1. Линейное пространство над числовым полем: определение, свойства и примеры.

***Определение:***

*Множество* ***L*** *называется* ***векторным (линейным) пространством****, над числовым полем* ***k****, если:*

1. *Задан закон (сложение), по которому* ∀*x, y* **∈** *L сопоставляется т.н. сумма x+y* **∈** *L;*
2. *Задан закон (умножение на число), по которому* ∀*x* **∈** *L и* ∀α **∈** *k сопоставляется произведение* ***αx* ∈ *L****;*
3. ∀*x, y, z* **∈** *L и* ∀*α, β* **∈** *k выполнены следующие* ***аксиомы****:*

* *x + y = y + x,*
* *(x + y) + z = x + (y + z),*
* *∃ 0* ***∈*** *L: x + 0 = x,*
* *∃ ‘-x’* ***∈*** *L: x + (-x) = 0,*
* *1* ***·*** *x = x,*
* *α(βx) = (αβ)x,*
* *(α + β)x = αx + βx,*
* *α(x + y) = αx + αy,*
* *Элементы* ***L*** *называются* ***векторами****;*
* ***0*** *называется* ***нулевым вектором (нулем)****;*
* ***‘-x’*** *называется* ***противоположным*** *вектору x.*

***Свойства:***

***Лемма 1.*** *Любое числовое поле включает в себя подполе рациональных чисел .*

***Лемма 2.***

1. *В любом векторном пространстве L существует* ***единственный*** *нулевой вектор.*
2. *В любом векторном пространстве для любого вектора существует* ***единственный*** *противоположный вектор.*
3. ∀*x****∈*** *L: 0 · x = 0.*
4. ∀*x****∈*** *L: (-1) · x = -x.*

***Примеры:***

1. *над - пространства геометрических векторов;*
2. *над ; над ; над k; над и т.п. – поле над подполем;*
3. *, ∈ k – пространство векторов-столбцов;*
4. *– пространство матриц размера m* x *n;*
5. *– пространство всех многочленов от t;*
6. *– пространство многочленов степени не выше n;*
7. *– пространство вещественных непрерывных функций на [a; b];*
8. *Пространство решений ОСЛУ;*
9. *0 = {0} – нулевое пространство.*
10. Базис и размерность линейного пространства. Координаты вектора. Теорема о существовании базиса.

***Определение базиса:***

*Если в пространстве L (над полем k) существует такая совокупность векторов , что любой вектор из L является их линейной комбинацией, то эта совокупность называется порождающей системой векторов пространства L.*

*Упорядоченная порождающая и при этом линейно независимая система векторов называется* ***Базисом*** *пространства L.*

***Определение координат вектора:***

*Коэффициенты линейной комбинации называется координатами вектора x относительно базиса .*

***Определение размерности линейного пространства:***

*Если в пространстве L можно найти n линейно независимых векторов, а всякие n+1 векторов этого пространства линейно зависимы, то число n называется размерностью пространства L, а L называется n-мерным.*

*Векторное пространство, в котором можно указать сколь угодно большое число линейно независимых векторов, называется бесконечномерным.*

***Теорема о существовании базиса:***

*В пространстве* ***L*** *размерности* ***n*** *существует* ***базис*** *из* ***n*** *векторов; более того, любая из* ***n*** *линейно независимых векторов пространства* ***L*** *является* ***базисом*** *этого пространства.*

***Доказательство:***

*Пусть линейно независимы, x****∈*** *L.*

*(от противного)*

***Ч.Т.Д.***

***Лемма.*** *Коэффициенты разложения вектора x по базису определяются однозначно.*

***Теорема.*** *При сложении двух векторов пространства L их координаты складываются. При умножении вектора на число все его координаты умножаются на это число.*

1. Признак линейной независимости системы векторов. Следствия.

