**Разница Windows, android, Linux**. В смысли работы с аппаратной частью одинаково функционирует на одном железе. Устанавливая программу под Windows мы устанавливаем готовый продукт, но он должен прописаться внутри системы и получить доступ к перефирийным устройствам. В Linux программы поставляются в исходники и компилируются по месту.

**Python-** интерпретируемый язык программирования, и медленней компилированных языков в 2-1000 раз. В компилируемых языках таких как СИ, С++ и т.п сначала пишется программа, а потом она компилируется компилятором под данный процессор. В python динамические типы данных, что приводит к не рациональному использованию памяти.

**Julia**- язык программирования предназначенный для математических вычислений, написан на СИ, и по заявлению производителей не менее быстрый чем С++.

**Алгебра** произошла от арабского слова альджабр перевод: восполнение. В математику входят такие разделы как Алгебра, Математический анализ, Дифференциальные уравнения, Теория вероятности, Топология, Математическая логика, Теория кодов, Дискретная математика, Математическая статистика и т.п. Математика дискретная: Алгебра, теория графов. Математика не прерывная: Математический анализ.

Математический анализ = Топология + Алгебра (существует 300 лет.)

Алгебра занимается алгебраическими операциями, и возникла около 100 лет назад.

Герман Вафель – “В математике определение есть акт творения, математическое понятие в момент определения”. Удивительным образом математическими методами и способы описываются законы реального мира.

**Алгебраическая операция**

Пусть дано множество

где и b = -a

– Элементы множества

(a,b) – то откуда берутся элементы.

|a,b A – какому свойству удовлетворяет

**Бинарная алгебраическая операция** — это любое отображение, которое к каждой паре элементов А, В ставит элемент С.

Бинарная алгебраическая операция равна умножению и сложению. С маленькой буквы умножение и сложение являются синонимами бинарной алгебраической операции, а с большой буквы являются отдельными конкретными операциями.

Сколько существуют алгебраических операций?

|| - официальный математический символ обозначающий модуль, и максимальное количество элементов.

Общее число различных элементов вычисляется по формуле =

Алгебраических операций так много, что их невозможно все исследовать, поэтому изучают так называемые «Хорошие» алгебраические операции на которые накладываются определенные ограничения.

**Ассоциативность**

- квантор всеобщности (для любых)

Когда операция умножения обозначается «\*», то она мультипликативная.

Множество А на котором задана ассоциативная бинарная алгебраическая операция называется полугруппой. Так называемых групп очень мало.

**Коммутативность**

Ассоциативность встречается часто, а коммутативность редко.

**Нейтральные элементы**

Если операция мультипликативная, то элемент имеет 3 обозначения: 1,e,E

Если он называется сложением и обозначается «+» то это аддитивная запись:

∃-квантор существования

Когда существует нейтральный элемент, то можно поставить обратный ему элемент.

Элемент «В» обратный элементу «А», если a\*b=b\*a=e

Если такой элемент единственный, то в мультипликации b = 1/a (обратный эл)

В аддитивном случае: a+b=b+a=0 b=-a

Множество «А» ка которых задана бинарная алгебраическая операция

1. Ассоциативная.

2. Есть нейтральный элемент.

3. Каждый элемент имеет обратный.

Называется **полем.**

Отто Юльевич Смит 1891-1936. Вице президент наук полярный исследователь. Первый исследователь в России тории групп. Создал кафедру в МГУ и был ее заведующем.

**Сложение и умножение.** Объекты изучаемые в школе бинарные алгебраические операции сложение, умножения. Запись: «+» - аддитивная, «\*» - мультипликативная. Если на множестве задана всего одна бинарная алгебраическая операция, то все равны, как ее называть и обозначать. Если операция коммутативная, то ее как правило называют сложением и используют аддитивную формулу записи. Если не коммутативная, то всегда называют умножением и используют мультипликативную форму записи.

# Пусть дано множество А на котором дано две алгебраические операции умножение и сложение, если не накладывать никаких условий, то как правило получаем много объектов бесполезных.

# Предположим, что операция сложения является коммутативной, ассоциативной у нее есть нейтральный элемент обозначенный 0 и каждый элемент имеет обратный от умножения потребуем чтобы оно было ассоциативной e или 1. Предупреждение 0 и 1 это просто нейтральный по сложению и совсем необязательно, что это число 0, 1. Это множество А с описанными свойствами **называется кольцом.**

# Формальное определение кольца. Множество К называется **кольцом** если на нем задано сложение и умножение.

# Аксиомы дистрибутивной связи умножения и сложения:

# Эта аксиом задает кольцо с нейтральным элементом

# В кольце можно «+», «-», «\*».

# В полугруппе можно «\*» «-» «+»

# В группе можно «-» «+» «\*»

# Замечание в аксиомах дистрибутивности, сложения и умножения не равноправны и полное название аксиом звучит так: дистрибутивность сложения относительно умножения.

