**Определение**: Пусть Х – произвольное множество. **Бинарной алгебраической операцией** на Х назовём произвольное отображение (функция)

**ԏ : Х \* Х** → Х

**Определение** Бинарная операция \* на множестве Х называется **ассоциативной**, если

(а \* b) \* с = а \* (b \* c) для всех a,b,c ∈ Х

**Определение  Коммутативная** операция, если

а \* b = b \* а  a,b ∈ Х

**Определение**: элемент e ∈ Х называется **единичным (нейтральным)** относительно рассматриваемой бинарной операции, если

е \* х = х \* е = х      ∀ х  ∈ Х

**Определение:** Множество Х с заданной на нем бинарной ассоциативной операцией называют **полугруппой.**

Полугруппу с единичным элементом называют **моноидом.**

**CardM** – количество элементов множества М или **|M| - мощность множества М.**

**Определение** Всякий подмоноид моноида М(Ω) называется **моноидом преобразований** множества М.

**Определение.** Элемент а моноида (M, \*, e) называется **обратимым**, если

∃ b ∈ M : ab = ba = e

**Определение.** Моноид G, все элементы которого обратимы называются группой

**Определение.** **Мн-во G называется группой**, если выполняются:

1) На множестве  G задана бинарная операция

2) операция ассоциативна

3) G обладает единичным (нейтральным элементом)

4) Существует обратный элемент

**Определение.**  **Коммутативная группа**, то есть группа, в которой операция a o b коммутативна, называется **абелевой**. В абелевых группах операция обозначается ⊕ или просто +, элемент, обратный к a, обозначается –a, а единица называется нулем

Группа с аддитивной операцией называется **аддитивной**. Группа с мультипликативной операцией называется **мультипликативной**.

**Для обозначения числа элементов используют CardG, |G|, (G: е)**

**Определение.** Подмножество H ⊂ G называется  **подгруппой** в G, если

1. e ∈ H,
2. h1,h2 ∈ H => h1 \* h2 ∈ H
3. h ∈ H => h-1 ∈ H

Подгруппа называется **собственной**, если H ≠ G и H ≠ е. Иначе она называется **тривиальной** (H = G или H = е).

**Определение.** Возьмём теперь в качестве семейства {Hi , i ∈ I } все те подгруппы, которые содержат данное мно-во S ⊂ G. Тогда их перечисление

                <S> = sHH

в силу теоремы 1 будет подгруппой в группе G, оно содержит S и является минимальной подгруппой содержащей S

**Определение.** Будем называть <S> **подгруппой порожденной множеством** S в группе G, а S – **множеством образующих подгруппы**  <S>

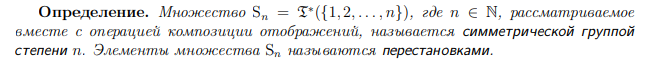
**Определение**. Пусть G – произвольная группа, a – некоторый её элемент. Возможно:

1. Все степени элемента a различны aman при m≠n. В этом случае говорят, что элемент aG имеет **бесконечный порядок**.
2. Имеются совпадения am=an при m≠n.

Пусть m>n; ama-n=ana-n=>am-n=e.

Т.е. существуют положительные степени элемента a равные е.

**Пусть q – наименьший положительный показатель для** aq=1, q>0**. То говорят, что** a **– элемент конечного порядка q**.

**Определение.** **Группу** S(Ω) **называют симметрической группой степени n и обозначают** Sn.****

Её элементы принято обозначать строчными буквами греческого алфавита и называть **перестановками.**

Наглядно перестановку :i(i), i=1, 2, …, n изображают **двухрядным символом**

**Определение.** Назовем две точки i,j∈={1, 2, …, n} **эквивалентными относительно циклической подгруппы** <π>⊂Sn или просто  π**-эквивалентными** j=S(i) для некоторого SZ.

Так как Sn конечная группа, то каждая ее подгруппа тоже конечная.