***Теорема линейной независимости системы векторов:***

*Система из m векторов линейно независима тогда и только тогда, когда ранг матрицы из координат векторов равен числу этих векторов.*

***Следствие:***

*Если в пространстве L имеется базис, то размерность этого пространства равна числу базисных векторов.*

***Следствие:***

*Система из* ***n*** *векторов в* ***n-мерном*** *векторном пространстве* ***линейно независима*** *тогда и только тогда, когда определитель из координат этих векторов относительно произвольного базиса* ***отличен*** *от нуля.*

1. Преобразование координат вектора при замене базиса пространства.

*Два базиса пространства L: «старый» и «новый» .*

*x L*

*Матрица называется матрицей перехода от старого базиса к новому базису . В её столбцах стоят координаты нового базиса в старом.*

***Правило преобразования координат:***

*Новый координатный столбец равен произведению матрицы перехода от нового базиса к старому на старый координатный столбец.*

1. Подпространства. Лемма о базисе подпространства. Пересечение подпространств.

***Определение подпространства:***

*Подмножество M линейного (векторного) пространства L называется подпространством, если оно само является линейным (векторным) пространством относительно тех же самых операций, что были в L (сложение и умножение на число).*

*M – подпространство конечного пространства L*

***Леммы:***

1. *Базис любого подпространства можно дополнить до базиса всего пространства.*

*Док-во:*

*Пусть m=dim < n=dimL и - базис M.*

*– линейно независимы и т.д.*

1. *P и Q – подпространства L – подпространство L.*
2. Сумма подпространств. Теорема о размерностях суммы и пересечения подпространств.

***Сумма подпротсранств:***

*P+Q {x + y: x P, y } – сумма подпространств P и Q*

***Теорема о размерностях суммы и пересечения подпространств:***

*dim(P + Q) + dim() = dimP + dimQ.*

*Док-во:*

*Пусть S=P + Q, T= и – базис T ≠ O.*

*– базис P*

*– базис Q*

1. *- порождающая система для S*

*y*

*- базис S dimS = p + (q - t)*

*Ч.Т.Д.*

1. Теорема о прямой сумме подпространств.

*Сумма подпространств P и Q называется прямой (обозначение PQ), если любой вектор* ***zP + Q*** *записывается в виде* ***z = x + y****, где x P и y Q , единственным способом.*

***Теорема 2.***

*Если P и Q – два подпространства векторного пространства, то равносильны следующие три утверждения:*

1. *Сумма P + Q прямая;*
2. *PQ = O;*
3. *Объединение базисов P и Q – базис P + Q.*
4. Евклидово пространство. Неравенство Коши - Буняковского. Линейная независимость ортогональной системы векторов.

***Определение:***

*Вещественное векторное пространство L называется евклидовым, если*

*а) задано правило, по которому сопоставляется число (скалярное произведение) (x, y)*

*б) это правило и удовлетворяет следующим требованиям:*

*1. (x, y) = (y, x),*

*2. (x + y, z) = (x, z) + (y, z),*

*3. () = ,*

*4. , если , и .*

***Неравенство Коши-Буняковского:***

*Для любых векторов в евклидовом пространстве*

*.*

*Док-во:*

*Ч.Т.Д.*

***Определение ортогональных векторов:***

*Векторы называются ортогональными, если (x, y) = 0.*

***Линейная независимость ортогональной системы векторов:***

*Лемма:*

*Ортогональная система векторов линейно независима.*

*Док-во:*

*Пусть ортогональны.*

*Ч.Т.Д.*

1. Теорема об ортогонализации. Следствия.

***Теорема об ортогонализации Грамма-Шмидта:***

*Пусть – линейно независимая система векторов в евклидовом пространстве. Исходя из неё, можно построить ортогональную систему векторов , такую что* ***, ; ; …;*** *.*

*Док-во:*

*Индукция по k.*

*k = 1 – очевидно.*

*Пусть верно для k – 1.*

*, (!)*

*Ч.Т.Д.*

***Следствия:***

1. *В любом евклидовом пространстве существует ортогональный базис.*
2. *В любом евклидовом пространстве существует ортогональный и нормированный (ортонормированный) базис. (если норма каждого базиса равна 1, то базис называется нормированным).*
3. Ортогональное дополнение подпространства, свойства.

