} x_4 = u_2, \\ y_4 = u_3, \\ z_4 = u_1; \end{cases} \quad \begin{cases} x_5 = u_3, \\ y_5 = u_1, \\ z_5 = u_2; \end{cases} \quad \begin{cases} x_6 = u_3, \\ y_6 = u_2, \\ z_6 = u_1. \end{cases}$$

(получающихся друг из друга перестановками) и других решений не имеет; обратно, если $x = a, \quad y = b, \quad z = c$ -решение системы $(**)$, то числа a, b, c являются корнями кубического уравнения $(*)$.

Лемма. Если u_1, u_2, u_3 – корни кубического уравнения $u^3 + pu^2 + qu + r = 0$, то имеют место следующие соотношения: $u_1 + u_2 + u_3 = -p$, $u_1u_2 + u_1u_3 + u_2u_3 = q$, $u_1u_2u_3 = -r$.

Эти соотношения называют формулами Виета для кубического уравнения. Покажем, откуда эти соотношения вытекают. Итак, пусть u_1, u_2, u_3 – корни кубического уравнения $u^3 + pu^2 + qu + r = 0$, тогда

$u^3 + pu^2 + qu + r = (u - u_1)(u - u_2)(u - u_3)$.

Раскрывая скобки в правой части, находим:

$u^3 + pu^2 + qu + r = u^3 - (u_1 + u_2 + u_3)u^2 (u_1u_2 + u_1u_3 + u_2u_3)u - u_1u_2u_3$.

Из равенства многочленов следует равенства соответствующих коэффициентов, т.е.

$-(u_1 + u_2 + u_3) = p$,

$u_1u_2 + u_1u_3 + u_2u_3 = q$,

$-u_1u_2u_3 = r$,

что и доказывает лемму.

Пример 1. Дано квадратное уравнение $x^2 + 6x + 10 = 0$; составить новое квадратное уравнение, корнями которого является квадраты корней данного уравнения.

Решение. Для решения этой задачи обозначим корни данного уравнения через x_1, x_2, корни исходного – через p, q. По теореме Виета

$\sigma_1 = x_1 + x_2 = -6, \sigma_2 = x_1x_2 = 10$

и точно так же,

$y_1 + y_2 = -p, \; y_1y_2 = q$

Но, по условию задачи, имеем $y_1 = x_1^2, \quad y_2 = x_2^2$ и потому

$p = -(y_1 + y_2) = -(x_1^2 + x_2^2) = -s_2 = -(\sigma_1^2 - 2\sigma_2) = -16,$

$q = y_1y_2 = x_1^2x_2^2 = \sigma_2^2 = 100.$

Таким образом, искомое квадратное уравнение имеет вид

$y^2 - 16y + 100 = 0.$

Тем же методом можно решить и более сложные задачи. Рассмотрим следующий пример.

Пример 2. Составить квадратное уравнение $z^2+pz+q=0$ корнями которого являются числа $z_1=x_1^6-2x_2^2,\quad z_2=x_2^6-2x_1^2,$ где x_1, x_2 - корни квадратного уравнения $x^2-x-3=0.$

Решение. Для решения снова воспользуемся формулами Виета, согласно которым

$\sigma_1=x_1+x_2=1,\quad \sigma_2=x_1x_2=-3.$

С другой стороны, по тем же формулам,

$-p=z_1+z_2=(x_1^6-2x_2^2)+(x_2^6-2x_1^2),$

$q=z_1z_2=(x_1^6-2x_2^2)(x_2^6-2x_1^2).$

Воспользуемся таблицей Приложения 1, легко выразим симметрические многочлены $p\ и\ q$ через σ_1, σ_2 и, подставив значения $\sigma_1=1$, $\sigma_2=-3$, вычислим интересующие нас коэффициенты $p\ и\ q$. Имеем

$$-p=(x_1^6+x_2^6)-2(x_1^2+x_2^2)=s_2-2s_2==(\sigma_1^6-6\sigma_1^4\sigma_2+9\sigma_1^2\sigma_2^2-2\sigma_2^3)-2(\sigma_1^2-2\sigma_2)=$$
$$=[1^6-6\cdot1^4\cdot(-3)+9\cdot1^2\cdot(-3)^2-2\cdot(-3)^3]-2[1^2-2\cdot(-3)]=140;$$
$$q=(x_1^6-2x_2^2)(x_2^6-2x_1^2)=\ x_1^6x_2^6-2(x_1^8+x_2^8)+4x_1^2x_2^2=\sigma_2^6-2s_8+4\sigma_2^2=$$
$$=\sigma_2^6-2(\sigma_1^8-8\sigma_1^6\sigma_2+20\sigma_1^4\sigma_2^2-16\sigma_1^2\sigma_2^3+2\sigma_2^4)+4\sigma_2^2=$$
$$=(-3)^6-2\cdot[1^8-8\cdot1^6\cdot(-3)+20\cdot1^4\cdot(-3)^2-16\cdot1^2\cdot\cdot(-3)^3+2\cdot(-3)^4]$$
$$+4\cdot(-3)^2=-833.$$

Таким образом, $p=-140, q=-833$, и потому искомое квадратное уравнение имеет вид $z^2-140z-833=0.$

Тема. Многочлены над полем рациональных, действительных и комплексных чисел. Алгебраические числа

План

1. Разложение многочлена с комплексными коэффициентами в произведение линейных множителей.

2. Минимальный многочлен алгебраического числа и его свойства.

3. Простое и составное алгебраические расширения.

4. Решение уравнений третьей и четвёртой степени.

1. Понятие расширения поля. Минимальный многочлен алгебраического числа и его свойства

Задание 1. Описать строение поля K=Q(α), где Q – поле рациональных чисел: $\alpha=\sqrt{7+\sqrt{2}}$.

Решение.

Построим минимальный многочлен числа α над полем рациональных чисел:

$$x=\sqrt{7+\sqrt{2}}\Rightarrow x^2=\left(\sqrt{7+\sqrt{2}}\right)^2\Rightarrow$$

$$x^2=7+\sqrt{2}\Rightarrow x^2-7=\sqrt{2}\Rightarrow\left(x^2-7\right)^2=\left(\sqrt{2}\right)^2\Rightarrow$$

$$x^4-14x+49=2\Leftrightarrow x^4-14x+47=0.$$

Число $\alpha=\sqrt{7+\sqrt{2}}$ будет корнем многочлена $p(x)=x^4-14x+47$ по построению, причём очевидно, что степень этого многочлена минимальна и равна $n=4$.

Следовательно, базис простого алгебраического расширения K=Q(α)над полем рациональных чисел также состоит из четырёх элементов:

$$\alpha^0=1,\ \alpha,\ \alpha^2,\ \alpha^3.$$

Так как $\alpha=\sqrt{7+\sqrt{2}}$, то базис примет вид:

$$1,\ \sqrt{7+\sqrt{2}},\ \left(\sqrt{7+\sqrt{2}}\right)^2,\ \left(\sqrt{7+\sqrt{2}}\right)^3 \ \Leftrightarrow$$

$$1,\ \sqrt{7+\sqrt{2}},\ 7+\sqrt{2},\ \left(\sqrt{7+\sqrt{2}}\right)^3.$$

Тогда произвольный элемент поля K=Q(α) будет иметь вид:

$$\forall \omega \in Q\left(\sqrt{7+\sqrt{2}}\right)\ \ \omega = a_0 + a_1\cdot\sqrt{7+\sqrt{2}} + a_2\cdot\left(7+\sqrt{2}\right) + a_3\cdot\left(\sqrt{7+\sqrt{2}}\right)^3,\ a_i \in Q,\ i=\overline{0,3}.$$

Задание 2. Избавиться от иррациональности в знаменателе дроби

$$\frac{\alpha^4+\alpha^2+2}{\alpha^2+2},\ \text{где}\ \alpha^3+\alpha-1=0.$$

Решение.

Пусть $\alpha^4+\alpha^2+2=f(\alpha);\ \alpha^2+2=g(\alpha)$, тогда $f(x)=x^4+x^2+2,\ g(x)=x^2+2$

Нетрудно проверить, что многочлен $p(x)=x^3+x-1$ не имеет рациональных корней и, значит, неприводим в кольце Q[x]. Так как p(α)=0, то этот многочлен является минимальным для числа α.

Используя замечание, найдем линейное выражение многочлена $f(x)$ через многочлены $g(x)$ и $p(x)$ методом неопределенных коэффициентов.

Из замечания следует, что степень $u(x)$ будет равна 2, а степень $v(x)$ – 1:

$$f(x)=x^4+x^2+2\ =(\underbrace{ax^2+bx+c}_{u(x)})g(x)+(\underbrace{dx+k}_{v(x)})p(x)\quad (5).$$

Выполнив действия в правой части равенства и приведя подобные, получим:

$$f(x)=x^4+x^2+2\ =(a+d)x^4+(b+k)x^3+(2a+c+d)x^2+(2b-d+k)x+(2c-k).$$

Используя определение равенства двух многочленов, придем к системе линейных уравнений

$$\begin{cases} a+d=1; \\ b+k=0; \\ 2a+c+d=1; \\ 2b-d+k=0; \\ 2c-k=-2. \end{cases}$$

Решив систему, находим: $\begin{cases} a=1; \\ c=-1; \\ b=d=k=0 \end{cases} \Rightarrow u(x)=x^2-1;\ v(x)=0.$

Поэтому:

$$f(\alpha)=\alpha^4+\alpha^2+2=(\alpha^2-1)\cdot g(\alpha)+0\cdot p(\alpha)=(\alpha^2-1)\cdot g(\alpha)=(\alpha^2-1)\cdot(\alpha^2+2).$$

Подставим в исходное выражение значение, полученное для $\alpha^4+\alpha^2+2$, получим:

$$\frac{\alpha^4+\alpha^2+2}{\alpha^2+2}=\frac{(\alpha^2-1)\cdot(\alpha^2+2)}{\alpha^2+2}=\alpha^2-1.$$

Задание 3. Пусть P=Q($\sqrt{2},\sqrt{3}$) – конечное расширение поля рациональных чисел. Найти число γ, такое, чтобы Q($\sqrt{2},\sqrt{3}$) = Q(γ).

Решение.

Будем искать число γ в виде:

$\gamma = \sqrt{2}+c\sqrt{3}$, где c – подходящее число из поля Q, (2).

Число *c* выберем следующим образом. Пусть $p_1(x)$ и $p_2(x)$ - минимальные многочлены чисел $\sqrt{2}$ и $\sqrt{3}$ соответственно:

$$p_1(x) = x^2 - 2,\ p_2(x) = x^2 - 3 \quad (3).$$

Из (2) следует, что $\sqrt{2} = \gamma - c\sqrt{3}$ (4).

Рассмотрим многочлен

$$q(x) = p_1(\gamma - cx) \quad (5),$$

коэффициенты которого принадлежат полю $Q(\gamma)$. Очевидно, что $\sqrt{3}$ является корнем этого многочлена, так как

$$q(\sqrt{3}) = p_1(\gamma - c\sqrt{3}) = p_1(\sqrt{2}) = 0.$$

С другой стороны, $\sqrt{3}$ есть корень $p_2(x)$, коэффициенты которого принадлежат полю Q, а следовательно, и полю $Q(\gamma)$. Потребуем, чтобы многочлены q(x) и $p_2(x)$ не имели других общих корней, кроме числа $\sqrt{3}$.

Так как многочлен $p_2(x)$ имеет только два корня: $\sqrt{3}$ и $-\sqrt{3}$, то $-\sqrt{3}$ может быть общим корнем $p_2(x)$ и q(x), только если число

$$\gamma - c\cdot(-\sqrt{3})$$

будет корнем многочлена $p_1(x)$, то есть, если

$$\gamma - c\cdot(-\sqrt{3}) = \sqrt{2} \quad (7) \text{ или } \gamma - c\cdot(-\sqrt{3}) = -\sqrt{2} \quad (7')$$

Поэтому, чтобы многочлены q(x) и $p_2(x)$ не имели других общих корней, кроме $\sqrt{3}$, достаточно потребовать, чтобы

$$c \neq \frac{\pm\sqrt{2} - \sqrt{2}}{2\sqrt{3}},$$

т.е., чтобы $c \neq 0$ и $c \neq -\frac{\sqrt{2}}{\sqrt{3}}$.

Возьмем, например, c = 1. Тогда из равенства (2)

$$\gamma = \sqrt{2} + \sqrt{3} \text{ и } Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3}).$$

Из решения этой задачи видно, что, вообще говоря, число γ может быть выбрано неоднозначно.

4. Решение уравнений третьей и четвертой степени

Пусть дано уравнение

$$x^3 + px = q \qquad (1).$$

Будем искать решение в виде

$$x = u - v \qquad (2)$$

Возводя равенство (2) в куб, получим

$$x^3 = u^3 - 3u^2v + 3uv^2 - v^3 \qquad (3)$$

Умножая обе части равенства (2) на $3uv$, будем иметь

$$3uvx = 3u^2v - 3uv^2 \qquad (4)$$

Складывая почленно равенства (3) и (4), придём к равенству

$$x^3 + 3uvx = u^3 - v^3 \qquad (5),$$

сравнивая которое с исходным уравнением (1), получим

$$3uv = p, \quad u^3 - v^3 = q \qquad (6)$$

Тем самым решение исходного уравнения сводится к отысканию функций u и v, удовлетворяющих равенствам (6). Из (6) получаем уравнение для u:

$$u^6 - qu^3 - \frac{p^3}{27} = 0 \qquad (7)$$

Окончательно, после несложных преобразований, получаем

$$x = u - v = \sqrt[3]{\sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} + \frac{q}{2}} - \sqrt[3]{\sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} - \frac{q}{2}} \qquad (8).$$

В отличие от остальных математиков эпохи Возрождения, по-прежнему не признававших отрицательные корни, Кардано в свое работе предпринял попытки рассмотреть и их. Он называл их «софистическими», то есть ложными. Если при решении квадратных уравнений отрицательные корни можно было не принимать во внимание, считая их не существенными, исходя из смысла задачи, то для уравнений третьей степени игнорировать «неприводимый» случай уже не получалось.

Решая этот случай заменой $x = u + v$, Тарталья и Кардано пришли к результату

$$x = u + v = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} \qquad (9).$$

Очевидно, что случай $\left(\frac{q}{2}\right)^2 < \left(\frac{p}{3}\right)^3$ (который и получил название «неприводимого») порождал «софистические» корни и выражение (9) теряло смысл. Парадокс ситуации проявлялся в том, что легко было найти примеры подобных уравнений, имеющих действительные корни. Более того, у таких уравнений все корни были действительными.

