ISBN 978-985-477-678-1

СПРАВОЧНЫЕ МАТЕРИАЛЫ К ГОСУДАРСТВЕННОМУ ЭКЗАМЕНУ ПО СПЕЦИАЛЬНОСТИ 1-02 05 01 "МАТЕМАТИКА И ИНФОРМАТИКА" ПО ДИСЦИПЛИНЕ "АЛГЕБРА"

Министерство образования Республики Беларусь
Учреждение образования
«Мозырский государственный педагогический университет
имени И. П. Шамякина»

СПРАВОЧНЫЕ МАТЕРИАЛЫ К ГОСУДАРСТВЕННОМУ ЭКЗАМЕНУ ПО СПЕЦИАЛЬНОСТИ 1-02 05 01 «МАТЕМАТИКА И ИНФОРМАТИКА» ПО ДИСЦИПЛИНЕ «АЛГЕБРА»

Мозырь
МГПУ им. И. П. Шамякина
2019

УДК 512 (079)
ББК 22.14я73
С74

Составитель
М. И. Ефремова, кандидат физико-математических наук, доцент,
доцент кафедры физики и математики УО «Мозырский государственный педагогический университет им. И. П. Шамякина»

Рецензенты:
кандидат педагогических наук, доцент
В. В. Пакштайте;
кандидат физико-математических наук, доцент
А. Э. Шмигирев

С74 **Справочные** материалы к Государственному экзамену по специальности 1-02 05 01 «Математика и информатика» по дисциплине «Алгебра» / сост. М. И. Ефремова. – Мозырь : МГПУ им. И. П. Шамякина, 2019. – 76 с.
ISBN 978-985-477-678-1.

Справочный материал предназначены для самостоятельной работы студентов при подготовке к Государственному экзамену по специальности 1-02 05 01 «Математика и информатика» по дисциплине «Алгебра». Издание включает в себя определения, теоремы без доказательства, примеры по отдельным вопросам программы Государственного экзамена.

УДК 512 (079)
ББК 22.14я73

ISBN 978-985-477-678-1

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Государственный экзамен по специальности проводится для выявления и оценки уровня подготовки выпускников физико-инженерного факультета специальности 1-02 05 01 «Математика и информатика» к выполнению функций преподавателя математики.

Справочные материалы направлены на углубление и систематизацию знаний и умений, приобретенных в результате изучения дисциплины «Алгебра».

С точки зрения профессиональной направленности курс алгебры занимает важное место в подготовке будущих учителей математики. Актуальность изучения алгебры определяется той ролью, которую играет математика в жизни современного общества, ее влиянием на темпы развития научно-технического прогресса, а для студентов – будущих учителей математики – профессиональной направленностью курса. Помимо активно идущего процесса «алгебраизации» самой математики усиливается роль алгебры в описании общей картины физического мира.

Учебно-воспитательный процесс при изучении алгебры должен быть организован таким образом, чтобы он давал возможность будущему преподавателю приобрести основные профессиональные качества:

- сформировать установку на творческую профессиональную деятельность;
- развить профессиональное мышление, которое обеспечило бы будущему специалисту возможность свободно оперировать профессиональными знаниями;
- видеть проблемы и пути их решения в самостоятельной практической деятельности, выбирать оптимальные пути решения и методы их осуществления;
- воспитывать в себе активную профессиональную позицию, умение вырабатывать и обосновывать свой подход в решении задач, обеспечивающих результативность учебно-воспитательной деятельности.

Реализации этих целей и служат справочные материалы, предназначенные для самостоятельной работы студентов специальности 1-02 05 01 «Математика и информатика». Они включают в себя определения, теоремы без доказательства, примеры по отдельным вопросам программы Государственного экзамена. Данная разработка содержит не весь материал курса алгебры, а лишь основные вопросы, знание которых обеспечивает необходимый уровень научной подготовки выпускников.

При подготовке справочных материалов использовались как авторские разработки, так и следующие источники:

- Шмигирев, Э.Ф. Линейные операторы векторных пространств / Э.Ф. Шмигирев, В.А. Сорочик. – Мозырь: МозГПИ им. Н. К. Крупской, 1999. – 60 с.
- Шмигирев, Э.Ф. Теория многочленов / Э.Ф. Шмигирев, С.В. Игнатович. – Мозырь: МозГПИ им. Н.К. Крупской, 2002. – 81 с.
- Шмигирев, Э.Ф. Линейная алгебра. Краткий курс лекций / Э.Ф. Шмигирев, А.Э. Шмигирев. – Мозырь: УО МГПУ, 2004. – 97 с.

На Государственном экзамене по специальности выпускник должен продемонстрировать умение систематизировать информационные сведения программы экзамена, знание основных теорем и понятий, понимание взаимосвязей между ними, умение ими пользоваться. С учетом этих требований экзаменующийся по каждому вопросу билета должен сделать обзор материала, соответствующего формулировке вопросов, сопровождая ответ доказательством отдельных теорем.

Справочные материалы помогут выпускникам подготовиться к Государственному экзамену и успешно сдать его. Изложенные вопросы алгебры могут быть использованы студентами как для самостоятельной подготовки к Государственному экзамену, так и на лекционных и практических занятиях по алгебре. Для эффективной реализации самостоятельной работы студентов представлен список рекомендуемой литературы.

1. Алгебраические операции. Понятие группы. Примеры групп. Подгруппа. Примеры подгрупп

Понятие бинарной алгебраической операции. Мультипликативная и аддитивная формы записи операций. Свойства операций. Понятие группы. Простейшие свойства групп. Примеры групп. Подгруппа. Примеры подгрупп. Критерий подгруппы.

Определение 1. *Говорят, что на множестве A определена* ***бинарная алгебраическая операция****, если всякой упорядоченной паре элементов этого множества ставится в соответствие третий, причем единственный, элемент из этого же множества.*

Таким образом, согласно определению, бинарная алгебраическая операция на множестве A – это отображение множества $A \times A = A^2$ во множество A.

Если бинарная алгебраическая операция "$*$" ставит в соответствие упорядоченной паре $(a,\ b)$ элемент c, то обычно пишут $a * b = c$. При этом c называют композицией элементов a и b.

Определение 2. *Бинарная алгебраическая операция "$*$", определенная на множестве A, называется* ***коммутативной****, если*

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

Определение 3. *Бинарная алгебраическая операция "$*$", определенная на множестве A, называется* ***ассоциативной****, если*

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

Определение 4. *Элемент $e \in A$ называется* ***нейтральным элементом*** *относительно операции "$*$", если $\forall a \in A\ (a * e = e * a = a)$.*

Определение 5. *Элемент $b \in A$ называется* ***симметричным*** *к элементу $a \in A$ относительно операции "$*$", если $a * b = b * a = e$, где e – нейтральный элемент.*

Определение 6. *Говорят, что операция "$*$", определенная на множестве A,* ***обратима****, если $\forall a, b \in A, \exists x, y \in A\ (a * x = b \wedge y * a = b)$. Иначе говоря, операция "$*$" обратима на A, если для любых элементов a и b из A, в этом множестве разрешимы уравнения $a * x = b$ и $y * a = b$. Если операция "$*$" коммутативна на A, то решения этих уравнений совпадают.*

Пусть на множестве A определены две бинарные алгебраические операции "$*$" и "$\circ$".

Определение 7. *Говорят, что операция "$*$"* ***дистрибутивна*** *относительно операции "$\circ$", если выполняется условие*

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

Наиболее употребительны мультипликативная и аддитивная формы записи бинарных алгебраических операций. При мультипликативной форме операцию называют умножением и обозначают символом "$\circ$". Нейтральный элемент относительно операции умножения называют ***единичным***, элемент симметричный к элементу a называют ***обратным*** a. При аддитивной форме операцию называют сложением и обозначают символом "$+$". Нейтральный элемент относительно этой операции называют ***нулевым*** элементом, элемент симметричный к элементу a называют ***противоположным*** a.

Определение 8. Алгеброй *называется непустое множество A с определенными на нем алгебраическими операциями.*

Одними из основных видов алгебр являются группы, кольца, поля.

Определение 9. *Непустое множество G с определенной на нем бинарной алгебраической операцией "$*$" называется* ***группой****, если выполняются следующие условия (аксиомы групп):*

1) $\forall a, b, c \in G\ ((a * b) * c = a * (b * c))$, *т. е. операция "$*$" на множестве G ассоциативна;*

2) $\exists e \in G, \forall a \in G\ (e * a = a * e = a)$, *т. е. в G существует нейтральный элемент относительно операции "$*$";*

3) $\forall a \in G, \exists b \in G\ (a * b = b * a = e)$, *т. е. для каждого элемента из G в этом множестве существует симметричный к нему элемент.*

Определение 10. *Группа G называется* ***абелевой*** *или* ***коммутативной****, если определенная в ней операция коммутативна, т. е. если*

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

Определение 11. *Группа G, состоящая из конечного множества элементов, называется* ***конечной****, в противном случае G называется* ***бесконечной*** *группой.*

Определение 12. *Число элементов конечной группы G называется* ***порядком*** *этой группы и обозначается G.*

Пусть в группе G определена операция "$*$". Тогда справедливы следующие свойства:

1) в G существует единственный нейтральный элемент относительно операции "$*$";

2) для каждого элемента из G, в G существует единственный симметричный к нему элемент;

3) $\forall a, b, c \in G\ (a * b = a * c\ \rightarrow b = c \wedge b * a = c * a\ \rightarrow b = c)$ – закон сокращений;

4) $\forall a, b \in G, \exists x, y \in G\ (a * x = b \wedge y * a = b)$ – обратимость операции "$*$". Говорят также в этом случае, что в G выполнима операция обратная "$*$" (для сложения – вычитание, для умножения – деление).

Последнее свойство равносильно аксиомам 2 и 3 из определения 9. Это дает возможность иначе определить понятие группы.

Определение 13. *Непустое множество G с определенной на нем алгебраической операцией "$*$" называется группой, если выполняются следующие условия:*

1) $\forall a, b, c \in G\ ((a * b) * c = a * (b * c))$, *т. е. операция "$*$" на множестве G ассоциативна;*

2) $\forall a, b \in G, \exists x, y \in G\ (a * x = b \land y * a = b)$ – *обратимость операции "$*$".*

Примеры групп

1. R – группа действительных чисел с операцией сложения (аддитивная группа действительных чисел).
2. C **–** аддитивная группа комплексных чисел.
3. $R^{\#}$ – группа ненулевых действительных чисел с операцией умножения (мультипликативная группа действительных чисел).
4. $C^{\#}$ – мультипликативная группа комплексных чисел.
5. $GL(n, R)$ – группа невырожденных матриц порядка n с действительными элементами. (Аналогично $GL(n, C)$).
6. S_n – группа подстановок степени n (симметрическая группа n-ой степени).

Пусть G и G' – группы с определенными в них соответственно операциями "$*$" и "$\circ$".

Определение 14. *Взаимно однозначное отображение φ группы G на группу G' называется **изоморфизмом**, если* $\forall a, b \in G\ (\varphi\ a * b = \varphi\ a \circ \varphi\ b)$.

Определение 15. Подмножество H группы G называется подгруппой группы G, если H само образует группу относительно операции определенной в G.

Примеры подгрупп

1. Множество Z целых чисел с операцией сложения образуют подгруппу аддитивной группы R, которая в свою очередь является подгруппой группы C.

2. Множество A_n всех четных подстановок образуют подгруппу симметрической группы S_n всех подстановок n-ой степени.

3. Матрицы с определителем 1 образуют подгруппу $SL(n, R)$ в группе $GL(n, R)$ всех невырожденных матриц порядка n.

Чтобы проверить, будет ли данное подмножество H в G подгруппой, надо, очевидно, проверить следующие условия:

1) $\forall x \in H, \forall y \in H\ (x * y \in H)$;
2) $e_G \in H$;
3) $\forall x \in H\ (x^{-1} \in H)$.

Оказывается, что вместо трех этих условий достаточно проверить только одно.

Критерий подгруппы

Непустое подмножество H в группе G будет подгруппой этой группы тогда и только тогда, когда: $\forall x \in H, \forall y \in H\ (x * y^{-1} \in H)$.

2. Кольцо. Примеры колец. Подкольцо. Примеры подколец. Критерий подкольца

Понятие кольца. Свойства колец. Примеры колец. Подкольцо. Примеры подколец. Критерий подкольца.

Определение 1. *Непустое множество* K *с двумя определенными на нем операциями сложением и умножением называется* ***кольцом****, если выполняются следующие условия (аксиомы кольца):*

1) $\forall a, b, c \in K\ ((a + b) + c = a + (b + c))$ – *ассоциативность сложения;*

2) $\forall a, b \in K\ (a + b = b + a)$ – *коммутативность сложения;*

3) $\exists 0 \in K, \forall a \in K\ (a + 0 = a)$ – *существование нулевого элемента;*

4) $\forall a \in K, \exists b \in K\ (a + b = 0)$ – *существование для каждого элемента ему противоположного* $(b = -a)$*;*

5) $\forall a, b, c \in K\ ((ab)c = a(bc))$ – *ассоциативность умножения;*

6) $\forall a, b, c \in K\ (a(b + c) = ab + ac \wedge (b + c)a = ba + ca$ – *дистрибутивность умножения относительно сложения.*

Если операция умножения, определенная в кольце K*, коммутативна, то это кольцо называется* ***коммутативным.***

Если кольцо K *содержит единичный элемент, то* K *называют* ***кольцом с единицей.***

Согласно аксиомам 1–4 K образует абелеву группу относительно операции сложения, ее называют ***аддитивной группой кольца*** K.

Примеры колец

При обычных операциях сложения и умножения кольцами являются множества:

– целых чисел Z;

– рациональных чисел Q;

– действительных чисел R;

– комплексных чисел C;

– $\{0\}$, состоящее из одного числа 0 (нулевое кольцо);

– nZ, состоящее из целых чисел, кратных некоторому числу n;

– комплексных чисел вида $m + ni$, где $m, n \in Z$ (кольцо целых гауссовых чисел);

– многочленов от одной или нескольких переменных над некоторым полем;

– квадратных матриц порядка n над некоторым полем.

Свойства кольца

1. *В кольце K операция сложения обратима, т. е. разрешимо уравнение вида $a+x=b$. Решение записывается в виде $x=b-a$ и называется разностью элементов b и a.*

2. $\forall a \in K\ (a * 0 = 0 * a = 0)$.
3. $\forall a, b \in K\ (a + b = a\ \rightarrow b = 0)$.
4. $\forall a, b \in K\ ((-a)b = a(-b) = -ab)$.
5. $\forall a, b, c \in K\ (a(b-c) = ab - ac \wedge (b-c)a = ba - ca)$ – дистрибутивность операции умножения относительно операции вычитания.

Примерами колец являются числовые кольца и кольца многочленов от неизвестного x с коэффициентами из данного числового поля или даже из данного числового кольца.

Определение 2. *Элементы a и b кольца K называются* ***делителями нуля,*** *если $a \neq 0, b \neq 0, ab = 0$ или $ba = 0$.*

Определение 3. Коммутативное кольцо *K называется* ***областью целостности****, если оно не содержит делителей нуля.*

Определение 4. *Подмножество L кольца K называется* ***подкольцом*** *из K, если L само образует кольцо относительно операций сложения и умножения, определенных в K.*

Теорема (критерий подкольца). *Подмножество L из кольца K тогда и только тогда образует подкольцо, когда оно замкнуто относительно операций умножения и вычитания, т. е. когда выполняются следующие условия:*

$$1)\ \forall a, b \in L\ (ab \in L);$$
$$2)\ \forall a, b \in L\ (a - b \in L).$$

Определение 5. *Говорят, что кольцо K* ***изоморфно*** *кольцу K', если между K и K' существует такое взаимно однозначное соответствие φ, которое удовлетворяет следующим условиям:*

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

2) $\forall a, b \in K\ (\varphi(ab) = \varphi(a)\varphi(b))$.

При этом φ называют изоморфизмом кольца K на кольцо K'.

Если K изоморфно K', то пишут $K \cong K'$.

Если выполняются условия 1 и 2, то говорят, что отображение φ сохраняет операции, определенные в K.

Аналогично определяется ***изоморфизм произвольных алгебр*** – это есть взаимно однозначное соответствие между алгебрами, сохраняющее операции, определенные в них.

3. Поле, его простейшие свойства. Примеры полей. Числовые поля

Понятие поля. Простейшие свойства поля. Примеры полей. Числовые поля.

Определение 1. Полем *называется коммутативное кольцо К с единицей, содержащее не менее двух элементов, в котором для каждого отличного от нуля элемента существует ему обратный элемент.*

Иначе говоря, поле – это коммутативное кольцо, содержащее не менее двух элементов, в котором все ненулевые элементы образуют группу относительно операции умножения (мультипликативную группу $K^{\#}$ поля K).

Приведем развернутое определение поля.

Определение 2. *Множество К с определенными в нем двумя бинарными алгебраическими операциями сложением и умножением, содержащее не менее двух элементов, называется полем, если выполняются следующие условия (аксиомы поля):*

1. $\forall a,b,c \in K\ (a+(b+c)=(a+b)+c)$.
2. $\forall a,b \in K\ (a+b=b+a)$.
3. $\exists 0 \in K, \forall a \in K\ (a+0=a)$,
4. $\forall a \in K, \exists a' \in K\ (a+a'=0), a'=-a$.
5. $\forall a,b,c \in K\ (a\cdot(b\cdot c)=(a\cdot b)\cdot c)$.
6. $\forall a,b \in K\ (a\cdot b=b\cdot a)$.
7. $\forall a,b,c \in K\ ((a+b)c=ac+bc \wedge c(a+b)=ca+cb)$.
8. $\exists 1 \in K, \forall a \in K\ (1\cdot a=a)$.
9. $\forall a \in K\ (a\neq 0 \Rightarrow \exists a'' \in K\ (a\cdot a''=1), a''=a^{-1},\ a\neq 0$.

Примеры полей

1. Полями являются множества рациональных чисел Q, действительных чисел R и комплексных чисел C.

2. При обычных операциях сложения и умножения чисел полями являются множества:

– комплексных чисел вида $a+bi$, где $a,b \in Q$ (поле гауссовых чисел);

– действительных чисел вида $a+b\sqrt{2}$, где $a,b \in Q$;

– действительных чисел вида $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, где $a,b \in Q$.

Теорема 1. *Поле не содержит делителей нуля.*

Кольцо целых чисел является примером кольца без делителей нуля, но оно не является полем. Однако для конечных коммутативных колец верна и обратная теорема.

Теорема 2. *Всякое конечное коммутативное кольцо без делителей нуля, содержащее более одного элемента, является полем.*

Произведение ab^{-1} можно записывать также в виде дроби $\frac{a}{b}$. Для любых элементов a и b из поля и любого натурального числа n справедливы равенства: $(ab)^{-1}=a^{-1}b^{-1}$, $(a^n)^{-1}=(a^{-1})^n=a^{-n}$, $a^0=0$. Таким образом, определены степени любого ненулевого элемента a поля K с целыми показателями. Правила оперирования с дробями и степенями обычные.

Определение 2. *Пусть e – единичный элемент поля K. Натуральное число m называется* ***характеристикой поля K****, если*

$$m\cdot e=\underbrace{e+e+\dots+e}_{m-\text{слагаемых}}=0$$

и не существует натурального числа меньшего m, для которого подобное равенство выполняется. Если указанное свойство не имеет места ни для какого натурального числа, то говорят, что поле K имеет ***характеристику 0.***

Теорема 3. *Характеристика любого поля либо равна нулю, либо является простым числом.*

Определение 3. *Подмножество P поля K называется* ***подполем*** *из K, если P само образует поле относительно операций сложения и умножения, определенных в K. Поле K в этом случае называют* ***расширением*** *поля P.*

Определение 4. Числовым полем *называется всякое подполе поля комплексных чисел C.*

Отметим, что числовое множество M тогда и только тогда образует поле, когда оно замкнуто относительно четырех арифметических действий – сложения, вычитания, умножения и деления чисел (исключая деление на 0).

Наименьшим числовым полем по отношению включения $\subseteq$ является поле рациональных чисел Q.