***Определение:***

*Ортогональное дополнение подпространства P:*

*Множество, в котором все векторы из пространства S, которые ортогональны всем векторам из P. (определение.)*

*Лемма.*

*Ортогональное дополнение - подпространство евклидова пространства S.*

*Теорема.*

*Ортогональное дополнение подпространства P – это подпространство, натянутое на вектора, дополняющие ортогональный базис P до ортогонального базиса S.*

*Док-во:*

*– ортогональный базис подпространства P – дополним до ортогонального базиса пространства S: .*

*Q – линейная оболочка этих векторов.*

*а) ;*

*б)*

***Свойства:***

* *;*
* *;*
* *;*
* *;*
* *;*
* *(ортогональная сумма).*

1. Проекция вектора на подпространство. Матрица Грама.

***Проекция вектора на подпространство:***

*a – ортогональная проекция вектора c на подпространство P*

*b – ортогональная составляющая (проекция на)*

*Пусть – ОНБ пространства P*

*Лемма.*

*Проекция линейной комбинации векторов равна той же линейной комбинации проекций.*

***Матрица Грама:***

*Пусть – любой базис подпространства P*

*Матрица Грама:*

*Определитель Грама:*

1. Линейные операторы. Матрица линейного оператора. Изменение матрицы оператора при замене базиса.

***Линейные операторы:***

*L, M – векторные пространства над полем k*

A *– оператор (отображение) из L в M*

*y=*A *y – образ вектора x, x – прообраз вектора y*

A *- линейный оператор, если*

*1)* A () = A+ A ;

*2)* A *() =* A *x* A *0=0)*

***Матрица линейного оператора:***

*dimL = n, dim = m,* A*: L →M*

*– базис L, – базис M*

*– матрица оператора в базисах и .*

*Столбцами матрицы являются координаты векторов относительно базиса .*

*(\*)*

*(\*)*

*Пусть теперь A= – произвольная матрица из .*

*Если , то по (\*) находим . Получили оператор (линейный!) с матрицей в базисах {} и {}.*

***Изменение матрицы оператора при замене базиса:***

*– два базиса L*

*()*

*( – матрица перехода от базиса к базису )*

*Лемма.*

*Определитель матрицы линейного оператора не зависит от выбора базиса.*

1. Ядро и образ линейного оператора. Теорема о размерностях ядра образа.

– ядро оператора

im = *L = – образ оператора*

*Теорема.*

*Ядро и образ линейного оператора – подпространства соответствующих пространств L и M.*

*dim ker = – дефект оператора*

*dim im = – ранг оператора*

*Теорема.*

*Док-во:*

*Пусть – базис . Пусть такой, что . линейно независимы.*

*Пусть , . Докажем, что .*

*а)*

*Пусть .*

*a =*

*б)*

*Пусть . a =*

*Пусть , c = a - .*

*Ч.Т.Д.*

1. Собственные векторы и собственные значения линейного оператора. Свойства собственных векторов.

*L – пространство над полем k,*

*Если существует ненулевой вектор и число , такие что*

*,*

*то число называется собственным значением (собственным числом) оператора , а вектор x – собственным вектором оператора .*

*Лемма 1. Любому собственному вектору соответствует единственное собственное значение.*

*Лемма 2. Если и – собственные вектора оператора с одним и тем же собственным значением , то любая их линейная комбинация или равна 0, или является собственным вектором оператора с собственным значением .*

*Следствие. Для любого собственного значения все собственные вектора вместе с нулевым вектором образуют подпространства пространства L.*

*Следствие. В n-мерном пространстве линейный оператор не может иметь более n собственных векторов с различными собственными значениями.*

1. Теорема о характеристическом многочлене линейного оператора.