Например, возьмём уравнение $x^3 = 7x + 6$. Здесь $p = 7,\ q = 6$. Для этих чисел выполняется

$$\left(\frac{q}{2}\right)^2 = 9,\ \left(\frac{p}{3}\right)^3 = \frac{343}{27};\ 9 < \frac{343}{27} \Rightarrow \left(\frac{q}{3}\right)^2 < \left(\frac{p}{3}\right)^3.$$

Подставляя их в равенство (9), получим

$$x = \sqrt[3]{3 + \sqrt{9 - \frac{343}{27}}} + \sqrt[3]{3 - \sqrt{9 - \frac{343}{27}}} = \sqrt[3]{3 + \sqrt{-\frac{100}{27}}} + \sqrt[3]{3 - \sqrt{-\frac{100}{27}}}.$$

Тем не менее, это уравнение имеет действительные корни

$$x_1 = 3,\ x_2 = -1,\ x_3 = -2.$$

Пытаясь разрешить возникшее противоречие, Кардано сделал важный шаг в понимании природы мнимых чисел. В задаче о делении 10 на две части, произведение которых было бы равно 40, в ответе получаются «софистические» числа $5 + \sqrt{-15}$ и $5 - \sqrt{-15}$. Кардано обращает внимание, что если проводить с ними вычисления как с обычными двучленами, то никакого противоречия не возникает:

$$-\sqrt{-15} \cdot \sqrt{-15} = 15.$$

И тогда эти числа есть решения задачи, которая сводится к системе

$$\begin{cases} x + y = 10, \\ xy = 40. \end{cases}$$

Значение публикации результатов Тартальи и Кардано трудно переоценить. Уже через несколько лет после выхода из печати «Великого искусства» английский

математик Р. Бомбелли предпринял первую попытку систематически изложить теорию мнимых чисел.

Решение уравнений четвёртой степени методом Феррари

В своих трудах Кардано не обходил вниманием и решение уравнений четвёртой степени. Он пытался решать их с помощью того же приёма, что и уравнения третьей степени, однако найти общую формулу решения (то есть разрешить в радикалах) ему так и не удалось. Слава открытия способа решения уравнений четвёртой степени принадлежит любимому ученику Кардано Лодовико Феррари.

Однажды Феррари предложили решить следующую задачу: «*Разделить число* 10 *на три части так, чтобы они составляли геометрическую прогрессию, причем произведение первых двух частей равнялось* 6 ».

Эта задача сводится к решению уравнения четвертой степени. Обозначим за x средний член последовательности, тогда по условию

$$\frac{6}{x} : x = x : \frac{x^3}{6} \Rightarrow \frac{6}{x} + x + \frac{x^3}{6} = 10 \Rightarrow x^4 + 6x^2 + 36 = 60x \qquad (1).$$

Используя прием решения кубических уравнений, Феррари прибавил к обеим частям последнего равенства $6x^2$, выделив из левой его части полный квадрат

$$(x+6)^2 = 60x + 6x^2 \qquad (2).$$

Идея дальнейшего решения полученного уравнения заключалась в том, чтобы его правую часть каким-то образом также преобразовать в полный квадрат. Идея потребовала введения некоторой новой переменной, которая, обращая в полный квадрат левую часть уравнения, делала бы то же самое с правой частью.

Пусть эта новая переменная будет y. Чтобы левая часть последнего уравнения обращалась при добавлении к ней переменной y в полный квадрат $(x+6+y)^2$, к ней необходимо прибавить $2(x+6)y + y^2$:

$$\begin{gathered}(x+6+y)^2 = 60x + 6x^2 + 2(x+6)y + y^2 \Rightarrow \\ (x+6+y)^2 = (2y+6)x^2 + 60x + (y^2 + 12y)\end{gathered} \qquad (3)$$

Чтобы правая часть последнего равенства стала полным квадратом, необходимо, чтобы $(2y+6)(y^2+12y) = 30^2$.

Получили кубическое уравнение, которое называют кубической резольвентой исходного уравнения четвёртой степени

$$y^3 + 15y^2 + 36y = 450 \qquad (4)$$

Найдя любой из корней этого уравнения и подставив его в качестве y в равенство $(x+6+y)^2 = (2y+6)x^2 + 60x + (y^2+12y)$, получим уравнение, у которого обе части есть полные квадраты двучленов. Извлекая корни из обеих частей находим четыре решения исходного уравнения.

В общем виде метод Феррари (в современном изложении) выглядит следующим образом. Пусть дано уравнение

$$x^4 + px^2 = qx^3 + r \qquad (5)$$

Введём новую переменную y, для которой потребуем

$$\left(x^2 + \frac{p}{2} + y\right)^2 = \left(2x^2 y - qx + \left(y^2 + py - r + \frac{p^2}{4}\right)\right) \qquad (6)$$

Чтобы правая часть равенства (6) оказалась полным квадратом, необходимо, чтобы

$$q^2 - 4 \cdot 2y\left(y^2 + py - r + \frac{p^2}{4} \right) = 0 \qquad (7)$$

Говоря современным математическим языком, это выражение есть дискриминант квадратного трёхчлена относительно переменной x, записанного в правой части равенства (6), коэффициенты которого зависят от новой переменной y. Известно, что квадратный трёхчлен можно свернуть как полный квадрат линейного двучлена тогда и только тогда, когда его дискриминант равен нулю, что собственно и использовал Феррари в своём методе. Сам дискриминант оказывается уравнением третьей степени от новой переменной y (кубическая резольвента).

Отыскав любой из корней y_0 кубической резольвенты (7) и подставив его в равенство (6), получим

$$\left(x^2 + \frac{p}{2} + y_0 \right)^2 = 2y_0 \left(x - \frac{q}{4y_0} \right)^2 \qquad (8)$$

Уравнение (8) распадается на два квадратных уравнения

$$\left[\begin{array}{l} x^2 + \frac{p}{2} + y_0 = \sqrt{2y_0} \cdot \left(x - \frac{q}{4y_0} \right) \\ x^2 + \frac{p}{2} + y_0 = -\sqrt{2y_0} \cdot \left(x - \frac{q}{4y_0} \right) \end{array} \right. \qquad (9)$$

Эти уравнения в совокупности и дают четыре корня исходного уравнения четвёртой степени.

Задания

1. Избавиться от иррациональности в знаменателе выражения $\frac{5}{1 - \sqrt[4]{2} + \sqrt{2}}$.

2. Избавиться от иррациональности в знаменателе выражения $\frac{\alpha^2 - 3\alpha - 1}{\alpha^2 + 2\alpha + 1}$, $\alpha^3 + \alpha^2 + 3\alpha + 4 = 0$;

3. Описать строение поля K=Q(α), где Q – поле рациональных чисел и найти элемент, обратный для элемента β: $\alpha = \sqrt{7 + \sqrt[3]{3}}$, $\beta = \sqrt[3]{3} - \sqrt{7 + \sqrt[3]{3}}$.

Тема. Натуральные числа. Система аксиом Пеано

Примеры решения задач

Задача 1. Доказать, используя аксиомы Пеано, что $(a+b)+c = a+(b+c)$ для любых натуральных чисел $a, b, c.$

Доказательство.

Индукция по $c.$ При $c = 1$ имеем: $(a+b)+1 = (a+b)' = a+b' = a+(b+1).$ Пусть теперь $(a+b)+x = a+(b+x).$ Тогда

$(a+b)+x' = ((a+b)+x)' = (a+(b+x))' = a+(b+x)' = a+(b+x'').$ Утверждение доказано.

Доказать, что $(a+b)c = ac+bc$ для любых натуральных чисел $a, b, c.$

Доказательство. Индукция по $c.$ При $c = 1$ утверждение очевидно. Пусть $(a+b)x = ax+bx.$ Тогда

$$(a+b)x' = (a+b)x + (a+b) = (ax+bx) + (a+b) =$$
$$= (ax+a) + (bx+b) = ax' + bx'.$$

Задача 2. Используя аксиомы действительных чисел, доказать, что $0 \cdot a = 0$ для любого действительного числа $a.$

Доказательство.

По аксиоме (9) $ba = (b+0)a = ba + 0a.$ Пусть x – число, противоположное к ba (оно существует по аксиоме (3)). Тогда $x + ba = x + (ba + 0a).$ По аксиомам (4) и (1) получаем: $0 = (x + ba) + 0a,$ т.е. $0a = 0.$

Задача 3. Используя аксиомы действительных чисел, доказать, что $1 > 0.$

Доказательство.

Предположим, что соотношение $1 > 0$ неверно. По аксиоме (6) $1 \neq 0.$ Значит, по аксиоме (13) $1 < 0.$ Пусть $a = -1$ (т.е. a – элемент, противоположный элементу 1 и существующий по аксиоме (3)). Тогда $a + 1 = 0.$ Прибавим к обеим частям неравенства $1 < 0$ число a: $1 + a < a$ (здесь мы используем аксиомы (14), (2), (4) и легко доказываемое утверждение $a + c = b + c \Rightarrow a = b).$ Отсюда $a > 0$ (интересный результат: $-1 > 0).$ Умножим на a (используя аксиому (15)): $a \cdot a > 0.$

Докажем теперь вспомогательное утверждение о том, что $(-1)^2 = 1.$ Действительно, так как $a + 1 = 0,$ то $(a+1)a = 0,$ т.е. $a^2 + a = 0.$ Прибавим 1: $(a^2 + a) + 1 = 1.$ Воспользуемся аксиомой (1): $a^2 + (a+1) = 1;\ a^2 + 0 = 1;\ a^2 = 1.$

Ранее было доказано, что $a^2 > 0.$ Следовательно, $1 > 0.$ Мы получили противоречие с предположением. Утверждение доказано.

Задания

1. Используя аксиомы Пеано, доказать, что для любых натуральных чисел справедливы равенства $1 \cdot a = a,\ ab = ba,\ (ab)c = a(bc).$

2. Пользуясь аксиомами действительных чисел, доказать их свойство плотности: для любых $a, b,$ если $a < b,$ то существует такое $x,$ что $a < x < b.$

3. Доказать, что для любого действительного числа $\varepsilon > 0$ существует натуральное число n такое, что $\frac{1}{n} < \varepsilon.$

Тема. Алгебраическая форма комплексного числа

Примеры решения задач

Задача 1. Даны в алгебраической форме два числа a и b:

Найти алгебраическую форму числа $\alpha = \frac{a}{b}$;

$$a = \left(-2\sqrt{3} - 10\right) + \left(10\sqrt{3} - 2\right)i, \quad b = 5 + i.$$

Решение.

В полученном выражении приводим подобные и получаем искомое комплексное число α.

$$\alpha = \frac{a}{b} = \frac{\left(-2\sqrt{3} - 10\right) + \left(10\sqrt{3} - 2\right)i}{5 + i} = \frac{\left(\left(-2\sqrt{3} - 10\right) + \left(10\sqrt{3} - 2\right)i\right)(5 - i)}{(5 + i)(5 - i)} =$$
$$= \frac{5 \cdot \left(-2\sqrt{3} - 10\right) - \left(-2\sqrt{3} - 10\right)i + 5 \cdot \left(10\sqrt{3} - 2\right)i - \left(10\sqrt{3} - 2\right)i^2}{25 - i^2} =$$

$$= \frac{\left(-10\sqrt{3}-50\right)-\left(-2\sqrt{3}-10\right)i+\left(50\sqrt{3}-10\right)i-\left(10\sqrt{3}-2\right)\cdot(-1)}{25-(-1)} =$$

$$= \frac{\left(10\sqrt{3}-2-10\sqrt{3}-50\right)+\left(50\sqrt{3}-10+2\sqrt{3}+10\right)i}{26} =$$

$$= \frac{-52+52\sqrt{3}i}{26} = -2+2\sqrt{3}i$$

Задача 2. Указать на комплексной плоскости все точки z, для которых выполняется неравенство. Сделать чертеж.

$1<\left|z-3-4i\right|\le 2$, где z – комплексное число.

Решение.

Представим комплексное число z в алгебраической форме $z=x+yi$, тогда заданное неравенство примет вид:

$1<\left|x+yi-3-4i\right|\le 2$ или $1<\left|(x-3)+(y-4)i\right|\le 2$

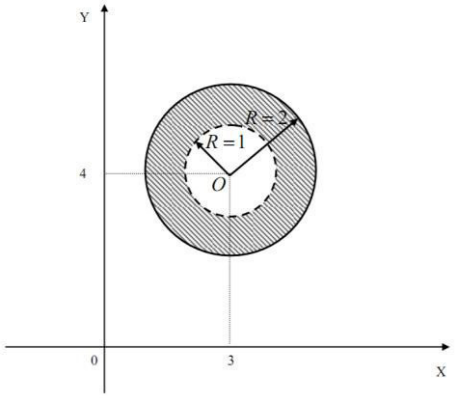
Введем в рассмотрение новое комплексное число $\tilde{z}=\tilde{x}+\tilde{y}i$, где $\tilde{x}=x-3$, $\tilde{y}=y-4$, тогда заданное неравенство можно записать в виде $1<\left|\tilde{z}\right|\le 2$. Модуль комплексного числа $\tilde{z}=\tilde{x}+\tilde{y}i$ равен $\left|\tilde{z}\right|=\sqrt{\tilde{x}^2+\tilde{y}^2}=\sqrt{(x-3)^2+(y-4)^2}$, следовательно, заданное неравенство принимает вид:

$1<\sqrt{(x-3)^2+(y-4)^2}\le 2$ или $1^2<(x-3)^2+(y-4)^2\le 2^2$

Рассмотрим первое неравенство $(x-3)^2+(y-4)^2>1^2$. Так как равенство $(x-3)^2+(y-4)^2=1^2$ является уравнением окружности с центром в точке $O(3;4)$ и радиусом $R=1$, то рассматриваемому неравенству удовлетворяют все точки комплексной плоскости, лежащие от точки $O(3;4)$ на расстоянии большем, чем $R=1$, т.е. все точки, лежащие с внешней стороны окружности $(x-3)^2+(y-4)^2=1^2$.