Все числовые поля являются полями нулевой характеристики.

Теорема 3. *Любое конечное поле характеристики p состоит из p^n элементов для некоторого числа натурального n.*

Теорема 4. *Если характеристика поля K равна p, то для любого элемента $a\in K$ выполняется равенство*

$$p\cdot a=\underbrace{a+a+\dots+a}_{p\,-\text{слагаемых}}=0.$$

4. Алгебраическая форма комплексного числа. Операции над комплексными числами в алгебраической форме. Геометрическая интерпретация комплексных чисел

Определение комплексных чисел. Операции над комплексными числами в алгебраической форме. Извлечение квадратного корня из комплексного числа в алгебраической форме. Геометрическая интерпретация комплексных чисел. Модуль и аргумент комплексных чисел.

Определение 1. Комплексным числом называют сумму действительного числа и чисто мнимого числа $a + bi$ (где a, b – действительные числа, а i – некоторый символ). Символ i называют мнимой единицей; $i^2 = -1$.

Определение 2. Представление комплексного числа z в виде $z = a + bi$, где $a, b \in R$, *называется* ***алгебраической формой комплексного числа.*** При этом ***a*** *называют* ***действительной частью,*** а ***b – мнимой частью*** комплексного числа.

Отметим следующие свойства комплексных чисел.

Свойство 1. *Два комплексных числа равны тогда и только тогда, когда равны действительные и мнимые части этих чисел.*

Свойство 2. *Справедливы следующие правила действий над комплексными числами, заданными в алгебраической форме:*

1) $a + bi \;+\; c + di \;=\; a + c \;+\; b + d\; i;$

2) $a + bi \;-\; c + di \;=\; a - c \;+\; b - d\; i;$

3) $a + bi \;\; c + di \;= ac + adi + bci + bdi^2 = \; ac - bd \;+\; ad + bc\; i;$

4) $\frac{a+bi}{c+di} = \frac{a+bi \;\; c-di}{c+di \;\; c-di} = \frac{ac+bd \;-\; ad+bc\; i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} - \frac{ad+bc}{c^2+d^2} i, \;\; c^2 + d^2 \neq 0$.

Определение 3. *Комплексные числа* z_1 *и* z_2, *заданные в алгебраической форме, называются* ***сопряженными****, если они отличаются только знаком перед мнимой частью.*

Число, сопряженное числу z, будем обозначать через z. Таким образом, если $z = a + bi$, то $z = a - bi$.

Корни из комплексных чисел

Пусть *n* – произвольное натуральное число и $z \in C$.

Определение. *Корнем n-ой степени из комплексного числа* z *называется такое комплексное число* α, *что* $\alpha^n = z$, *и обозначается* $\alpha = \sqrt[n]{z}$.

Рассмотрим случай, когда *n* = 2.

Пусть $z = a + bi$. Предположим, что квадратный корень из числа z существует и равен $u + vi$, то есть $\sqrt{a + bi} = u + vi$.

Возведя обе части равенства в квадрат, получим:

$a + bi = u^2 + 2uv - v^2$.

Приравняв действительные и мнимые части, имеем систему уравнений:

$$\begin{cases} u^2 - v^2 = a\,; \\ 2uv = b\,. \end{cases} \qquad (1)$$

Возводим далее обе части каждого из уравнений в квадрат и затем почленно складываем уравнения. В результате придем к равенству: $(u^2 + v^2)^2 = a^2 + b^2$. Отсюда

$$u^2 + v^2 = \sqrt{a^2 + b^2}\,. \qquad (2)$$

Из уравнений (1) и (2) имеем:

$$u^2 = \frac{1}{2}\left(\sqrt{a^2 + b^2} + a\right),$$
$$v^2 = \frac{1}{2}\left(\sqrt{a^2 + b^2} - a\right),$$

Тогда

$$u = \sqrt{\frac{1}{2}\left(\sqrt{a^2 + b^2} + a\right)}\,, \qquad (3)$$

$$v = \sqrt{\frac{1}{2}\left(\sqrt{a^2 + b^2} - a\right)}\,. \qquad (4)$$

При любых a и b подкоренные выражения в формулах (3) и (4) неотрицательные. Поэтому u и v – действительные числа. Для нахождения корня $u + vi$ значения u и v, заданные формулами (3) и (4), нельзя комбинировать произвольно. Согласно равенству (2), нужно комбинировать значения u и v, для которых знак произведения uv совпадает со знаком числа b.

Таким образом, корень квадратный из комплексного числа $z = a + bi$ существует, и значения его определяются формулами:

$$\sqrt{a + bi} = \pm\left(\sqrt{\frac{1}{2}\left(\sqrt{a^2 + b^2} + a\right)} + i\sqrt{\frac{1}{2}\left(\sqrt{a^2 + b^2} - a\right)}\right), \text{ если } b > 0,$$

$$\sqrt{a + bi} = \pm\left(\sqrt{\frac{1}{2}\left(\sqrt{a^2 + b^2} + a\right)} - i\sqrt{\frac{1}{2}\left(\sqrt{a^2 + b^2} - a\right)}\right), \text{ если } b < 0.$$

Геометрическое изображение комплексных чисел

Возьмем на плоскости декартову прямоугольную систему координат. Каждая точка плоскости в выбранной системе координат определяется парой действительных чисел (a, b), где a – абсцисса, а b – ордината точки. С другой стороны, каждая точка плоскости определяет пару действительных чисел – координат точки. Таким образом, между множеством точек плоскости и множеством $R^2 = \{(a, b) | a, b \in R\}$ всех упорядоченных пар действительных чисел существует взаимно однозначное соответствие. Очевидно также, что существует взаимно однозначное соответствие между множеством всех комплексных чисел $\mathrm{C} = \{a + bi | a, b \in R^2\}$ и множеством R^2, следовательно, это соответствие существует между множеством С и множеством точек плоскости. Это позволяет изображать комплексные числа точками плоскости. Условимся комлексное число $z = a + bi$ изображать точкой $A(a, b)$ плоскости, абсцисса которой в выбранной декартовой системе координат равна a, а ордината – b. Ввиду взаимно однозначного соответствия между множеством C комплексных чисел и множеством точек плоскости, каждому комплексному числу $z = a + bi$ соответствует одна и только одна точка $A(a, b)$ плоскости и, наоборот, каждая точка $B(c, d)$ соответствует одному и только одному комплексному числу $z_1 = \mathrm{c} + di$. Плоскость, на которой изображаются комплексные числа, называется ***<u>комплексной плоскостью.</u>*** Действительные числа на комплексной плоскости изображаются точками оси абсцисс *Ox*, в связи с этим эту ось называют ***<u>действительной осью.</u>*** Мнимые числа, то есть числа вида bi, изображаются на комплексной плоскости точками оси ординат *Oy*. Поэтому ось *Oy* называют ***<u>мнимой осью</u>*** комплексной плоскости.

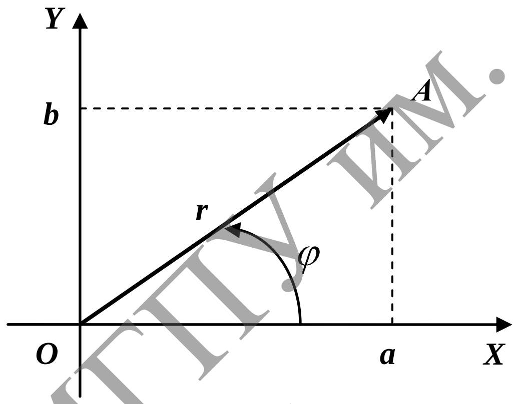

Рисунок 1

Точка $A(a, b)$, изображающая комплексное число z, вполне определяется также своими полярными координатами, то есть расстоянием *r* от начала координат до точки *A* и углом φ между положительным направлением оси *Ox* и направлением из начала координат на данную точку. Между декартовыми и полярными координатами точки *A* существует следующая связь:

$$r = \sqrt{a^2 + b^2}; \quad \cos\varphi = \frac{a}{r}; \quad \sin\varphi = \frac{b}{r};$$

$$a = r \cdot \cos\varphi; \quad b = r \cdot \sin\varphi. \qquad (1)$$

5. Тригонометрическая форма комплексного числа. Операции над комплексными числами в тригонометрической форме. Корень n-ой степени из комплексных чисел. Корни из единицы

Тригонометрическая форма комплексных чисел. Умножение, деление и возведение в степень комплексных чисел с целым показателем. Корень n-ой степени из комплексных чисел. Корни из единицы.

Пусть $z = a + bi$ – произвольное комплексное число. Это число в декартовой системе координат на комплексной плоскости изображается точкой $A(a, b)$ (рисунок 1).

Точка $A(a, b)$, изображающая комплексное число z, вполне определяется также своими полярными координатами, то есть расстоянием r от начала координат до точки A и углом φ между положительным направлением оси Ox и направлением из начала координат на данную точку. Между декартовыми и полярными координатами точки A существует следующая связь:

$$r = \sqrt{a^2 + b^2}\,;\ \cos\varphi = \frac{a}{r};\ \ \sin\varphi = \frac{b}{r};\ \ a = r \cdot \cos\varphi;\ \ b = r \cdot \sin\varphi. \qquad (1)$$

Учитывая эти соотношения, получим следующее представление комплексного числа z:

$$z = a + bi = r(\cos\varphi + i\sin\varphi). \qquad (2)$$

Представление комплексного числа z в виде (2) называется ***тригонометрической формой комплексного числа.*** При этом r называют ***модулем*** комплексного числа z и обозначают символом $|z|$, а φ – ***аргументом*** комплексного числа z и обозначают через $\arg z$.

Отметим, аргумент φ числа z определяется не однозначно, а с точностью до слагаемых, кратных 2π.

Два комплексных числа, заданных в тригонометрической форме, равны тогда и только тогда, когда равны модули этих чисел, а аргументы либо равны, либо отличаются слагаемыми, кратными 2π.

Рассмотрим, как выполняются операции умножения и деления над комплексными числами, заданными в тригонометрической форме.

Пусть $z_1 = r_1(\cos\varphi_1 + i \cdot \sin\varphi_1)$ и $z_2 = r_2(\cos\varphi_2 + i \cdot \sin\varphi_2)$ – произвольные комплексные числа. Найдем их произведение:

$$z_1 z_2 = \big(r_1(\cos\varphi_1 + i \cdot \sin\varphi_1)\big) \cdot \big(r_2(\cos\varphi_2 + i \cdot \sin\varphi_2)\big) =$$
$$= r_1 r_2\big((\cos\varphi_1 \cdot \cos\varphi_2 - \sin\varphi_1 \cdot \sin\varphi_2) + i \cdot (\sin\varphi_1 \cdot \cos\varphi_2 +$$
$$+ \sin\varphi_2 \cdot \cos\varphi_1)\big) = r_1 r_2\big(\cos(\varphi_1 + \varphi_2) + i \cdot \sin(\varphi_1 + \varphi_2)\big).$$

Согласно полученному равенству, модуль произведения двух комплексных чисел равен произведению модулей этих чисел, а аргумент произведения равен сумме аргументов сомножителей.

Пусть $z_2 \neq 0$. Найдем частное $\frac{z_1}{z_2}$.

$$\frac{z_1}{z_2} = \frac{r_1\ \cos\varphi_1 + i \cdot \sin\varphi_1}{r_2\ \cos\varphi_2 + i \cdot \sin\varphi_2} = \frac{r_1\ \cos\varphi_1 + i \cdot \sin\varphi_1\ r_2\ \cos\varphi_2 - i \cdot \sin\varphi_2}{r_2\ \cos\varphi_2 + i \cdot \sin\varphi_2\ r_2\ \cos\varphi_2 - i \cdot \sin\varphi_2} =$$

$$= \frac{r_1}{r_2} \cdot \frac{\cos\varphi_1 \cdot \cos\varphi_2 + \sin\varphi_1 \cdot \sin\varphi_2\ - i \cdot\ \sin\varphi_1 \cdot \cos\varphi_2 + \sin\varphi_2 \cdot \cos\varphi_1}{\cos^2\varphi_2 + \sin^2\varphi_2} =$$

$$= \frac{r_1}{r_2} \cdot\ \cos\ \varphi_1 - \varphi_2\ + i \cdot \sin\ \varphi_1 - \varphi_2\ .$$

Из полученного равенства следует, что модуль частного двух комплексных чисел равен частному модулей делимого и делителя, а аргумент частного равен разности аргументов делимого и делителя.

Пусть z_1 и z_2 – произвольные комплексные числа. Имеют место следующие свойства модулей комплексных чисел:

1) $z_1 z_2\ =\ z_1\ \ z_2$;
2) $z_1 + z_2\ \leq\ z_1\ +\ z_2$;
3) $z_1 - z_2\ \leq\ z_1\ +\ z_2$;
4) $z_1\ = 0\ \Leftrightarrow\ z_1 = 0$;
5) $z^{-1}\ =\ z\ ^{-1}$при $z_1 \neq 0$.

Формула Муавра

Рассмотрим далее вопрос о возведении комплексного числа в целую степень. Эту операцию также удобнее выполнять, если число представлено в тригонометрической форме.

Теорема. *Для любого целого числа n и комплексного числа* $z = r(\cos\varphi + i \cdot \sin\varphi)$ *справедливо равенство*

$$z^n =\ r(\cos\varphi + i \cdot \sin\varphi)\ ^n = r^n(\cos n\varphi + i \cdot \sin n\varphi), \qquad (3)$$

которое ***называется формулой Муавра.***

Извлечение корня произвольной натуральной степени n

Вопрос об извлечении корня произвольной натуральной степени n из комплексного числа *z* проще решается, когда *z* представлено в тригонометрической форме.

Пусть $z = r(\cos\varphi + i \cdot \sin\varphi)$, где $r \neq 0$.

Предположим, что $\sqrt[n]{z}$ существует и равен $\rho(\cos\theta + i \cdot \sin\theta)$.

Тогда

$$\rho(\cos\theta + i \cdot \sin\theta)\ ^n = r(\cos\varphi + i \cdot \sin\varphi). \qquad (4)$$

Используя формулу Муавра, получим

$$\rho^n\ \cos n\theta + i \cdot \sin n\theta\ = r(\cos\varphi + i \cdot \sin\varphi). \qquad (5)$$

Два комплексных числа, представленных в тригонометрической форме, равны тогда и только тогда, когда равны модули этих чисел, а аргументы либо равны, либо отличаются слагаемым, кратным 2π.

Поэтому из равенства (6) вытекает, что $\rho^n = r, \quad n\theta = \varphi + 2\pi k, k \in Z$. Отсюда $\rho = \sqrt[n]{r}$ и $\theta = \frac{\varphi+2\pi k}{n}$.

Таким образом,

$$\sqrt[n]{r\,(\cos\varphi + i \cdot \sin\varphi)} = \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i \cdot \sin\frac{\varphi+2\pi k}{n}\right), \qquad (6)$$

где k – произвольное натуральное число. Однако чтобы получить все корни n-ой степени из z, достаточно брать k, равным $0, 1, 2, \dots, n-1$. При этих значениях k получим *n* различных корней *n*-ой степени из z. При других целых k корни будут повторяться.

Таким образом, операция извлечения корня в поле комплексных чисел выполнима. Каким бы ни было натуральное число *n* и комплексное число $z \neq 0$, существует *n* различных корней *n*-ой степени из z, которые находятся по формуле:

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

Корни из единицы

Определение. *Корнем n-ой степени из числа 1 называется такое комплексное число ε, что $\varepsilon^n = 1$.*

Представим число 1 в тригонометрической форме:

$1 = cos\,\varphi\, 0 + i \cdot sin\, 0$.

Используя формулу (6) нахождения корней *n*-ой степени из комплексного числа, получим

$$\sqrt[n]{1} = \cos\frac{2\pi k}{n} + i \cdot \sin\frac{2\pi k}{n}, k = \overline{0, n-1}.$$

Таким образом, существует *n* различных корней *n*-ой степени из единицы, которые находятся по формуле:

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i \cdot \sin\frac{2\pi k}{n},\ k = \overline{0, n-1}. \qquad (7)$$

6. Делимость в кольце целых чисел. Алгоритм Евклида. Нахождение наибольшего общего делителя двух целых чисел с помощью алгоритма Евклида

Определение делимости. Свойства делимости целых чисел. Теорема о делении с остатком. Алгоритм Евклида. Нахождение наибольшего общего делителя двух целых чисел с помощью алгоритма Евклида. Связь наибольшего общего делителя и наименьшего общего кратного двух натуральных чисел.

Определение 1. Говорят, что целое число a ***делится на*** целое число b (либо b делит a), если существует такое целое число q, что $a = b \cdot q$. При этом a называют ***делимым***, b – ***делителем*** числа a, q – ***частным*** при делении a на b.

Если a делится на b, то пишут $a \vdots b$ (читается: «a делится на b») либо $b \,\big|\, a$ («b делит a»).

Очевидно, что отношение делимости является бинарным отношением на множестве Z.

Приведем свойства этого отношения.

1. Отношение делимости $\vdots$ на множестве Z рефлексивно, т. е. $\forall a \in Z \,\big|\, a \vdots a$.

2. Отношение $\vdots$ на Z транзитивно, т. е. $\forall a, b, c \in Z \,\big|\, a \vdots b \wedge b \vdots c \Rightarrow a \vdots c$.

3. Отношение делимости сохраняется при изменении знаков делимого и делителя, т. е. $\forall a, b \in Z \,\big|\, a \vdots b \Rightarrow -a \vdots b \wedge a \vdots -b \wedge \wedge (-a) \vdots (-b)$.

4. $\forall a, b, c \in Z \,\big|\, a \vdots c \wedge c \vdots b \Rightarrow (a + b) \vdots c$.

5. $\forall a, b, c \in Z \,\big|\, a \vdots c \Rightarrow a \cdot b \vdots c$.

6. $\forall a, b, c \in Z \,\big|\, a \vdots c \wedge b \vdots c \Rightarrow (a \pm b) \vdots c$.

7. $\forall a \in Z \,\big|\, 0 \vdots a$.

8. $\forall a \in Z \,\big|\, a \vdots 1$.

9. $\forall a, b \,\big|\, a \neq 0 \Rightarrow 0 \cdot b \neq a$, т. е. деление на нуль невозможно.

10. $\forall a, b \in Z \,\big|\, a \vdots b \Rightarrow a \geq b$. *В частности,* $a \vdots b \wedge b \vdots a \Rightarrow a = b$.

Определение 2. Говорят, что произведено ***деление с остатком*** целого числа a на целое число b, если найдены такие целые числа q и r, что $a = b \cdot q + r$, где r удовлетворяет условию $0 \leq r < b$.

В этом случае q называют ***неполным частным*** или просто ***частным***, а r – ***остатком***.

Теорема 1 (о делении с остатком). Каковы бы ни были целые числа a и $b \neq 0$, всегда возможно деление с остатком a на b, частное q и остаток r при таком делении определяются однозначно.

Следствие. Число a делится на число b тогда и только тогда, когда остаток от деления a на b равен 0.

Определение 3. Число d называют ***общим делителем*** чисел

$$a_1, a_2, \dots, a_k, \qquad (1)$$

если d делит каждое из этих чисел. Общий делитель d чисел (1) называют наибольшим общим делителем этих чисел, если d делится на любой их общий делитель.

Теорема 2. Наибольший общий делитель чисел $a_1, a_2, \dots, a_k$ определяется однозначно с точностью до знака.

Условимся в качестве наибольшего общего делителя чисел $a_1, a_2, \dots, a_k$ брать его положительное значение и обозначать через $(a_1, a_2, \dots, a_k)$.

Алгоритм Евклида

Ниже мы опишем способ нахождения наибольшего общего делителя чисел, доказывающий его существование для любых чисел a и b (кроме случая, когда $a = 0$ и $b = 0$).

Предварительно приведем два свойства наибольшего общего делителя чисел в виде лемм.

Лемма 1. Если $a \vdots b$, *то* $a, b = b$.

Лемма 2. Пусть $a = bq + r$, тогда $a, b = (b, r)$.