*Теорема 1. Все собственные значения линейного оператора совпадают с корнями характеристического многочлена матрицы этого оператора в каком-нибудь базисе.*

*Замечание. Характеристические многочлены подобных матриц равны:*

*Пусть , тогда*

*По лемме*

*Т.о., можно называть характеристическим многочленом оператора .*

*n = 2*

*Для произвольного n:*

*Теорема 2.(Гамильтона-Кэли) Если – характеристический многочлен оператора , то .*

1. Теорема о линейной независимости собственных векторов. Матрица линейного оператора в базисе из собственных векторов.

*Теорема. Собственные вектора оператора , имеющие попарно различные собственные значения , линейно независимы.*

*Док-во (индукцией по m):*

*1) m=1.*

*2) Пусть теорема верна для m – 1.*

*3) Предположим, что линейно независимы.*

*и пусть*

*– противоречие.*

*Ч.Т.Д.*

*Матрица:*

*и т.д.*

*Теорема. Пусть – действующий в n-мерном пространстве над полем k линейный оператор. Если характеристический многочлен оператора в имеет n различных корней в поле k, то матрица этого оператора в базисе из собственных векторов является диагональной, и диагональные элементы этой матрицы – это собственные значения оператора .*

*Геометрический смысл. В пространстве L имеется n таких «направлений», что любой вектор, имеющий одно из этих «направлений», преобразуется оператором в коллинеарный.*

*Замечание. В случае кратных корней характеристического многочлена оператора его матрица всё равно может оказаться диагонализируемой (если число линейно независимых собственных векторов совпадет с размерностью пространства).*

1. Сопряженные операторы в евклидовом пространстве.

*Пусть – линейный оператор в евклидовом пространстве S. Линейный оператор называется сопряженным с , если для всех*

*Теорема 1. Для любого линейного оператора существует единственный сопряженный оператор. Его матрица в любом ОНБ является транспонированной к матрице оператора .*

*Док-во:*

*Ч.Т.Д.*

*Единственность доказывается от противного:*

*Замечание. Свойства соответствуют всем свойствам .*

1. Ортогональные матрицы. Ортогональные операторы.

***Определение ортогональной матрицы:***

*Вещественная матрица P называется ортогональной, если .*

*строки матрицы P ортогональны и нормированы*

*столбцы матрицы P ортогональны и нормированы*

***Определение ортогонального оператора:***

*Оператор* **P** *называется ортогональным, если для всех*

*.*

*Свойства ортогонального оператора :*

*1) ;*

*2) ;*

*3) сохраняет углы;*

*4) переводит любую ортонормированную систему векторов;*

*5)Матрица в ОНБ ортогональна;*

*6)Все вещественные собственные значения равны или 1, или -1.*

*Замечание. Все мнимые корни характеристического многочлена оператора , если они есть, также имеют модуль, равный 1.*

1. Свойства собственных значений симметричного оператора.

*Все собственные значения симметричного оператора – вещественные.*

*Док-во:*

*В выбранном ОНБ*

*а)*

*б)*

*Ч.Т.Д.*

1. Свойства собственных векторов симметричного оператора.

*Собственные вектора симметричного оператора, принадлежащие разным собственным значениям, ортогональны.*

*Док-во:*

*Ч.Т.Д.*

*Теорема 2.*

*Если – симметричный оператор в евклидовом пространстве S, то в S существует ОНБ, состоящий из собственных векторов оператора .*

1. Квадратичные формы, матричная запись. Линейное преобразование переменных в квадратичной форме.

*Квадратичной формой называется однородный многочлен второй степени от n переменных.*

*– матрица квадратичной формы (симметрическая!)*

*Линейное преобразование:*

*Если , то (невырожденное линейное преобразование).*

1. Метод Лагранжа приведения квадратичной формы к диагональному виду. Закон инерции (без док-ва).

***Теорема (Лагранжа).*** Любая квадратичная форма при помощи невырожденного линейного преобразования может быть приведена к диагональному виду.

Док-во: индукция по числу переменных.

*1) n = 1*

*2) Пусть для n - 1 утверждение теоремы верно.*

*3) см. (\*) из 21 вопр. Считаем, что .*

*; существует невырожденное преобразование:*

***Закон инерции.*** *Число положительных и отрицательных коэффициентов в диагональном виде вещественной квадратичной формы не зависит от способа приведения этой формы вещественными невырожденными преобразованиями к диагональному виду.*

1. Приведение квадратичной формы к диагональному виду ортогональным преобразованием.