Рассмотрим второе неравенство $(x-3)^2+(y-4)^2\le 2^2$. Так как равенство $(x-3)^2+(y-4)^2=2^2$ является уравнением окружности с центром в точке $O(3;4)$ и радиусом $R=2$, то рассматриваемому неравенству удовлетворяют все точки комплексной плоскости, лежащие от точки $O(3;4)$ на расстоянии меньшем или равном $R=2$, т.е. все точки, лежащие с внутренней стороны окружности и на окружности $(x-3)^2+(y-4)^2=2^2$.

Таким образом, геометрическим местом точек, координаты которых удовлетворяют одновременно двум неравенствам, является кольцо, ограниченное сверху окружностью $(x-3)^2+(y-4)^2=2^2$, а снизу – окружностью $(x-3)^2+(y-4)^2=1^2$. При этом точки верхней окружности также являются решением заданного двойного неравенства, а точки нижней окружности – не являются.



Задача 3. Найти сумму, разность, произведение и частное чисел a и b в алгебраической форме.

$$a=-\frac{3\sqrt{2}}{2}-\frac{3\sqrt{2}}{2}i,\quad b=5i$$

Решение.

Сложение, вычитание и умножение комплексных чисел в алгебраической форме производят по правилам соответствующих действий над многочленами.

Найдем сумму чисел a и b:

$$a+b=-\frac{3\sqrt{2}}{2}-\frac{3\sqrt{2}}{2}i+5i=-\frac{3\sqrt{2}}{2}+\left(5-\frac{3\sqrt{2}}{2}\right)i$$

Найдем разность чисел a и b:

$$a-b=-\frac{3\sqrt{2}}{2}-\frac{3\sqrt{2}}{2}i-5i=-\frac{3\sqrt{2}}{2}+\left(-5-\frac{3\sqrt{2}}{2}\right)i$$

Найдем произведение чисел a и b:

$$a\cdot b=\left(-\frac{3\sqrt{2}}{2}-\frac{3\sqrt{2}}{2}i\right)\cdot 5i=-\frac{3\sqrt{2}}{2}\cdot 5i+\left(-\frac{3\sqrt{2}}{2}i\right)\cdot 5i=$$

$$=-\frac{15\sqrt{2}}{2}i-\frac{15\sqrt{2}}{2}i^2=-\frac{15\sqrt{2}}{2}i-\frac{15\sqrt{2}}{2}\cdot(-1)=\frac{15\sqrt{2}}{2}-\frac{15\sqrt{2}}{2}i$$

Найдем частное чисел a и b (см. задание 1):

$$\frac{a}{b}=\frac{-\frac{3\sqrt{2}}{2}-\frac{3\sqrt{2}}{2}i}{5i}=\frac{\left(-\frac{3\sqrt{2}}{2}-\frac{3\sqrt{2}}{2}i\right)(0-5i)}{(0+5i)(0-5i)}=$$

$$=\frac{\left(-\frac{3\sqrt{2}}{2}-\frac{3\sqrt{2}}{2}i\right)(-5i)}{-5i\cdot 5i}=\frac{\frac{3\sqrt{2}}{2}\cdot 5i+\frac{3\sqrt{2}}{2}i\cdot 5i}{-25i^2}=$$

$$=\frac{\frac{15\sqrt{2}}{2}i+\frac{15\sqrt{2}}{2}i^2}{-25i^2}=\frac{\frac{15\sqrt{2}}{2}i+\frac{15\sqrt{2}}{2}\cdot(-1)}{-25\cdot(-1)}=$$

$$=\frac{\frac{15\sqrt{2}}{2}i-\frac{15\sqrt{2}}{2}}{25}=-\frac{3\sqrt{2}}{10}+\frac{3\sqrt{2}}{10}i$$

Задания

1. Запишите решения системы в алгебраической форме

a) $\begin{cases} z_1-3z_2=i, \\ 2z_1+z_2=1; \end{cases}$ b) $\begin{cases} z_1+2z_2=1+i, \\ 3z_1+iz_2=2-3i \end{cases}$.

2. Существуют ли такие действительные числа x и y, для которых числа z_1 и z_2 являются сопряжёнными:

a) $z_1=8x^2-20i^{15}$, $z_2=9x^2-4+10yi^3$;

b) $z_1=4x+y+(1+i)y$, $z_2=8+ix$?

3. Сколько решений имеет система уравнений:

a) $\begin{cases} |z|=3, \\ |z-1+i|=1; \end{cases}$ b) $\begin{cases} |z|=1, \\ |z+3i|=2; \end{cases}$ c) $\begin{cases} |z|=1, \\ |z-1|=1. \end{cases}$?

4. Вычислить:

a) (1+i)^7 ; b) $\left(\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^{12}$; c); $(1-i)^4$; d) $\frac{(3+i\sqrt{3})^4}{\left(-\frac{1}{2}+i\frac{\sqrt{3}}{2}\right)^6}$.

5. Найти комплексное число вида z = x + i·y, где:

y = -1, |z| = $\sqrt{3}$, угол $\varphi \in [\frac{3\pi}{2}; 2\pi]$.

Тема. Тригонометрическая форма комплексного числа

Примеры решения задач

Задача 1. Даны в алгебраической форме два числа a и b:

а) Найти тригонометрическую форму числа $\alpha = \frac{a}{b}$;

б) Решить уравнение $z^3 + \alpha = 0$;

в) Изобразить числа α, $-\alpha$ и полученные корни уравнения $z^3 + \alpha = 0$ точками на комплексной плоскости.

$$a = \left(-2\sqrt{3} - 10\right) + \left(10\sqrt{3} - 2\right)i, \quad b = 5 + i.$$

Решение.

а) Комплексное число в тригонометрической форме имеет вид:

$\alpha = |\alpha| \cdot (\cos\varphi + i \cdot \sin\varphi)$,

где $|\alpha|$ – модуль комплексного числа α, φ – аргумент комплексного числа.

Если комплексное число задано в алгебраической форме $\alpha = x + yi$, то модуль комплексного числа находят по формуле $|\alpha| = \sqrt{x^2 + y^2}$, а аргумент комплексного числа из выражений $\cos\varphi = \frac{x}{\sqrt{x^2+y^2}}$, $\sin\varphi = \frac{y}{\sqrt{x^2+y^2}}$.

В нашем примере $\alpha = -2 + 2\sqrt{3}i$, т.е. $x = -2$, $y = 2\sqrt{3}$, следовательно, модуль $|\alpha| = \sqrt{(-2)^2 + \left(2\sqrt{3}\right)^2} = \sqrt{4+12} = \sqrt{16} = 4$.

Выражения $\cos\varphi = \frac{-2}{4} = -\frac{1}{2}$, $\sin\varphi = \frac{2\sqrt{3}}{4} = \frac{\sqrt{3}}{2}$ выполняются для $\varphi = \frac{2\pi}{3} + 2\pi k$, $k \in Z$.

Таким образом, комплексное число α в тригонометрической форме имеет вид:

$$\alpha = 4 \cdot \left(\cos\left(\frac{2\pi}{3} + 2\pi k \right) + i \cdot \sin\left(\frac{2\pi}{3} + 2\pi k \right) \right)$$

Так как $\cos\left(\frac{2\pi}{3} + 2\pi k\right) = \cos\frac{2\pi}{3}$, $\sin\left(\frac{2\pi}{3} + 2\pi k\right) = \sin\frac{2\pi}{3}$, то принято тригонометрическую форму комплексного числа записывать без $2\pi k$, при этом угол $\frac{2\pi}{3}$ называют главной частью аргумента комплексного числа. Итак, искомая тригонометрическая форма комплексного числа α имеет вид:

$$\alpha = 4 \cdot \left(\cos\frac{2\pi}{3} + i \cdot \sin\frac{2\pi}{3} \right)$$

б) Решим уравнение $z^3+\alpha=0$, где z – комплексное число. Из уравнения имеем $z=\sqrt[3]{-\alpha}=(-\alpha)^{\frac{1}{3}}$. Для возведения комплексного числа $\alpha=|\alpha|\cdot(\cos\varphi+i\cdot\sin\varphi)$ в n-ую степень используется формула Муавра: $\alpha^n=|\alpha|^n\cdot(\cos n\varphi+i\cdot\sin n\varphi)$.

Из пункта а) имеем $\alpha=-2+2\sqrt{3}i$, следовательно, $-\alpha=2-2\sqrt{3}i$. Представим число $-\alpha$ в тригонометрической форме аналогично пункту б):

$$|-\alpha|=\sqrt{2^2+\left(-2\sqrt{3}\right)^2}=\sqrt{4+12}=\sqrt{16}=4=|\alpha|,$$

$$\cos\varphi=\frac{2}{4}=\frac{1}{2},\ \sin\varphi=\frac{-2\sqrt{3}}{4}=-\frac{\sqrt{3}}{2},\ \ \varphi=\frac{5\pi}{3}+2\pi k,\ k\in Z.$$

Отсюда, $-\alpha=4\cdot\left(\cos\left(\frac{5\pi}{3}+2\pi k\right)+i\cdot\sin\left(\frac{5\pi}{3}+2\pi k\right)\right)$.

Числа α и $-\alpha$ имеют одинаковый модуль, но разные аргументы, которые отличаются друг от друга на величину угла π, что соответствует изменению направления радиус-вектора комплексного числа на противоположное, т.е. на 180° градусов. Следуя этому правилу можно сразу записать тригонометрическую форму числа $-\alpha$, зная тригонометрическую форму числа α.

По формуле Муавра при $n=\frac{1}{3}$ имеем:

$$(-\alpha)^{\frac{1}{3}}=4^{\frac{1}{3}}\cdot\left(\cos\left(\frac{1}{3}\left(\frac{5\pi}{3}+2\pi k\right)\right)+i\cdot\sin\left(\frac{1}{3}\left(\frac{5\pi}{3}+2\pi k\right)\right)\right).$$

Отсюда, $z=\sqrt[3]{-\alpha}=\sqrt[3]{4}\cdot\left(\cos\left(\frac{1}{3}\left(\frac{5\pi}{3}+2\pi k\right)\right)+i\cdot\sin\left(\frac{1}{3}\left(\frac{5\pi}{3}+2\pi k\right)\right)\right)$.

Уравнение третьей степени $z^3+\alpha=0$ имеет ровно три корня, которые можно найти, взяв $k=0,1,2$. Итак, искомые корни заданного уравнения имеют вид:

при $k=0$ $\quad z_1=\sqrt[3]{4}\cdot\left(\cos\frac{5\pi}{9}+i\cdot\sin\frac{5\pi}{9}\right)$

при $k=1$ $\quad z_2=\sqrt[3]{4}\cdot\left(\cos\frac{11\pi}{9}+i\cdot\sin\frac{11\pi}{9}\right)$

при $k=2$ $\quad z_3=\sqrt[3]{4}\cdot\left(\cos\frac{17\pi}{9}+i\cdot\sin\frac{17\pi}{9}\right)$.

в) Если комплексное число задано в алгебраической форме $\alpha=x+yi$, то в комплексной плоскости ему соответствует точка с координатами $(x;y)$. Если комплексное число задано в тригонометрической форме $\alpha=|\alpha|\cdot(\cos\varphi+i\cdot\sin\varphi)$, то ему соответствует точка конца вектора, который начинается в начале координат, имеет длину равную $|\alpha|$ и образует угол φ с положительным направлением оси Ox.

Имеем

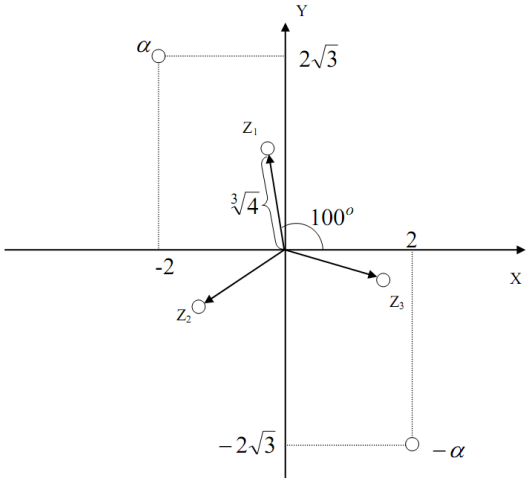
$\alpha=-2+2\sqrt{3}i,\quad x=-2,\ y=2\sqrt{3}$

$-\alpha=2-2\sqrt{3}i,\quad x=2,\ y=-2\sqrt{3}$

$z_1=\sqrt[3]{4}\cdot\left(\cos\frac{5\pi}{9}+i\cdot\sin\frac{5\pi}{9}\right),\ |\alpha|=\sqrt[3]{4},\ \varphi=\frac{5\pi}{9}=100^o$

$z_2=\sqrt[3]{4}\cdot\left(\cos\frac{11\pi}{9}+i\cdot\sin\frac{11\pi}{9}\right),\ |\alpha|=\sqrt[3]{4},\ \varphi=\frac{11\pi}{9}=220^o$

$$z_3 = \sqrt[3]{4}\cdot\left(\cos\frac{17\pi}{9}+i\cdot\sin\frac{17\pi}{9}\right),\ \ |\alpha| = \sqrt[3]{4},\ \varphi = \frac{17\pi}{9} = 340^o$$



Задача 2. Найти произведение и частное чисел a и b в тригонометрической форме.

$$a = -\frac{3\sqrt{2}}{2} - \frac{3\sqrt{2}}{2}i,\ \ b = 5i$$

Решение.