# **Примеры колец:**

# Кольцо целых чисел

# Если 0 не входит, то N полугруппа.

# Неформальное **определение поля**. Если в коммутативном кольце относится умножения не нулевым элементом имеют обратный, то такое кольцо поле.

# Множество рациональных чисел образуют поле. Если добавить перед точки, то множество рациональных чисел превратятся в комплекс чисел.

# Кольцо многочленов К называется **кольцом многочленов**.

# Коэффициент если не нулевой называется старшим коэффициентом.

# На множестве коэффициентов определены операции сложения умножения.

# Операция сложения коэффициентов одной степени складывается.

# Если некоторая степень отсутствует, то коэффициент при ней = 0.

# Неформальное описания множества, перемножаем используя дистрибутивность.

# Эти две формы определяют сложение и умножение 4 степени нужно проверить что это множество K[x] является кольцом и при проверки нужно использовать только 2 определение и тем что К кольцо.

# **Квадратная матрица** — квадратная таблица разбивается на строки и столбцы.

# Диагональ с лева на право, является **главной диагональю.**

# Диагональ с права на лево, является **побочной диагональю.**

# На множестве матриц вводим операции сложения и умножения.

# В матрице в качестве коэффициента может использоваться любое кольцо из многочленов матрицы. Это же относится и к коэффициентам многочлена.

# Важное для программирования и криптографии **кольцо остатков**.

# Остаток от деления на N число называется кольцом вычитания или кольцом остатка.

# На этом множестве зададим сложение и умножение это обычно сложение и умножение чисел но в качестве ответа берется остаток от деления на n.

# **Следствие из аксиомы кольца.**

# **1.** если нейтральной элемент существует, то от единственный.

# **2.** если операция ассоциативна и у элемента «а» есть обратный, то он единственный. Если операция не ассоциативна, то элемент может иметь несколько обратных.

# **Замечание:** элемент который обратный сам себе в математике не редкость.

# Если обратный элемент единственный то его можно обозначить он зависит только от «а» и разночтений не будет.

# Это образное выражение «элемент обратный к а»

# **Замечание:** если операция не ассоциативная, то понятия степени бессмысленно. Если операция ассоциативна, то порядок скобок не важен и понятия степени законно.

# Из соображений удобства вычитаний, нулевую степень лучше считать нейтральным элементом и степень обратного элемента отрицательным числом.

# **3**.В кольце К при умножении на нейтральный элемент по сложению получится всегда 0.

# По аксиоме о существовании обратного по сложению существует элемента, такой что a\*0 +b=0 a\*0+b = (a\*0+a\*0)+b

# **Система линейных уравнений.**

# Пусть К некоторое кольцо например целых чисел многочлена и матриц. Решением СЛУ являются элементы а1 а2 … an называется решением системы если подстановка в их систему у нас получится верное равенство в кольце А.

# Система называется **не совместная** если она немеет решений.

# **Системы называются эквивалентными** если они имеют одно и то же множество решений.

# **Замечание:** все несовместные системы эквивалентны.

# **Предупреждение:** матрицы прямоугольные их можно складывать только если они имеют одинаковый размер.

# **Определение поле:** Коммутативное кольцо в котором есть нейтральный по умножению и все не нулевые обратно 0 не равно 1.

В поле можно «+», «-», «\*», «/».

Поле рациональных чисел

- **поле Галуа**

- самое маленькое поле

**СЛУ только над полем**

**Система называется эквивалентной** если они имеют одно и тоже множество решение.

**Преобразование СЛУ называется эквивалентным**, если оно приводит систему в эквивалентную ей.

**Эквивалентных преобразований.**

1. э.п. Умножение i — тую строку на не нулевой элемент (преобразование обратно)

2. э.п. j-тую строку умножаем на ненулевой элемент прибавляя к i-той строке

3. э.п поменять местами i-тую строку и j-тую.

**Теорема:** 1 и 2 этап является эквивалентными преобразованиями a=(a1,an)-если этот набор был решением исходной системы, то он станет решением получившейся системы. Алгоритм Гаусса или алгоритм решения системы линейных уравнений.

От СЛУ сразу переходим к **расширенной матрице.**

1. шаг рассматриваем 1 столбец матрицы и находим элемент неравный нулю. Если то меняем местами 1 строку и ту строку в которой первый элемент не нулевой.

2. шаг применяем 1 э.п. и умножаем первую строку на (если бы у нас было просто кольцо, то в нем мог бы просто не существовать).

3. шаг применяя 2 э.п обнуляем 1 столбец, тоесть исключаем переменную

4. шаг

Если на последней ступеньке окажутся k неизвестных на который наложены и эти k называются свободные. А остальные n-k называются зависимыми они однозначно выражаются и называются **свободными.**

Над бесконечном полем СЛУ может иметь 0 решений, 1 решение (когда свободных переменных нет), и решений бесконечно много.

**Алгоритм Гаусса или метод исключения.**

Модификации метода Гаусса используют во многих разделах математики.