*k =*

*Теорема (приведение квадратичной формы к главным осям). Любая вещественная квадратичная форма с матрицей A при помощи некоторого ортогонального преобразования переменных X = CY может быть приведена к диагональному виду*

*Коэффициенты совпадают с собственными значениями матрицы А. Столбцы ортогональной матрицы С являются собственными векторами матрицы А, соответствующими собственным значениям .*

*Док-во:*

1. *Пусть получен вид (1), тогда*

1. *Существование преобразования - по индукции.*

*n = 1 (любая форма от одной переменной диагональна)*

*Пусть для n – 1 утверждение верно.*

*т.к.*

*– ОНБ – ортогональная матрица*

*Пусть – с помощью ортогонального преобразования с матрицей D (порядка n – 1).*

*– ортогональная матрица. :*

*и*

*– ортогональная матрица. :*

*Ч.Т.Д.*

*Замечания.*

*1. Если C – ортогональная матрица из собственных векторов матрицы А, то X = CY и приводит форму к диагональному виду.*

*2. Собственные векторы, соответствующие разным собственным значениям уже ортогональны.*

1. Классификация центральных поверхностей второго порядка.

*– матрица (симметрическая) квадратичной формы*

*,*

*I) (центральные поверхности 2-го порядка)*

*а) 1 или -1, или 0*

*– эллипсоид*

*Симметричен относительно координат плоскостей, осей и НК.*

*(0;0;0) – центр эллипсоида;*

*Точки пересечения с координатными осями – вершины эллипсоида;*

*a, b, c – полуоси эллипсоида (в каноническом уравнении).*

*б) 1 или -1, или 0*

*– однополостный гиперболоид*

*– дву(х)полостный гиперболоид*

*Симметричны относительно координатных плоскостей, осей и НК.*

*(0;0;0) – центр гиперболоидов;*

*Точки пересечения с координатными осями – вершины гиперболоидов;*

*a, b – поперечные полуоси гиперболоидов ( в канонических уравнениях), с – продольная полуось.*

*– конус 2-го порядка*

*( в канонических уравнениях)*

*Симметричен относительно координатных плоскостей, осей и НК.*

*(0;0;0) – центр и вершина конуса.*

*Сечение конуса может быть эллипсом (если плоскость пересекает все образующие), гиперболой (если плоскость параллельна двум образующим), параболой (если плоскость параллельна одной образующей).*

1. Классификация нецентральных поверхностей второго порядка.

*– матрица (симметрическая) квадратичной формы*

*,*

*II)*

*а) или 1, или -1, или 0*

*– эллиптический параболоид*

*( в каноническом уравнении)*

*(0;0;0) – вершина эллиптического параболоида.*

*Oz – ось симметрии (есть плоскости симметрии, как и у всех поверхностей 2-го порядка)*

*– эллиптический цилиндр*

*- прямая*

*( в каноническом уравнении)*

*б) или 1, или 0*

*– гиперболический параболоид*

*(0;0;0) – вершина гиперболического параболоида.*

*Oz – ось симметрии*

*– гиперболический цилиндр*

*– две пересекающиеся плоскости*

*III)*

*а) или 1, или -1, или 0*

*– параболический цилиндр*

*Замечания.*

*1) уравнения вида ортогональным преобразованием (поворотом плоскости Oyz) приводится к виду .*

*2)Ортогональным преобразованием уравнение параболического цилиндра можно привести к виду (p > 0).*

*– параболический цилиндр*

*– две параллельные плоскости*

*– плоскость x = 0*

1. Группы. Симметрические группы. Подгруппы.