Найдем тригонометрическую форму числа a:

$$a = -\frac{3\sqrt{2}}{2} - \frac{3\sqrt{2}}{2}i,\ \ |a| = \sqrt{\left(-\frac{3\sqrt{2}}{2}\right)^2 + \left(-\frac{3\sqrt{2}}{2}\right)^2} = 3,$$

$$\cos\varphi = \frac{-\frac{3\sqrt{2}}{2}}{3} = -\frac{\sqrt{2}}{2},\ \sin\varphi = \frac{-\frac{3\sqrt{2}}{2}}{3} = -\frac{\sqrt{2}}{2},\ \varphi = \frac{5\pi}{4} + 2\pi k,\ k \in Z.$$

Итак, модуль числа a равен 3, главная часть аргумента числа a равна $\frac{5\pi}{4}$, тригонометрическая форма числа a имеет вид:

$$a = 3\cdot\left(\cos\frac{5\pi}{4}+i\cdot\sin\frac{5\pi}{4}\right)$$

Найдем тригонометрическую форму числа b:

$$b = 5i = 0 + 5i,\ \ |b| = \sqrt{0^2+5^2} = 5,$$

$$\cos\varphi = \frac{0}{5} = 0,\ \sin\varphi = \frac{5}{5} = 1,\ \varphi = \frac{\pi}{2} + 2\pi k,\ k \in Z.$$

Итак, модуль числа b равен 5, главная часть аргумента числа b равна $\frac{\pi}{2}$, тригонометрическая форма числа b имеет вид:

$$b = 5\cdot\left(\cos\frac{\pi}{2}+i\cdot\sin\frac{\pi}{2}\right)$$

Найдем произведение чисел a и b в тригонометрической форме. При умножении двух комплексных чисел, заданных в тригонометрической форме, их модули перемножаются, а аргументы складываются. Следовательно,

$$a = 3\cdot\left(\cos\frac{5\pi}{4}+i\cdot\sin\frac{5\pi}{4}\right),\ \ b = 5\cdot\left(\cos\frac{\pi}{2}+i\cdot\sin\frac{\pi}{2}\right)$$

$$a\cdot b = 3\cdot 5\cdot\left(\cos\left(\frac{5\pi}{4}+\frac{\pi}{2}\right)+i\cdot\sin\left(\frac{5\pi}{4}+\frac{\pi}{2}\right)\right) = 15\cdot\left(\cos\frac{7\pi}{4}+i\cdot\sin\frac{7\pi}{4}\right)$$

Найдем частное чисел a и b в тригонометрической форме. При делении двух комплексных чисел, заданных в тригонометрической форме, их модули делятся, а аргументы вычитаются. Следовательно,

$$a = 3 \cdot \left(\cos \frac{5\pi}{4} + i \cdot \sin \frac{5\pi}{4} \right), \quad b = 5 \cdot \left(\cos \frac{\pi}{2} + i \cdot \sin \frac{\pi}{2} \right)$$

$$\frac{a}{b} = \frac{3}{5} \cdot \left(\cos\left(\frac{5\pi}{4} - \frac{\pi}{2} \right) + i \cdot \sin\left(\frac{5\pi}{4} - \frac{\pi}{2} \right) \right) = \frac{3}{5} \cdot \left(\cos \frac{3\pi}{4} + i \cdot \sin \frac{3\pi}{4} \right).$$

10.3. Презентации по дисциплине Алгебра и теория чисел

1. Бинарные операции и алгебраические структуры
2. Группы, кольца, поля

10.4. Материалы для проведения текущей и промежуточной аттестаций представлены в фондах оценочных средств по дисциплине Алгебра и теория чисел

Л Е К Ц И Я 2

1. **Бинарные отношения и их свойства.**
2. **Отношения эквивалентности и порядка.**
3. **Разбиение множества. Фактор-множество.**

Бинарным отношением, заданным на множестве $A \neq \varnothing$, называется всякое **подмножество** множества $A \times A = A^2$.

Обозначение: $\langle a, b \rangle \in \rho$ или $a \rho b$ – элементы a и b находятся в отношении ρ.

Специальные символы: $=$, $<$, $\parallel$, $\perp$ и т.д.

ПРИМЕРЫ. I. $A=\{1, 2, 4\}$.

$A \times A = A^2 = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,4\rangle, \langle 2,1\rangle, \langle 2,2\rangle, \langle 2,4\rangle, \langle 4,1\rangle, \langle 4,2\rangle, \langle 4,4\rangle\}$.

$\rho = \{\langle 1,2\rangle, \langle 1,4\rangle, \langle 2,1\rangle, \langle 4,2\rangle, \langle 4,4\rangle\}$ – бинарное отношение на множестве A, т.к. $\rho \subset A$.

II. $A=N$, $(\forall a, b \in A) \langle a, b\rangle \in \rho \Leftrightarrow a-b=0$.

III. A – множество слов русского алфавита;

$(\forall x, y \in A) \langle x, y\rangle \in \rho \Leftrightarrow$ слова x и y начинаются с одинаковых букв.

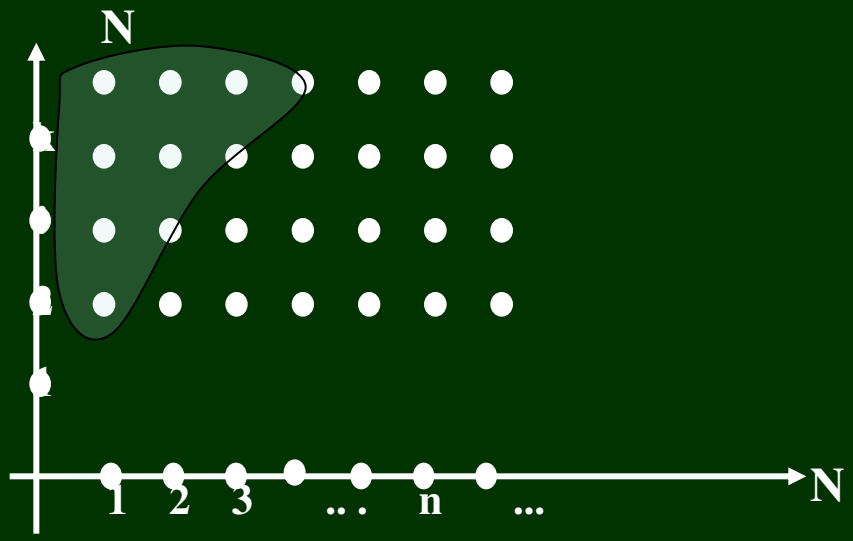
IV. A – множество людей, живущих на Земле;

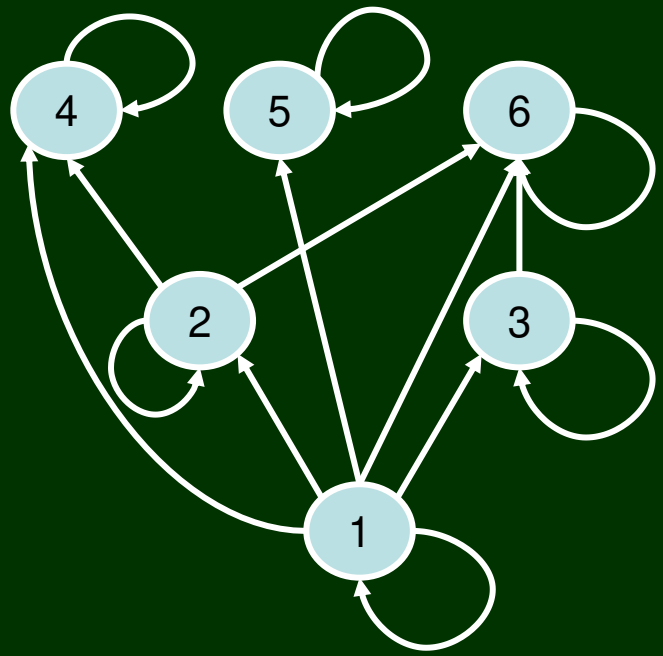
$(\forall x, y \in A) \langle x, y\rangle \in \rho \Leftrightarrow$ человек x – брат человека y.

СПООБЫ ЗАДАНИЯ БИНАРНЫХ ОТНОШЕНИЙ

Пусть < - отношение «меньше» на N.

Можно писать 3 < 5 или (3, 5) ∈ «<«





Пусть « | » - отношение «делит» на N: a | b, если b делится на a.

Например, 3 | 12, 5 | 5, 1 | k для любого k.

Отношение «делит» на множестве { 1, 2, 3, 4, 5, 6 }
может быть изображено в виде **графа**

Бинарным отношением, ***обратным*** к отношению ρ, заданному на A≠∅, называется отношение

$$\rho^{-1} = \{\langle b, a\rangle \mid \langle a, b\rangle \in \rho\}.$$

Дополнением к бинарному отношению ρ, заданному на A, называется отношение

$$\overline{\rho} = (A \times A) \setminus \rho,\ \overline{\rho} = \{\langle a,b\rangle / \langle a,b\rangle \notin \rho\}.$$

ПРИМЕР.

A={1, 2, 4}, ρ={<1,2>, <1,4>, <2,1>, <4,2>, <4,4>}.

Тогда ρ^{-1} ={<2,1>, <4,1>, <1,2>, <2,4>, <4,4>};

$$\overline{\rho} = \{\langle 1,1\rangle, \langle 2,2\rangle, \langle 2,4\rangle, \langle 4,1\rangle\}.$$

СВОЙСТВА БИНАРНЫХ ОТНОШЕНИЙ

1. Бинарное отношение ρ, заданное на множестве $A \neq \varnothing$, называется ***рефлексивным***, если

$$(\forall a \in A)\ \langle a, a\rangle \in \rho \quad (\text{или } a \rho a).$$

2. Бинарное отношение ρ, заданное на множестве $A \neq \varnothing$, называется ***антирефлексивным***, если

$$(\forall a \in A)\ \langle a, a\rangle \notin \rho.$$

3. Бинарное отношение ρ, заданное на множестве $A \neq \varnothing$, называется ***симметричным***, если

$$(\forall a, b \in A)\ (\langle a, b\rangle \in \rho \Rightarrow \langle b, a\rangle \in \rho).$$

4. Бинарное отношение ρ, заданное на множестве $A \neq \varnothing$, называется ***антисимметричным***, если

$(\forall a, b \in A)\ (\langle a, b\rangle \in \rho$ и $\langle b, a\rangle \in \rho \Rightarrow a = b)$.

5. Бинарное отношение ρ, заданное на множестве $A \neq \varnothing$, называется ***асимметричным***, если

$(\forall a, b \in A)\ (\langle a, b\rangle \in \rho$ никогда не следует $\langle b, a\rangle \in \rho)$.

6. Бинарное отношение ρ, заданное на множестве $A \neq \varnothing$, называется ***транзитивным***, если

$(\forall a, b, c \in A)\ (\langle a, b\rangle \in \rho$ и $\langle b, c\rangle \in \rho \Rightarrow \langle a, c\rangle \in \rho)$.

7. Бинарное отношение ρ на множестве $A \neq \varnothing$ называется:

- ***отношением эквивалентности***, если оно рефлексивно, симметрично и транзитивно одновременно;

- ***отношением строгого порядка***, если оно антирефлексивно, асимметрично и транзитивно;

- ***отношением нестрогого порядка,*** если оно рефлексивно, антисимметрично и транзитивно.

- ***отношением линейного порядка***, если $(\forall a, b \in A)$ выполняется одно и только одно из условий: **$a=b$, $a \rho b$ или $b \rho a$.**

ПРИМЕРЫ

1. Отношение равенства «=» на любом числовом множестве есть отношение эквивалентности.

2. Отношение перпендикулярности прямых «⊥» антирефлексивно, симметрично и не транзитивно.

3. Отношение делимости на множестве N натуральных чисел рефлексивно, антисимметрично и транзитивно, => есть отношение нестрогого нелинейного порядка.

Говорят, что набор подмножеств непустого множества А образует ***разбиение*** этого множества, если :

1) хотя бы одно из подмножеств непусто;

2) никакие два подмножества не пересекаются;

3) объединение всех подмножеств совпадает с множеством А.

Подмножества называются ***классами разбиения***.

ПРИМЕР

$A = \{a, b, c, d\}$ $A_1 = \{a, c\}$ $A_2 = \{b\}$ $A_3 = \{d\}$.

Набор подмножеств $A_1 = \{a, c\}$, $A_2 = \{b\}$, $A_3 = \{d\}$ образует разбиение множества А.

Пусть на А задано разбиение $A_1, A_2,..., A_n$.

Множество $\hat{A} = \{A_1, A_2,..., A_n\}$ называется ***<u>фактор-множеством</u>*** множества А по данному разбиению.

ТЕОРЕМА.

I. По каждому отношению эквивалентности, заданному на А можно построить разбиение этого множества.

II. Обратно, каждому разбиению множества А соответствует некоторое отношение эквивалентности.

Доказательство.

I. $A \neq \varnothing$, ρ - отношение эквивалентности на A.

Построим подмножества множества A:

$(\forall a \in A)\ A_a = \{x \in A \mid x \rho a\},\ A_a \subseteq A.$

1. Т.к. ρ рефлексивно, то $a \rho a \Rightarrow a \in A_a \Rightarrow A_a \neq \varnothing$.
2. Пусть $A_a \cap A_b = \{c\}$, $\Rightarrow c \in A_a$ и $c \in A_b \Rightarrow c \rho a$ и $c \rho b$.

Т.к. ρ симметрично, то $c \rho a \Rightarrow a \rho c$.

Тогда $a \rho c$ и $c \rho b \Rightarrow a \rho b$ (т.к. ρ транзитивно), $\Rightarrow a \in A_b$.

Аналогично, $b \in A_a$, $\Rightarrow A_a = A_b$.

3. Т.к. $(\forall a \in A)\ A_a \subseteq A \Rightarrow \bigcup_{a \in A} A_a \subseteq A$ (1)

$(\forall a \in A)\ a \in A_a \Rightarrow A \subseteq \bigcup_{a \in A} A_a$ (2).

Из (1), (2) $\Rightarrow \bigcup_{a \in A} A_a = A.$

II. Пусть задан набор классов, определяющий разбиение A. Построим бинарное отношение ρ: $(\forall a, b \in A)$ $a \rho b \Leftrightarrow$ a, b $\in$ одному и тому же классу разбиения.

1. Т.к. каждый элемент из A лежит сам с собой в одном классе, то $(\forall a \in A)$ $a \rho a$, ρ рефлексивно.
2. Пусть $a \rho b$, => a, b $\in$ одному классу, => b, a $\in$ тому же классу, => $b \rho a$, => ρ симметрично.
3. Пусть $a \rho b$ и $b \rho c$ => a, b $\in$ одному классу и b, c $\in$ одному классу, => a, c тоже $\in$ одному классу и $a \rho c$, => ρ транзитивно.

Из 1 – 3 следует, что ρ – отношение эквивалентности на A.

ПРИМЕР. Z – множество целых чисел, $m > 1$, $m \in Z$.

Отношение $\rho = \{x\rho y \mid x, y \in Z; (x - y) : m\}$ называется ***отношением сравнения по модулю m:*** $x \equiv y \pmod m$.

Т.к. $(\forall x \in Z)\ (x - x) = 0 : m \Rightarrow x\rho x$ и ρ рефлексивно.

Пусть $x\rho y \Rightarrow (x - y) : m \Rightarrow (y - x) : m \Rightarrow y\rho x \Rightarrow$

ρ симметрично.