Будем полагать, что, по крайней мере, одно из чисел a и b отлично от 0. Для определенности пусть $b \neq 0$. Тогда делим a на b с остатком. Получим равенство $a = b \cdot q_0 + r_1$, где $0 \leq r_1 < b$. Если $r_1 = 0$, то $a \vdots b$ и согласно лемме 1 $a, b = b$. Если $r_1 \neq 0$, то далее делим b на r_1 с остатком, получим равенство

$$b = r_1 \cdot q_1 + r_2,$$

где $0 \leq r_2 < r_1$. При $r_2 \neq 0$ далее делим r_1 на r_2 с остатком и т. д. Так как остатки r_1, r_2,…, получаемые в процессе последовательного деления убывают и являются натуральными числами, то этот процесс не бесконечен, т. е. на каком-то n-ом шаге мы неизбежно получим в остатке 0. Представим описанный процесс последовательного деления в виде системы равенств:

$$\begin{array}{ll}
a = b \cdot q_0 + r_1 & 0 \leq r_1 < b \\
b = r_1 \cdot q_1 + r_2 & 0 \leq r_2 < r_1 \\
r_1 = r_2 \cdot q_2 + r_3 & 0 \leq r_3 < r_2 \\
\dots\dots\dots\dots\dots & \\
r_{n-2} = r_{n-1} \cdot q_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\
r_{n-1} = r_n \cdot q_n. &
\end{array} \qquad (2)$$

Согласно лемме 2 из первого равенства системы (2), имеем: $a, b = b, r$. Аналогично из последующих равенств системы (2) получим:

$b, r_1 \;\; = (r_1, r_2)$
$(r_1, r_2) = (r_2, r_3)$
……………...
$r_{n-2}, r_{n-1} \;\; = (r_{n-1}, r_n).$

Наконец из последнего равенства системы, согласно лемме 1, следует:

$r_{n-1}, r_n \;\; = r_n.$

Из полученных равенств непосредственно следует:

$$a, b \;\; = r_n. \qquad (3)$$

Описанный процесс последовательного деления называется ***алгоритмом Евклида.***

Итак, нами доказано, что наибольший общий делитель чисел a и b существует и равен последнему остатку r_n, отличному от нуля (р-во 3) алгоритма Евклида, примененного к числам a и b.

Приведем свойства наибольшего общего делителя чисел.

Свойство 1. Наибольшим общим делителем чисел $a_1, a_2, \dots, a_k$ является наибольший по величине положительный общий делитель этих чисел.

Свойство 2. Если $a, b \;\; = d$, то $k \cdot a, k \cdot b \;\; = k \cdot d$, где k – произвольное натуральное число.

Свойство 3 (*свойство линейности наибольшего общего делителя чисел*). Пусть $d = (a, b)$. Тогда существуют такие целые числа x и y, что выполняется равенство

$$a \cdot x + b \cdot y = d. \qquad (4)$$

Представление $a, b \;\; = d$, в виде равенства (4) называется ***линейным представлением*** наибольшего общего делителя чисел.

Свойство 4. Если $(a_1, a_2) = d_1$, $(d_1, a_3) = d_2$,…, $(d_{k-2}, a_k) = d_{k-1}$, то $a_1, a_2, \dots, a_k \;\; = d_{k-1}$.

Согласно данному свойству, чтобы найти наибольший общий делитель нескольких чисел $a_1, a_2, \dots, a_k$,, можно вначале найти $(a_1, a_2) = d_1$, затем $(d_1, a_3) = d_2$ и т. д. В конечном итоге получим $a_1, a_2, \dots, a_k \;\; = d_{k-1}$.

Определение 4. Число m называется ***общим кратным*** чисел $a_1, a_2, \dots, a_k$, если m делится на каждое из этих чисел. Общее кратное m чисел $a_1, a_2, \dots, a_k$ называется ***наименьшим общим кратным*** этих чисел, если оно делит их любое общее кратное.

Теорема 4. Наименьшее общее кратное чисел $a_1, a_2, \dots, a_k$ определяется однозначно с точностью до знака, т. е. если m_1 и m_2 – наименьшие общие кратные этих чисел, то либо $\mathrm{m}_1 = \mathrm{m}_2$, либо $\mathrm{m}_1 = -\mathrm{m}_2$.

В дальнейшем в качестве наименьшего общего кратного чисел $a_1, a_2, \dots, a_k$ условимся брать его положительное значение и обозначать его через $a_1, a_2, \dots, a_k$.

Теорема 5. Наименьшее общее кратное натуральных чисел a и b равно произведению этих чисел, деленному на их наибольший общий делитель, т. е.

$$a, b \; = \frac{a \cdot b}{(a,b)}. \quad (5)$$

7. Матрицы. Операции над матрицами. Кольцо квадратных матриц

Матрицы. Виды матриц. Умножение матриц на скаляр. Сложение и умножение матриц. Транспонирование матриц. Кольцо квадратных матриц.

Под полем P будем понимать числовое поле, т. е. числовое множество, замкнутое относительно четырех арифметических действий: сложения, вычитания, умножения и деления чисел (исключая деление на ноль).

Определение 1. *Матрицей размера $m \times n$ над полем P называется прямоугольная таблица, составленная из чисел поля P и содержащая в себе m строк и n столбцов.*

Матрицы в дальнейшем будем обозначать большими буквами латинского алфавита *A, B, C, …* . Матрица *A* размера $m \times n$ записывается следующим образом:

$$A = \begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{matrix} . \tag{1}$$

Числа, из которых составлена матрица, называют элементами этой матрицы. Первый индекс элемента матрицы указывает номер строки, а второй − номер столбца, в котором он стоит.

Матрицу (1) размера $m \times n$ будем также записывать в более компактной форме: $A = \; a_{ij} \;_{m\times n}$.

Определение 2. *Две матрицы $A = (a_{ij})_{m\times n}$ и $B = (b_{ij})_{m\times n}$ одинакового размера называются **равными**, если равны их соответствующие элементы, т. е. $a_{ij} = b_{ij} \;\; i = 1, m; j = 1, n$.*

Определение 3. *Матрица A называется **квадратной матрицей** порядка n, если число строк в ней равно числу столбцов и равно n.*

Определение 4. *Квадратная матрица порядка n называется **матрицей треугольного вида**, если все ее элементы, расположенные ниже или выше главной диагонали (диагональ от a_{11} к a_{nn}), равны* 0.

Определение 5. *Квадратная матрица называется **матрицей диагонального вида**, если все ее элементы, расположенные не на главной диагонали, равны* 0.

Определение 6. *Диагональная матрица порядка n, все элементы главной диагонали которой равны между собой, называется **скалярной матрицей порядка n.***

Частными случаями скалярных матриц являются:

$$E = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$ – единичная матрица;

$$O = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$ – нулевая матрица.

Строки (столбцы) матрицы $A = (a_{ij})_{m\times n}$ будем рассматривать в дальнейшем как n-мерные (m-мерные) числовые векторы.

Определение 7. *Элементарными преобразованиями матрицы называют следующие преобразования:*

1) перемена местами двух строк (столбцов) матрицы;

2) умножение одной из строк (одного из столбцов) матрицы на число, отличное от нуля;

3) *прибавление к одной из строк матрицы (к одному из столбцов) другой ее строки (другого столбца), умноженной (умноженного) на произвольное число;*

4) исключение из матрицы нулевой строки (нулевого столбца).

Операции над матрицами

К матрицам могут быть применимы операции сложения, умножения, а также умножения матриц на числа. Классы матриц определенного вида относительно указанных операций образуют известные типы алгебраических систем. В этом плане матрицы являются неисчерпаемым источником примеров таких систем. Это позволяет широко использовать аппарат теории матриц в абстрактной алгебре. Алгебра матриц является также эффективным средством исследования и решения систем линейных уравнений, а также изучения преобразований векторных пространств.

Будем рассматривать матрицы над числовым полем P, т. е. будем полагать, что элементы всякой матрицы принадлежат полю P.

Операция сложения вводится только для матриц одинакового размера.

Определение 8. *Суммой матриц* $A = (a_{ij})_{m\times n}$ *и* $B = (b_{ij})_{m\times n}$ *одинакового размера* $m \times n$ *называется матрица* $A + B = (a_{ij} + b_{ij})_{m\times n}$.

Согласно определению элементы суммы $A + B$ равны суммам соответствующих элементов слагаемых матриц. Очевидно, что операция сложения является алгебраической операцией на множестве матриц одинаковой размерности $m \times n$. Приведем далее свойства операции сложения на этом множестве.

Свойство 1. $(A + B) + C = A + (B + C)$ (*ассоциативность*).

Свойство 2. $A + B = B + A$ (*коммутативность*).

Свойство 3. $A + O = A$, где O − нулевая матрица размерности $m \times n$, т. е. матрица, все элементы которой равны нулю.

Свойство 4. *Для всякой матрицы A существует противоположная ей матрица −A, такая, что A+(−A) = O. Очевидно, что противоположной матрице A является матрица, все элементы которой противоположны соответствующим элементам матрицы A.*

Согласно приведенным свойствам множество матриц одного и того же размера $m \times n$ образует ***абелеву группу относительно операции сложения.*** В частности, отсюда следует, что на этом множестве определена операция, обратная сложению, − *вычитание.*

Определение 9. *Произведением матрицы* $A = \ a_{ij}\ _{m\times n}$ *на число* $\alpha \in P$ *называется матрица* $\alpha A = \ a_{ij}\ _{m\times n}$.

Согласно определению при умножении матрицы на число каждый элемент матрицы умножается на это число.

Приведем некоторые свойства операции умножения матриц на числа.

Свойство 5. $(\alpha\beta)A = \alpha(\beta A)$ (*ассоциативность*).

Свойство 6. $(\alpha + \beta)A = \alpha A + \beta A$ (*дистрибутивность относительно сложения чисел*).

Свойство 7. $\alpha(A + B) = \alpha A + \alpha B$ (*дистрибутивность относительно сложения матриц*).

Свойство 8. $1 \times A = A$ и $-1 \times A = -A$.

Из приведенных выше свойств операции сложения матриц и операции умножения матриц на числа из поля P вытекает, что множество матриц одного и того же размера $m \times n$ образует ***векторное пространство над полем P.***

Произведение матрицы A на матрицу B определяется только для случая, когда число столбцов матрицы A равно числу строк матрицы B.

Определение 10. *Произведением матрицы* $A = \ a_{ij}\ _{m\times n}$ *на матрицу* $B = \ b_{lk}\ _{n\times s}$ *называется матрица* $AB = \ c_{pq}\ _{m\times s}$, *элементы которой определяются равенствами* $c_{pq} = a_{p1} \times a_{1q} + a_{p2} \times a_{2q} + \cdots +$ $+a_{pn} \times a_{qn}$. (2)

Согласно этой формуле элемент c_{pq}, стоящий в p-ой строке и q-ом столбце матрицы AB, равен сумме произведений элементов p-й строки матрицы A на соответствующие элементы q-го столбца матрицы B. Элемент c_{pq} можно рассматривать как скалярное произведение p-ой строки матрицы A на q-ый столбец матрицы B.

В произведении AB матрицу A называют левым множителем, а матрицу B − правым. Говорят также, что произведено умножение матрицы B на матрицу A слева.

Очевидно, что $AB \neq BA$.

Свойство 9. $A\ \ BC\ =\ AB\ \ C$ (*ассоциативность*).

Свойство 10. $AB \neq BA$ (*некоммутативность в общем случае*).

Свойство 11. $A(B + C) = AB + AC$ *и* $B + C\ \ A = BA + CA$ (*дистрибутивность относительно операции сложения*).

Свойство 12. $AE = EA = A$, где E − единичная матрица.

Свойство 13. $\alpha(AB) = (\alpha A)B$, где $\alpha \in P$.

Обозначим через M_n множество всех квадратных матриц порядка n. Из приведенных свойств операций сложения и умножения матриц следует, что это множество образует ***кольцо с единицей*** относительно указанных операций. Это кольцо содержит делители нуля.

Определение 11. *Матрицы $A, B \in M_n$ называют* ***перестановочными****, если $AB = BA$.*

Легко убедиться, что скалярная матрица перестановочна с любой матрицей.

8. Системы линейных уравнений. Решение систем линейных уравнений методом последовательного исключения неизвестных

Понятие системы линейных уравнений. Совместные и несовместные системы, определенные и неопределенные системы. Следствие системы линейных уравнений. Равносильные системы. Элементарные преобразования систем. Решение систем линейных уравнений методом последовательного исключения неизвестных (метод Гаусса).

Определение 1. *Системой линейных уравнений с* n *неизвестными над полем* P *называется система вида:*

$$\begin{aligned} &a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1\\ &a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2\\ &\dots\\ &a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{aligned} \qquad (1)$$

где $x_1, x_2, \dots, x_n$ – неизвестные, b_i, a_{ij} $(i = 1, 2, \dots, m; j = 1, 2, \dots, n)$ – числа из поля P. Числа a_{ij} называют коэффициентами, а b_i – свободными членами системы.

Определение 2. *Числовой* n*-мерный вектор* $c = (\alpha_1, \alpha_2, \dots, \alpha_n)$ *называется* ***решением*** *системы (1), если при подстановке в систему вместо неизвестных* $x_1, x_2, \dots, x_n$ *чисел* $\alpha_1, \alpha_2, \dots, \alpha_n$ *соответственно, все уравнения системы обращаются в верные числовые равенства.*

Определение 3. *Система линейных уравнений называется* ***совместной,*** *если она имеет хотя бы одно решение, в противном случае система называется* ***несовместной.*** *Совместная система, имеющая только одно решение, называется* ***определенной.*** *Система, имеющая более одного решения, называется* ***неопределенной.***

Неопределенная система линейных уравнений над числовым полем P имеет бесконечное множество решений.

Определение 4. *Система линейных уравнений*

$$\begin{aligned} &c_{11}x_1 + c_{12}x_2 + \cdots + c_{1n}x_n = d_1\\ &c_{21}x_1 + c_{22}x_2 + \cdots + c_{2n}x_n = d_2\\ &\dots\\ &c_{l1}x_1 + c_{l2}x_2 + \cdots + c_{ln}x_n = d_l \end{aligned} \qquad (2)$$

называется ***следствием*** *системы (1), если всякое решение системы (1) является также и решением этой системы (2), т. е. если множество всех решений системы (1) является подмножеством множества решений системы (2). Системы (1) и (2) называются* ***равносильными,*** *если каждая из них является следствием другой, т. е. если множества решений обеих систем совпадают.*

Очевидно, что всякая подсистема, в частности, всякое уравнение системы является ее следствием.

Решить систему – это значит выяснить, совместна она или несовместна, и в случае совместности найти все ее решения.

Определение 5. Элементарными преобразованиями системы *линейных уравнений называются следующие преобразования:*

1) перемена местами двух уравнений системы;

2) умножение уравнения системы на числа, отличные от нуля;

3) прибавление к одному из уравнений системы другого ее уравнения, умноженного на произвольное число.

Теорема. *Всякая последовательность элементарных преобразований системы линейных уравнений приводит к системе, равносильной исходной.*

Одним из наиболее универсальных методов решения систем линейных уравнений является метод последовательного исключения неизвестных, называемый также методом Гаусса. Он состоит в том, что данная система линейных уравнений с помощью элементарных преобразований преобразуется в равносильную ей систему специального вида, которая легко исследуется и решается.

Пусть дана система линейных уравнений (1). В ходе элементарных преобразований системы могут встретиться уравнения вида

$$0 \cdot x_1 + 0 \cdot x_2 + 0 \cdot x_3 = b. \quad (3)$$

При этом возможны два случая:

A. В уравнении (3) свободный член отличен от нуля, т. е. $b \neq 0$. Такому уравнению не удовлетворяют никакие значения неизвестных.

B. В уравнении (3) $b = 0$. В таком случае этому уравнению удовлетворяют любые значения неизвестных, т. е. уравнение является тождеством вида $0 = 0$. Такие уравнения удаляют из системы.

В системе (1) среди коэффициентов перед каждой из неизвестных x_j, есть отличные от нуля. В противном случае эта система была бы системой с меньшим числом неизвестных, чем n. Не ограничивая общности, можно считать, что $a_{11} \neq 0$. В противном случае этого можно было бы добиться перестановкой уравнений в системе, либо перенумерацией переменных (перестановкой слагаемых в уравнениях системы). На первом шаге исключим переменную x_1, из всех уравнений системы, начиная со второго. Для этого из второго уравнения вычтем первое, умноженное на $\frac{a_{21}}{a_{11}}$, затем из третьего уравнения вычтем первое, умноженное на $\frac{a_{31}}{a_{11}}$ и т. д.

В результате получим систему вида

$$\begin{array}{r} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a'_{22}x_2 + \cdots + a'_{2n}x_n = b'_2 \\ \cdots \\ a'_{l2}x_2 + \cdots + a'_{ln}x_n = b'_l \end{array} \qquad (4)$$

Без ограничения общности можно считать, что в системе (4) коэффициент $a_{22} \neq 0$. Этого можно добиться перестановкой уравнений в системе либо изменением нумерации неизвестных в системе.

На втором шаге исключаем неизвестную x_2 из всех уравнений системы (4) начиная с третьего. Для этого из третьего уравнения вычитаем второе, умноженное на $\frac{a_{32}}{a_{22}}$, затем из четвертого уравнения вычитаем второе, умноженное на число $\frac{a_{42}}{a_{22}}$ и т. д. В результате на этом шаге получим систему вида

$$
\begin{array}{l}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\
\quad a'_{22}x_2 + \cdots + a'_{2n}x_n = b'_2 \\
\quad a''_{33}x_3 + \cdots + a''_{3n}x_n = b''_3 \\
\quad \ldots \\
\quad a''_{s2}x_2 + \cdots + a''_{sn}x_n = b''_s
\end{array} \qquad (5)
$$

Продолжая этот процесс, мы обязательно придем к одному из двух случаев:

1. После некоторого шага получена система, содержащая уравнение вида

$0 \cdot x_1 + 0 \cdot x_2 + 0 \cdot x_3 = b$, где $b \neq 0$ (случай (А)). Тогда исходная система несовместна.

2. После всех преобразований получена система вида

$$
\begin{array}{l}
b_{11}x_1 + b_{12}x_2 + \cdots + b_{1r}x_r \ldots + b_{1n}x_n = c_1 \\
\quad b_{21}x_1 + \cdots + b_{2r}x_r + \cdots + b_{2n}x_n = c_2 \\
\qquad \ldots \\
\qquad b_{rr}x_r + \cdots + b_{rn}x_n = c_r
\end{array} \qquad (6)
$$

где коэффициенты $b_{11}, b_{22}, \ldots, b_{rr}$ отличны от нуля.

Отметим, что в процессе преобразований мы можем получить тождества вида $0 = 0$ (случай (В)), которые удаляются из системы. Поэтому $m \geq l \geq s \geq \cdots \geq r$.

Для системы (6) также возможны два случая А $r = n$. Тогда из последнего уравнения находим $x_r = \frac{c_r}{b_{rr}}$.

Очевидно, это значение x_r, будет единственным. Далее найденное значение x_r подставляем в предпоследнее уравнение системы (6) и находим единственное значение неизвестной x_{r-1}, и т. д.

Итак, в случае $r = n$, т. е. когда в системе (6) число уравнений равно числу неизвестных, система (6), а следовательно, и система (1) имеет единственное решение, т. е. является определенной.

Пусть $r < n$. Тогда из последнего уравнения выражаем неизвестную x_r через неизвестные $x_{r+1}, \ldots, x_n$.

$$x_r = c_r - x_{r,r+1} - \cdots - b_{rn}x_n.$$

Подставляя это выражение для x_r в предпоследнее уравнение системы (6), выражаем аналогично неизвестную x_{r-1} через неизвестные $x_{r+1}, \dots, x_n$ и т. д. Наконец, подставляя найденные выражения для неизвестных $x_r, x_{r-1}, \dots, x_2$ в первое уравнение, получаем выражение x_1, через неизвестные $x_{r+1}, \dots, x_n$.