*Множество G с бинарной операцией «» называется группой, если:*

*Операция «» ассоциативна; в G существует нейтральный элемент e; для любого существует обратный элемент, т.е. такой элемент , что .*

*Если, кроме того, операция «» коммутативна, то группа G называется коммутативной, или абелевой.*

*Теорема. Пусть группа G – группа с нейтральным элементом e. Тогда e – единственный нейтральный элемент в группе. Кроме того, любой элемент группы G обладает единственным обратным элементом.*

*Док-во: предположим, что какой-то элемент c также является нейтральным элементом группы G. Тогда c = ce = e. Если же и b – два обратных элемента для , то b = be = b(ad) = (ba)=e=.*

*Ч.Т.Д.*

*Если M = , то любое отображение M на себя – это подстановка*

*s =, где .*

*– это перестановка , их число n! равно числу элементов группы S() = . Она называется симметрической группой степени n.*

*Подгруппой группы G = (G,) называется такое подмножество , которое само является группой относительно операции «», заданной в G*

*(запись: H <G).*

*Теорема. H < G = (G,).*

*Замечания:*

*1) H <G,)*

*2) Если H – конечное подмножество группы G, то H < G*

*Теорема 2. Пересечение двух (и вообще любого количества) подгрупп группы является подгруппой той же группы.*

1. Гомоморфизмы групп. Гомоморфный образ и полный прообраз подгруппы. Теорема Кэли (без док-ва).

*Пусть (,) и (,) – две группы, а f – отображение множества в множество . Отображение f называется гомоморфизмом группы в группу , если для любых имеет место равенство f(ab)=f(a)f(b).*

*Гомоморфизм называется эпиморфизмом на , если каждый элемент из является образом хотя бы одного элемента из , т.е. .*

*Гомоморфизм называется мономорфизмом на , если он разные элементы отображает в .*

*Если – гомоморфизм групп, то образ всей группы называют также образом гомоморфизма f и обозначают im f.*

*Ядром гомоморфизма f (запись: ker f) называется полный прообраз подгруппы {}, состоящей из одного нейтрального элемента группы .*

*Теорема Кэли.*

*Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы .*

*Следствие. Существует лишь конечное число неизоморфных конечных групп фиксированного порядка n.*

1. Смежные классы. Индекс подгруппы в группе. Теорема Лагранжа.

*H <G = (G, ); на G определим отношение эквивалентности ~:*

*(другими словами, b =ah, где , или короче: ).*

*Соответствующие классы эквивалентности называются левыми смежными классами группы G по подгруппе H.*

*Аналогично определяют правые смежные классы Ha с помощью условия*

*при введении отношения эквивалентности. В коммутативных группах понятия левых и правых смежных классов совпадают, поскольку aH = Ha.*

*Замечание. Если подгруппа H конечна, то все смежные классы по этой подгруппе имеют одинаковое число элементов, равное | H |.*

*Индексом (G: H) подгруппы H в группе G называется число различных левых (равно как и правых) смежных классов по подгруппе H, если это число конечно.*

*Теорема Лагранжа.*

*Порядок конечной группы G равен произведению порядка подгруппы H на индекс этой подгруппы, т.е. .*

*Следствие.*

*Порядок подгруппы конечной группы является делителем порядка группы.*

1. Нормальные подгруппы. Лемма о ядре гомоморфизма. Факторгруппы. Теорема о гомоморфизмах групп (без док-ва).

*Подгруппа H группы G называется нормальной подгруппой (запись: ), если левый aH и правый Ha смежные классы совпадают (т.е. каждое произведение , где , равно произведению при каком-то ).*

*В коммутативных группах все подгруппы нормальны.*

*Лемма. Пусть – гомоморфизм. Ядро ker f является нормальной подгруппой; смежные классы по ядру – это полные прообразы элементов из .*

*Док-во:*

*H = ker f – подгруппа; докажем, что она нормальна в . и :*

*, откуда . Аналогично проверяется, что . Следовательно, . . Ясно, что все элементы из xH и только они отображаются гомоморфизмом f в элемент f(x).*

*Ч.Т.Д.*

*Пусть . G\H – множество смежных классов по H.*

*определение (\*) корректно и G\H становится группой (нейтральный элемент eH=H, ).*

*Факторгруппой группы G по нормальной подгруппе H называется фактормножество G\H с бинарной операцией (\*). Факторгруппа обозначается G \ H.*

*по правилу – эпиморфизм.*

*Теорема. Гомоморфный образ группы изоморфен факторгруппе этой группы по ядру гомоморфизма.*

1. Циклические группы. Теорема о порядке элементов конечной группы.