В алгебре используют:

1 СЛУ

2 нахождение ранга матрицы

3 нахождение обратной матрицы

4 вычисление определителя

5 нахождения базиса пространства

Матрицы по крайней мере квадратные образуют кольцо, там определено «\*», «+» и больше ничего там не живет.

Элементарные преобразования легко можно задать при помощи умножения и сложения матриц.

Если на множестве задана 1 операция , то это может быть группа, полугруппа, если 2 операции связаны дистрибутивность, то будет кольцо или поле.

Введем новое объект: действие полю на коммутативной группе.

**Введение в алгебраически структуры.**

Если на множестве задана одна операция, то это может быть группа или подгруппа.

Если две операции связаны дистрибутивность, то кольцо и поле.

V – Коммутативная группа.

(Когда один элемент из поля, а второй из группы, то это действие поля на группу)

P – Поле ()

Так же как и в случае алгебраической операции, таких отображений очень много, они должно улидотворять следующим свойствам:

Так как группа коммутативна операцию будем обозначать “+” а поле будем обозначать “+” и “\*”

1)



2)



3)



4)

Действие «\*»

В поле Р = «+» или «\*»

В группе V = «» - сложение в группе.

**Векторным пространством надо полем V** называется коммутативная группа P над которой заданы действия:4 аксиомы действия и 10 аксиомы поля и 4 аксиомы группы.

Квадратные матрицы над полем поле являются векторным пространством, если задать следующие действия поле на матрицу. 

Многочлены над полем P[x], то векторное пространство, если действие

Большинство классов функций изучаемые в математическом анализе является векторным пространством над полем D.

**Следствие из аксиомы векторного пространства:**

нейтральный элемент группы V называется нулевым вектором

0-вектор пространства

0-нейтральный элемент в группе V

0-нейтральный по сложению в поле P

0-нулевая матрица

0-нулево отображение



 Наше доказательство из теории колец не подходит.

Здесь можно пользоваться только аксиомами из векторного пространства



(Так как N – группа, то у элемента V есть обратный по сложению)

Если задана:

1. алгебраическая операция группа или подгруппа

2. алгебраические операции поле или кольцо.

Если на коммутативной группе задано действие поле, то это векторное пространство.

**Вектор** - это элемент векторного пространства



Пусть V – векторное пространство над полем 



* Линейная комбинация.

Комбинация называется нетривиальной, если все коэффициенты альфа не равны нулю.

Линейная зависимость.

Вектора V1, V2 ... Vn **- называются линейно зависимыми**, если существует не тривиальная линейная комбинация равная 0 вектору, тоисть хотя бы один альфа не равен нулю.

**Линейная независимость:**

Вектора V1, V2 ... Vn называются линейно независимыми если из это следует, что 

**Свойства линейно зависимых и линейно независимых векторов.**

**1.** Если { V1, V2 ... Vn } линейно зависимы тогда любое его расширение тоже будет линейно зависимым. Так как V1, V2 ... Vn - линейно зависимые то существует линейная комбинация.

**2.** Любое множество векторов содержащее нулевой вектор - линейно зависимое.

Пусть { V1, V2 ... Vn } - вектора которые содержат .

 - эквивалентная линейная комбинация

**3.** Если { V1, V2 ... Vn } - линейно независимо, то любое его подмножество линейно независимо

**Доказательство:**

Пусть  - подмножество, тогда

 Значит , при 

4. Если  - линейно зависимо, то один из них можно выразить через другие

**Доказательство:**

 - так как комбинация нетривиальна, то хотя бы один из альфа не равен 0.

Не теряя общности можно сказать, что 

Мы рассматриваем не частный случай, а произвольный. Просто выполнены комбинации не меняющие уравнения. Просто изменили нумерацию векторов



**Теорема:**

Из любого конечного множества векторов можно выделить линейно независимое подмножество которое будет задавать такое же подпространство что и в исходном.

**Определение:**

Пусть V - векторное пространство над полем P. W содержится V - подмножество множества V. W < V - если оно будет векторным пространством относительно сложения заданным V и действия P заданного под V, то оно **называется подпространством.**

Как проверяется является ли подмножество W подпространством или нет?

Если проверять по определению нужно проверять как минимум 8 аксиом поэтому проверять с помощью критерия подпространства:

Подмножество W будет подпространством <=>

1. 
2. 

**Доказательство:**

Так как W подмножество V то все аксиомы так как они верны для всех элементов из V так же верны для всех элементов из W сложность только в том, чтобы W была замкнута относительно + и относительно действия поля P.

Подпространство это такое подмножество которое является векторным пространством, имеющие относительно тех же операций, что заданы в начальном пространстве.

V пространство на поле Р - 

**Линейная оболочка натянутая на вектора** V1, Vn.

**Утверждение:**

Определенное на бесконечности множество векторов, является векторным подпространством, так как все векторы принадлежат V, то не сложено использовать критерий подпространства.