Если  Card<>=q, то можно считать  0≤S<q.

**Определение. Цикл длины 2 называется транспозицией**. Любая транспозиция имеет вид (ij) и оставляет на месте все символы отличные от i и j. Из предыдущей теоремы вытекает следствие.

**Определение.** Функция f(X1, …, Xn) называется **кососимметрической**, **если**f=-f для любой транспозиции ∈Sn, то есть f…, Xj, …, Xi, …=f(…, Xi, …, Xj, …)

**Определение.** Перестановка π∈Sn называется **четной**, если =1, и **нечетной**, если =-1.

**Определение.** Для любых двух множеств X и Y всякое подмножество 0⊂XY называются бинарным отношением между X и Y. (или просто на X, если X=Y)

Для упорядоченной (x,y)∈0 используют обозначение x0y и говорят, что x находится в отношении 0 к y.

**Определение. Бинарное отношение** **~ на X называется отношением эквивалентности**, если x,  x',  x''∈X выполнены условия:

i x~x рефлективность

ii x~x'=>x'~x симметричность

iii x~x'⋀ x'~x''транзитивность

a≁b означает отрицаение эквивалентности

**Определение.** Подмножество x={xX|x'~x}⊂X всех элементов, эквивалентных данному x, **называется классом эквивалентности**, содержащим x.

Замечание. Так как x~x, тоxx

**Определение.** Любой элемент x'x называется **представителем класса** x.

**Определение**.    Две группы G и G` с операциями \* и ○ называются изоморфными если существует отображение f: G→G` для которого выполняется:

1. **f(a\*b) = f(a○b)**
2. **f - биекция**

**Изоморфность групп обозначается G≅G`.**

**Определение**.     Изоморфизм 𝜑: G→G будем называть **автоморфизмом** группы G.

Если 𝜑, 𝜓 - автоморфизм группы G, то 𝜑 ○ 𝜓 - также автоморфизм группы G.

**Определение**.     Отношение f: G → G` группы (G, \*) в (G, ○) называют гомоморфизмом, если

    ∀ a,b ∈G        f(a\*b) = f(a)○f(b).

Ядром гомоморфизма f называют множество

    Ker f = {g∈G | f(g)=e`∈G`}

    единичная группа↑

Гомоморфное отображение группы в себя называется эндоморфизмом.

**Определение**.     Подгруппа H группы G называется нормальной в G, если Hx = xH ∀x∈G

    (x-1Hx = H)

В этом случае пишут H ⊴ G, а если H ≠ G, то H ⊲ G.

Говорят, что элемент g сопряжен с элементом g посредством элемента x, если g = x-1gx и пишут, что g = gx.

**Определение**.     Группы не содержащие собственных нормальных подгрупп, называются простыми.

***Кольцо*** *–* ***это алгебраическая система, которая является абелевой группой хотя бы по одной операции.***

*Если умножение обладает еще и свойством* ***коммутативности****, то это уже коммутативное кольцо. А если это* ***коммутативное кольцо*** *еще и с единицей (то есть моноид по умножению), то его прямо так и называют –* ***кольцо с единицей***

**Определение** кольца:

Пусть дано K – непустое множество, на котором заданы две бинарные операции + (сложение) и \* (умножение), удовлетворяющие следующим условиям:

1. (K, +) – абелева группа
2. (K, \*) – полугруппа
3. (а + b) + c = ac + bc, c (a + b) = ca + cb (дистрибутивность), для всех а, b, c из К

Тогда К называется кольцом.

(К, +) – называется аддитивной группы

(К, \*) – мультипликативной полугруппой

Если (К, \*) – моноид, то говорят, что (К, +, \*) – кольцо с единицей.

1 – единица по умножению (то есть элемент e)

0 – единица по сложению (то есть элемент e)

**Определение** подкольца:

    Подмножество L кольца К называется подкольцом, если:

        х,у ∈ L => х – у ∈ L и ху ∈ L то есть L – подгруппа аддитивной группы и подполугруппа мультипликативной полугруппы кольца.