*– гомоморфизм*

*Группа , состоящая из степенной одного элемента a, называется циклической группой, порожденной этим элементом.*

*Теорема. Подгруппа D, порожденная элементом a группы G, изоморфна либо бесконечной циклической группе , либо циклической группе порядка .*

*, где , .*

*kerf = {0} D*

*kerf {0}*

*Порядком элемента a из группы G называется порядок конечной циклической подгруппы, порожденной этим элементом. Если же эта подгруппа изоморфна , то будем говорить, что элемент a имеет бесконечный порядок.*

*Теорема. В конечной группе порядок любого элемента есть делитель порядка группы.*

*Следствие. Любая группа простого порядка циклична.*

1. Кольца. Делители нуля. Обратимые элементы кольца.

*(Непустое) множество А называется кольцом, если на нем определены две бинарные операции + (сложение) и (умножение), обладающие следующими свойствами:*

*(А, +) является абелевой группой;*

*Умножение ассоциативно;*

*Операции сложения и умножения связаны дистрибутивными законами (a + b) c = ac + bc, c (a + b) = ca + cb .*

*Теорема. Если в кольце один из сомножителей равен нулю, то и всё произведение равно нулю.*

*Док-во: .*

*Аналогично для .*

*Замечание. Обратное утверждение верно, но не во всех кольцах.*

*Элементы a и b кольца, для которых ab = 0 или ba = 0 и при этом , называются делителями нуля.*

*Теорема. Если ab = ac или ba = ca, то b = c, если только и не является делителем нуля.*

*Обратимый элемент — элемент кольца с единицей, для которого существует обратный элемент относительно умножения.*

1. Поля. Теорема о конечных кольцах без делителей нуля.

*Полем называется коммутативное кольцо K, содержащее не менее двух элементов, в котором все ненулевые элементы образуют группу по умножению (мультипликативную группу K\*).*

*Замечание. Из определения следует, что поле всегда содержит единицу.*

*Теорема. Поле не имеет делителей нуля.*

*Док-во:*

*ab = 0 и*

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

*Док-во:*

1. Идеалы коммутативных колец. Главные идеалы. Идеалы в полях.

*Подкольцо H коммутативного кольца А называется идеалом, если произведение ha = ah лежит в H при любых и .*

*Теорема 1.*

*В кольце А множество всех кратных любого фиксированного элемента является идеалом в A.*

*Идеал кольца А, состоящий из кратных элемента а, называется главным идеалом, порожденным элементом а, и обозначается (а).*

*Теорема 2.*

*Любое поле не содержит идеалов, отличных от нулевого или единичного.*

*Док-во: пусть H – идеал поля K, .*

1. Кольца классов вычетов. Идеалы кольца целых чисел. Кольца .

*Пусть H = (h) – идеал коммутативного кольца A.*

*Два элемента a и b кольца A называются сравнимыми по модулю h (или по идеалу H), если их разность a – b принадлежит идеалу H.*

*Запись: .*

*‘’ – отношение эквивалентности, , т.к. (H, +) (A, +).*

*Смежный класс a + H называется классом вычетов по модулю h (или по идеалу H).*

*Кольцо A / H называется кольцом классов вычетов по модулю h (или по идеалу H).*

*Пример:* ***, n = 2, 3, 4, …***

*Следствие из теоремы о простом идеале. Кольцо классов вычетов кольца целых чисел по модулю n является полем тогда и только тогда, когда n – простое число.*

1. Характеристика кольца. Теорема о характеристике кольца без делителей нуля.