Неизвестные $x_1, \dots, x_r$, которые выражаются через неизвестные $x_{r+1}, \dots, x_n$, называют базисными неизвестными, в свою очередь неизвестные $x_{r+1}, \dots, x_n$ называют свободными неизвестными системы.

Свободным неизвестным можно придавать произвольные значения. При этом будем получать различные решения системы.

Таким образом, в случае $r < n$, т. е. когда в системе (6) число уравнений меньше числа неизвестных, система имеет бесконечное множество решений, и следовательно, является неопределенной.

На практике обычно элементарные преобразования проводят не над самой системой линейных уравнений, а над расширенной матрицей этой системы.

***Определение 6**. Матрицей размера $m \times n$ над полем P называется прямоугольная таблица вида*

$$A = \begin{matrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{matrix}, \qquad (7)$$

где a_{ij} – числа из поля P, их называют элементами матрицы.

Строки матрицы очевидно представляют собой n-мерные, а ее столбцы m-мерные числовые векторы.

Две матрицы A и B размера $m \times n$ равны тогда и только тогда, когда равны их соответствующие элементы.

Матрица, у которой число строк равно числу столбцов $(m = n)$ называется квадратной. Порядком квадратной матрицы называется число ее строк (или столбцов).

Нулевой матрицей называется матрица, все элементы которой равны нулю.

Диагональной называется квадратная матрица, у которой все элементы, стоящие не на главной диагонали, равны нулю.

Диагональная матрица, у которой все диагональные элементы равны единице, называется единичной.

***Определение 7.** Матрица A (7) называется **ступенчатой,** если она удовлетворяет следующим условиям:*

1) нулевые строки (если таковые есть) расположены ниже всех ненулевых строк;

2) если $a_{1k_1}, a_{2k_2}, \dots, a_{rk_r}$ – первые отличные от нуля элементы *соответственно в первой, второй,..., r-ой 1, то* $k_1 < k_2 < \dots < k_r$.

К ***элементарным преобразованиям матрицы*** *относятся следующие преобразования:*

1) перемена местами (транспозиция) двух строк (столбцов) матрицы;

2) умножение одной из строк (одного из столбцов) матрицы на число из поля P*, отличное от нуля;*

3)прибавление к одной из строк матрицы другой ее строки, умноженной на число.

Из всякой ненулевой матрицы с помощью элементарных преобразований можно получить ступенчатую матрицу.

Определение 8. Матрицей системы линейных уравнений (1) *называется матрица А вида (7), составленная из коэффициентов при неизвестных системы. Расширенной матрицей системы (1) называется матрица* B*, полученная из матрицы системы добавлением к ней столбца свободных членов, т.е.*

$$B = \begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{matrix}.$$

Очевидно, что всякая система линейных уравнений вполне определяется своей расширенной матрицей.

При решении системы линейных уравнений методом Гаусса обычно выписывается расширенная матрица этой системы, из которой затем с помощью элементарных преобразований получают ступенчатую матрицу. Очевидно, что всякому элементарному преобразованию матрицы B соответствует некоторое элементарное преобразование системы. Поэтому полученная ступенчатая матрица определяет систему, равносильную исходной. Записав эту систему, находим ее решения, как это описано для системы (6).

9. Методы решения невырожденных систем линейных уравнений: матричный и метод Крамера

Матричная запись системы линейных уравнений. Решение невырожденных систем линейных уравнений матричным способом. Формулы Крамера.

Пусть дана система m линейных уравнений с n неизвестными*:*

$$\begin{matrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{matrix}. \qquad (1)$$

Обозначим: А − матрица системы; Х = $\begin{matrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{matrix}$ − столбец неизвестных;

В = $\begin{matrix} b_1 \\ b_2 \\ \ldots \\ b_n \end{matrix}$ − столбец свободных членов.

Тогда систему (1) можно представить в матричной форме

$$AX = B. \qquad (2)$$

Если в системе (1) число уравнений равно числу неизвестных (n = m), причем матрица A системы обратима, то, умножив обе части равенства (2) слева на A^{-1}, получим $X = A^{-1} \cdot B$. (3)

На формуле (3) основан так называемый ***матричный способ решения*** систем линейных уравнений. Этот способ применим для систем, в которых число уравнений равно числу неизвестных и матрицы которых обратимы. Решение системы будет единственным.

Метод Крамера

Пусть дана система n линейных уравнений с n неизвестными:

$$\begin{matrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2} + \cdots + a_{mn}x_n = b_m \end{matrix}. \qquad (4)$$

$A = (a_{ij})$ − матрица этой системы. Определитель матрицы A будем называть определителем системы (4) и обозначать через Δ.

***Теорема* (*Правило Крамера*)**. *Система (4) n линейных уравнений с n неизвестными, определитель которой отличен от нуля, имеет решение, причем единственное. Это решение определяется формулами*

$$x_1 = \frac{\Delta_1}{\Delta};\ x_2 = \frac{\Delta_2}{\Delta};\ \ldots,\ x_n = \frac{\Delta_n}{\Delta}, \qquad (5)$$

где Δ_j $(j\ = 1, n)$ *определитель, полученный из определителя* Δ *системы (4) заменой в нем j-го столбца столбцом свободных членов.*

10. Критерий совместности систем линейных уравнений

Векторная форма записи системы линейных уравнений. Основная и расширенная матрицы системы. Необходимое и достаточное условие совместности системы линейных уравнений.

Будем рассматривать матрицы и системы над числовым полем P.

Пусть дана матрица $A = (a_{ij})_{m\times n}$. Строки этой матрицы будем рассматривать как n-мерные, а ее столбцы − как m-мерные числовые векторы. В соответствии с этим будем говорить о системе строк (столбцов) матрицы как о системе числовых векторов.

Определение 1. Основной матрицей *или просто матрицей системы линейных уравнений*

$$\begin{matrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{matrix} \qquad (1)$$

называется матрица

$$A = \begin{matrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} \end{matrix},$$

составленная из коэффициентов при неизвестных этой системы.

Расширенной матрицей *системы линейных уравнений* (1) *называется матрица*

$$B = \begin{matrix} a_{11} & \dots & a_{1n} & b_1 \\ \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a_{mn} & b_m \end{matrix},$$

полученная из матрицы А системы, добавлением к ней столбца свободных членов.

Систему линейных уравнений (1) можно представить в более компактной векторной форме.

Введем обозначения

$$a_1 = \begin{matrix} a_{11} \\ a_{21} \\ \dots \\ a_{m1} \end{matrix}; \; a_2 = \begin{matrix} a_{12} \\ a_{22} \\ \dots \\ a_{m2} \end{matrix}; \; \dots; \; a_n = \begin{matrix} a_{1n} \\ a_{2n} \\ \dots \\ a_{mn} \end{matrix}; \; b = \begin{matrix} b_1 \\ b_2 \\ \dots \\ b_m \end{matrix}.$$

Далее рассмотрим уравнение

$$x_1a_1 + x_2a_2 + \cdots + x_na_n = b\,. \qquad (2)$$

Легко заметить, что система линейных уравнений (1) равносильна уравнению (2). Поэтому уравнение (2) является некоторой формой записи системы (1). Ее называют ***векторной формой записи*** этой системы.

Теорема 1 (Кронекер-Капелли)*. Система линейных уравнений* (1) *совместна тогда и только тогда, когда ранг ее основной матрицы равен рангу расширенной матрицы системы.*

Приведем еще критерий неопределенности системы линейных уравнений.

Теорема 2. *Совместная система тогда и только тогда является неопределенной, когда ранг матрицы этой системы меньше числа неизвестных в ней.*

11. Линейные пространства. Примеры. Простейшие свойства векторных пространств

Определение линейного пространства. Простейшие свойства линейных пространств. Примеры линейных пространств. Арифметическое n-мерное линейное пространство.

Пусть V – непустое множество, элементы которого будем обозначать малыми буквами латинского алфавита $a, b, c, \dots$ и пусть P – числовое поле, элементы которого будем обозначать малыми буквами греческого алфавита $\alpha, \beta, \gamma, \dots$.

Будем говорить, что на множестве V определена операция умножения на числа из поля Р, если задано отображение $(P \times V) \to V$, т. е. всякому числу $\alpha \in P$ и всякому элементу $a \in V$ ставится в соответствие, причем однозначно, некоторый элемент из множества V. Этот элемент будем называть произведением элемента a на число α *и* обозначать символом αa.

Определение 1. Непустое множество V называется **линейным (векторным) пространством** над полем P, а элементы из V векторами, если на V определена бинарная алгебраическая операция сложения и операция умножения на числа из поля P, причем выполняются следующие условия (аксиомы векторного пространства):

1. Множество V относительно операции сложения образует абелеву группу, т. е.

(а) операция сложения на множестве V ассоциативна:

$$\forall a, b, c \in V\ ((a + b) + c = a + (b + c));$$

(б) операция сложения на множестве V коммутативна:

$$\forall a, b \in V\ (a + b = b + a);$$

(в) во множестве V существует нулевой элемент:

$$\exists 0 \in V, \forall a \in V\ (a + 0 = a).$$

Нулевой элемент 0 называют нулевым вектором;

(г) для каждого элемента из множества V в этом множестве существует ему противоположный:

$$\forall a \in \mathrm{V}, \exists b \in \mathrm{V} (a + b = 0).$$

Элемент, противоположный a, обозначают через $-a$.

2. Операция умножения элементов из V на числа из P ассоциативна, т. е.

$$\forall \alpha, \beta \in P, \forall a \in \mathrm{V}\ ((\alpha\beta)\, a = \alpha\, (\beta a)).$$

3. Операция умножения элементов из V на числа из Р дистрибутивна относительно операции сложения, определенной на V, т. е.

$$\forall \alpha \in P, \forall a, b \in V\ (\alpha\, (a + b) = \alpha a + \alpha b).$$

4. Операция умножения элементов из V на числа из P дистрибутивна относительно операции сложения чисел, т. е.

$$\forall \alpha, \beta \in P, a \in V\ ((\alpha + \beta)\, a = \alpha a + \beta a).$$

5. $\forall a \in V\ (1 \cdot a = a)$.

Приведем основные свойства векторных пространств, вытекающие из определения.

Свойство 1. *В пространстве V существует единственный нулевой вектор 0.*

Свойство 2. *Для всякого вектора* $a \in V$ *в* V *существует единственный ему противоположный вектор.*

Свойство 3. *Для любых векторов* a *и* b *в пространстве V разрешимо уравнение вида* $a + x = b$. *Решение этого уравнения записывается* $x = b + \ -a\ = b - a$ *и называется разностью векторов* b *и* a. *Говорят также, что в V операция сложения обратима, т. е. определена операция, обратная сложению - вычитание.*

Свойство 4. *Сумма произвольного конечного числа векторов пространства V не зависит от того, в каком порядке выполняется сложение.*

Приведенные выше свойства следуют из того, что V образует группу относительно сложения.

Свойство 5. $\forall a \in V\ (0a = 0)$.

Свойство 6. $\forall \alpha \in P(\alpha 0 = 0)$.

Свойство 7. $\forall \alpha \in P,\ \forall a \in V\ (\alpha a = 0 \Rightarrow \alpha = 0$ либо $a = 0)$.

Свойство 8. $\forall \alpha \in P,\ \forall a \in V\ ((-\alpha)a = -\alpha a)$.

Свойство 9. $\forall \alpha \in P,\ \forall a \in V\ (\alpha(-a) = -\alpha a)$.

Свойство 10. $\forall \alpha \in P,\ \forall a, b \in V\ (\alpha(a - b) = \alpha a - \alpha b)$ (дистрибутивность операции умножения векторов на числа относительно операции вычитания векторов).

Свойство 11. $\forall \alpha, \beta \in P,\ \forall a \in V\ ((\alpha - \beta)a = \alpha a - \beta a)$.

Если поле P является полем действительных чисел, то пространство V называется ***действительным векторным пространством.*** *Если же P есть поле C комплексных чисел, то V называют* ***комплексным векторным пространством.***

Примеры векторных пространств

Множество всех комплексных чисел относительно операций сложения чисел и умножения комплексных чисел на действительные числа образует действительное векторное пространство.

Множество всех свободных векторов W_3 *обычного геометрического пространства образует действительное пространство относительно операций сложения векторов и умножения векторов на действительные числа.*

Множество $R[x]$ всех многочленов с действительными коэффициентами образует действительное векторное пространство относительно операций сложения многочленов и умножения многочленов на действительные числа.

Здесь операция сложения многочленов рассматривается как сложение векторов, а операция умножения многочленов на числа - как умножение векторов на числа.

Важным примером векторных пространств является арифметическое векторное пространство.

Определение 2. *Совокупность n чисел $\alpha_1, \alpha_2, \dots, \alpha_n$ поля P, расположенных в определенном порядке, называется n-мерным числовым вектором над полем P.*

Для обозначения n-мерных числовых векторов используют записи

$$a = (\alpha_1, \alpha_2, \dots, \alpha_n)$$

либо

$$a = \begin{matrix} \alpha_1 \\ \alpha_2 \\ \dots \\ \alpha_n \end{matrix} .$$

Числа $\alpha_1, \alpha_2, \dots, \alpha_n$ называют координатами или компонентами вектора a (α_1 - первая, α_2 – вторая, . . ., α_n – n-я координаты вектора a).

Определение 3. *Два числовых вектора $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ и $b = \beta_1, \beta_2, \dots, \beta_n$ называются равными, если равны их соответствующие координаты, т. е. если $\alpha_1 = \beta_1,\ \alpha_2 = \beta_2, \dots, \alpha_n = \beta_n$.*

Множество всех *n*-мерных числовых векторов над полем *P* будем обозначать через P_n. Введем на этом множестве операции сложения векторов и умножения векторов на числа из поля *P*.

Определение 4. *Суммой числовых векторов $a = \alpha_1, \alpha_2, \dots, \alpha_n$* и $b = (\beta_1, \beta_2, \dots, \beta_n)$ *называется вектор $a + b = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n)$.*

Определение 5. *Произведением вектора $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ на число $\lambda \in P$ называется вектор $\lambda a = (\lambda\alpha_1, \lambda\alpha_2, \dots, \lambda\alpha_n)$.*

Теорема 1. *Множество P_n образует векторное пространство над полем P относительно операций сложения числовых векторов и умножения векторов на числа из поля P.*

Определение 6. *Пространство P_n n-мерных числовых векторов называется **арифметическим n-мерным векторным пространством над полем** P.*

12. Линейная зависимость и независимость системы векторов.

Определение линейно зависимой и линейно независимой системы векторов. Свойства линейной зависимости векторов. Критерий линейной зависимости. Основная лемма о линейной независимости векторов.

Пусть V – векторное пространство над числовым полем P. Будем полагать, что все векторы, о которых идет речь ниже, принадлежат V.

Определение 1. *Система векторов $a_1, a_2, \dots, a_n$ называется* ***линейно зависимой,*** *если можно подобрать такие числа $\alpha_1, \alpha_2, \dots, \alpha_n$ из поля P, среди которых есть отличные от нуля, что будет выполняться равенство:*

$$\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n = 0\,. \qquad (1)$$

Система векторов $a_1, a_2, \dots, a_n$ называется ***линейно независимой,*** *если равенство* (1) *выполняется только тогда, когда $\alpha_1 = \alpha_2 = \dots = \alpha_n = 0$.*

Теорема 1. *Система векторов $a_1, a_2, \dots, a_n$ тогда и только тогда линейно зависима, когда хотя бы один из векторов системы линейно выражается через остальные.*

Приведенная теорема дает возможность иначе определить понятие линейной зависимости векторов.

Определение 3. *Система векторов $a_1, a_2, \dots, a_n$ называется* ***линейно зависимой****, если хотя бы один из векторов этой системы линейно выражается через остальные. Если же ни один из векторов системы линейно не выражается через остальные векторы, то система называется линейно независимой.*

Приведем свойства линейной зависимости векторов.

1. *Всякая система, содержащая нулевой вектор, линейно зависима.*

2. *Если система векторов линейно независима, то линейно независима и любая подсистема этой системы векторов. Данное свойство равносильно следующему.*

3. *Если линейно зависима некоторая подсистема системы векторов, то линейно зависима и сама система.*

4. *Если система векторов $a_1, a_2, \dots, a_n$ линейно независима, а система $a_1, a_2, \dots, a_n, b$ линейно зависима, то вектор b линейно выражается через векторы $a_1, a_2, \dots, a_n$.*

Определение 4. *Говорят, что система векторов $a_1, a_2, \dots, a_m$* ***линейно выражается*** *через систему векторов $b_1, b_2, \dots, b_n$, если всякий вектор первой системы линейно выражается через векторы второй системы.*

Отношение линейной выражаемости на множестве систем векторов рефлексивно и транзитивно.

Теорема 2. *Пусть система векторов* $a_1, a_2, \dots, a_m$ *линейно независима и линейно выражается через систему* $b_1, b_2, \dots, b_n$, *тогда число векторов в первой системе не больше чем во второй, т. е.* $m \leq n$.

Следствие 1. *Если система* $a_1, a_2, \dots, a_m$ *линейно выражается через систему* $b_1, b_2, \dots, b_n$ *и* $m \leq n$, *то система* $a_1, a_2, \dots, a_m$ *линейно зависима.*

Следствие 2. *В* n*-мерном арифметическом пространстве* P_n *линейно зависима любая система, состоящая из более, чем* n *векторов.*

13. Базис и ранг системы векторов. Ранг матрицы

Понятие базиса и ранга системы векторов. Неизменность ранга при элементарных преобразованиях. Максимальная линейно независимая подсистема и ее свойства. Ранг системы векторов и его свойства. Ранг матрицы. Вычисление ранга матрицы.

В дальнейшем нам понадобится следующее свойство линейной зависимости числовых векторов.

Теорема 1. *Система n-мерных числовых векторов*

$$\begin{aligned} a_1 &= a_{11}, a_{12}, \dots, a_{1n} \\ a_2 &= a_{21}, a_{22}, \dots, a_{2n} \\ &\dots\dots\dots\dots\dots\dots \\ a_m &= a_{m1}, a_{m2}, \dots, a_{mn} \end{aligned} \qquad (1)$$

в которой число векторов больше их размерности $(m > n)$, *линейно зависима.*

Определение 1. *Говорят, что система векторов*

$$a_1, a_2, \dots, a_m \qquad (2)$$

линейно выражается через систему векторов

$$b_1, b_2, \dots, b_m, \qquad (3)$$

если всякий вектор системы (2) линейно выражается через векторы системы (3).

Отношение линейной выражаемости на множестве систем векторов пространства *V* рефлексивно и транзитивно (предлагается убедиться в этом самостоятельно).

Определение 2. *Две системы векторов называются эквивалентными, если каждая из них линейно выражается через другую.*

Теорема 2. (основная теорема о линейной зависимости векторов).

Пусть система (2) *линейно независима и линейно выражается через систему векторов* (3). *Тогда число векторов в системе (2) не больше, чем в системе (3), т. е.* $m \le n$.

Определение 3. *Базисом системы векторов* $a_1, a_2, \dots, a_n$ *называется линейно независимая подсистема данной системы, через которую линейно выражается любой вектор системы.*

Теорема 3. *Любые два базиса системы векторов состоят из одного и того же числа векторов.*

Определение 4. *Рангом системы векторов* $a_1, a_2, \dots, a_n$ *называется число векторов в базисе этой системы.*

Заметим, что базис системы векторов можно рассматривать как максимальную линейно независимую подсистему этой системы, т. е. такую линейно независимую подсистему, при добавлении к которой произвольного вектора системы, она становится линейно зависимой. Действительно, согласно свойству линейной зависимости векторов, любой вектор системы линейно выражается через максимальную линейно независимую систему, и следовательно, она образует базис системы. Соответственно ранг системы векторов можно рассматривать как максимальное число линейно независимых векторов в этой системе.

Теорема 4. *Ранги эквивалентных систем векторов равны*.

Пусть дана матриц A размером $m \times n$

$$A = \begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{matrix}.$$

Строки и столбцы этой матрицы рассматриваются как соответственно n-мерные и m-мерные числовые векторы. Поэтому можно говорить о системе строк (столбцов) матрицы как о системе n-мерных (m-мерных) числовых векторов.