Очевидно, что пересечение любого семейств подколец в К является подкольцом.

] T – некоторое подмножество К, тогда <T> - пересечению всех подколец К, содержащих Т будут подкольцом, которое называется подкольцом, порожденном подмножеством Т.

Если Т подкольцо, то <Т> = Т

**Определение** коммутативного кольца:

    Если ху = ух, для любых х, у ∈ К, то кольцо К называется коммутативным.

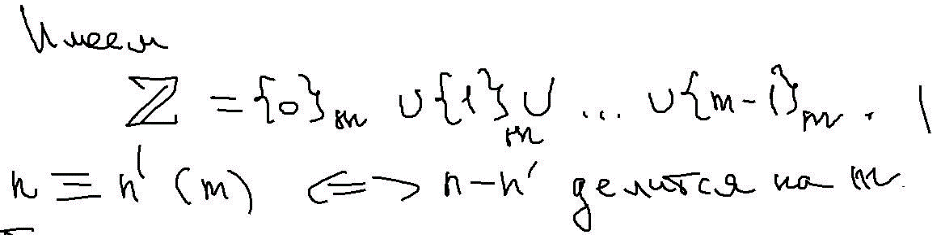
Кольцо классов вычетов

] m ∈ N, m > 1, mZ – подкольцо кольца Z.

**Определение**. Два целых числа n, n’ называется сравнимыми по модулю m, если при делении на m они дают одинаковые остатки. При этом пишут n ≡ n’ (m) или n ≡ n’ (mod m), а число m называется модулем сравнения.

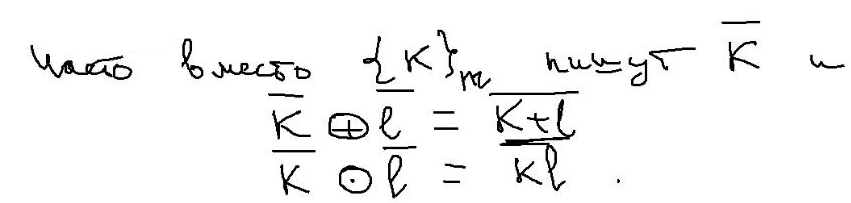
Мы имеем разбиение Z на классы чисел сравнимыми между собой по модулю m и называемых классами вычетов по модулю m.

Каждый класс вычетов имеет вид {r}m = r + mZ = { r + mk, k ∈ Z}



**Определение** кольцо классов вычетов по модулю m:

Кольцо {Zm, ⊕, ⊗} будем называть кольцом классов вычетов по модулю m.



**Определение** гомозорфизм колец

] (K, +, \*) и (K’,⊕, ⊗) – кольца. Отношение f  : K -> K’ называется гомоморфизмом, если оно сохраняет обе операции:

    f(a+b) = f(a) ⊕ f(b)

    f(a\*b) = f(a) ⊗ f(b)

Утверждение

1. f(0) = 0’
2. f(na) = n(fa), a ∈ K, n ∈ Z
3. ЕСЛИ У НАС КОЛЬЦА С ЕДИНИЦЕЙ, то f(1) = 1’, где 1’ – единица кольца K’ (этот пункт не обязателен, а вот 1 и 2 обязательны, см. начало предложения)

**Определение** Ядра гомоморфизма

Ядром гомоморфизма колец К и К’ f называется множество: Kerf = { a ∈ K | f(a)= 0’}

Утверждение

    Kerf является подкольцом кольца К.

**Определение** Мономорфизма

Если Kerf = 0, то гомоморфизм f называется мономорфизмом.

**Определение** Эпиморфизма

Imf = f(K) = {a’ ∈ K’, | ∃ a ∈ K : f(a) = a’ }

Если Imf = K’, то f называется эпиморфизмом.