*Пусть – кольцо с единицей. Число называется характеристикой кольца A, если (кол-во единиц равно m) и никакое положительное число, меньшее m, эти свойством не обладает.*

*Если указанное свойство не имеет места ни для какого положительного числа, то говорят, что кольцо имеет характеристику 0.*

*Теорема. Характеристика m любого кольца без делителей нуля (в частности, поля) или равна 0, или является простым числом.*

*Док-во:*

*Пусть . Противоречие.*

*Ч.Т.Д.*

1. Простые идеалы. Поля .

*Идеал H кольца A называется простым, если из того, что , следует, что или .*

*Теорема. Идеал H кольца A называется простым, тогда и только тогда, когда кольцо классов вычетов A/H не содержит делителей нуля.*

*Док-во:*

*A/H не имеет делителей нуля*

*.*

*Следствие. Кольцо классов вычетов кольца целых чисел по модулю n является полем тогда и только тогда, когда n – простое число.*

*Поле классов вычетов по простому модулю – поля из p элементов обозначаются как GF(p).*

1. Евклидовы кольца. Идеалы евклидова кольца.

*Евклидовым кольцом называется кольцо D без делителей нуля, в котором каждому ненулевому элементу a сопоставляется целое неотрицательное число , называемое нормой, со следующими свойствами:*

*а) для всех из D;*

*б) для любых , существует элемент такой, что , где r = 0 или .*

*Теорема. В евклидовом кольце все идеалы главные.*

*Док-во:*

*Пусть – идеал евклидова кольца D. Выберем в H элемент с наименьшей нормой . Тогда любой можно представить в виде , откуда . Не может быть, чтобы , следовательно, .*

*Ч.Т.Д.*

*Следствие. Любое евклидово кольцо содержит единицу.*

*Док-во: применим теорему к единичному идеалу, которым является все кольцо D. Тогда D = (a) .*

*Ч.Т.Д.*

1. Теорема о наибольшем общем делителе.

*Теорема:*

*В евклидовом кольце D любые два элемента a и b имеют наибольший общий делитель d, который представляется в виде d = sa + tb, где s, t .*

*Док-во:*

*– идеал! По теореме 1 этот идеал главный, т.е.*

*. Следовательно, такие, что .*

1. Кольца многочленов. Приводимость многочленов над полем.

*Многочленом (полиномом) от неизвестной x над кольцом A называется выражение вида*

*,*

*( полагаем равным ).*

*Многочлен g(x) из кольца K[x] называется приводимым (над полем K), если*

*g(x) = для подходящих непостоянных многочленов ; в противном случае многочлен g(x) называется неприводимым.*

1. Теорема о кольцах класса вычетов K[*x*] / (g(*x*)).

*Кольцо классов вычетов L = K[x]/(g(x)) по модулю неприводимого многочлена есть поле.*

*Док-во:*

*Пусть т.к g(x) неприводим. Следовательно, .*

*Т.к. , то .*

1. Расширения полей. Поля Галуа .

***Теорема о кольцах класса вычетов K[x] / (g(x)).***

*Кольцо классов вычетов L = K[x]/(g(x)) по модулю неприводимого многочлена есть поле.*

*По теореме о кольцах класса вычетов K[x]/(g(x)), поле L называется расширением поля K.*

*Конечные поля, содержащие элементов (они существуют для любого n), называются полями Галуа и обозначаются GF(). В частности .*

1. Малая теорема Ферма для конечных полей.

*Теорема 1. Пусть – степень простого числа. Любой ненулевой элемент поля GF(q) удовлетворяет уравнению .*

*Для q = p: . (малая теорема ферма)*

1. Мультипликативная группа конечного поля.

*Мультипликативная группа K\* поля K – это группа, содержащая все ненулевые элементы из K, и операция в ней совпадает с операцией умножения в K.*

1. Логарифмы Якоби.

*Теорема. Число примитивных элементов поля GF(q) равно .*

*Если – примитивный элемент поля GF(q), то все ненулевые элементы имеют вид .*

*Логарифм Якоби L(n) определяется равенством .*

*Тогда . Добавим символ: .*