Определение 5. *Строчечным (столбцовым) рангом матрицы А называется ранг системы ее строк (столбцов).*

Теорема 5. *(о ранге матрицы). Строчечный ранг матрицы равен ее столбцовому рангу.*

Согласно этой теореме, имеет смысл говорить просто о ранге матрицы, не употребляя слова "строчечный" и "столбцовый".

Таким образом, ***ранг матрицы*** *– это максимальное число линейно независимых строк (столбцов) этой матрицы.*

Теорема 6. *Всякое элементарное преобразование матрицы не меняет ранга матрицы.*

Теорема 7. *Ранг ступенчатой матрицы равен числу ненулевых строк в ней.*

Последние теоремы дают один из способов вычисления ранга матрицы, который заключается в приведении матрицы к ступенчатому виду с помощью элементарных преобразований, а затем подсчете ненулевых строк полученной матрицы.

14. Базис и размерность линейного пространства. Координаты вектора в данном базисе. Матрица перехода от одного базиса пространства к другому. Связь между координатами вектора в различных базисах пространства

Под V мы будем понимать векторное пространство над числовым полем P.

Определение 1. *Векторное пространство V называется n-мерным, если в нем существует линейно независимая система, состоящая из n векторов, а всякая система из n + 1 векторов пространства уже линейно зависима. Число n в этом случае называют размерностью пространства V.*

В дальнейшем n-мерное векторное пространство над полем P будем обозначать через V_n.

Определение 2. *Базисом векторного пространства V называется линейно независимая система векторов этого пространства, через которую линейно выражается любой вектор пространства.*

Например, базис пространства P_n образует система единичных векторов. Действительно, она линейно независима, и всякий вектор $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ пространства P_n линейно выражается через нее, а именно:

$$a = \alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n.$$

Теорема 1. *Всякий базис пространства V_n состоит из n векторов.*

Верна также теорема, обратная приведенной.

Теорема 2. *Если базис пространства V состоит из n векторов, то его размерность равна n.*

На основании приведенных теорем можно дать другое определение размерности пространства.

Определение 3. *Размерностью пространства V называется число векторов в базисе этого пространства.*

Пусть $e_1, e_2, \dots, e_n$ − базис пространства V_n и a − произвольный вектор этого пространства. Тогда существуют такие числа $x_1, x_2, \dots, x_n$ из поля P, что

$$a = x_1 e_1 + x_2 e_2 + \dots + x_n e_n.$$

Такое представление вектора a называется разложением этого вектора по векторам базиса $(e_1, e_2, \dots, e_n)$. Коэффициенты $x_1, x_2, \dots, x_n$ этого разложения называют координатами вектора a в базисе.

Обычно координаты вектора a в заданном базисе записывают либо в виде строки, либо в виде столбца. При этом строку $(x_1, x_2, \dots, x_n)$ называют координатной строкой, а столбец

$\begin{matrix} x_1 \\ x_2 \\ \dots \\ x_n \end{matrix}$ − координатным столбцом вектора a в заданном базисе пространства.

Теорема 3. *Координаты всякого вектора a пространства V_n в заданном базисе пространства определяются однозначно.*

Пусть a и b − произвольные векторы пространства V_n. Запишем их разложения по векторам базиса пространства:

$$a = x_1e_1 + x_2e_2 + \ldots + x_ne_n,$$
$$b = y_1e_1 + y_2e_2 + \ldots + y_ne_n.$$

Найдем разложение суммы a + b по векторам базиса, сложив почленно два последних равенства:

$$a + b = (x_1 + y_1)e_1 + (x_2 + y_2)e_2 + \ldots + (x_n + y_n)e_n.$$

Отсюда следует, что координаты суммы векторов $a + b$ равны суммам соответствующих координат слагаемых векторов a и b. Это значит, что координатная строка (столбец) суммы $a + b$ равна сумме координатных строк (столбцов) векторов a и b. Аналогично, координатная строка (столбец) произведения вектора a на число α равна произведению координатной строки (столбца) вектора a на число α.

Матрица перехода от одного базиса пространства к другому

Пусть даны два базиса пространства V_n.

$$e_1, e_2, \ldots, e_n \qquad (1)$$
$$f_1, f_2, \ldots, f_n \qquad (2)$$

Разложим векторы базиса (2) по векторам базиса (1)

$$\begin{matrix} f_1 = t_{11}e_1 + t_{21}e_2 + \ldots + t_{n1}e_n \\ f_2 = t_{12}e_1 + t_{22}e_2 + \ldots + t_{n2}e_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ f_n = t_{1n}e_1 + t_{2n}e_2 + \ldots + t_{nn}e_n \end{matrix} \qquad (3)$$

Из координат полученных разложений составим матрицу

$$T_{ef} = \begin{matrix} t_{11} & t_{12} & \dots & t_{1n} \\ t_{21} & t_{22} & \dots & t_{2n} \\ \dots & \dots & \dots & \dots \\ t_{n1} & t_{n2} & \dots & t_{nn} \end{matrix} \qquad (4)$$

Полученная матрица называется матрицей перехода от базиса (1) к базису (2). Столбцы матрицы T_{ef} представляют собой координатные столбцы векторов базиса (2) в базисе (1). Так как всякий базис пространства является линейно независимой системой векторов, то и координатные столбцы векторов базиса линейно независимы. Таким образом, столбцы матрицы T_{ef}, а следовательно, и ее строки линейно независимы. Это значит, что матрица T_{ef} невырожденная. Обратно, всякая невырожденная матрица порядка n над полем P может служить матрицей перехода от одного базиса к некоторому другому базису пространства. Так как T_{ef} невырожденная матрица то она обратима, т. е. существует обратная ей матрица T_{ef}^{-1}. Систему (3) можно представить в матричной форме следующим образом

$$f_1, f_2, \dots, f_n \;= (e_1, e_2, \dots, e_n)T_{ef}.$$

Умножив обе части этого равенства справа на T_{ef}^{-1}, получим

$$f_1, f_2, \dots, f_n \;\; T_{ef}^{-1} = (e_1, e_2, \dots, e_n).$$

Откуда следует, что T_{ef}^{-1} является матрицей перехода от базиса (2) к базису (1). Таким образом, матрицы перехода от базиса (1) к базису (2) и от (2) к (1) взаимообратны.

Преобразование координат вектора при переходе от одного базиса пространства к другому

Пусть вектор a имеет следующие разложения по векторам базисов (1) и (2)

$$a = x_1e_1 + x_2e_2 + \dots + x_ne_n \qquad (5)$$

$$a = y_1f_1 + y_2f_2 + \dots + y_nf_n\,. \quad (6)$$

Координатные столбцы вектора а в базисах (1) и (2) будем обозначать соответственно через $a_{\ e}$ и $a_{\ f}$ т. е.

$$a_{\ e} = \begin{matrix} x_1 \\ x_2 \\ \dots \\ x_n \end{matrix} \;; \quad a_{\ f} = \begin{matrix} y_1 \\ y_2 \\ \dots \\ y_n \end{matrix} \;.$$

Теорема 1. *Координатные столбцы вектора* а *в базисах* (1) и (2) *связаны соотношением*

$$a_{\ e} = T_{ef}\; a_{\ f}.$$

15. Линейные операторы конечномерных пространств. Матрица линейного оператора в данном базисе и ее свойства

Свойства линейных операторов. Примеры линейных операторов. Матрица линейного оператора в данном базисе и ее свойства. Изменение матрицы линейного оператора при переходе к другому базису.

Под V мы будем понимать ниже векторное пространство над числовым полем P.

Определение 1. Говорят, что в векторном пространстве V задан оператор, если указано правило (закон), согласно которому всякому вектору пространства V ставится в соответствие другой, причем единственный, вектор того же пространства.

Как следует из определения, оператор пространства есть функция, область определения которой совпадает с V, а область значения – подмножество из V. Операторы пространства называют также преобразованиями этого пространства. В дальнейшем операторы пространства будем обозначать символами φ, ψ, τ...

Если оператор φ пространства V вектору a ставит в соответствие вектор b, то будем писать $\varphi\ \ a\ \ = b$. При этом b будем называть образом вектора a, а вектор a – прообразом вектора b при действии оператора φ.

Определение 2. Оператор φ пространства V называется ***линейным оператором*** этого пространства, если выполняются следующие два условия:

$$1)\ \forall a, b \in V\ \Big|\ \varphi\ \ a + b\ \ = \varphi\ \ a\ \ + \varphi\ \ b\ \ ;$$

$$2)\ \forall a \in V, \forall \alpha \in P\ \Big|\ \varphi\ \ \alpha a\ \ = \alpha\varphi\ \ a\ \ .$$

Условия 1 и 2 приведенного определения равносильны одному следующему:

$$\forall a, b \in V, \forall \alpha, \beta \in P\ \Big|\ \varphi\ \ \alpha a + \beta b\ \ = \alpha\varphi\ \ a\ \ + \beta\varphi\ \ b\ \ .$$

Приведем примеры линейных операторов пространств.

Пример 1. Поставим в соответствие каждому вектору a пространства V нулевой вектор 0 этого пространства. Тем самым мы зададим оператор пространства, который обозначим через θ. Этот оператор является линейным оператором пространства V. Действительно:

$$\forall a, b \in V, \forall \alpha, \beta \in P\ \Big|\ \varphi\ \ \alpha a + \beta b\ \ = 0$$

$$\alpha\varphi\ \ a\ \ + \beta\varphi\ \ b\ \ = \alpha 0 - \beta 0 = 0\ \Rightarrow\ \varphi\ \ \alpha a + \beta b\ \ = \alpha\varphi\ \ a\ \ + \beta\varphi\ \ b\ \ .$$

Оператор θ, который каждый вектор пространства V переводит в нулевой вектор 0, называется нулевым оператором пространства V.

Пример 2. Поставим в соответствие всякому вектору a пространства V этот же вектор a. Заданный оператор φ является линейным оператором пространства, так как

$$\forall a, b \in V, \forall \alpha, \beta \in P \mid \varphi(\alpha a + \beta b) = \alpha a + \beta b = \alpha\varphi(a) + \beta\varphi(b).$$

Оператор пространства V, который всякий вектор пространства оставляет на месте называется единичным или тождественным оператором и обозначается символом ε.

Пример 3. Пусть φ оператор ортогонального проектирования пространства W_3 свободных векторов на плоскость XOY. Известно, что проекция суммы векторов равна сумме проекций этих векторов и проекция произведения вектора на число равна произведению проекции этого вектора на число. Это значит, что для оператора φ в данном случае выполняются условия 1 и 2 из определения 2. Следовательно, φ является линейным оператором пространства W_3.

Пример 4. Пусть $R[x]$ – множество многочленов с действительными коэффициентами степени не больше натурального числа n. Как известно это множество образует векторное пространство над полем действительных чисел R размерности $n+1$, относительно операций сложения многочленов и умножения многочленов на действительные числа. Пусть φ – оператор пространства $R(x)$, который всякому многочлену $f(x)$ ставит в соответствие производную этого многочлена (оператор дифференцирования), т. е. $\varphi(f(x)) = f'(x)$. Этот оператор является линейным оператором пространства $R(x)$, так как

1) $\forall f(x), g(x) \in R[x] \mid \varphi(f(x) + g(x)) = (f(x) + g(x))' = f'(x) +$
$+ g'(x) = \varphi(f(x)) + \varphi(g(x))$;

2) $\forall f(x) \in R[x], \forall \alpha \in P \mid \varphi(\alpha f(x)) = (\alpha f(x))' = \alpha f'(x) =$
$= \alpha\varphi(f(x))$.

Приведем свойства линейных операторов пространства.

Свойство 1. При действии линейного оператора φ пространства V нулевой вектор 0 отображается в себя, т. е. $\varphi(0) = 0$.

Свойство 2. При действии линейного оператора φ пространства V образ вектора противоположного вектору a равен противоположному образа этого вектора, т. е.

$$\forall a \in V \mid \varphi(-a) = -\varphi a.$$

Свойство 3. При действии линейного оператора φ пространства V всякая линейная комбинация векторов из V отображается в линейную комбинацию образов этих векторов с теми же коэффициентами, т. е.

$$\forall a_1, a_2, \dots, a_k \in V, \forall \alpha_1, \alpha_2, \dots, \alpha_k \in P$$

$$\varphi(\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_k a_k) = \alpha_1\varphi(a_1) + \alpha_2\varphi(a_2) + \dots + \alpha_k\varphi(a_k).$$

Под V_n ниже мы будем понимать n-мерное векторное пространство над полем P.

Задать линейный оператор пространства – это значит указать при необходимости образ любого вектора пространства при действии этого оператора. Оказывается, чтобы найти образ любого вектора пространства достаточно знать образы векторов произвольного базиса $e_1, e_2, \ldots, e_n$ пространства V_n при действии оператора φ.

Теорема. Пусть $e_1, e_2, \ldots, e_n$ – базис пространства V_n**.** Какова бы ни была система векторов $b_1, b_2, \ldots, b_n$ существует, причем единственный, линейный оператор φ пространства V_n**,** такой что $\varphi\ a_1 = b_1; \varphi\ a_2 = = b_2; \ldots; \varphi\ a_n = b_n$.

Следствие. Всякий линейный оператор φ пространства V_n вполне определяется отображением произвольного, но фиксированного базиса пространства, т. е. зная образы векторов фиксированного базиса, можно указать образ любого вектора пространства при действии оператора φ.

Матрица линейного оператора

Пусть φ – линейный оператор пространства V_n и $e_1, e_2, \ldots, e_n$ – базис этого пространства. Разложим образы $\varphi(e_1), \varphi(e_2), \ldots, \varphi(e_n)$ по векторам заданного базиса:

$$\begin{matrix} \varphi\ e_1 = a_{11}e_1 + a_{21}e_2 + \ldots + a_{n1}e_n \\ \varphi\ e_2 = a_{12}e_1 + a_{22}e_2 + \ldots + a_{n2}e_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \varphi\ e_n = a_{1n}e_1 + a_{2n}e_2 + \ldots + a_{nn}e_n \end{matrix} \quad (1)$$

Из координат полученных разложений составим матрицу:

$$A = \begin{matrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{matrix} .$$

Полученная матрица A называется *матрицей оператора φ в базисе* $e_1, e_2, \ldots, e_n$. Столбцы матрицы представляют собой координатные столбцы образов базисных векторов в этом же базисе. Так как координаты вектора в заданном базисе определяются однозначно, то каждому линейному оператору φ пространства V_n однозначно соответствует матрица этого оператора в заданном базисе.

Обратно: Всякая квадратная матрица $A = a_{ij}$ порядка n над полем P равенствами системы (1) однозначно определяет образы векторов базиса, и, следовательно, согласно теореме о единственности линейного оператора однозначно задает некоторый линейный оператор φ пространства V_n. Таким образом, между множеством линейных операторов пространства V_n и множеством квадратных матриц порядка n над полем P можно установить взаимно однозначное соответствие.

Пример. Найти матрицу линейного оператора $A\ x_1, x_2, x_3 = = (x_1, 2x_2, 3x_3)$.

$$\begin{aligned} \varphi(e_1) &= \varphi(1,0,0) = (1,0,0) \\ \varphi(e_2) &= \varphi(0,1,0) = (0,2,0) \\ \varphi(e_3) &= \varphi(0,0,1) = (0,0,3) \end{aligned} \quad \Rightarrow \quad A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Пусть φ — линейный оператор пространства V_n, который в базисе $e_1, e_2, \dots, e_n$ имеет матрицу

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Рассмотрим, как связаны между собой векторы a и $\varphi(a)$. Пусть векторы a и $\varphi(a)$ имеют следующие разложения по векторам базиса

$$a = x_1e_1 + x_2e_2 + \dots + x_ne_n \qquad (2)$$

$$\varphi(a) = y_1e_1 + y_2e_2 + \dots + y_ne_n. \qquad (3)$$

Подействуем оператором φ на обе части равенства (1)

$$\varphi(a) = x_1\varphi(e_1) + x_2\varphi(e_2) + \dots + x_n\varphi(e_n). \qquad (4)$$

Выполним подстановку из системы (1) в равенство (4)

$$\varphi(a) = x_1(a_{11}e_1 + a_{21}e_2 + a_{n1}e_n) + x_2(a_{12}e_1 + a_{22}e_2 + a_{n2}e_n) + \dots +$$
$$+x_n(a_{1n}e_1 + a_{2n}e_2 + a_{nn}e_n) = e_1(x_1a_{21} + x_2a_{22} + \dots + x_na_{2n}) +$$
$$+e_2(x_1a_{11} + x_2a_{12} + \dots + x_na_{1n}) + \dots + e_n(x_1a_{n1} + x_2a_{n2} + \dots + x_na_{nn}). \qquad (5)$$

Координаты всякого вектора в заданном базисе определяются однозначно. Сопоставив равенство (3) и (5), находим

$$\begin{cases} y_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n \\ y_2 = a_{12}x_1 + a_{22}x_2 + \dots + a_{2n}x_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ y_n = a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n \end{cases} \qquad (6)$$

Система (6) выражает связь между векторами a и $\varphi(a)$. В матричной форме это запишется

$$\begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} \quad \text{или} \quad [\varphi(a)] = A[a], \qquad (7)$$

где $[\varphi(a)]$ и $[a]$ — координатные столбцы векторов $\varphi(a)$ и a.

16. Собственные векторы и собственные значения линейных операторов

Характеристический многочлен матрицы и линейного оператора. Свойства собственных векторов линейного оператора. Матрица линейного оператора в базисе из собственных векторов. Критерий диагонализуемости матрицы линейного оператора.

Определение 1. Ненулевой вектор $a \in V_n$ называется ***собственным вектором оператора φ,*** если имеет место равенство $\varphi\ a\ = \lambda a$ при некотором $\lambda \in C$. В этом случае λ называют ***собственным значением оператора φ,*** соответствующим собственному вектору a.

Свойства собственных векторов линейных операторов:

1. Всякий собственный вектор a оператора φ соответствует только одному собственному значению.

2. Пусть a и b – собственные векторы оператора φ, соответствующие одному и тому же собственному значению λ, тогда сумма этих векторов $a + b$ также является собственным вектором, соответствующим собственному значению λ.

3. Пусть a является собственным вектором оператора φ, соответствующим собственному значению λ, тогда $\forall \alpha \in P, \alpha \neq 0\ \alpha a$ также является собственным вектором, соответствующим собственному значению λ.

Следствие. Всякая ненулевая линейная комбинация собственных векторов оператора φ, соответствующих одному и тому же собственному значению λ, также является собственным вектором оператора, соответствующим собственному значению λ.

Теорема 2. Собственные векторы $a_1, a_2, \dots, a_n$ (1), соответствующие попарно различным собственным значениям $\lambda_1, \lambda_2, \dots, \lambda_n$, образуют линейно независимую систему.

Характеристический многочлен линейного оператора

Собственные векторы и собственные значения играют весьма существенную роль при исследовании структуры линейного отображения. Поэтому естественным является вопрос о способе их нахождения. Такой способ будет указан ниже.

Предположим, что зафиксирован некоторый базис $a_1, a_2, \dots, a_n$ пространства V_n и что отображение φ задано в этом базисе матрицей

$$A = \begin{matrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{matrix}.$$

Если, как обычно, координаты вектора x обозначить $x_1, x_2, \ldots, x_n$, то векторное равенство $\varphi\ x\ = \lambda x$ будет равносильно следующим x соотношениям:

$$\begin{array}{c} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = \lambda x_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = \lambda x_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = \lambda x_n \end{array}.$$

После приведения подобных членов получаем:

$$\begin{array}{c} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = \lambda x_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = \lambda x_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n = \lambda x_n \end{array}. \qquad (2)$$

Рассматривая данную систему равенств как систему из n линейных однородных уравнений с n неизвестными $x_1, x_2, \ldots, x_n$, мы можем теперь сказать, что координаты любого собственного вектора, отвечающего собственному значению λ, удовлетворяют системе (2). Следовательно, для всякого собственного значения λ система (2) должна допускать *ненулевое* решение. Отсюда вытекает, что определитель этой системы должен быть равен нулю. Таким образом, любое собственное значение λ должно удовлетворять условию

$$. \quad \begin{vmatrix} a_{11}-\lambda & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22}-\lambda & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn}-\lambda \end{vmatrix} = 0 \qquad (3)$$

Обратно, если какое-то число λ из поля P удовлетворяет этому условию, то это число является собственным значением: действительно, тогда система (2) будет иметь ненулевое решение $x_1, x_2, \ldots, x_n$, т. е. найдется ненулевой вектор x, такой, что $\varphi\ x\ = \lambda x$.