Пусть $x\rho y,\ y\rho z \Rightarrow (x - y) : m,\ (y - z) : m \Rightarrow$

$x - z = [(x - y) + (y - z)] : m \Rightarrow x\rho z$, и

ρ транзитивно, $\Rightarrow \rho$ – отношение эквивалентности.

Классы разбиения по отношению ρ – множества всех целых чисел, которые при делении на m дают одинаковые остатки: $Z_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$.

Темы рефератов

1. *Операции над бинарными отношениями.*
2. *n – арные отношения и их свойства.*
3. *Упорядоченные множества. Минимальные и наименьшие элементы.*

Литература

1. Л.Я. Куликов. Алгебра и теория чисел.

М., Высшая школа, 1979. Стр. 48-54, 65-70.

2. Л.В. Лободина. Элементы абстрактной и компьютерной алгебры. Борисоглебск, 2006. Стр. 5-10.

Л Е К Ц И Я 3

1. Отображения или функции.
2. Свойства отображений.
3. Обратимость отображений.

Бинарное отношение f, заданное на паре множеств A и B, называется ***отображением*** или ***функцией*** из A в B, если:

1) $(\forall a \in A)(\exists b \in B)\ \langle a, b\rangle \in f$;

2) $(\forall a \in A)(\forall b, c \in B)\ (\langle a, b\rangle \in f \text{ и } \langle a, c\rangle \in f) \Rightarrow b = c$.

Обозначение: $\langle a, b\rangle \in f \Leftrightarrow f(a)=b$.

Элемент b – ***образ*** элемента a, элемент a – ***прообраз*** b.

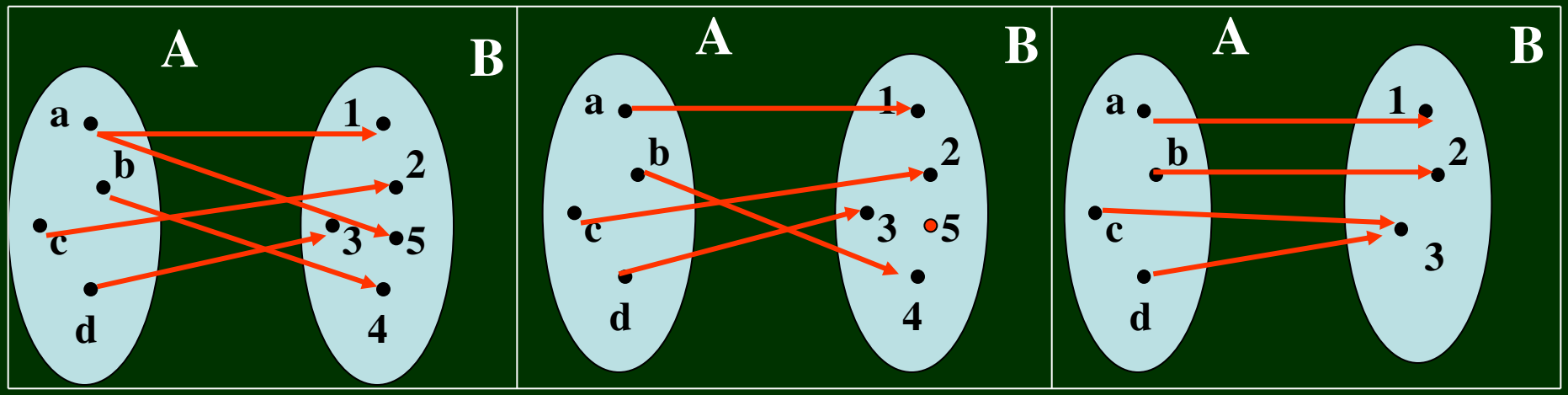
Условие 2) $\Leftrightarrow$ условию 3) $f(a)=b,\ f(a)=c \Rightarrow b = c$.

Бинарное отношение f, заданное на паре множеств A и B, называется отображением или функцией из A в B, если ***каждый*** элемент из A имеет ***единственный*** образ в B.

Отображение f из A в B называется ***инъективным (или инъекцией)***, если $(\forall a, b \in A)\ f(a) = f(b) \Rightarrow a = b$.

Отображение f из A в B называется ***сюръективным (или сюръекцией, или отображением «на»)***, если $(\forall b \in B)(\exists a \in A)\ f(a) = b$.

Отображение f из A на B называется ***биективным (или биекцией или взаимно-однозначным)***, если оно инъективно и сюръективно одновременно.



ПРИМЕРЫ.

1. $f = \{\langle x, y\rangle \in R \times R \,/\, x = y^2\}$.

f – ***не отображение***, т. к. для $x = 4$: $y = \sqrt{2}$ и $y = -\sqrt{2}$, $\Rightarrow f(4) = 2$ и $f(4) = -2$, но $2 \neq -2$.

2. $f = \{\langle x, y\rangle \in R \times R \,/\, x^2 = y\}$.

$(\forall x \in R)(\exists! y \in R)\ y = f(x) = x^2 \Rightarrow f$ – ***отображение.***

f ***не инъективно***, т.к. $f(2) = f(-2) = 4$, но $2 \neq -2$.

f ***не сюръективно***, т.к. если $y < 0$, то $(\forall x \in R)\ x^2 \neq y$.

3. $f = \{\langle x, y\rangle \in R \times R \,/\, y = 2x\}$.

$(\forall x \in R)(\exists! y \in R)\ y = 2x, \Rightarrow f$ – ***отображение.***

Т.к. $(\forall x, x_1 \in R)\ f(x) = f(x_1) \Leftrightarrow \frac{y}{2} 2x = 2x_1 \Leftrightarrow x = x_1$ $\Rightarrow f$ ***инъекция.***

Т.к. $(\forall y \in R)(\exists\ x = \frac{y}{2} \in R)\ f(x) = f(\frac{y}{2}) = 2 \cdot \frac{y}{2} = y$, то f - ***сюръекция***. Следовательно, f - ***биекция***.

Пусть $f=\{\langle x, y\rangle / x \in X, y \in Y\}$– отображение из X в Y.
Соответствие $f^{-1}=\{\langle y, x\rangle$ / где $\langle x, y\rangle \in f\}$
называется ***обратным*** к отображению f.

ТЕОРЕМА
Соответствие f^{-1}, обратное к отображению f, само является отображением тогда и только тогда, когда отображение f биективно.

Доказательство.
I. Пусть $f: X \to Y$ – биекция, => f – сюръекция =>
$(\forall y \in Y)(\exists x \in X) \langle x, y\rangle \in f \Leftrightarrow \langle y, x\rangle \in f^{-1}$.

Пусть $\langle y, x\rangle \in f^{-1}$ и $\langle y, x_1\rangle \in f^{-1} \Rightarrow \langle x, y\rangle$ и $\langle x_1, y\rangle \in f$.
Т.к. f инъекция, то из $y = f(x) = f(x_1)$ следует $x = x_1$.
Получили: $(\forall y \in Y)(\exists! x \in X) \langle y, x\rangle \in f^{-1}, \Rightarrow$
f^{-1} - ***отображение*** Y в X.

II. Пусть $f^{-1}: Y \to X$ – отображение, $\Rightarrow$
$(\forall y \in Y)(\exists!\ x \in X) \langle y, x\rangle \in f^{-1}, \Rightarrow (\forall y \in Y)(\exists\ x \in X)$
$\langle x, y\rangle \in f, \Rightarrow f$ – ***сюръекция*** (1).
Пусть $f(x) = f(x_1) = y, \Rightarrow \langle x, y\rangle$ и $\langle x_1, y\rangle \in f, \Rightarrow$
$\langle y, x\rangle$ и $\langle y, x_1\rangle \in f^{-1}, \Rightarrow f^{-1}(y) = x$ и $f^{-1}(y) = x_1$.
Т.к. f^{-1} - отображение Y в X, то $x = x_1$.
Получили: $f(x) = f(x_1) \Rightarrow x = x_1, \Rightarrow f$ ***инъективно*** (2).
Из (1), (2) следует, что f ***биективно***.

Темы рефератов:

1. Перестановки и подстановки на конечных множествах.
2. Композиция отображений.

Литература

1. Л.Я. Куликов. Алгебра и теория чисел.

М., Высшая школа, 1979. Стр. 54 - 65.

2. Л.В. Лободина. Элементы абстрактной и компьютерной алгебры. Борисоглебск, 2006. Стр. 11 - 12.

Л Е К Ц И Я 4

1. Алгебраические операции.
2. Свойства бинарных алгебраических операций.
3. Алгебраические структуры с одной и двумя бинарными операциями.

Бинарная алгебраическая операция, заданная на множестве $A \neq \varnothing$, – это отображение f: $A \times A \to A$:

$(\forall a, b \in A)(\exists c \in A)$ $f: \langle a, b \rangle \to c$

Обозначение: $afb = c$. Для обозначения бинарных операций обычно используют специальные знаки:

« +», « * »,«-», « : », « ∘ » и т.д.

Унарная алгебраическая операция, заданная на множестве A, – это отображение f: $A \to A$:

$(\forall a \in A)(\exists c \in A)$ $f(a) = c$.

Нульарная алгебраическая операция, заданная на множестве A, – это выделение в A некоторого фиксированного элемента.

Примеры бинарных операций: обычное «+» и «·» чисел,
примеры унарных операций: «$^{-1}$» и «–», $\mathbf{x^n}$ или √,
примеры нульарных операций - выделение **0** или **1.**

Т.к. бинарная алгебраическая операция – это ***отображение из A^2 в A***, то для ее задания достаточно ***каждой*** паре элементов из А сопоставить ***единственный*** элемент этого же множества А.

Например, отображение «*»: $N\times N\to N$, при котором $(\forall x, y \in N) \langle x, y\rangle \to 1$ задает алгебраическую операцию

$$«*»: (\forall x, y \in N)\ x*y = 1.$$

СВОЙСТВА АЛГЕБРАИЧЕСКИХ ОПЕРАЦИЙ

Операция «·», заданная на $A \neq \varnothing$, называется:

ассоциативной, если:

$$(\forall a, b, c \in A)\ \ a\cdot(b\cdot c) = (a\cdot b)\cdot c;$$

коммутативной, если: $(\forall a, b \in A)\quad a\cdot b = b\cdot a.$

Говорят, что операция «·» обладает:

левым [***правым***] ***нейтральным*** **элементом**, если:

$$(\exists e_L \in A)(\forall a \in A)\qquad e_L\cdot a = a$$

$$[(\exists e_R \in A)(\forall a \in A)\qquad a\cdot e_R = a];$$

двусторонним нейтральным **элементом** (или просто **нейтральным**), если:

$$(\exists e \in A)(\forall a \in A)\qquad e\cdot a = a\cdot e = a.$$

Операция «·», заданная на $A \neq \varnothing$, называется:

обратимой слева *[****справа****]*, если:

$$(\forall a \in A)(\exists b \in A) \quad b \cdot a = e_L,$$

$$[(\forall a \in A)(\exists c \in A) \quad a \cdot c = e_R];$$

двусторонне обратимой (или просто ***обратимой***), если она обратима и справа и слева:

$$(\forall a \in A)\ (\exists b \in A) \quad a \cdot b = b \cdot a = e;$$

сократимой слева *[****справа****]*, если:

$$(\forall a, b, c \ \ A) \quad c \cdot a = c \cdot b \ \Rightarrow \ a = b,$$

$$[a \cdot c = b \cdot c \ \Rightarrow \ a = b].$$

сократимой, если она сократима и слева и справа.

Пусть на A $\neq\varnothing$ заданы бинарные алгебраические операции - «*» и «·».

Операция «$\circ$» называется ***дистрибутивной слева*** [***справа***] относительно операции «*», если:

$$(\forall a, b, c \in A) \quad c \cdot (a*b) = (c\cdot a)*(c \cdot b)$$

$$[(a*b) \cdot c = (a \cdot c)*(b \cdot c)].$$

Операция «$\circ$» называется ***дистрибутивной*** относительно операции «*», если она дистрибутивна относительно данной операции и слева и справа.

Например, на всех числовых множествах, «·» дистрибутивно относительно «+»:

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

1. Проверку свойств бинарной операции, заданной на множестве $A \neq \varnothing$, необходимо начинать с условия алгебраичности операции на А.

Например, операция «–» ***не алгебраическая*** на N, т.к. если $a < b$, то $a - b < 0$, $\Rightarrow \notin N$.

2. Если по данной операции в множестве А нет нейтрального элемента, то не имеет смысла говорить об обратимости этой операции.

3. Если операция коммутативна на А, то любое из свойств, которое выполняется для нее ***слева,*** будет выполняться и с ***справа***, и наоборот.

Пусть <A, ·> - непустое множество с заданной бинарной операцией «·».

1. ***Структура*** <A, ·> называется ***группоидом***, если «·» является алгебраической операцией на A:

$$(\forall a, b \in A) \quad (a \cdot b \in A).$$

2. Группоид <A, ·> называется ***полугруппой***, если «·» ассоциативна на A.

3. Полугруппа <A, ·> называется ***моноидом*** (***полугруппой с единицей***) , если по операции «·» в A существует нейтральный элемент.

4. Моноид <A, ·> называется ***группой***, если операция «·» обратима на A.

5. Если операция «·» коммутативна на A, то структура <A, ·> называется ***коммутативной*** или ***абелевой.***

ПРИМЕРЫ.

1. Множество натуральных чисел не образует алгебраической структуры по операции вычитания, т.к. если a, b $\in$N и a<b, то a-b<0, => a-b $\notin$N.

2. <Z, -> - группоид, т.к. операция «-» на Z алгебраическая, но не ассоциативная.

3. <N, +> - абелева полугруппа. Т.К. операция «+» не обратима на N, то <N, +> группой не является.

4. <Z, +> и <R’, ·> - абелевы группы, т.к. операции «+» и «·» ассоциативны, коммутативны, обладают нейтральными элементами и обратимы на соответствующих множествах.

Темы рефератов:

1. *Общее понятие алгебраической структуры или алгебры.*

2. *Отношение конгруэнции и его свойства.*

Литература

1. Л.Я. Куликов. Алгебра и теория чисел.

М., Высшая школа, 1979. Стр. 75-93.

2. Л.В. Лободина. Элементы абстрактной и компьютерной алгебры. Борисоглебск, 2006. Стр. 12-19.