Если пространство V задано порождающим множеством, то из него можно выделить подмножество которое по-прежнему будет порождающим, но будет линейно независимым и **называться оно будет базисом**. В каждом векторном пространстве есть базисы.

**Доказательство:**

Если вектора линейно зависимы, то они сразу образуют базис. V = < V1, V2 ... Vn > .

Пусть они линейно зависимы то существуют элементы 

не теряя общности можно считать, что V1 = B2 V2 + ... + Bn Vn мы можем отбросить вектор V1 из нашего множества, и он по-прежнему останется порождаемым. У нас останется множество из (n-1) вектора. Не позже чем на (n-1) шаге, у нас получится линейно независимое множество.

**Координаты вектора**



Координаты вектора V в базисе е1…еn

Векторное пространство строк - это абстрактная модель векторного пространства.

P-поле. P^n = {}



Операция сложения- покоординатная сумма.

Операция в действии- это умножения каждой координаты на альфа.

 



**Канонический базис**

**Пространство называется N-мерным**, если его базис содержит N-элементов.

Если пространство имеет хотя бы один базис из N-элементов, то можно рассмотреть аналог векторного пространства не над полем P, а над кольцом К (4 аксиомы группы и четыре аксиомы действия). Такие математические объекты называются модулем.

Над модулями много чудес:

1. у некоторых модулей нет базиса.

2. у некоторых базис есть, но имеет разное кол-во элементов и при том бесконечное.

У каждого вектора координаты базиса единственные.

**Доказательство:**

Пусть напротив



 - Однородная система линейных уравнений. Множество решений - является векторным пространством (подпространством в пространстве строк P^n, если кол-во не известных = n).

**Доказательство:**

Так как все решения, то можно воспользоваться критерием подпространства.



**Определение:** любое отдельно взятое решение неоднородной системы уравнений называется **частным решением**.

Пусть  - отдельно взятое частное решение.

Утверждение:

произвольное решение не однородной системы линейных уравнений имеет вид:

, а – некоторое решение однородной системы

**Доказательство:**

 - произвольное решение неоднородной системы.

 - частное



**Линейные отображения.**

Пусть V, W - два линейных подпространства над одним и тем же P.

Отображения из V стремится к W называется линейным, если. 

Эквивалентная формулировка, которая выявляет суть происходящего:



90% всей прикладной математики - это либо вектора пространства, либо кольцо многочленов, либо кольцо матриц.

Как задавать линейные отображения?

1. Чтобы описать линейно отображения в пространстве V - {e1, e2 ... en} и в пространстве W - {f1, f2 ... fn} - это базис.

Так как {e1, e2 ... en} - базис, то



2. По определению линейного отображения: 

Линейное отображение однозначно определяется образами базисных векторов.

Так как каждая  принадлежит пространству W, то его можно выразить через базис {f,…,f(n)}



 - матрица линейного отображения

**Замечание:** конечно эта матрица зависит от базиса она записана. Если базис меняется, то и матрица меняется.

Как задается матрица линейного отображения?

Столбцы матрицы - образы базисных векторов.



Координаты умножение координатного отображения на координаты вектора

Образа

Любимый в мат анализе случай, когда пространство W имеет div1, то есть совпадает с полем P.



Первична супер позиция отображения, а произведение матриц это вынужденная мера для описания линейных отображений.

**Бинарные отношения. Сравнения элементов.**

Пусть A - некоторое множество, рассмотрим прямое произведение

 - множество упорядоченных пар.



**Бинарное отношение** – это любое подмножество прямого произведения А\*А.

А={0,1,2}

На трех элементах можно ввести 512 различных бинарных отношений.

Изучать все бинарные отношения – нерациональная задача.

**Отношение называется**

* симметричным, если 
* антисимметричным, если 
* транзитивным, если 

Отношение называется **отношением эквивалентности** если оно рефлексивно, семетрично и транзитивно.

**Отношение является не строгова** порядка если рефлексивно антисимметрично, транзитивно.



**Свойства эквивалентности.**

Бинарное отношение на множестве A называется эквивалентным рефлексивно, транзитивно, симметрично.

Принято отношение эквивалентности обозначать: a ~ b.

Если a ~ b, то b ~ a

Если a ~ b, b ~ с => a ~ c

Эквивалентность это обобщение понятие равенство.

**Эквивалентные** - совпадения многих параметров элементов.

**Определение:**



Классы эквивалентности либо совпадают либо непересикаются. Тоисть множество A раскладывается на множество непересекающихся классов элементов.

Доказательство:

 

По определению класса эквивалентности значит c ~ a, c ~ b, так как отношение эквивалентности антисимметрично a ~ c, c ~ b и силу транзитивности a ~ b

Значит 

Таким образом пересекающиеся классы совпадают. Если у нас есть отношения эквивалентности мы можем рассмотреть новое множество, элементами которого являются эти классы эквивалентности.