Раскрывая определитель, стоящий в левой части равенства (3), мы получим, очевидно, многочлен n-й степени относительно λ. Его называют ***характеристическим многочленом линейного оператора φ, а также матрицы A.*** Следовательно, условие (3) представляет собой алгебраическое уравнение n-й степени относительно λ. Это уравнение называется ***характеристическим уравнением матрицы A.***

Итак, *собственными значениями отображения φ являются те и только те числа λ из поля P, которые служат корнями характеристического уравнения (3). Для любого собственного значения λ соответствующие ему собственные векторы x составляют множество всех ненулевых решений системы* (2).

Возвращаясь к характеристическому уравнению (3), заметим, что определитель в левой части (3) является определителем матрицы $A - \lambda E$,

где E – единичная матрица порядка n. Поэтому характеристическое уравнение можно представить в следующей матричной записи:
$A-\lambda E \ = 0.$ (4)
Пользуясь формой (4) характеристического уравнения, легко доказать следующее предложение: *если матрицы A и A' подобны, то их характеристические уравнения совпадают.* Действительно, по определению подобия матриц найдется такая невырожденная матрица T, что $A' = T^{-1}AT$.

Отсюда получаем

$$A' - \lambda E \ = \ T^{-1}AT - T^{-1} \ \lambda E \ T \ = \ T^{-1} \ A - \lambda E \ T \ = \ T^{-1} \ \cdot \ A - \lambda E \ \cdot$$
$$\cdot \ T \ = \ A - \lambda E \ .$$

Мы воспользовались в процессе преобразований теоремой об определителе произведения нескольких матриц, из которой, в частности, следует, что

$$T^{-1} \ \cdot \ A - \lambda E \ \cdot \ T \ = \ E \ = 1.$$

Так как при переходе от данного базиса к другому матрица отображения задается подобной матрицей, то из только что доказанного предложения вытекает, что характеристическое уравнение матрицы линейного отображения не меняется при переходе к новому базису. В связи с этим мы можем просто говорить о *характеристическом уравнении отображения,* не указывая конкретно матрицы, которой это отображение задается в том или ином базисе**.**

Линейные операторы с простым спектром

Линейное отображение может быть задано разными способами. Одна из возможных форм задания – с помощью матрицы, отвечающей отображению в том или другом базисе. Все свойства отображения можно в принципе «извлечь» из его матрицы. Естественно ожидать, что, чем проще матрица данного отображения, тем легче изучать свойства этого отображения.

Один из наиболее простых классов матриц составляют так называемые *диагональные матрицы,* т. е. квадратные матрицы вида:

$$\begin{matrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_m \end{matrix} \qquad (5)$$

(все элементы вне главной диагонали равны нулю). Представляет интерес следующая задача: охарактеризовать линейные отображения, матрицы которых при некотором выборе базиса являются диагональными. Относительно таких отображений принято говорить, что их матрицы ***приводятся к диагональной форме.*** В этом пункте мы выясним, при каких условиях матрица отображения приводится к диагональной форме.

Пусть отображение φ имеет в базисе $a_1, a_2, \ldots., a_n$ диагональную матрицу (5). По определению матрицы отображения (5) имеем:

$$(\varphi\ a_1\ \ \varphi(a_2)\ \ldots.\varphi(a_n)) = (a_1, a_2, \ldots., a_n)\ \begin{matrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \lambda_m \end{matrix}\ , \qquad (6)$$

что равносильно равенствам:

$$\varphi\ a_1\ = \lambda_1 a_1, \varphi\ a_2\ = \lambda_2 a_2, \ldots, \varphi\ a_n\ = \lambda_n a_n. \qquad (7)$$

Но равенства (7) означают, что базис $a_1, a_2, \ldots., a_n$ состоит из собственных векторов отображения φ.

Обратно, если какой-либо базис $a_1, a_2, \ldots., a_n$ состоит из собственных векторов отображения $\boldsymbol{\varphi}$, то выполняются равенства (7), а значит, и равенство (6). Следовательно, матрица отображения φ в этом базисе диагональная.

Итак, *матрица отображения φ в некотором базисе тогда и только тогда является диагональной, когда этот базис состоит из собственных векторов отображения φ.*

Определение 2. Линейный оператор φ векторного пространства V_n над полем P называется ***оператором с простым спектром***, если он имеет n попарно различных собственных значений; набор всех собственных значений оператора называется *спектром оператора.*

Теорема 3. Если φ — оператор с простым спектром пространства V_n, то существует базис пространства, составленный из собственных векторов оператора. В этом базисе матрица оператора φ имеет диагональный вид:

$$A = \begin{matrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \lambda_n \end{matrix}\ ,$$

где $\lambda_1, \lambda_2, \ldots, \lambda_n$ – собственные значения оператора φ.

Определение 3. Говорят, что квадратная матрица A над полем P ***приводится к диагональному виду***, если она подобна некоторой диагональной матрице над этим полем.

Теорема 4. Квадратная матрица A порядка n над полем P тогда и только тогда приводится к диагональному виду, когда существует базис $e_1, e_2, \ldots, e_n$ пространства V_n, составленный из собственных векторов матрицы A.

Теорема 5. Если матрица A порядка n над полем P имеет n попарно различных собственных значений, то она приводится к диагональному виду.

17. Изоморфизм линейных пространств

Понятие изоморфизма линейных пространств. Свойства изоморфных пространств. Критерий изоморфности конечномерных пространств.

Определение 1. *Векторные пространства V и V' над одним и тем же полем P называются изоморфными, если между множествами V и V' можно установить такое взаимооднозначное соответствие φ, при котором будут выполняться условия:*

1) $\forall a, b \in V \,|\, \varphi(a + b) = \varphi(a) + \varphi(b)$;

2) $\forall a \in V \,|\, \varphi(\alpha a) = \alpha\varphi(a)$.

Если пространства V и V' изоморфны, то пишут $V \cong V'$. Взаимооднозначное соответствие φ между V и V', удовлетворяющее условиям 1 и 2 приведенного определения, называется изоморфизмом пространств V и V'.

Приведем свойства изоморфизмов пространств.

Свойство 1. *При изоморфизме φ пространств V и V' нулевой вектор пространства V отображается в нулевой вектор пространства V', то есть $\varphi\ 0\ = 0'$.*

Свойство 2. *При изоморфизме φ пространств V и V' всякая линейно независимая система векторов пространства V переходит в линейно независимую систему векторов пространства V'.*

Свойство 3. $\forall a \in V \,|\, \varphi(-a) = -\varphi(a)$.

Свойство 4. При изоморфизме пространств V и V' базис пространства V отображается в базис пространства V'.

Теорема 1. *Векторные пространства V и V' над одним и тем же полем P изоморфны тогда и только тогда, когда они имеют одинаковую размерность.*

Согласно приведенной теореме, наиболее существенной характеристикой векторного пространства является его размерность. В частности, все n-мерные векторные пространства над полем P изоморфны арифметическому n-мерному векторному пространству P_n. Это значит, что, изучая пространство P_n, мы можем иметь полную информацию о свойствах других n-мерных векторных пространств над полем P относительно определенных в них операций.

18. Евклидовы пространства

Скалярное произведение. Евклидовы пространства. Свойства евклидовых пространств. Норма вектора и ее свойства. Неравенство Коши-Буняковского. Угол между векторами в евклидовом пространстве. Ортогональные векторы.

Мы будем рассматривать действительные векторные пространства, т. е. пространства над полем действительных чисел R. В действительном векторном пространстве аксиоматически вводится понятие скалярного произведения векторов, которое в свою очередь дает возможность определить понятия длины вектора и угла между векторами. В качестве аксиом скалярного произведения векторов выступают известные свойства скалярного произведения геометрических векторов.

Определение 1. Действительное векторное пространства E называется ***евклидовым***, если всякой паре векторов a и b из E. Поставлено в соответствие действительное число a, b, называемое скалярным произведением векторов a и b, и при этом выполняются следующие условия (аксиомы скалярного произведения):

1) $\forall a, b \in E \mid \; a, b \; = (b, a)$;

2) $\forall a, b \in E, \forall \alpha \in R \mid \; \alpha a, b \; = \alpha(a, b)$;

3) $\forall a, b, c \in E \mid \; a + b, c \; = \; a, c \; + (b, c)$;

4) $\forall a \in E \mid a \neq 0 \Rightarrow \; a, a \; > 0$.

Евклидово пространство размерности n будем обозначать символом E_n.

Приведем простейшие свойства скалярного произведения векторов, вытекающие из определения.

Свойство 1. $\forall a, b \in E, \forall \alpha, \beta \in R \mid \; \alpha a, \beta b \; = \alpha\beta(a, b)$.

Свойство 2. $\forall a, b, c \in E \mid \; a, b + c \; = \; a, b \; + (a, c)$.

Свойство 3. $\forall a \in E \mid \; 0, a \; = 0$. В частности $(0, 0) = 0$.

Пример 1. Скалярное произведение векторов a и b пространства W_3 свободных векторов, определенное как произведение длин этих векторов на косинус угла между ними, очевидно, удовлетворяет условиям 1)–4) приведенного выше определения. Поэтому пространство W_3 является евклидовым пространством в смысле этого определения.

Пример 2. В арифметическом n-мерном векторном пространстве R_n скалярное произведение векторов

$$a = \; \alpha_1, \alpha_2, \ldots, \alpha_n \; \text{ и } b = \; \beta_1, \beta_2, \ldots, \beta_n$$

определим как сумму произведений соответствующих координат этих векторов, т. е. $a, b \; = \alpha_1\beta_1 + \alpha_2\beta_2 + \ldots + \alpha_n\beta_n$. Можно убедиться, что введенное таким образом понятие скалярного произведения в пространстве R_n удовлетворяет условиям 1)–4) определения, приведенного выше. Поэтому при введении этого понятия пространство R_n становится евклидовым пространством размерности n.

Используя понятие скалярного произведения векторов, введем далее в евклидовом пространстве E понятия длины вектора и угла между векторами.

Определение 2. Длиной вектора а пространства E называется неотрицательное значение квадратного корня из числа (a, a).

Длина вектора а обозначается символом a. Таким образом, согласно определению $a \; = \; \overline{(a, a)}$.

Так как согласно аксиоме 4 и свойству 3 для всякого вектора a из E выполняется условие $(a, a) \leq 0$, то приведенное определение длины вектора является корректным.

Приведем свойства длины вектора.

Свойство 4. $a \; = 0 \; \Leftrightarrow a = 0$.

Свойство 5. $\forall a \in E, \forall \alpha \in R \,\Big|\; \alpha a \; = \; \alpha \; \cdot \; a$.

Теорема 1 (Неравенство Коши-Буняковского).

$$\forall a, b \in E \,\Big|\; (a, b) \; \leq \; a \; \cdot \; b \; .$$

Определение 3. Углом между векторами $a \; \neq \; 0$ и $b \; \neq \; 0$ евклидова пространства E называется число φ такое, что $\cos \varphi = \frac{(a,b)}{a \, \cdot \, b}$, $0 \leq \varphi \leq \pi$.

Так как из теоремы 1 следуют неравенства $-1 \leq \frac{(a,b)}{a \, \cdot \, b} \leq 1$ для любых ненулевых векторов a и b, то угол между ними всегда определен.

Ортогональные векторы. Процесс ортогонализации

Определение 4. Векторы a и b пространства E, называются ***ортогональными***, если их скалярное произведение равно нулю, т. е. если $a, b \; = 0$.

Очевидно, что ненулевые вектора a и b тогда и только тогда ортогональны, когда угол между ними равен $\frac{\pi}{2}$. Нулевой вектор 0 всегда ортогонален к любому вектору пространства E.

Теорема 2. Пусть вектор a ортогонален к каждому из векторов $b_1, b_2, \ldots, b_k$. Тогда a ортогонален к любой линейной комбинации этих векторов.

Определение 5. Система векторов $a_1, a_2, \ldots, a_k$ пространства E называется ***ортогональной***, если любые два вектора этой системы ортогональны.

Теорема 3. Всякая ортогональная система $a_1, a_2, \ldots, a_k$ ненулевых векторов линейно независима.

Следствие. Всякая ортогональная система из n ненулевых векторов пространства E_n образует базис этого пространства.

Определение 6. Ортогональная система векторов образующая базис пространства E_n называется ортогональным базисом этого пространства.

Ниже будет доказано, что всякое пространство E_n обладает ортогональным базисом. Предварительно опишем способ построения исходя из заданной системы векторов

$$a_1, a_2, \dots, a_k \tag{3}$$

Соответствующей ей ортогональной системе ненулевых векторов

$$b_1, b_2, \dots, b_k \tag{4}$$

Этот способ называют процессом ортогонализации.

Примем $b_1 = a_1$. Вектор b_2 будем искать в виде $b_2 = a_2 - \lambda a_1$, где число λ определим исходя из условия ортогональности векторов b_1 и b_2.

$$b_1\,, b_2 \;=\; a_2 - \lambda b_1, a_1 \;=\; a_2, a_1 \; - \lambda(a_1, a_1) = 0.$$

Откуда

$$\lambda = \frac{a_2, a_1}{(a_1, a_1)}.$$

Построенный вектор $b_2 = a_2 - \lambda a_1$ ненулевой, в противном случае векторы a_1 и a_2 были бы линейно зависимы, а следовательно, была линейно зависима и система (3), что противоречит выбору.

Пусть уже построена ортогональная система из $m\,(m < k)$ ненулевых векторов

$$b_1, b_2, \dots, b_m\,.$$

Следующий вектор b_{m+1} ищем в виде

$$b_{m+1} = a_{m+1} - \lambda_1 b_1 - \lambda_2 b_2 - \dots - \lambda_m b_m\,. \tag{5}$$

Коэффициенты $\lambda_1, \lambda_2, \dots, \lambda_m$ находим из условия ортогональности вектора b_{m+1} к векторам $b_1, b_2, \dots, b_m$

$$\lambda_1 = \frac{(a_{m+1}, b_1)}{(b_1, b_1)}; \quad \lambda_2 = \frac{(a_{m+1}, b_2)}{(b_2, b_2)}; \quad \dots; \quad \lambda_m = \frac{(a_{m+1}, b_m)}{(b_m, b_m)}\,.$$

Построенный таким образом вектор b_{m+1} является ненулевым, в противном случае, из равенства (5) следовало бы, что вектор a_{m+1} линейно выражается через векторы $b_1, b_2, \dots, b_m$, а следовательно, и через векторы $a_1, a_2, \dots, a_m$, что невозможно.

Этот процесс продолжается до тех пор, пока не найдем последний ненулевой вектор

$$b_k = a_k - \gamma_1 b_1 - \gamma_2 b_2 - \dots - \gamma_{k-1} b_{k-1},$$

где $\gamma_1 = \frac{a_k,\, b_1}{b_1,\;\, b_1}$, $\gamma_2 = \frac{a_k,\, b_2}{b_2,\;\, b_2}$, ..., $\gamma_{k-1} = \frac{a_k,\, b_{k-1}}{b_1, b_{k-1}}$.

В результате получим ортогональную систему ненулевых векторов

$$b_1, b_2, \dots, b_m.$$

Теорема 4. Всякое евклидово пространство E_n обладает ортогональным базисом.

Определение 7. Вектор a пространства E_n называется ***нормированным*** или ***ортом***, если его длина равна единице.

Для всякого ненулевого вектора a пространства E_n существует ***коллинеарный*** ему нормированный вектор, и именно вектор $e = \frac{1}{a} a$.

Определение 8. Ортонормированным базисом пространства E_n называется ортогональный базис этого пространства, состоящий из нормированных векторов.

Очевидно, что всякое евклидово пространство E_n обладает ортонормированным базисом.

Теорема 5. Базис $e_1, e_2, \ldots, e_n$ пространства E_n тогда и только тогда является ортонормированным, когда скалярное произведение любых векторов $a, b \in E_n$ равно сумме произведений соответствующих координат векторов a и b в этом базисе.

19. Кольцо полиномов от одной переменной

Определение полинома от одной переменной над кольцом. Сложение и умножение полиномов. Кольцо полиномов. Стандартная запись полиномов. Степень полинома и ее свойства.

Под K ниже мы будем понимать область целостности с единицей, то есть K – это кольцо, которое содержит единичный элемент 1 и $\forall a, b \in K \mid ab = 0 \Leftrightarrow a = 0 \vee b = 0$.

Определение* 1. *Многочленом *от одной переменной над областью целостности К называется выражение вида:*

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{1}$$

где $a_n, a_{n-1}, \dots, a_1, a_0$ *– элементы из К, которые называют коэффициентами многочлена, n – произвольное целое неотрицательное число,* x *– символ, называемый переменной или неизвестной*.

Выражение x^k ($k = \overline{0, n}$ в (1) будем называть n-ой степенью переменной x, а выражение $a_k x^k$ – членом k-ой степени многочлена (1).

Полагается, что $x^1 = x,\ x^0 = 1, 1 \cdot x = x$.

Согласно приведенному определению всякий многочлен от одной переменной есть формальное выражение, которое полностью определяется своими коэффициентами.

Для сокращения записей многочлены от одной переменной будем обозначать символами $f(x), g(x), \dots, h(x), \dots$.

Множество всех многочленов от одной переменной x над областью целостности K будем обозначать через $K[x]$.

***Определение* 2.** *Два многочлена* $f(x)$ *и* $g(x)$ *из множества* $K[x]$ *называют равными, если они состоят из одних и тех же членов без учета членов с нулевыми коэффициентами.*

Согласно приведенному определению, если опустить члены с нулевыми коэффициентами, то в результате получим многочлен, равный исходному. Тогда многочленами от одной переменной над областью целостности K являются следующие выражения: $x = 1 \cdot x^1, x^k = 1 \cdot x^k, ax^k$, $a = ax^0$, где $a \in K$.

По определению 2 всякий многочлен $f(x) \in K[x]$ определяется только составом своих членов с ненулевыми коэффициентами. Отсюда следует, что при изменении порядка следования членов в многочлене (1) получается многочлен, равный исходному. В частности, всякий многочлен $f(x) \in K[x]$ можно записывать в порядке возрастания степеней его членов, то есть в виде

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n.$$

Из определения 2 также следует, что многочлен $f(x) \in K[x]$ тогда и только тогда равен нулю, когда все его коэффициенты равны нулю.

***Определение* 3.** *Степенью многочлена $f(x) \in K[x]$ называется наибольшая из степеней его членов с ненулевыми коэффициентами.*

Член многочлена $f(x)$, по которому определяется его степень, *называется старшим членом*, а его коэффициент – *старшим коэффициентом многочлена $f(x)$*.

По определению 3 всякий элемент $a \in K$, отличный от нуля, является многочленом нулевой степени из $K[x]$. Для нулевого многочлена, то есть нулевого элемента из *К*, степень не определена.

Введем операции сложения и умножения на множестве $K[x]$.

Пусть даны многочлены

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \qquad (2)$$

из множества $K[x]$, степени которых равны n и m соответственно. Для определенности будем считать, что $n \geq m$.

***Определение* 4.** *Суммой многочленов $f(x)$ и $g(x)$ называется многочлен*

$$f(x) + g(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0, \qquad (3)$$

где $c_k = a_k + b_k$ при $k \leq m$ и $c_k = a_k$ при $k > m$ $\quad k = 1, n$.

Очевидно, что степень суммы многочленов не больше максимальной из степеней слагаемых многочленов.