Л Е К Ц И Я 5

1. **Группы. Простейшие свойства групп.**

2. **Гомоморфизмы и изоморфизмы групп.**

3. **Простейшие свойства изоморфизмов групп.**

Определение 1

Алгебраическая структура $\mathbf{<G, \cdot, ^{-1}, e>}$,

где $G \neq \varnothing$, «$\cdot$» - бинарная, «$^{-1}$» - унарная,

e - нульарная операции на G называется ***группой,*** если:

1) «$\cdot$» ассоциативна - $(\forall x, y \in G)\quad x \cdot (y \cdot z) = (x \cdot y) \cdot z$;

2) e – нейтральный элемент по операции «$\cdot$»;

3) $(\forall x \in G)\ (\exists x^{-1} \in G)\quad x \cdot x^{-1} = x^{-1} \cdot x = e$ – обратимость.

Определение 2

Алгебраическая структура $\langle G, \cdot \rangle$, где $G \neq \varnothing$, «$\cdot$» - бинарная операция на G, называется ***группой,*** если:

1)«$\cdot$» ассоциативна;

2)$(\forall a, b \in G)\ (\exists x, y \in G)\ \ a \cdot x = b$ и $y \cdot a = b$,

(говорят, что в группе разрешимы уравнения вида $a \cdot x = b$ и $y \cdot a = b$).

Теорема

Определения группы 1 и 2 эквивалентны.

I. Пусть $\langle G, \cdot, e, ^{-1} \rangle$ - группа по определению 1.

Тогда по условию «$\cdot$» ассоциативна, обладает нейтральным e и обратима.

Доказать: **G –** группа по определению 2, т.е., что в **G** для любых a и b разрешимы уравнения

$a \cdot x = b$ и $y \cdot a = b$.

II. Пусть $\langle G, \cdot \rangle$ - группа по определению 2.

Тогда по условию «$\cdot$» ассоциативна и уравнения

$a \cdot x = b$ и $y \cdot a = b$ разрешимы в **G** для любых a и b.

Доказать: **G –** группа по определению 1, т.е., что

«$\cdot$» на **G** ассоциативна, обладает нейтральным e и обратима

ПРОСТЕЙШИЕ СВОЙСТВА ГРУПП

1. В группе существует единственный нейтральный:

пусть e, f – нейтральные элементы группы $\langle G, \cdot \rangle$.

Тогда: $e \cdot f = f$, т.к e – нейтральный элемент

и $e \cdot f = e$, т.к. f – нейтральный элемент, =>

$e = f$.

2. В группе каждый элемент обладает единственным обратным:

пусть b, c – обратные для элемента $a \in G$.

Тогда: $a \cdot b = b \cdot a = e$, т.к. b - обратный для a

и $a \cdot c = c \cdot a = e$, т.к. c - обратный для a, =>

$b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = e \cdot c = c$.

3. В группе каждое из уравнений $a \cdot x = b$ и $y \cdot b = a$ имеет единственное решение для любых $a, b \in G$.

Доказательство => из свойства 2.

4. В группе $(a^{-1})^{-1} = a$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$:

$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot e \cdot b = b^{-1} \cdot b = e$,

$\Rightarrow (b^{-1} \cdot a^{-1})$ – обратный для $(a \cdot b)$;

но $(a \cdot b)^{-1}$ – обратный для $(a \cdot b)$ по определению,
=> они совпадают (из единственности обратного).

5. В группе операция двусторонне сократима.

Гомоморфизмом группы $\langle G, \cdot \rangle$ в группу $\langle S, * \rangle$ называется отображение $f: G \to S$, такое что

$$(\forall x, y \in G)\ f(x \cdot y) = f(x) * f(y),$$

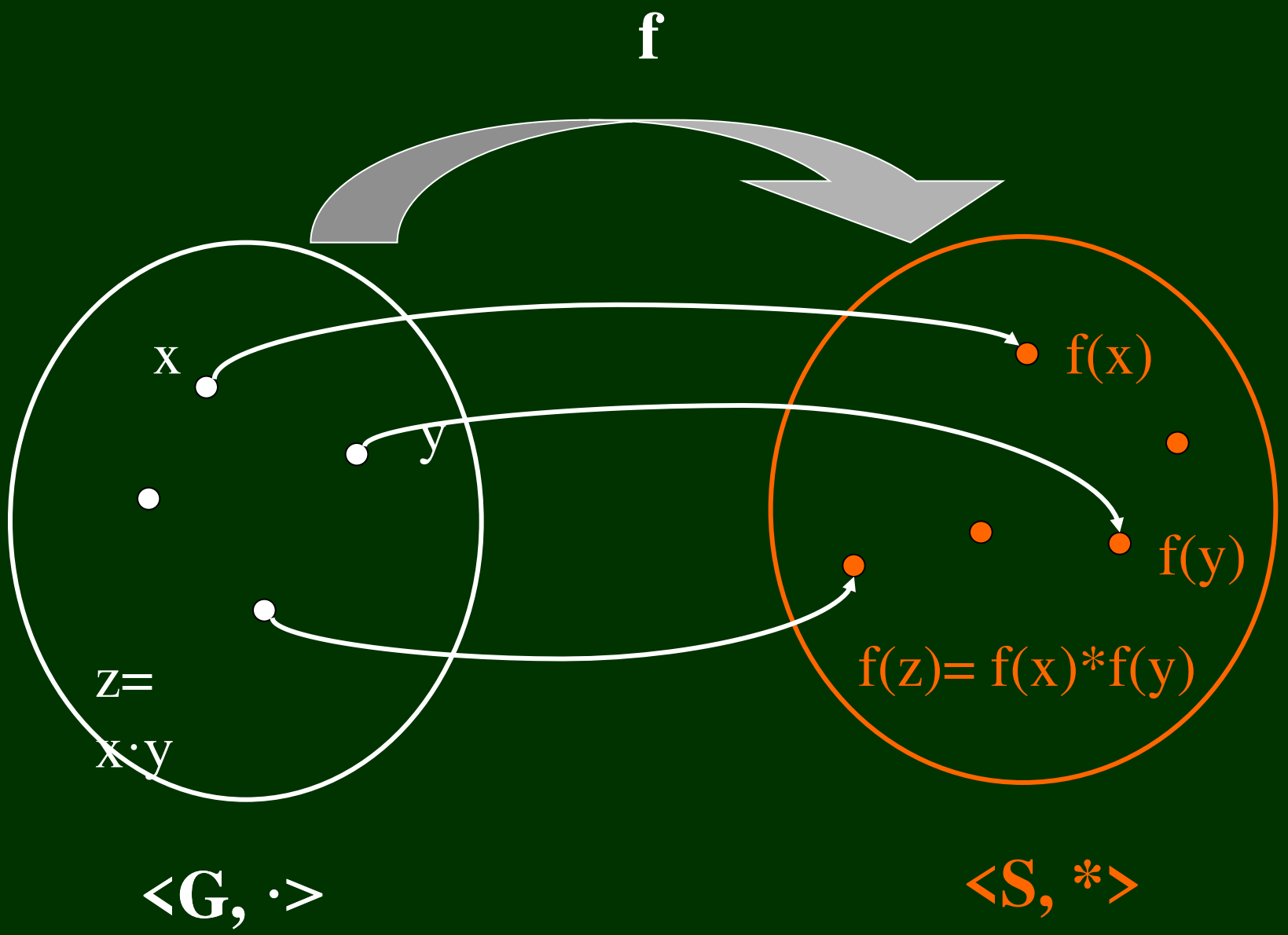
говорят, что f ***сохраняет операцию*** группы.

Множество $f(G)=\{s \in S \mid (\exists x \in G)\ s = f(x)\}$ называется ***гомоморфным образом*** группы G ($f(G) \subseteq S$).

Гомоморфизм групп называется ***изоморфизмом***, если f – биективное отображение.

Обозначение: $G \sim S$ – гомоморфные группы,

$G \cong S$ – изоморфные группы.


f
x
y
z=
x·y
f(x)
f(y)
f(z)= f(x)*f(y)
<G, ·>
<S, *>

ПРИМЕРЫ

1. $\langle Z, + \rangle \cong \langle 2Z, + \rangle$, т.к. биективное отображение

$f: Z \to 2Z \quad (\forall x \in Z)\ f(x) = 2x$ сохраняет операцию группы $\langle Z, + \rangle$:

$(\forall x, y \in Z)\ f(x + y) = 2(x + y) = 2x + 2y = f(x) + f(y)$.

2. $\langle R^+, \cdot \rangle \cong \langle R, + \rangle$, т.к. , *биекция (доказать!!!)*

$f: R^+ \to R \quad (\forall x \in R^+)\ f(x) = \lg x$ сохраняет операцию группы $\langle R^+, \cdot \rangle$:

$(\forall x, y \in R^+)\ f(x \cdot y) = \lg(x \cdot y) = \lg x + \lg y = f(x) + f(y)$.

ПРОСТЕЙШИЕ СВОЙСТВА ГОМОМОРФИЗМОВ ГРУПП

1.Гомоморфизм групп переводит нейтральный элемент в нейтральный: $f(e_G) = e_S$

2.При гомоморфизме групп обратный элемент переходит в обратный: $f(x^{-1}) = [f(x)]^{-1}$.

3.Гомоморфный образ группы есть группа.

ЗАМЕЧАНИЕ

Изоморфные алгебраические структуры с точки зрения алгебры одинаковы, а гомоморфные лишь похожи.

Темы рефератов:

Различные виды гомоморфизмов групп:

эпиморфизмы, автоморфизмы и их свойства.

Литература

1. Л.Я. Куликов. Алгебра и теория чисел.

М., Высшая школа, 1979. Стр.94 - 100.

2. Л.В. Лободина. Элементы абстрактной и компьютерной алгебры. Борисоглебск, 2006. Стр.29 – 31, 35 - 37.

Л Е К Ц И Я 7

1. **Гомоморфизмы и изоморфизмы колец и полей.**

2. **Подкольца и подполя.**

3. **Кольцо многочленов от одной переменной.**

4. **Кольцо классов вычетов по mod m.**

Гомоморфизмом кольца **<К, +, ·>** в кольцо **<S, ⊕, °>** называется отображение f: К → S, такое что

1) $(\forall x, y \in К)\ f(x + y) = f(x) \oplus f(y)$;
2) $(f(x \cdot y) = f(x) \circ f(y)$;
3) $(\forall x \in К)\ f(-x) = - f(x)$;
4) $f(1_К) = 1_S$.

Говорят, что f ***сохраняет главные операции*** кольца.

Гомоморфизм колец называется ***изоморфизмом***, если f – биективное отображение.

Обозначение: К ~ S – гомоморфные кольца,

G ≅ S – изоморфные кольца.

Аналогичные определения можно дать для полей.

Теорема

Если отображение **f: <K, +, ·> → <S, ⊕, ° >** переводит 1_K кольца К в 1_S кольца S и сохраняет обе операции кольца К, то f переводит 0_K кольца К в 0_S кольца S и является гомоморфизмом колец.

Доказательство.

Рассмотрим аддитивные группы колец при отображении f:

f: <K, +, -, 0_K > → <S, ⊕, -, 0_S >

По условию f сохраняет операцию «+», => по теореме о гомоморфизмах групп f: $0_K \to 0_S$ и $(\forall x \in K)\,(f(-x) = -f(x))$,

=> f есть гомоморфизм колец.

ПРИМЕР

1. Отображение f кольца матриц вида $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \quad a,b \in Q$

на кольцо Q рациональных чисел, где есть гомоморфизм колец. $f\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) = a$

2. Отображение f кольца матриц вида $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}, \quad a \in Q$

на кольцо Q рациональных чисел, где есть изоморфизм колец. $f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) = a$

Определение

Пусть **f: <K, +, ·> → <S, ⊕, ° >** - гомоморфизм колец. Множество всех элементов кольца К, которые отображаются в 0_S кольца S, называется ***ядром*** гомоморфизма f и обозначается $\mathrm{Ker}\, f = \{x \in K \mid f(x) = 0_S\}$.

Можно доказать, что ядро гомоморфизма образует подгруппу аддитивной группы кольца К.

Определение

Подмножество S кольца **<K, +, ·>** называется ***подкольцом*** кольца К, если оно само образует кольцо относительно операций, заданных на К.

Теорема (критерий подкольца)

Подмножество S кольца **<K, +, ·>** является *подкольцом* $\Leftrightarrow$ когда:

(1) $(\forall\ a, b \in S)\quad (a - b) \in S$;

(2) $(\forall\ a, b \in S)\quad a \cdot b \in S$.

Доказательство.

1. Пусть S – подкольцо кольца **<K, +, ·>**, => по определению S само является кольцом по операциям «+» и «·» и условия (1), (2) следуют из аксиом кольца.

2. Пусть $S \subset K$ и (1), (2) выполняются.

Из (1) (*по критерию подгруппы*) => S - подгруппа аддитивной группы К, => <S, +> - аддитивная группа (*по определению подгруппы*).

Из (2) => <S, · > - группоид. Т.к. законы дистрибутивности «·» относительно «+» выполняются на всем множестве К, то они выполняются и на его подмножестве S. Т.о. для S выполнены все аксиомы кольца, => S – подкольцо кольца К (*по определению подкольца*).

Пример 1. Кольцо многочленов от одной переменной

Пусть К – кольцо без делителей 0 или поле.
Многочленом от одной переменной над кольцом (полем) К называется формальная сумма вида:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i, \quad a_i \in K,$$

Число n $\in$N называется ***степенью*** многочлена f(x), a_n – ***старшим коэффициентом***.

На множестве всех многочленов от одной переменной над К заданы обычные операции «+» и «·» многочленов.

Это множество образует относительно заданных операций *кольцо многочленов от одной переменной над кольцом (полем) К.*

Обозначение: **K [x].**

Нулем кольца K [x] является ***нулевой многочлен*** $\mathcal{O}(x)$:

$$\mathcal{O}(x) = 0\cdot x^n + 0\cdot x^{n-1} + \ldots + 0\cdot x + 0.$$

Степень многочлена $\mathcal{O}(x)$ *не определена*; в качестве степени $\mathcal{O}(x)$ можно брать любое натуральное n.

Противоположным для многочлена $f(x) = \sum_{i=0}^{n} a_i x^i, \quad a_i \in K$

является многочлен $-f(x) = \sum_{i=0}^{n} (-a_i) x^i, \quad a_i \in K.$

Сами элементы кольца (поля) K можно рассматривать как многочлены ***нулевой степени*** над K, поскольку они не содержат переменной x.