Так же множества называется **фактором множества**: A|~

**Отношение эквивалентности такое:**

Скажем что а~b натуральные элементы, если их разность делится на 5

[0] = {1, 5, 10, 15}

[1] = {1, 6, 11…}

[2] = {2, 7, 12…}

[3] = {3, 8, 13…}

[4] = {4, 9, 14, 19 ..}

Если элемент, а принадлежит классу эквивалентности то он является представителем данного класса.

Если множество A является группой кольцом или полем то при выборе соотвецтвующей эквивалентности будут получаться факторы группы, факторы кольца.

Отношение нестрогова порядка рефлексивно, антисимметрично, транзитивно.

**Определение:** элемент а называется **max** если a>= b для любого b принадлежащего A который с ним сравним. Элемент а называется **наибольшим** если он сравним со всеми элементами и max.

Изображение частного одна порядочных множеств виде графов.

* Сравнимые между собой элементы соединены прямой.
* Те элементы которые больше находятся выше.

4

2

3

5

1

Элемент а является наименьшим если он сравним со всеми и **min**. Элемент а называется **минимальным** если а <= b для любого b принадлежащее A который сравним с ним.

**Множество называется линейно упорядоченным** если у него все элементы сравнимы между собой. В нем (max и наибольший) и (min и наименьший) совпадают.

Пусть A - частично упорядоченное множество и B подмножество A.

а является **верхней гранью**, если а принадлежит A, a>=b, b принадлежит B.

а является **нижней гранью** множества B, если он меньше всех элементов B.

Как верхний, так и нижней граней может не быть а может быть бесконечность.

Верхняя грань называется **супремум,** если она меньше всех граней, то она единственна.

**Инфинум** такая нижняя грань-такая грань которая больше или равно всех остальных нижней граней.

**Множество называется вполне упорядоченным** если оно линейно упорядочено и любое его подмножество имеет минимальный элемент.

У подмножества (0;1) минимального элемента нет.

Множество натуральных чисел- вполне упорядоченное множество.

Отображение из множества A во множество B, называется **инъекцией** (разные элементы переходят в разное).

Отображение называется **сюръективным** если для любого b принадлежащее B существует такое a принадлежащее A такое что f(a) сюръекция.

Отображение называется **биекция** если отображение и инъекция и сюръекция.

**Множества называются равномощными** если можно установить биекцию (взаимно однозначное соотвецтвие).

В бесконечных множествах может быть такое что множество и подмножества имеют одинаковую мощность. Множества действительных и натуральных чисел не равномощно. Действительные числа имеют мощность континуума.

W0 - весь пересчитанные натуральный ряд. 1,2,3 ... W0.

Трансцендентное число называется придельным если у него нет предыдущего элемента.

**Метод математической индукции.**

Пусть некоторое утверждение сформулировано для любого числа n.

1. база индукции (проверка утверждения n = 1)

2. Предположение индукции (предполагает, что утверждение доказано для натурального числа n).

3. Шаг индукции (докажем, что утверждение верно для n+1).

Пусть все три шага выполнено, но тем не менее утверждение верно не для всех натуральных чисел. Так как множество натуральных числе вполне упорядочено, тоисть минимальнольное (m), зависит для m-1 утверждение верно, тогда можно сделать шаг индукции.

**Метод трансцендентной индукции.**

Пусть утверждение сформулировано для всех трансцендентных чисел.

Доказываем это также:

1. база.

2. предположение индукции

3. Шаг индукции.

**Элементы комбинаторики, перестановки, размещения, сочетания с повторением.**

**Определения:** пусть А - некоторое множество любая биекция множества А на себя **перестановка**. Если множества А конечное, то не теряя общности можно считать что это номера элементов А={1,2,... n}.

1. сколько перестановок на множестве А



Обобщение факториала по непрерывности определен в гама функции.

**Формула стерлинга.**



**Число называется алгебраическим** если оно является корнем некоторого многочлена с целыми коэффициентами.

**Число называется трансцендентным** если оно не является корнем никакого многочлена с целыми коэффициентами.

**Теорема:**

Числа е и PI трансцендентно.

**Перестановки образуют группу**.

**Операция является супер позиция отображений,** если A принадлежит n(элементы), то Sn группа перестановок.

**Доказательство:**

Так как суперпзиция любых отображений ассоциативна то ассоциативность есть.

Нейтральный элемент. Тождественная перестановка является нейтральным элементом. У каждой перестановки есть обратная.



**Определение:**

Пусть А - некоторый математический объект, биекция этого объекта на себя, сохраняющая его математические свойства, **называется симметрией.**

Группа перестановок - группа симетрии если на множестве нет никаких структур.

**Размещение.**

Пусть дано множество из n элементов. Любое упорядоченное подмножество из m элементов - **размещение из n по m b** и называется 

Сколько размещений из n по m



Алгоритм Гаусса используется:

1. При решение систем линейных уравнений.

2. Нахождений обратных матриц.

3. Нахождение базиса.

4. Нахождение определителя.