***Определение* 5.** *Произведением многочленов $f(x)$ и $g(x)$ называется многочлен*

$$f\ x\ g\ x\ = a_n b_m x^{n+m} + \ a_n b_{m-1} + a_{n-1} b_m\ x^{m+n-1} +$$
$$+\ a_n b_{m-2} + a_{n-1} b_{m-1} + a_{n-2} b_m\ x^{m+n-2} + \cdots +\ a_1 b_0 + a_0 b_1\ x +$$
$$+a_0 b_0. \qquad (4)$$

***Теорема* 1.** *Степень произведения многочленов f(x) и g(x) равна сумме степеней этих многочленов.*

Очевидно, что сумма и произведение многочленов *f(x)g(x)* из *K[x]* также являются многочленами из этого множества и определяются однозначно. Это значит, что операции сложения и умножения многочленов являются алгебраическими на множестве *K[x]*.

***Теорема* 2.** *Множество $K[x]$ многочленов от одной переменной над областью целостности К также образуют область целостности относительно операций сложения и умножения многочленов.*

20. Наибольший общий делитель двух полиномов и алгоритм Евклида

Делимость в кольце полиномов. Деление с остатком. Наибольший общий делитель полиномов. Алгоритм Евклида. Линейное выражение наибольшего общего делителя.

Пусть P – произвольное поле. Так как всякое поле является областью целостности, то все изложенное выше для многочленов из $K[x]$ справедливо также и для многочленов из кольца $P[x]$, то есть многочленов от одной переменной над полем P. Ниже мы будем рассматривать только многочлены из кольца $P[x]$.

Определение* 1.** *Говорят, что многочлен f(x)* ***делится на *многочлен g(x), если в кольце $P[x]$ найдется такой многочлен $q(x)$, что*

$$f(x) = g(x) \cdot q(x). \tag{1}$$

Если $f(x)$ делится на $g(x)$, то пишут: $f(x) \vdots g(x)$ (читается: "$f(x)$ делится на $g(x)$"), либо $g(x) \,\big|\, f(x)$ (читается: "$g(x)$ делит $f(x)$"). $f(x)$ называют ***делимым***, $g(x)$ – делителем, и $q(x)$ – частным от деления $f(x)$ на $g(x)$. Приведем основные свойства отношения делимости в кольце $P[x]$.

Свойство 1. Всякий многочлен $f(x)$ делится на себя, то есть

$$\forall f\ \ x\ \ \in P\ \ x\ \big|\ f\ \ x\ \ \vdots\ f\ \ x\ .$$

Свойство 2. $\forall f\ \ x\ ,g\ \ x\ ,h\ \ x\ \ \in P\ \ x\ \ \big|\ f\ \ x\ \ \vdots\ g\ \ x\ \wedge g\ \ x\ \ \vdots\ h\ \ x\ \Rightarrow$
$\Rightarrow\ f(x) \vdots h(x)$.

Свойство 3. $\forall f\ \ x\ ,g\ \ x\ ,h\ \ x\ \ \in P\ \ x\ \ \big|\ f\ \ x\ \ \vdots\ g\ \ x\ \wedge\ g\ \ x\ \ \vdots\ h\ \ x\ \Rightarrow$
$\Rightarrow (f(x) \pm\ g(x)) \vdots h(x)$.

Свойство 4 $.\forall f\ \ x\ ,g\ \ x\ ,h\ \ x\ \ \in P\ \ x\ \ \big|\ f\ \ x\ \ \vdots\ h\ \ x\ \Rightarrow$
$\Rightarrow f(x)g(x) \vdots h(x)$.

Свойство 5. $\forall f\ \ x\ \ \in P\ \ x\ \ \big|\ 0 \vdots f(x)$.

Свойство 6. $\forall f\ \ x\ \ \in P\ \ x\ ,\forall \alpha \in P\ \big|\ a \neq\ 0\ \Rightarrow\ f(x) \vdots a$.

Свойство 7. Пусть слагаемые $f_1, f_2, \ldots, f_{k-1}$ суммы многочленов $f\ = f_1 +\ f_2 +\ \ldots + f_{k-1} + f_k$ делятся на $g(x)$, а f_k не делится на $g(x)$, тогда сумма f не делится на $g(x)$.

Определение* 2.** *Многочлены $f(x)$ и $g(x)$ из кольца $P[x]$ называются* ***ассоциированными*, если $f(x) \vdots g(x)$ и $g(x) \vdots f(x)$.*

Теорема 1. *Многочлены f(x) и g(x) тогда и только тогда ассоциированы, когда они либо совпадают, либо отличаются только множителем нулевой степени, то есть $f\ \ x\ \ = ag(x)$.*

Деление с остатком

Будем полагать, что все многочлены, о которых будет идти речь ниже, принадлежат кольцу $P[x]$.

Определение* 3.** *Говорят, что произведено* ***деление с остатком *многочлена $f(x)$ на многочлен $g(x)$, если найдены такие многочлены $q(x)$ и $r(x)$ из кольца $P[x]$***,*** *что*

$$f(x) = g(x)q(x) + r(x).$$

При этом многочлен $r(x)$ либо равен нулю, либо его степень меньше степени многочлена $g(x)$. В этом случае $q(x)$ называют неполным частным или просто частным, а $r(x)$ – остатком от деления $f(x)$ на $g(x)$.

Теорема 2. *Каковы бы ни были многочлены $f(x)$ и $g(x) \neq 0$, всегда возможно деление с остатком $f(x)$ на $g(x)$. Частное $q(x)$ и остаток $r(x)$ при этом определяются однозначно.*

Определение 4. *Многочлен $d(x)$ называется* ***общим делителем*** *многочленов*

$$f_1(x), f_2(x), \dots, f_n(x) \tag{2}$$

если он делит каждый из этих многочленов. Общий делитель $d(x)$ многочленов (2) *называется* ***наибольшим общим делителем*** *этих многочленов, если он делится на любой их общий делитель.*

Теорема 3. *Наибольший общий делитель многочленов* (2) *определяется однозначно с точностью до множителя нулевой степени.*

В дальнейшем наибольший общий делитель многочленов $f_1(x), f_2(x), \dots, f_n(x)$ будем обозначать через $f_1(x), f_2(x), \dots, f_n(x)$.

Далее мы опишем так называемый ***алгоритм Евклида***, который доказывает существование наибольшего общего делителя для любых двух многочленов $f(x)$ и $g(x) \neq 0$, а именно дает способ его отыскания для таких многочленов.

Предварительно приведем две леммы.

Лемма 1. Пусть $f(x) \vdots g(x)$, тогда $(f(x), g(x)) = g(x)$.

Лемма 2. Пусть $f\ x\ = g\ x\ \cdot q\ x\ + r\ x$, тогда $f\ x\ , g\ x\ =$ $= (g(x), r(x))$.

Алгоритм Евклида заключается в следующем.

Делим вначале $f(x)$ на $g(x)$ с остатком. Получим равенство

$$f(x) = g(x) \cdot q_1(x) + r_1(x),$$

где либо $r_1\ x\ = 0$, либо степень $r_1(x)$ меньше степени $g(x)$. Если $r_1(x) \neq 0$, то далее делим $g(x)$ на $r_1(x)$с остатком. Получим

$$g(x) = r_1(x) \cdot q_2(x) + r_2(x),$$

где либо $r_2(x) = 0$, либо степень $r_2(x)$ меньше степени $r_1(x)$.

При $r_2(x) \neq 0$ делим $r_1(x)$ на $r_2(x)$ с остатком

$$r_1\ x\ = r_2\ x\ \cdot q_3\ x\ + r_3\ x\ .$$

Здесь либо $r_3\ x\ = 0$, либо степень $r_3\ x$ меньше степени $r_2(x)$ и т. д.

В процессе последовательного деления степени получаемых остатков $r_1\ x\ ,\ r_2\ x\ , r_3\ x\ , \ldots$ убывают, оставаясь целыми неотрицательными числами. Поэтому этот процесс не может продолжаться бесконечно, то есть на каком-то s-ом шаге мы получим в остатке $r_s\ x$, который далее разделит $r_{s-1}\ x$ без остатка. Покажем, что $r_s\ x =$ $= (f(x), g(x))$. Для этого запишем весь процесс последовательного деления в виде системы равенств:

$$\begin{aligned}
&f(x) = g(x) \cdot q_1(x) + r_1(x);\\
&g(x) = r_1(x) \cdot q_2(x) + r_2(x);\\
&r_1\ x\ = r_2\ x\ \cdot q_3\ x\ + r_3\ x\ ;\\
&\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots;\\
&r_{s-2}\ x\ = r_{s-1}\ x\ \cdot q_s\ x\ + r_s\ x\ ;\\
&r_s\ x\ = r_s\ x\ \cdot q_{s-1}\ x\ ;\\
&r_{s-1}\ x\ = r_s\ x\ \cdot q_{s+1}\ x\ .
\end{aligned} \qquad (3)$$

По лемме 2 из 1-го, 2-го и т. д. равенств системы (3) соответственно получим

$$\begin{aligned}
&(f(x), g(x)) = (g(x), r_1(x))\\
&(g(x), r_1(x)) = (r_1(x), r_2(x))\\
&(r_1(x), r_2(x)) = (r_2(x)), r_3(x))\\
&\ldots \ldots \ldots \ldots \ldots \ldots \ldots \ldots\\
&(r_{s-2}(x), r_{s-1}(x)) = (r_{s-1}(x)), r_s(x)).
\end{aligned} \qquad (4)$$

Наконец, по лемме 1 из последнего равенства системы следует:

$$(r_{s-1}(x)), r_s(x)) = r_s(x). \qquad (5)$$

Теперь из (4) и (5) непосредственно вытекает, что

$$(f(x), g(x)) = r_s(x).$$

Описанный процесс последовательного деления и называется ***алгоритмом Евклида***. Таким образом, нами доказано, что $(f(x), g(x))$ существует и он равен последнему остатку, отличному от нуля, алгоритма Евклида, примененного к многочленам $f(x)$ и $g(x)$. Очевидно, что $(f(x), g(x)) \in P[x]$.

Теорема 4 (свойство линейности НОД многочленов). *Пусть* $d(x) = (f(x), g(x))$, *тогда существуют такие многочлены* $\varphi(x)$ *и* $\psi(x)$ *в кольце* $P[x]$, *что*

$$f(x) \cdot \varphi(x) + g(x) \cdot \psi(x) = d(x). \qquad (6)$$

Представление $d(x) = (f(x), g(x))$ в виде равенства (6) называется ***линейным представлением*** наибольшего общего делителя многочленов $f(x)$ и $g(x)$.

21. Деление полинома на двучлен (х-а). Схема Горнера. Корни полинома

Деление с остатком многочлена на двучлен. Схема Горнера. Теорема Безу. Понятие корня полинома. Кратные корни многочлена. Число корней полинома.

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ – многочлен степени $n \geq 1$ из кольца $P[x]$, a – произвольный элемент из поля P. Разделим $f(x)$ на двучлен $x - a$ с остатком. Получим равенство

$$f(x) = (x-a)q(x) + r, \tag{1}$$

где $q(x)$ – частное и r – остаток. Так как делитель $(x - a)$ – многочлен первой степени, то остаток r либо равен нулю, либо является многочленом нулевой степени, то есть элементом из поля P, отличным от нуля. Очевидно, что частное $q(x)$ имеет степень $n - 1$. Пусть

$$q(x) = b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1}. \tag{2}$$

Выполним подстановку из (2) в (1)

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n =$$
$$= (x-a)(b_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1}) + r.$$

Выполнив умножение в правой части и приведя подобные члены, получим $a_0x^n + a_1x^{n-1} + \cdots + a_n = b_0x^n + (b_1 - ab_0)x^{n-1} + {}$ $+ (b_2 - ab_2)x^{n-2} + \cdots + + (b_{n-1} - ab_{n-2})x + (r - ab_{n-1})$.

Приравняв коэффициенты при одинаковых степенях переменной, получим систему равенств, из которых находим затем коэффициенты частного $q(x)$ и остаток r.

$$\begin{array}{c} a_0 = b_0 \\ a_1 = b_1 - ab_0 \\ a_2 = b_2 - ab_1 \\ \dots \\ a_k = b_k - ab_{k-1} \\ \dots \\ a_n = r - ab_{n-1} \end{array} \Rightarrow \begin{array}{c} b_0 = a_0 \\ b_1 = a_1 + ab_0 \\ b_2 = a_2 - ab_1 \\ \dots \\ b_k = a_k + ab_{k-1} \\ \dots \\ r = a_n + ab_{n-1} \end{array} \tag{3}$$

По формулам (3) можно вычислить коэффициенты частного и остаток r. Эти вычисления удобно проводить с помощью так называемой схемы Горнера, представляющей собой следующую таблицу:

Таблица 1. – Схема Горнера

a_0	a_1	a_2	…	a_k	…	a_n
$b_0 = a_0$	$b_1 = a_1 + ab_0$	$b_2 = a_2 - ab_1$	…	$b_k = a_k + ab_{k-1}$	…	$r = a_n + ab_{n-1}$

В первой строке таблицы записываются коэффициенты многочлена $f(x)$. В первой клетке второй строки записывается a_0, стоящее сверху в первой строке. Остальные клетки второй строки заполняются по одной и той же схеме. Например, чтобы найти b_k, нужно к a_k, стоящему сверху в первой строке, прибавить элемент b_{k-1}, стоящий в предыдущей клетке второй строки, умноженный на a.

Если вместо переменной *x* в многочлен $f(x)$ подставить элемент a из поля *P* или из его расширения, то, очевидно, получим также элемент, принадлежащий полю *P* или его расширению. Этот элемент обозначается через $f(a)$ и *называется значением многочлена при* $x = a$.

Определение* 1.** *Элемент a из поля P или из его расширения* ***называется корнем многочлена $f(x)$*, если значение этого многочлена при* $x = a$ *равно нулю, то есть* $f(a) = 0$.

Теорема 1 *(Безу). Остаток* r *при делении многочлена f(x) на двучлен* $(x - a)$ *равен значению этого многочлена при* $x = a$*, то есть* $r = f(a)$.

Теорема 2. *Элемент* a *тогда и только тогда является корнем многочлена* $f(x)$*, когда* $f(x)$ *делится на двучлен* $x - a$.

Последняя теорема позволяет иначе определить корень многочлена.

Определение 2. *Элемент* a *из поля P или из его расширения называется корнем многочлена* $f(x)$*, если* $f(x)$ *делится на двучлен* $x - a$*. При этом элемент a называется k-кратным корнем многочлена* $f(x)$*, если* $f(x)$ *делится на* $(x - a)^k$*, но уже не делится на* $(x - a)^{k+1}$.

***Теорема 3* (*о наибольшем возможном числе корней многочлена*).** *Всякий многочлен степени* $n \geq 0$ *имеет не более чем* n *корней, даже если считать каждый корень столько раз, какова его кратность.*

Теорема 4. *Пусть* $f(x)$ *и* $g(x)$ *– многочлены, степени которых не превышают* n*. Если значения многочленов* $f(x)$ *и* $g(x)$ *совпадают при более чем* n *значениях переменной x, то эти многочлены равны.*

22. Алгебраическая замкнутость поля комплексных чисел

Определение алгебраически замкнутого поля. Теорема об алгебраической замкнутости поля комплексных чисел (основная теорема алгебры). Разложение полинома над полем комплексных чисел в произведение линейных множителей.

Определение 1. *Поле P называется* ***алгебраически замкнутым****, если всякий многочлен из кольца $P[x]$, степени $n \geq 1$, разлагается над полем P в произведение линейных множителей.*

Приведем еще одно определение алгебраически замкнутого поля.

Определение 2. *Поле P называется* ***алгебраически замкнутым****, если всякий многочлен из кольца $P[x]$, степени $n \geq 1$, имеет в поле P хотя бы один корень.*

Покажем, что приведенные определения эквивалентны.

Пусть поле P алгебраически замкнуто по первому определению, тогда всякий многочлен ненулевой степени из кольца $P[x]$ представим над полем *P* в виде:

$$f(x) = (a_0x + a_1)(b_0x + b_1)\dots(d_0x + d_1),$$

где $a_0, a_1, \dots, d_0, d_1$ – элементы поля P. В таком случае $f(x)$ имеет корни $-\frac{a_1}{a_0}$; $-\frac{b_1}{b_0}$; …; $-\frac{d_1}{d_0}$ принадлежащие полю P. Следовательно, поле P алгебраически замкнуто по второму определению.

Пусть теперь поле P алгебраически замкнуто по второму определению, то есть всякий многочлен $f(x)$ из кольца $P[x]$, степени $n \geq 1$, имеет в поле P хотя бы один корень. Пусть α_1 – корень многочлена $f(x)$, принадлежащий полю P. Тогда над полем P $f(x)$ представим в виде произведения:

$$f(x) = (x - \alpha_1)f_1(x).$$

Если $f_1(x)$ многочлен ненулевой степени, то он в свою очередь имеет корень α_2 из поля *P*. Тогда

$f(x) = (x - \alpha_1)(x - \alpha_2)f_2(x)$, где $f_2(x)$ – многочлен над полем P. Если степень многочлена $f_2(x)$, отлична от нуля, то он имеет корень α_3, принадлежащий ролю P, и т. д. В конечном итоге получим представление многочлена $f(x)$ над полем *P* в виде:

$$f(x) = c(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)\dots(x - \alpha_n), \text{ где } c \in P,$$

то есть всякий многочлен из кольца $P[x]$, степени $n \geq 1$, разлагается над полем P в произведение линейных множителей. Иначе говоря, поле P алгебраически замкнуто по первому определению.

Ниже покажем так называемую основную теорему алгебры, утверждающую, что поле *C* комплексных чисел алгебраически замкнуто.

***Теорема 1.* (*Основная теорема алгебры*)** *Всякий многочлен* $f\ \ x$ *из кольца* $C[x]$ *степени* $n \geq 1$ *имеет, по крайней мере, один комплексный корень*.

Приведем следствия из основной теоремы алгебры.

***Следствие* 1.** *Всякий многочлен* $f\ \ x$ *степени* $n \geq 1$ *разлагается над полем комплексных чисел в произведение линейных множителей, то есть поле C комплексных чисел алгебраически замкнуто по определению* 1.

***Следствие* 2.** *Всякий многочлен* $f\ \ x$ *из кольца* $C[x]$ *степени* $n \geq 1$ *имеет точно* n *комплексных корней.*

***Следствие* 3.** *Неприводимым над полем C комплексных чисел может быть только многочлен первой степени*.

***Следствие* 4.** *Пусть* $\alpha = a + bi\ (a, b \in R, b \neq 0)$ *мнимый корень многочлена* $f\ \ x$ *с действительными коэффициентами, тогда число* $\alpha = a - bi$ *также является корнем многочлена* $f\ \ x$.

***Следствие* 5.** *Неприводимым над полем R действительных чисел может быть только многочлен не выше второй степени*.

***Следствие* 6.** *Всякий многочлен* $f\ \ x$ *степени* $n \geq 1$ *из кольца* $R\ \ x$ *разлагается над полем R действительных чисел в произведение линейных и квадратных неприводимых множителей. Всякому линейному множителю соответствует действительный корень, а всякому квадратному – пара сопряженных мнимых корней многочлена.*

23. Неприводимые полиномы. Разложение полинома в произведение неприводимых множителей

Взаимно простые полиномы и их свойства. Понятие полинома, неприводимого над полем. Примеры. Свойства неприводимых полиномов. Разложение полинома в произведение неприводимых множителей.

Определение* 1.** *Многочлены $f(x)$ и $g(x)$ называются* ***взаимно простыми*, если их наибольший общий делитель является многочленом нулевой степени, то есть элементом поля P, отличным от нуля. При этом пишут* $(f(x), g(x)) = 1$.

Теорема 1. *Многочлены $f(x)$ и $g(x)$ тогда и только тогда* ***взаимно просты****, когда в кольце $P[x]$ найдутся такие многочлены $\varphi(x)$ и $\psi(x)$, что*

$$f(x)\varphi(x) + g(x)\psi(x) = 1. \qquad (1)$$

Приведем некоторые ***свойства взаимно простых*** многочленов.

Свойство 1. Пусть $h(x) \mid f(x) \cdot g(x)$, причем $(h(x), f(x)) = 1$. Тогда $h(x) \mid g(x)$.