Так как в K нет делителей 0, то в кольце K [x] также нет делителей 0. Только поэтому степень произведения многочленов равна сумме степеней сомножителей.

Пример 2. Кольцо классов вычетов по mod m

Пусть Z – кольцо целых чисел, $m > 1$ – фиксированное целое число.

Зададим на Z отношение «≡»: $b \equiv a \pmod m$ ⇔

⇔ b и a при делении на m дают одинаковые остатки

Говорят, что *a сравнимо с b по модулю m.*

«≡» - отношение эквивалентности на Z.

Классы разбиения по отношению «≡» :

$K_r = \{r+m\cdot q \mid q \text{ - целое}\} = \{\ldots,-3m+r, -2m+r, -m+r, r, m+r, 2m+r, 3m+r,\ldots\}$.

Классы обозначают $K_r = \overline{r}$ и называют ***классами вычетов*** или просто ***вычетами по mod m.***

Каждый класс K_r содержит бесконечно много целых чисел, самих классов существует ровно *m:*

$$Z_m = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$

Зададим на Z_m операции «+» и «·»:

$$\bar{r} + \bar{r_1} = \overline{r + r_1}, \quad \bar{r} \cdot \bar{r_1} = \overline{r \cdot r_1}.$$

Множество Z_m по операциям «+» и «·» образует кольцо, которое называют кольцом ***классов вычетов по mod m***.

Если число m простое, то Z_m образует поле.

ПРИМЕРЫ

1. m =6, тогда $Z_6 = \{\bar{0}, \bar{1}, \ldots, \bar{5}\}$; $\bar{2} + \bar{5} = \overline{2+5} = \bar{7} = \bar{1}$, *т.к.* $7 \equiv 1 (\mathrm{mod}\ 6)$,

$\bar{2} \cdot \bar{5} = \overline{2 \cdot 5} = \overline{10} = \bar{4}$, *т.к.* $10 \equiv 4 (\mathrm{mod}\ 6)$.

В кольце Z_6 есть делители нуля:

$\bar{6} = \overline{2 \cdot 3} = \bar{2} \cdot \bar{3}$. $\bar{2} \neq \bar{0}$, $\bar{3} \neq \bar{0}$, *но* $\bar{6} = \bar{0}$, $\Rightarrow$ $\bar{2} \cdot \bar{3} = \bar{0}$, $\Rightarrow$ $\bar{2}$ *и* $\bar{3}$

- делители нуля.

2. m =5, тогда делителей 0 в кольце Z_5 нет и оно является полем. Действительно, т.к. 5 – простое, то оно раскладывается на множители единственным способом: 5 = 5·1, потому:

$\bar{5} = \overline{5 \cdot 1} = \bar{5} \cdot \bar{1}$, *но* $\bar{5} = \bar{0}$, *т.к.* $5 \equiv 0 (\mathrm{mod}\ 5)$.

Темы рефератов:

1. Понятие характеристики поля.

2. Упорядоченные кольца и поля.

Литература

1. Л.Я. Куликов. Алгебра и теория чисел. М., Высшая школа, 1979. Стр. 107-112.

2. Л.В. Лободина. Элементы абстрактной и компьютерной алгебры. Борисоглебск, 2006. Стр. 37 – 39.

3. Ф.Л. Варпаховский, А.С. Солодовников и др. Алгебра. Группы, кольца, поля. Векторные и евклидовы пространства. Линейные отображения. М., «Просвещение», 1978. Стр. 50 – 60.

Л Е К Ц И Я 8

1. Поле комплексных чисел.
2. Алгебраическая форма комплексного числа.
3. Тригонометрическая и показательная формы комплексного числа.
4. Корни n-й степени из комплексных чисел.

Пусть $\mathbf{C} = R \times R = \{ \langle a, b \rangle \mid a, b \in R \}$

ОПРЕДЕЛЕНИЕ

1. Множество **C** назовем ***множеством комплексных чисел***, а его элементы – ***комплексными числами***.

2. Два комплексных числа $\langle a, b \rangle$ и $\langle c, d \rangle$ называются ***равными***, если равны соответствующие элементы этих пар: $a = c$, $b = d$.

Таким образом, комплексное число есть ***упорядоченная пара действительных чисел***.

На **C** зададим операции «+» и «·»:

$$\langle a, b \rangle + \langle c, d \rangle = \langle a + b, c + d \rangle \qquad (1),$$

$$\langle a, b \rangle \cdot \langle c, d \rangle = \langle a \cdot c - b \cdot d,\ a \cdot d + b \cdot c \rangle \qquad (2).$$

Операции «+» и «·» на **C** обладают свойствами:

– коммутативность и ассоциативность;

– «·» дистрибутивно относительно «+»;

– нейтральный элемент по «+» - пара **<0, 0>**; по умножению – пара **<1, 0>**;

– для числа **<a, b>** противоположным элементом является число **<-a, -b>**.

Проверим существование для $\langle a, b\rangle \neq 0$ обратного элемента по «·»:

$$\langle a, b\rangle \neq 0 \Leftrightarrow \langle a, b\rangle \neq \langle 0, 0\rangle \Leftrightarrow a^2 + b^2 \neq 0,$$

Из определения обратного $\langle a, b\rangle \cdot \langle a, b\rangle^{-1} = \langle 1, 0\rangle$

Т.к. $\langle a, b\rangle^{-1} \in \mathbf{C}$, то $(\exists\, x, y \in R)$ $\langle a, b\rangle^{-1} = \langle x, y\rangle$, =>

чтобы найти обратный к <a, b>, нужно решить уравнение

$$\langle a, b\rangle \cdot \langle x, y\rangle = \langle 1, 0\rangle \quad \Leftrightarrow$$

$$\begin{cases} a \cdot x - b \cdot y = 1, \\ a \cdot y + b \cdot x = 0 \end{cases} \Leftrightarrow \begin{cases} x = \dfrac{a}{a^2 + b^2}, \\ y = -\dfrac{b}{a^2 + b^2}. \end{cases}$$

Т.о, для $\langle a, b\rangle \neq 0$ обратный элемент имеет вид:

$$\langle a, b\rangle^{-1} = \left\langle \frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right\rangle.$$

ТЕОРЕМА

Множество комплексных чисел **C** относительно заданных операций «+» и «·» образует ***поле***, которое называется ***полем комплексных чисел***.

ЛЕММА

Подмножество $\mathbf{C_R \subset C}$, $\mathbf{C_R} = \{\langle a, 0\rangle \mid a \in R\}$ изоморфно полю действительных чисел.

Доказательство.

Рассмотрим отображение f: $\mathbf{R \to C_R}$, $\mathbf{f(a) = \langle a, b\rangle}$.

Очевидно, f – биекция. $(\forall\ a, b \in R)$

(1) $f(a+b) = \langle a+b, 0\rangle = \langle a, 0\rangle + \langle b, 0\rangle = f(a) + f(b)$;

(2) $f(a \cdot b) = \langle a \cdot b, 0\rangle = \langle a, 0\rangle \cdot \langle b, 0\rangle = f(a) \cdot f(b)$, =>

f сохраняет основные операции поля R ,

=> f – изоморфизм, => $\mathbf{\langle C_R, +, \cdot\rangle}$ - поле (*как изоморфный образ поля*), => $\mathbf{C_R}$ - ***подполе*** поля **C.**

Действительным комплексным числом называют пару <a, 0>, которую отождествляют с числом a:

$$\langle a, 0\rangle \equiv a.$$

В частности, $\langle 0, 0\rangle \equiv 0$; $\langle 1, 0\rangle \equiv 1$; $\langle -1, 0\rangle \equiv -1$.

ТЕОРЕМА

В поле комплексных чисел разрешимо уравнение

$$z^2 = -1 \quad (*).$$

Доказательство.

Пусть $z = \langle 0, 1\rangle$, $\Rightarrow \langle 0, 1\rangle \cdot \langle 0, 1\rangle = \langle 0\cdot 0 - 1\cdot 1, 0\cdot 1 + 1\cdot 0\rangle = \langle -1, 0\rangle \equiv -1$.

Пару <0, 1>, которая является решением уравнения (*) называют ***мнимой единицей*** и обозначают ***i:*** $\Rightarrow$

$$\langle 0, 1\rangle \equiv i, \quad i^2 = -1.$$

ТЕОРЕМА

Любое комплексное число представимо в виде

$$z = a + b \cdot i \quad (**)$$

Доказательство.

Пусть $z = \langle a, b\rangle$, $a, b \in R$. Тогда:

$z = \langle a, b\rangle = \langle a, 0\rangle + \langle 0, b\rangle = \langle a, 0\rangle + \langle b, 0\rangle \cdot \langle 0, 1\rangle$.

Т.к. $\langle a, 0\rangle \equiv a$, $\langle b, 0\rangle \equiv b$, $\langle 0, 1\rangle \equiv i$, то $z = a + b \cdot i$

Представление (**) называют ***алгебраической формой*** комплексного числа.

$a = \mathrm{Re}\, z$ - действительная часть комплексного числа z,

$b = \mathrm{Im}\, z$ – мнимая часть комплексного числа z.

Операции над комплексными числами в алгебраической форме :

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

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

$$\frac{a + bi}{c + di} = \frac{(a + bi) \cdot (c - di)}{c^2 + d^2}, \quad c^2 + d^2 \neq 0.$$

ПРИМЕР

Выполнить операции над комплексными числами:

$$(15+23i)-(20-12i)\cdot(6+6i).$$

$$1)\ (20-12i)\cdot(6+6i)=(120-72i^2)+(120-72)i=$$

$$=120+72+48i=192+48i;$$

$$2)\ 15+23i-(192+48i)=(15-192)+(23-48)i=-177-25i.$$

ТЕОРЕМА

В поле **C** комплексных чисел нельзя задать отношение порядка « $>$» так, чтобы оно обладало одновременно свойствами:

а) линейности:

$(\forall\, z, u \in \mathbf{C})\quad z = u \text{ или } z > u \text{ или } u > z;$

б) монотонности относительно «+»:

$(\forall\, z, u, v \in \mathbf{C})\quad u > v \Rightarrow (u + z) > (v + z)$

в) монотонности относительно «·»:

$(\forall\, z, u, v \in \mathbf{C})\quad u > v \Rightarrow (u \cdot z) > (v \cdot z) \text{ при } z > 0$

$u > v \Rightarrow (u \cdot z) < (v \cdot z) \text{ при } z < 0.$

Доказательство.

Допустим, на **C** можно задать отношение « > » со свойствами а)-в). Тогда $1 > 0$. Если бы $1 < 0$, то $-1 > 0$ и $(-1)\cdot(-1) = 1 > 0$ – противоречие условию $1 < 0$.

По а) для числа $i \neq 0$ должно выполняться либо $i > 0$ либо $0 > i$. Пусть $i > 0$, тогда по в):

$$i \cdot i > 0 \cdot i \quad \Leftrightarrow \quad i^2 > 0 \Leftrightarrow \quad -1 > 0$$ –противоречие.

Пусть $i < 0$, тогда по в):

$$i \cdot i > 0 \cdot i \quad \Leftrightarrow \quad i^2 > 0 \Leftrightarrow \quad -1 > 0$$ –противоречие.

Т.о. для числа i оказывается невозможным ни одно из условий: $i = 0$, $i > 0$, $0 > i$, что доказывает невозможность нашего допущения.

ЗАМЕЧАНИЕ

Из теоремы => что числа z, v $\in$C (если z, v $\notin$R) ***не сравнимы между собой***, т. е. нельзя сказать, что одно из них больше или меньше другого.

Для комплексного числа $z = a + b \cdot i$, $b \neq 0$, нельзя также утверждать, положительно оно или отрицательно, т.к. оно ***не сравнимо*** с нулем.

ОПРЕДЕЛЕНИЕ

Для комплексного числа $z = a + b \cdot i$

число $\overline{z} = a - b \cdot i$ называется ***комплексно сопряженным числом.***

Свойства комплексно сопряженных чисел

1. Сумма и произведение сопряженных чисел – действительные числа:

$$z + \bar{z} = (a + bi) + (a - bi) = 2a \in R;$$
$$z \cdot \bar{z} = (a + bi) \cdot (a - bi) = a^2 - (bi)^2 = a^2 + b^2 \in R.$$

2. Число z $\in$ **C** сопряжено само с собой $\Leftrightarrow$ z $\in$ R:

$$a)\ z \in R \quad \Rightarrow \quad z = a + 0i \quad \Rightarrow \quad \bar{z} = a - 0i \quad \Rightarrow \quad z = \bar{z};$$
$$b)\ z = \bar{z} \quad \Rightarrow \quad a + bi = a - bi \quad \Rightarrow \quad b = -b,\ b \in R \quad \Leftrightarrow$$
$$b = 0 \quad \Leftrightarrow \quad z = a \in R.$$

3. $\overline{\overline{z}} = z$, *так как*:

$$z = a + bi \quad \Rightarrow \quad \overline{z} = a - bi \quad \Rightarrow \quad \overline{\overline{z}} = a - (-b)i = a + bi = z.$$

4. $\overline{z} + \overline{z_1} = \overline{z + z_1}; \qquad \overline{z} \cdot \overline{z_1} = \overline{z \cdot z_1};$

$$\overline{\left(\frac{z}{z_1}\right)} = \frac{\overline{z}}{\overline{z_1}}; \qquad \overline{(z^n)} = (\overline{z})^n.$$

$$z = a + bi, \qquad z_1 = c + di, \qquad \Rightarrow$$

$$z \cdot z_1 = (a + bi) \cdot (c + di) =$$

$$= (ac - bd) + (ad + bc)i;$$

$$\overline{z} \cdot \overline{z_1} = (a - bi) \cdot (c - di) =$$

$$= (ac - bd) - (ad + bc)i = \overline{z \cdot z_1}.$$

Тригонометрическая и показательная формы

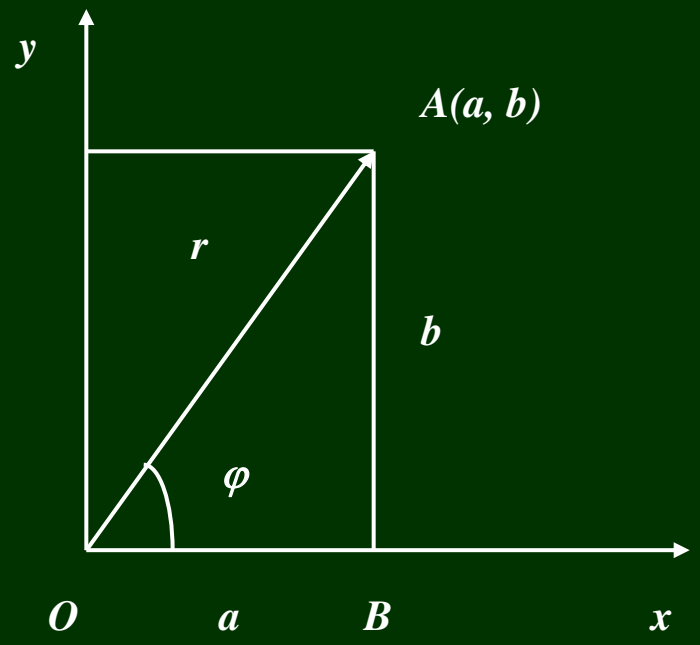


Рис. 1

Число $z = a + b\,i$ изображено на плоскости точкой А (a, b) . Ось ОХ – действительная ось, ось ОУ – мнимая ось.