**Алгоритм Евклида. Деление с остатком.**

Пусть К-кольцо необязательно коммутативное (кольцо матриц)



Символ | означает, что а делит b

(делит слева)

(делит справа)

Когда говорят что элемент b делится на a малое имеется ввиду умножение на обратный.

Свойства делимости.



Нулевой элемент **а называется делителем нуля** если существует такой элемент b, такой что a\*b=0.

Все кольца матрицы имеют делители нуля.

Кольца вычетов Zn если n>0 тоже имеют делитель 0.

**Основное свойство колец без делителей нуля.**

a\*b=a\*c => b=c.

**Замечание:** Это пример логического сокращения, а совсем не результат умножения на a^-1, потому что обратного элемента а может и не быть.

**Доказательство:**

Так как a\*b=a\*c это равносильно a\*b=-a\*c=a\*(b-c)=0 и так как в кольце нет нуля то один из сомножителей должен быть равен нулю. Так как а!=0, то остается один вариант b-c=0 равносильно b=c=0.

**Утверждение:** Пусть К-кольцо без делителя нуля, тогда кольцо многочленов K[x] тоже немеют делители нуля.

**Доказательство:** Берем два многочлена:

f и g 

Так как в кольце К нет делителей нуля произведение не нулевых коэффициента не может быть равно нулю.

В любом поле нет делителей нуля.

**Доказательство:**

Пусть а!= 0, но а\*b=0 так как а не нулевой элемент и принадлежит полю то у него существует обратный элемент по умножению.



Кольцо К является евклидовым если на множестве его не нулевых элементов определена функция  , которая каждому элементу а ставит в соотвецтвии число называемое евклидовой степенью или просто степенью.

Кроме того на кольце К определен алгоритм деления или алгоритм Евклида.

 ,где элемент r = 0.

Элемент а - делимое

b - делитель

g - не полное частное

r - остаток

Евклидовых колец очень мало.

Пример 1:

Кольцо Z целых чисел является евклидовым. Евклидовой степени является модуль числа. Алгоритм деления с остатком это алгоритм деления уголком.

Пример 2:

Пусть P[x] - поле когда кольцо многочленов с коэффициентом в поле. Степень обычная степень многочлена. Алгоритм деления - деления многочлена на многочлен с остатком.

Многочлены от двух (P[x,y]) и более переменных евклидовыми не являются.

НОД - наибольший общий делитель.

НОК - наименьшее общее кратное.

Пусть К кольцо



1. условие общее d|a и d|b.

2. наибольший если s|a и s|b равносильно s|d(делится на все остальные делители).

В кольцах элементы упорядочены.

Двойственным к НОД является НОК.



**Замечание:** Далеко не во всех кольцах есть НОД и НОК.

**Теорема:** Пусть К-евклидово кольцо тогда в нем два любые не нулевых элемента a и b имеют НОД, единственный с точностью до умножения на обратный элемент.

**Доказательство:**

О единственности: Если у нас два НОД то есть d1 и d2,то из определения НОД следует что d1|d2 равносильно d2=d1\*c1 d2|d1 равносильно d1=d2\*c2.

d1 = d1\*c1\*c2 равносильно с1\*с2=1 (взаимообратные)

**Алгоритм нахождения НОД**

а=b\*q+r p(r)<p(b)

b=r\*q1+r1 p(r1)<p(r)

r=r1\*q2+r2 p(r2)<p(r1)

.......

r(n-2) = r(n-1)\*qn+rn p(rn)<p(r(n-1))

Так как степень N число и она не может уменьшаться бесконечно и rn будет ненулевым остатком. НОД будет последний ненулевой остаток rn. Значит проверим что rn общий делитель. Из последней строки следует что rn / r(n-1), из предпоследней строки следует что rn / r(n-2). Из второй строки следует что rn|b из первой rn|a. Пусть S|a и S|b проверим что s|rn.

Теперь просматриваем нашу таблицу сверху вниз. Из первой S|r из второй S|r1 из предпоследней S|rn.

**Следствие из алгоритма Евклида.**

Если



То есть НОД – это линейная комбинация элементов a и b.

**Доказательство:** Так как НОД это rn то просматриваем нашу таблицу снизу вверх. Из предпоследней строки rn выразим через (r(n-1);r(n-2)), из третей строки r(n-1) выразим через (r(n-2);r(n-3)), из первой строки r выразим через (a;b).

**Теорема:** кольцо вычетов Zp где p простое число, является полем.

**Доказательство:**

Так как кольца вычетов это коммутативные кольца то единственное что нужно проверить, что у любого ненулевого элемента а есть обратный элемент по умножению.

 Так как р – простое число, то p|1 b p|p – НОД (a,p)=1

Тогда по следствию алгоритма Евклида



Таким образом элемент V является обратным по умножению.

Однозначность разложения на простые множители.

Пусть К-кольцо без делителей нуля.

Элемент а,b называются **ассоциированными,** a|b и b|a тоисть они отличаются на обратные элементы.