Свойство 2. Пусть $(f(x), g(x)) = 1$. Многочлен $h(x)$ тогда и только тогда делится на произведение $f(x) \cdot g(x)$, когда $h(x) \vdots f(x)$ и $h(x) \vdots g(x)$.

Свойство 3. Пусть многочлен $g(x)$ взаимно прост с каждым из многочленов $f_1(x), f_2(x), \dots, f_k(x)$. Тогда $g(x)$ взаимно прост и с произведением этих многочленов

Аналогами простых чисел в теории многочленов являются так называемые неприводимые над полем многочлены. Согласно свойствам отношения делимости всякий многочлен $f(x)$ из кольца $P[x]$ делится на любой многочлен нулевой степени этого кольца и на любой ассоциированный с ним многочлен.

Определение* 2.** *Многочлен $f(x)$ из кольца $P[x]$ степени $n \geq 1$ называется* ***неприводимым над полем P*, если он не имеет других делителей, кроме многочленов нулевой степени и многочленов, ассоциированных с $f(x)$. Если же многочлен $f(x)$, кроме указанных, имеет и другие делители из кольца $P[x]$, то его называют приводимым над полем P.*

Очевидно, что многочлен $f(x)$ тогда и только тогда приводим над полем P, когда его можно представить в виде произведения $f(x) = f_1(x) \cdot f_2(x)$, где f_1 и f_2 – многочлены из кольца $P[x]$, степень каждого из которых меньше степени многочлена $f(x)$.

Ниже под приводимым (неприводимым) многочленом будет подразумеваться многочлен, приводимый (неприводимый) над полем P, если не будет указано поле, над которым он рассматривается. Ясно, что если $f(x)$ – многочлен над полем P, то его можно рассматривать и как многочлен над любым расширением поля P. И неприводимый над полем P многочлен может быть уже приводимым над расширением поля P.

Пример 1. Многочлен $f\ x\ = x^2 - 2$ неприводим над полем Q рациональных чисел. Действительно, если он приводим над полем Q, то его можно представить в виде произведения $f\ x\ = \ ax + b\ \ cx + d\ $, где a, b, c, d – рациональные числа. В таком случае многочлен $f\ x\ = = x^2 - 2$ имеет рациональный корень $-\frac{b}{a}$, то есть $\overline{\ 2} = \frac{b}{a}$ – рациональное число. Чего не может быть. Над полем R действительных чисел многочлен $f\ x\ = x^2 - 2$ уже приводим, а именно, разлагается над R в произведение линейных множителей $f(x) = (x + \sqrt{2})(x - \sqrt{2})$.

Приведем ***свойства неприводимых*** многочленов.

Свойство 1. Пусть $p(x)$ – многочлен неприводимый над полем P, тогда всякий многочлен ассоциированный с $p(x)$ также неприводим над P.

Свойство 2. Пусть $p(x)$ неприводим над полем P и $f(x)$ – произвольный многочлен из кольца $P[x]$. Тогда либо $f(x)$ делится на $p(x)$, либо $(f, p) = 1$.

Свойство 3. Пусть $p(x)$ и $q(x)$ неприводимы над полем P и $p(x) \vdots q(x)$, тогда $p(x)$ и $q(x)$ ассоциированы.

Свойство 4. Пусть неприводимый многочлен делит произведение многочленов $f_1\ x\ , f_2\ x\ , \ldots, f_n(x)$, тогда *p(x)* делит хотя бы один из сомножителей этого произведения.

Теорема 2. *Всякий многочлен $f(x) \in P[x]$ степени $n \geq 1$ либо неприводим над полем P, либо разлагается над этим полем в произведение неприводимых множителей. Причем, такое разложение однозначно с точностью до порядка следования сомножителей и множителей нулевой степени.*

Может случиться, что в разложении многочлена $f(x)$ в произведение неприводимых множителей будут встречаться ассоциированные многочлены. В таком случае $f(x)$ можно представить в виде

$$f\ x\ = c\ \ p_1(x)\ ^{k_1} \cdot\ p_2(x)\ ^{k_2} \cdot \ldots \cdot\ p_n(x)\ ^{k_n}, \qquad (2)$$

где $p_1\ x\ , p_2\ x\ , \ldots, p_n(x)$ – попарно различные (неассоциированные) неприводимые многочлены над полем P.

Представление многочлена $f(x)$ в виде (2) называется каноническим разложением $f(x)$ над полем P.

Определение 3. *Неприводимый многочлен $p_j(x)$ называется k-кратным неприводимым множителем многочлена $f(x)$, если $f(x)$ делится на $(p_j(x))^k$, но не делится на $(p_j(x))^{k+1}$.*

Согласно (2) неприводимые многочлены $p_1\ x\ , p_2\ x\ , \ldots, p_l(x)$ входят в каноническое разложение многочлена $f(x)$ соответственно с кратностями $k_1, k_2, \ldots, k_l$.

24. Симметрические полиномы. Основная теорема о симметрических полиномах

Кольцо симметрических полиномов. Элементарные симметрические полиномы. Основная теорема о симметрических полиномах и ее приложение к вычислению корней полинома.

Далее будем рассматривать многочлены над полем P.

Определение 1. *Многочлен* $f(x_1, x_2, \dots, x_n)$ *из кольца* $P[x_1, x_2, \dots, x_n]$ *называется* ***симметрическим****, если в результате любой перестановки переменных в этом многочлене получается многочлен, равный исходному*.

Например, многочлен

$$f = x_1^3x_2^2x_3 + x_1^3x_2x_3^2 + x_1^2x_2^3x_3 + x_1^2x_2x_3^3 + x_1x_2^3x_3^2 + x_1x_2^2x_3^2$$

является симметрическим, так как он не меняется при любой перестановке переменных.

Приведем некоторые свойства симметрических многочленов.

Свойство 1. *Сумма, разность и произведение симметрических многочленов из кольца* $P[x_1, x_2, \dots, x_n]$ *также являются симметрическими многочленами из этого кольца.*

Согласно приведенному свойству множество симметрических многочленов образует подкольцо кольца $P[x_1, x_2, \dots, x_n]$.

Свойство 2. *Пусть выражение*

$$ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n} \qquad (1)$$

является членом симметрического многочлена f. *Тогда членом этого многочлена также является и всякое выражение, полученное из* (1) *в результате перестановки показателей при переменных.*

Свойство 3. *Пусть выражение* (1) *является высшим членом симметрического многочлена* f, *тогда выполняются неравенства*

$$k_1 \geq k_2 \geq k_3 \geq \dots \geq k_n\ . \qquad (2)$$

Определение 2. Элементарными симметрическими многочленами от n переменных называются следующие многочлены:

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \dots + x_n \\ \sigma_2 &= x_1x_2 + x_1x_3 + \dots + x_{n-1}x_n \\ \sigma_3 &= x_1x_2x_3 + x_1x_2x_4 + \dots + x_{n-1}x_{n-2}x_n \\ &\dots \\ \sigma_n &= x_1\,x_2\dots x_n\ . \end{aligned} \qquad (3)$$

Существует связь элементарных симметрических многочленов с известными формулами Виета.

Теорема **(Виета).** Пусть $h\ x\ = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ – многочлен кольца $P[x]$ и $x_1, x_2, \dots, x_n$ – корни этого многочлена, тогда

$$\begin{gathered} x_1 + x_2 + \ldots + x_n = -a_1 \\ x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = a_2 \\ x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-1}x_{n-2}x_n = -a_3 \\ \ldots \\ x_1\, x_2 \ldots x_k + \cdots + x_{n-k+1} \ldots x_{n-1}x_n = (-1)^k a_k \\ \ldots \\ x_1\, x_2 \ldots x_n = (-1)^n a_n \; . \end{gathered} \tag{4}$$

Согласно формулам Виета значение симметрического многочлена σ_n $(k = \overline{1,n})$ от корней многочлена $h(x)$ равно коэффициенту a_k этого многочлена, взятому со знаком $(-1)^k$.

Теорема **(основная теорема о симметрических многочленах).** *Всякий симметрический многочлен* $f(x_1, x_2, \ldots, x_n)$ *из кольца* $P[x_1, x_2, \ldots, x_n]$ *можно представить в виде многочлена от элементарных симметрических многочленов* σ_1, σ_2, *...,* σ_n *над полем P, то есть* $f(x_1, x_2, \ldots, x_n) = g(\sigma_1, \sigma_2, \ldots, \sigma_n)$, *где* g *многочлен из кольца* $P[\sigma_1, \sigma_2, \ldots, \sigma_n]$.

Приведем важное следствие к э этой теореме.

Следствие. *Пусть*

$$h(x) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n -$$

многочлен из кольца $\mathrm{P}[x]$ *и пусть* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *– все корни этого многочлена. Тогда всякий симметрический многочлен* $f(x_1, x_2, \ldots, x_n)$ *из кольца* $P[x_1, x_2, \ldots, x_n]$ *при* $x_1 = \alpha_1, x_2 = \alpha_2, \ldots, x_n = \alpha_n$ *принимает значение принадлежащее полю P, то есть* $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Метод, с помощью которого симметрический многочлен f выражается через элементарные симметрические многочлены $\sigma_1, \sigma_2, \ldots, \sigma_n$, описанный в теореме, применяется при решении задач. При этом если f не является однородным, то предварительно его представляют в виде суммы однородных многочленов. Затем каждое слагаемое отдельно выражается через $\sigma_1, \sigma_2, \ldots, \sigma_n$.

25. Определитель матрицы. Обратная матрица

Определитель матрицы. Свойства определителя. Определитель произведения матриц. Обратная матрица. Критерий существования обратных матрицы. Свойства обратных матриц.

Пусть дана квадратная матрица порядка n:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Определение 1. Определителем *квадратной матрицы A n-го порядка называется алгебраическая сумма $n!$ членов, каждый из которых представляет собой произведение n элементов матрицы A, взятых по одному от каждой строки и каждого столбца этой матрицы, причем произведение входит в определитель со знаком $+$, если соответствующая ему подстановка индексов четная и со знаком $-$ в противном случае.*

Определитель квадратной матрицы A порядка n будем называть определителем n-го порядка и обозначать

$$|A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Элементы, строки и столбцы матрицы A будем называть при этом соответственно элементами, строками и столбцами определителя $|A|$.

Таким образом, согласно определению

$$|A| = \sum_{\alpha_1,\alpha_2,\dots,\alpha_n} (-1)^t a_{1\alpha_1} a_{2\alpha_2} \dots a_{n\alpha_n},$$

где t − число инверсий в перестановке $\alpha_1, \alpha_2, \dots, \alpha_n$ и сумма состоит из всех слагаемых, для которых перестановки $\alpha_1, \alpha_2, \dots, \alpha_n$ различны.

Свойства определителей

Определение 2. *Преобразование матрицы, при котором ее строки становятся столбцами с сохранением порядка следования, называется транспонированием. Матрицу, транспонированную к матрице A, будем обозначать A^T.*

Свойство 2. *Определитель квадратной матрицы A равен определителю транспонированной к ней матрицы, т. е. $|A| = |A^T|$.*

Данное свойство устанавливает равноправие строк и столбцов определителя. Это значит, что все свойства, касающиеся строк определителя, справедливы и для его столбцов.

Свойство 3. *Определитель, содержащий нулевую строку, равен нулю.*

Свойство 4. *Если все элементы строки определителя* Δ *умножить на число* k*, то на число* k *умножится определитель* Δ.

Следствие 1. *Общий множитель всех элементов строки можно выносить за знак определителя.*

Свойство 5. *При перемене местами двух строк определителя* Δ *меняется его знак, абсолютная величина определителя не меняется*.

Перемену местами двух строк (столбцов) определителя будем также называть транспозицией строк (столбцов).

Свойство 6. *Определитель, содержащий две одинаковые строки, равен нулю.*

Свойство 7. *Определитель, имеющий две пропорциональные строки, равен нулю.*

Свойство 8. *Определитель, у которого все элементы одной из строк, например,* i*-ой строки, представимы в виде суммы двух слагаемых, равен сумме двух определителей, все строки которых, кроме отмеченной* i*-ой строки, совпадают с соответствующими строками исходного определителя;* i*-я же строка первого определителя составлена из первых слагаемых, а* i*-я строка второго определителя составлена из вторых слагаемых элементов* i*-ой строки исходного определителя, то есть*

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} + b_{i1} & a_{i2} + b_{i2} & \dots & a_{in} + b_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ b_{i1} & b_{i2} & \dots & b_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$$

$$= \Delta_1 + \Delta_2.$$

Это свойство распространяется и на случай, когда все элементы одной из строк представимы в виде суммы m элементов ($m > 2$). Такой определитель равен сумме m соответствующих определителей.

Свойство 9. *Определитель не изменится, если к одной из его строк прибавить другую строку, умноженную на произвольное число.*

Свойство 10. *Если одна из строк определителя является линейной комбинацией других его строк, то он равен нулю.*

Определение 2. *Определителем треугольного вида называется определитель, все элементы которого, расположенные ниже или выше главной диагонали (диагональ от верхнего левого к нижнему правому углу), равны нулю.*

Свойство 11. *Определитель треугольного вида равен произведению диагональных элементов.*

Миноры и алгебраические дополнения

Пусть дан определитель *n*-го порядка:

$$\Delta = \begin{array}{ccccc} a_{11} & \dots & a_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ij} & \dots & a_{in} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & & a_{nj} & \dots & a_{nn} \end{array}.$$

Определение 3*. Минором элемента a_{ij} определителя Δ называется определитель порядка $n-1$, полученный из определителя Δ вычеркиванием в нем i-ой строки и j-го столбца.*

Минор элемента a_{ij} определителя Δ обозначается через M_{ij}.

Определение 4*. Алгебраическим дополнением элемента a_{ij} определителя Δ называется минор M_{ij} этого элемента, умноженный на $-1\ ^{i+j}$.*

Обозначается через A_{ij}.

Согласно определению $A_{ij} = \ -1\ ^{i+j} M_{ij}$.

Теорема 1*. Определитель равен сумме произведений элементов одной из его строк (одного из столбцов) на их алгебраические дополнения, т. е.*

$$\Delta = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in}, \quad (1)$$

$$\Delta = a_{1j}A_{1j} + a_{2j}A_{2j} + \dots + a_{nj}A_{nj}. \quad (2)$$

Равенство (1) называется разложением определителя Δ по i-ой строке, а равенство (2) называется разложением определителя Δ по j-ому столбцу.

Определитель произведения матриц

Теорема 2*. Определитель произведения двух квадратных матриц равен произведению определителей этих матриц*

Следствие 1*. Если квадратная матрица обратима, то ее определитель отличен от нуля.*

Следствие 2. *Пусть A − обратимая матрица, тогда*

$$A^{-1} = \frac{1}{A}.$$

Обратимые матрицы. Условие обратимости матрицы. Вычисление обратной матрицы

Определение 5. *Матрица A называется обратимой, если существует обратная ей матрица, т. е. такая матрица* A^{-1}, что $AA^{-1} = A^{-1}A = E$, где E *− единичная матрица.*

Определение 6*. Квадратная матрица A называется невырожденной (неособенной), если ее определитель отличен от нуля, и вырожденной (особенной), если определитель матрицы равен нулю.*

Приведем достаточное условие обратимости матрицы.

Теорема 3. *Всякая невырожденная матрица обратима.*

При вычислении обратной матрицы A^{-1} способом, основанном на элементарных преобразованиях строк, справа к матрице A приписывается единичная матрица E. Получают так называемую комбинированную матрицу $A|E$. Затем над строками комбинированной матрицы проводятся элементарные преобразования с тем, чтобы на месте матрицы A получить единичную матрицу E. Тогда на месте матрицы E будет расположена матрица A^{-1}. Действительно, согласно доказательству теоремы 3 преобразование матрицы A в единичную матрицу равносильно умножению слева на матрицу $A^{-1} = Э_k \dots Э_2 Э_1$. Но элементарные преобразования проводятся над строками всей комбинированной матрицы, поэтому матрица E также умножается на матрицу A^{-1}, и в результате получим

$$A^{-1}A \; \big| \; A^{-1}E = E \; \big| \; A^{-1}.$$

Пусть $A = (a_{ij}) = \begin{matrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{matrix}$ – квадратная матрица порядка n.

Определение 7. *Присоединенной для матрицы А называется матрица*

$A^* = \begin{matrix} A_{11} & A_{21} & \dots & A_{1n} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{matrix}$, *составленная из алгебраических дополнений элементов матрицы*.

Отметим, что алгебраические дополнения элементов строк матрицы А в матрице A^* располагаются в столбцах.

Теорема 4. *Пусть А – обратимая матрица, тогда* $A^{-1} = \frac{1}{A} \cdot A^*$.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Беклемишев, Д. В. Курс аналитической геометрии и линейной алгебры / Д. В. Беклемишев – М.: ФИЗМАТЛИТ, 2005. – 304 с.
2. Белоногов, В. А. Задачник по теории групп / В. А. Белоногов. – М.: Наука, 2000. – 239 с.
3. Беняш-Кривец, В.В. Лекции по алгебре: группы, кольца, поля: учебное пособие для студентов математических специальностей / В.В. Беняш-Кривец, О.В. Мельников. – Минск: БГУ, 2008. – 116 с.
4. Березкина, Л. Л. Аналитическая геометрия и линейная алгебра / Л. Л. Березкина – Минск: РИВШ, 2012. – 354 с.
5. Ильин, В. А. Линейная алгебра / В. А. Ильин, Э. Г. Позняк. – М.ФИЗМАТЛИТ, 2009. – 280 с.
6. Кострикин, А. И. Введение в алгебру. Ч. 1. Основы алгебры / А. И. Кострикин. – М.: Физматлит., 2000. – 272 с.
7. Куликов, Л. Я. Сборник задач по алгебре и теории чисел / Л. Я. Куликов, А. И. Москаленко, А. А. Фомин. – М.: Просвещение, 1993. – 228 с.
8. Куликов, Л. Я. Алгебра и теория чисел / Л. А. Куликов. – М.: Высшая школа, 1979. – 560 с.
9. Курош, А. Г. Курс высшей алгебры / А. Г. Курош. – М.: Наука, 1971. – 432 с.
10. Милованов, М. В. Алгебра и аналитическая геометрия. В 2 ч. / М. В. Милованов, Р. И. Тышкевич, А. С. Феденко. – Минск: Амалфея, 2001.,Ч. 1. – 400 с., Ч. 2. – 352 с.
11. Проскуряков, И. В. Сборник задач по линейной алгебре / И. В. Проскуряков. – М.: Наука, 1978. – 384 с.
12. Размыслович, Г. П. Сборник задач по геометрии и алгебре / Г. П. Размыслович, М. М. Феденя, В. М. Ширяев. – Минск: Изд-во “Унiверсiтэцкае”, 1999. – 393 с.
13. Фаддеев, Д. К. Задачи по высшей алгебре / Д. К. Фаддеев, И. С. Соминский. – СПб.: Лань, 2001. – 288 с.
14. Умнов, А. Е. Аналитическая геометрия и линейная алгебра / А. Е. Умнов. – М.: МФТИ, 2011. – 570 с.

Справочное издание

СПРАВОЧНЫЕ МАТЕРИАЛЫ К ГОСУДАРСТВЕННОМУ ЭКЗАМЕНУ
ПО СПЕЦИАЛЬНОСТИ 1-02 05 01 «МАТЕМАТИКА И ИНФОРМАТИКА»
ПО ДИСЦИПЛИНЕ «АЛГЕБРА»

Составитель
Ефремова Марина Ивановна

Корректор *В. В. Кузьмич*
Оригинал-макет *Л. И. Федула*

Подписано в печать 27.05.2019. Формат 60x84 1/16. Бумага офсетная.
Ризография. Усл. печ. л. 4,42. Уч.-изд. л. 3,08.
Тираж 44 экз. Заказ 18.

Издатель и полиграфическое исполнение:
учреждение образования «Мозырский государственный
педагогический университет имени И. П. Шамякина».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий N 1/306 от 22 апреля 2014 г.
Ул. Студенческая, 28, 247777, Мозырь, Гомельская обл.
Тел. (0236) 32-46-29