Рассмотрим полярную систему координат (r, φ), где r – *радиус-вектор* точки А, φ - угол между радиус-вектором и положительным направлением оси ОХ.

Связь между декартовыми и полярными координатами точки А получим из Δ АОВ:

$$OA^2 = OB^2 + AB^2, \quad \Rightarrow \quad r^2 = a^2 + b^2, \quad \Rightarrow r = \sqrt{a^2 + b^2},$$

$$\cos\varphi = \frac{a}{r}, \quad \sin\varphi = \frac{b}{r}, \quad \Rightarrow \quad a = r\cos\varphi, \quad b = r\sin\varphi, \quad \Rightarrow$$

$$z = a + bi = r(\cos\varphi + i\sin\varphi) \quad (1).$$

ОПРЕДЕЛЕНИЕ

Равенство (1) называется ***тригонометрической формой*** комплексного числа.

Число $r \in R$ называется ***модулем*** комплексного числа z, а число $\varphi \in R$ - ***аргументом*** числа z:

$$r = |z|, \quad \varphi = \mathrm{Arg}\, z.$$

ЗАМЕЧАНИЯ

1. Для числа $z = 0$ модуль равен 0, а аргумент однозначно не определен. В качестве аргумента 0 может выступать любое $\alpha \in R$.

2. Аргумент числа z определен однозначно с точностью $2\pi k$, $k \in Z$:

если $\varphi = \operatorname{Arg} z$, то $\psi = \varphi + 2\pi k = \operatorname{Arg} z$.

3. Сопряженные числа имеют равные модули, аргументы их отличаются только знаком. Геометрически они представляют собой точки плоскости, симметричные относительно оси OX.

ТЕОРЕМА

Всякое комплексное число $z \neq 0$ можно представить в форме (1) единственным образом (*с учетом замечания*)

Пусть $z = r(\cos\varphi + i\sin\varphi), \quad z_1 = \rho(\cos\psi + i\sin\psi).$

1. При умножении чисел в тригонометрической форме их модули перемножаются, а аргументы складываются:

$$z \cdot z_1 = r \cdot \rho(\cos(\varphi + \psi) + i\sin(\varphi + \psi)).$$

2. При делении чисел в тригонометрической форме, $z_1 \neq 0,$ их модули делятся, а аргументы вычитаются:

$$\frac{z}{z_1} = \frac{r}{\rho}(\cos(\varphi - \psi) + i\sin(\varphi - \psi)).$$

Доказательство.

$$z \cdot z_1 = r(\cos\varphi + i\sin\varphi) \cdot \rho(\cos\psi + i\sin\psi) =$$

$$= r \cdot \rho(\cos\varphi \cdot \cos\psi + i^2 \cdot \sin\varphi \cdot \sin\psi + i\cos\varphi \cdot \sin\psi + i\sin\varphi \cdot \cos\psi) =$$

$$= r \cdot \rho((\cos\varphi \cdot \cos\psi - \sin\varphi \cdot \sin\psi) + i(\cos\varphi \cdot \sin\psi + \sin\varphi \cdot \cos\psi)) =$$

$$= r \cdot \rho(\cos(\varphi + \psi) + i\sin(\varphi + \psi))$$

ОПРЕДЕЛЕНИЕ

Натуральная степень числа $z \neq 0$ определяется рекуррентно:

1) $z^0 = 1$;

2) $z^{k+1} = z^k \cdot z$ для всех $k < n$.

3. При возведении числа $z \neq 0$ в степень с натуральным показателем, модуль возводится в эту степень, а аргумент умножается на показатель степени:

$$z = r(\cos\varphi + i\sin\varphi), \quad \Rightarrow \quad z^n = r^n \cdot (\cos(n\varphi) + i\sin(n\varphi)) \quad (*)$$

Формула (*) получила название ***формулы Муавра***.

Доказательство (методом индукции по n).

1. База индукции. n = 0, => $z^0 = 1$ (по определению),

$$r^0 \cdot (\cos(0 \cdot \varphi) + i \sin(0 \cdot \varphi)) = 1$$

2. Предположение индукции. Пусть при n=k формула Муавра выполняется.

3. Шаг индукции. Пусть n=k+1, =>

$$z^n = z^{k+1} = z^k \cdot z^1 = r^k \cdot (\cos(k\varphi) + i \sin(k\varphi)) \cdot r \cdot (\cos\varphi + i \sin\varphi) =$$

$$= r^{k+1} \cdot (\cos(k\varphi + \varphi) + i \sin(k\varphi + \varphi)) =$$

$$= r^{k+1} \cdot (\cos(k+1)\varphi + i \sin(k+1)\varphi).$$

Показательная форма комплексного числа

По формуле Эйлера: $\cos\varphi + i\sin\varphi = e^{i\varphi}$,

тогда для комплексного числа в тригонометрической форме получим: $z = r(\cos\varphi + i\sin\varphi) = r\cdot e^{i\varphi}$.

Равенство $z = r\cdot e^{i\varphi}$ выражает показательную форму комплексного числа.

ПРИМЕР. Вычислить:

$$\frac{(1-i)^{12}}{\left(1+i\sqrt{3}\right)^{6}}.$$

Решение.

1) $z = 1 - i, \quad \Rightarrow \quad a = \operatorname{Re} z = 1, \quad b = \operatorname{Im} z = -1, \quad \Rightarrow$

$$r = |z| = \sqrt{a^2 + b^2} = \sqrt{2}, \quad \cos\varphi = \frac{a}{r} = \frac{1}{\sqrt{2}}, \quad \sin\varphi = \frac{b}{r} = \frac{-1}{\sqrt{2}}, \quad \Rightarrow$$

$$Argz = \varphi = \frac{7\pi}{4}, \quad \Rightarrow \quad z = 1 - i = \sqrt{2}\left(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}\right), \quad \Rightarrow$$

$$z^{12} = (1-i)^{12} = \left(\sqrt{2}\right)^{12} \cdot \left(\cos\frac{12\cdot 7\pi}{4} + i\sin\frac{12\cdot 7\pi}{4}\right) = 2^6 \cdot \left(\cos 21\pi + i\sin 21\pi\right) =$$

$$= 2^6 \cdot \left(\cos\pi + i\sin\pi\right) = -2^6.$$

$$(1-i)^{12} = -2^6.$$

2) $z = 1 + i\sqrt{3}, \quad \Rightarrow \quad a = \operatorname{Re} z = 1, \quad b = \operatorname{Im} z = \sqrt{3}, \quad \Rightarrow$

$$r = \sqrt{4} = 2, \quad \cos\varphi = \frac{1}{2}, \quad \sin\varphi = \frac{\sqrt{3}}{2}, \quad \Rightarrow \quad Argz = \varphi = \frac{\pi}{3}, \quad \Rightarrow$$

$$z = 1 + i\sqrt{3} = 2\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right), \quad \Rightarrow \quad \left(1 + i\sqrt{3}\right)^6 = 2^6 \cdot \left(\cos\frac{6\pi}{3} + i\sin\frac{6\pi}{3}\right) =$$

$$= 2^6 \cdot \left(\cos 2\pi + i\sin 2\pi\right) = 2^6.$$

$$\left(1 + i\sqrt{3}\right)^6 = 2^6.$$

3) $$\frac{(1-i)^{12}}{\left(1 + i\sqrt{3}\right)^6} = \frac{-2^6}{2^6} = -1.$$

$$z = 1 + i\sqrt{3} = 2\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right) = 2 \cdot e^{i\frac{\pi}{3}}$$

Корни n-й степени из комплексного числа

ОПРЕДЕЛЕНИЕ

Корнем n-й степени из комплексного числа z называется комплексное число u такое, что $u^n = z$.

ТЕОРЕМА

Корень n-й степени из комплексного числа

$z = r\cdot(\cos\varphi + i\cdot\sin\varphi)$ имеет ровно n различных значений, которые находятся по формуле:

$$u_k = \sqrt[n]{r}\cdot\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right), \quad k = 0,1,\ldots,n-1 \quad (**).$$

Доказательство.

1. Пусть z=r·(cosφ+*i*·sinφ). Для z = 0 – очевидно.

2. Каждое из чисел вида (**) есть корень n-й степени из z – очевидно.

3. Пусть u = ρ(cosΨ + *i*·sin Ψ) - корень n-й степени из z. По определению $u^n = z$, => по формуле Муавра:

$$\rho^n \cdot (\cos(n\psi) + i\sin(n\psi)) = r(\cos\varphi + i\sin\varphi),$$

$$\Rightarrow \quad \textit{из} \quad \textit{единственности} \quad \textit{тригонометрической}$$

$$\textit{формы} \quad \textit{числа}: \quad \rho^n = r, \quad n\psi = \varphi + 2\pi k, \quad \Rightarrow$$

$$\rho = \sqrt[n]{r}, \quad \psi = \frac{\varphi + 2\pi k}{n},$$

Получили: $u = \sqrt[n]{r} \cdot \left(\cos \frac{\varphi + 2\pi k}{n} + i \sin \frac{\varphi + 2\pi k}{n} \right).$

Если $k < 0$ *или* $k > n-1$, *то* $(\exists q \in Z)\,(k = qn + k_1)$,

где $0 \le k_1 \le n-1$. *Тогда*

$$\frac{\varphi + 2\pi k}{n} = \frac{\varphi + 2\pi(qn + k_1)}{n} = \frac{\varphi + 2\pi k_1}{n} + 2\pi q, \quad \Rightarrow$$

$$\cos \frac{\varphi + 2\pi k}{n} = \cos\left(\frac{\varphi + 2\pi k_1}{n} + 2\pi q \right) = \cos \frac{\varphi + 2\pi k_1}{n};$$

$$\sin \frac{\varphi + 2\pi k}{n} = \sin\left(\frac{\varphi + 2\pi k_1}{n} + 2\pi q \right) = \sin \frac{\varphi + 2\pi k_1}{n}, \quad \Rightarrow$$

различных значений u_k *будет ровно* k, $k = 0,1,\ldots,n-1$.

Замечание

Геометрически все корни n-й степени из комплексного числа u = r·(cosφ + *i*·sinφ) расположены в вершинах правильного n-угольника, вписанного в окружность с центром в точке O(0, 0) и радиусом r = |z|.

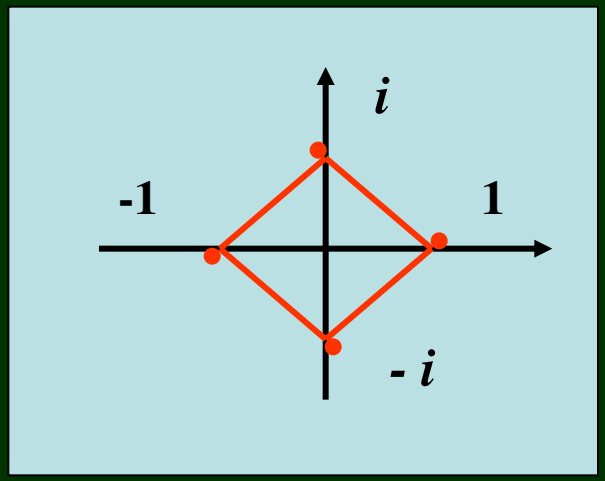
Особое значение имеют корни n-й степени из 1. Так как |1| = 1, Arg 1 = 0, т.е. 1 = cos0 +*i*sin0, то все значения корня n-й степени из 1 вычисляются по формуле:

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k \in \{0, 1, \ldots, n-1\}.$$

Замечание

1. Геометрически все корни n-й степени из 1 расположены в вершинах правильного n-угольника, вписанного в единичную окружность с центром в точке O(0, 0).

2. Значение $\varepsilon_0 = 1$ расположено на оси OX в точке (1, 0). Каждое следующее значение можно получить из предыдущего поворотом на угол $\frac{2\pi k}{n}$



Значения $\sqrt[4]{1}$:

$$\varepsilon_0 = 1, \quad \varepsilon_1 = i,$$

$$\varepsilon_2 = -1, \quad \varepsilon_3 = -i$$

ОПРЕДЕЛЕНИЕ

Комплексное число ***w*** называется ***первообразным корнем n-й степени из 1***, если множество чисел $\{w^0, w^1, \ldots, w^{n-1}\}$ является множеством всех решений уравнения $z^n = 1$.

ТЕОРЕМА

Пусть u_k – одно из значений корня n-й степени из числа u, *w* - первообразный корень n-й степени из 1. Тогда все значения корня n-й степени из числа u можно получить, умножив u_k на степени *w*: $u_k \cdot w^0, u_k \cdot w^1, u_k \cdot w^2, \ldots, u_k \cdot w^{n-1}$.

Темы рефератов:

1. Мультипликативная группа корней n-й степени из 1 .
2. Показательная форма комплексных чисел.

Литература

1. Л.Я. Куликов. Алгебра и теория чисел. М., Высшая школа, 1979. Стр. 157-172.

2. Л.В. Лободина. Элементы абстрактной и компьютерной алгебры. Борисоглебск, 2006. Стр. 89 – 100.

3. Ф.Л. Варпаховский, А.С. Солодовников и др. Алгебра. Группы, кольца, поля. Векторные и евклидовы пространства. Линейные отображения. М., «Просвещение», 1978. Стр. 65 – 71.