В кольце целых чисел ассоциированными являются +-а.

Элемент **p называется простым** если он делится только на обратные элементы и элементы с ним ассоциированы.

**Однозначность разложения на простые множители.**

Кольца Q называется кольцом с однозначным разложением на простые множители если из этого следует что а=u\*p1...pn a=v\*q1...1m u и v это обратные элементы а, p и q просты то отсюда следует что n=m и С до перестановке множителей p1 ассоциировано с q1, p2 ассоциировано с q2 и тд.

Пример: 6=2\*3=3\*2=-1\*2\*-3=-1\*-2\*3=1\*-2\*3=....

В кольце многочленов принята несколько другая терминология. Простые элементы кольца многочленов называются **неприводимыми многочленами.**

**Многочлен называется неприводимым** если он не раскладывается в произведение многочлена нашей степени.

Однако нет формулы, которая выводила бы простые числа.

К-коммутативное кольцо ассоциированная с единицей.

**Утверждение:**

Евклидово кольцо не имеет делителя нуля.

Пусть напротив существует два элемента: а!=0 b!=0 a\*b=0

В силу монотонности евклидовой степени должно выполнятся неравенство: p\*(c\*b)>=p(a)

a\*b=0 p(0) а степень для нуля вообще не определена.

**Определение:**

Если есть два разложения где u,v-обратные

a=u\*p...pn

a=v\*q...qm

**Теорема:** в евклидовых кольцах есть однозначность разложения на простые множители - факториальное кольцо.

**Следствие 1**(основная теорема арифметики):

В кольце целых чисел есть однозначность разложения на простые множители.

**Доказательство:** так как кольцо целых чисел евклидово, то его факториальность следует из теоремы.

**Следствие 2:**

Кольцо многочленов надо полем P[x] является кольцо с однозначным разложением на простые множители.

**Доказательство:** так как кольцо многочлена над полем евклидово то его факториальность следует из теоремы.

**Доказательство основной теоремы:**

**Определение:** кольцо К называется кольцом с разложением на простые множители, если для любого а из а принадлежит К существует а=v\*p1...pn p1...pn (простые).

**Лемма 1:** в евклидовом кольце есть разложение на простые множители.

**Доказательство:**

База индукции P(а)=0 (степень от а=0) докажем что когда элемент а обратим а принадлежит К, а=v (разложение).Пусть а=b\*c так как P(а)=0 то в силу монотонности степени следует что p(b)=p(c)=0. По алгоритму Евклида поделим с остатком элементы b на а.b=a\*q+r, где p(r)<p(a)=0 следовательно r=0 b=a\*q=(b\*c)\*q следует b\*(1-c\*q), так как К без делителей нуля то следует c\*q=1 c принадлежит К. Аналогично поменяв местами b и c мы получим что с обратный.Так как произведение обратных элементов тоже обратно. а-обратный, и сам является разложением на простые множители. Обратные элементы ассоциированы с единицей и поэтому в теории колец их иногда называют единицами.

Предположение индукции: пусть для всех p(a)<n доказано что у низ есть разложение на простые множители.В силу монотонности степени p(b)<n p(c)<n



Рассмотрим случай, когда у элемента b степень не уменьшилась Р(b)=n



В силу монотонности степени

1-qc=0 => 

Получается что а и b ассоциированы и если у других разложений нет а значит а простой элемент является своим собственным разложением на простые множители.

**Критерий** - это очень ценное математическое рассуждение когда вместо конечных проверок используют определенные правила.

**Лемма 2:** (критерий однозначности разложения на простые множители)

Пусть К-кольцо c разложением на простые множители, оно будет факториальным если p|a\*b => p|a или p|b

**Доказательство:** Пусть кольцо факториальное. Проверим что критерия выполняется

 В силу однозначности разложения n = m + 1. P будет ассоциирован с

одним из 

пусть выполнено условия критерия. Проверим что кольцо факториально



по условию критерия простой элемент q1 делит первый множитель или второй. Если он делит первый или второй то дальше ...

Вместо q1 берем q2 и также находим для него ассоциированный логическим сокращением элемент который есть кольцо без делителей нуля но вычеркиваем q1 и p1. После m таких циклов все второе разложение сведется к обратному элементу v а первая к элементу u.

**Лемма 3:** В евклидовых кольцах выполняется критерия однозначности разложения.

**Доказательство:** В лемме 1 доказывается что в евклидовы кольца имеют разложения поэтому можно говорить о критерии.

Пусть p|a так как p простой элемент следовательно НОД(а,p)=1.

По следствию алгоритма Евклида:



**Многочлен как функция.**

**Определение:** Пусть К-кольцо. К[x]- кольцо многочлена.

f(x) принадлежит К[x].

Многочлену поставим соотвецтвии функции, называется полиномиальные. 

Многочлены могут быть разные, задаваемые ими функции могут совпадать.



Корень многочлена f(x) называется такой альфа принадлежащий А в котором этот многочлен =0, f(a)=0.

**Теорема Остен Безу:** элемент альфа является корнем многочлена f(x) когда



**Доказательство**: делим многочлен f(x) c остатком на (х-альфа)

Деление возможно, так как при х коэффициент 1

f(x)=(x-a)\*g(x)+r

Допустим альфа - корень тогда

f(а)=(a-а\*g(а)+r) f(а)=r

f(x)=(x-а)\*g(x)

f(а)=(а-а)\*g(а)=0

Она связывает понятие корня из математического анализа с многочленом из алгебры. Понятие корня- понятие из математического анализа.

Корень альфа называется корнем кратности К тогда и только тогда, когда



**Теорема:** Пусть Р-поле

f(x) принадлежит P[x]-многочлен надо полем f(x) имеет корни с учетом их кратности не больше чем его степень.

**Доказательство:**

Пусть альфа1...альфаk -все разные корни очевидно что многочлены х-альфа1 неприводимы тоисть просты элемента кольца.

Пусть S1...Sk - их кратности.

Из теоремы Безу следует (х-альфа1)^S1|f(x)

Так как кольцо многочленов над полем факториально,



Степени f(x)

**Следствие:** многочлен n степени над полем однозначно задается значениями в (n+1) точке.

**Доказательство:**

Пусть f(x) и g(x) принимают одни и те же значения в (n+1) точке.

Тогда многочлен n(x) равен из разности, в n+1 точке имеет нули а его степень n противоречие.

**Алгоритм нахождения обратной матрицы.**

11

Элементарными преобразованиями строк, мы А превращаем в единичную, тогда на месте единичной матрицы появится матрица 11

**Доказательство:**

Так как каждое элементарное преобразование строк равносильно умножению матрицы слева на трансвекцию или диагональную матрицу, то преобразование матрицы в единичную:

11

**Следствие из разложения на простые множители**

Явная формула для НОК и НОД

11

**Замечание:**

Не обязательно все показатели не равны нулю.

11 11

На практике проще всего НОД искать по алгоритму Евклида.

**Многочлен как функция. Интерполяционная форма Лагранжа.**

Пусть Р-поле.

11 - значения f(x) в точке.

Требуется построить многочлен n-1 принимающий

11

**Дифференцирование.**

Кольцо 11, так как на алгебраических объектах не всегда можно ввести топологию, то понятие предела малосодержательных.

**Определение:**

Пусть К-кольцо – коммутативное с единицей.

Дифференцированием называется любое отображение 11

11

**Теорема:**

Полное описание дифференцирований в кольце

Дифференцирование однозначно определяется производной от многочлена х, при этом d(x) – может быть любым многочленом K[x].

Дифференцирование называется классическим, если d(x)=1.

**Доказательство:**

Шаг 1.

11

Шаг 2.

11

Шаг 3.

Чему равна производная 11?

11

Применяя математическую индукцию 11

Таким образом неопределенным осталось только производная от х, так как на нее нет никаких ограничений, то d(x) может быть любым многочленом из K[x].

Пусть Р-поле и d-класс производных в кольце P[x].

**Кратные корни и производные.**

**Теорема:**

Корень является кратным, когда он является корнем и многочлена, и его производной.

**Доказательство:**

Пусть а-корень кратности К, тогда по определению кратного корня

11

Обратно.

Пусть а-корень многочлена f(x) и корнем его производной, проверим, что его кратность не меньше двух.

Пусть напротив 11 , тогда 11

**Следствие:**

Многочлен f(x) может быть в поле Р не иметь корней или эти корни найти крайне затруднительно.

Приближенные вычисления не хороши тем, что с их помощью нельзя доказать, что корни равны.

Если многочлен f(x) или в поле, или в расширении имеет кратные корни, то мы можем найти их, не находя их.

Если у него есть кратные корни, то 11.

**Поле Дробей.**

Пусть К-кольцо без делителей нуля, коммутативное и с однозначным разложением на простые множители. Кольцо Z или P[x]. Мы построим поле, содержащее кольцо К, которое называют полем дробей.

**Определение:**

Полем дробей называется 11 множество формальных дробей.

**Определение:**

**Дроби называется эквивалентными или равными**

11

**Множество эквивалентных дробей называется классом эквивалентности.**

Элементы поля дробей, являются не сами дроби, а их классы эквивалентности.

**В поле дробей умножение:**

11

Так как операция задается на классах, а выражаются через представителей, то нужно проверить корректность ее задания, то есть от замены представителей результат не изменяется.

11

Операция «+»

11

Нужно проверить 4 аксиомы группы по сложению, 4 аксиомы группы по умножению, 4 аксиомы дистрибутивности.

11

**Простейшие дроби.**

Пусть К евклидово кольцо Q его поле дробей например поле Q чисел a/b называется правильной если f(a)<f(b)

Дробь называется простейшей если она имеет вид такой где a/p^n p-простой f(a)<f(p)

7/36=a1/2 + a2/4 + a3/3 +a4/9