Если рассматривать только кольца с единицей, то в определение гомморфизма следует добавить условие f(1) = 1’.

**Определение** левый и правый делителя нуля

Если ab = 0 при a ≠ 0 и b ≠ 0 в кольце К, то **а** называется левым, **b** называется правым делителем нуля.

**Определение** кольца без делителей нуля

Если других делителей нуля, кроме самого нуля нет, то К называется кольцом без делителей нуля

**Определение** целостного кольца

Коммутативное кольцо с единицей равной нулю (1 ≠0) и без делителей нуля называется целостным кольцом.

Определение элемент а кольца К называется обратимым (делителем единицы), если существует элемент а-1 : aa-1 = a-1a = 1. (для коммутативного кольца).

Для ??? колце можно ввести понятия правого обратного и левого обратного для элемента а

в – правый обратный для а, если ав = 1.

С – левый обратный для а, если са = 1

Если кольцо коммутатиное, то левый и правый обратные для а совпадают.

Определение кольца с делителем (или телом) будем называть кольцо К у которого К\* = К  - {0} является группой по умножению.

**Определение** гомозорфизм колец

] (K, +, \*) и (K’,⊕, ⊗) – кольца. Отношение f  : K -> K’ называется гомоморфизмом, если оно сохраняет обе операции:

    f(a+b) = f(a) ⊕ f(b)

    f(a\*b) = f(a) ⊗ f(b)

Утверждение

1. f(0) = 0’
2. f(na) = n(fa), a ∈ K, n ∈ Z
3. ЕСЛИ У НАС КОЛЬЦА С ЕДИНИЦЕЙ, то f(1) = 1’, где 1’ – единица кольца K’ (этот пункт не обязателен, а вот 1 и 2 обязательны, см. начало предложения)

**Определение** Ядра гомоморфизма

Ядром гомоморфизма колец К и К’ f называется множество: Kerf = { a ∈ K | f(a)= 0’}

Утверждение

    Kerf является подкольцом кольца К.

**Определение** Мономорфизма

Если Kerf = 0, то гомоморфизм f называется мономорфизмом.

**Определение** Эпиморфизма

Imf = f(K) = {a’ ∈ K’, | ∃ a ∈ K : f(a) = a’ }

Если Imf = K’, то f называется эпиморфизмом.

Если рассматривать только кольца с единицей, то в определение гомморфизма следует добавить условие f(1) = 1’.

**Определение** левый и правый делителя нуля

Если ab = 0 при a ≠ 0 и b ≠ 0 в кольце К, то **а** называется левым, **b** называется правым делителем нуля.

**Определение** кольца без делителей нуля

Если других делителей нуля, кроме самого нуля нет, то К называется кольцом без делителей нуля

**Определение** целостного кольца

Коммутативное кольцо с единицей  и без делителей нуля называется целостным кольцом.

Определение элемент а кольца К называется обратимым (делителем единицы), если существует элемент а-1 : aa-1 = a-1a = 1. (для коммутативного кольца).

Для ?целостных? колец можно ввести понятия правого обратного и левого обратного для элемента а

в – правый обратный для а, если ав = 1.

С – левый обратный для а, если са = 1

Если кольцо коммутатиное, то левый и правый обратные для а совпадают.

Определение кольца с делителем (или телом) будем называть кольцо К у которого К\* = К  - {0} является группой по умножению.

**Определение** элемент а кольца К называется обратимым (делителем единицы), если существует элемент а-1 : aa-1 = a-1a = 1. (для их а рекукоммутативного кольца).

Для ??? кольца можно ввести понятия правого обратного и левого обратного для элемента а

в – правый обратный для а, если ав = 1.

С – левый обратный для а, если са = 1

Если кольцо коммутатиное, то левый и правый обратные для а совпадают.

**Определение** кольца с делителем (или телом) будем называть кольцо К у которого К\* = К  - {0} является группой по умножению.

**Определение.** **Полем** Р будем называть коммутативное кольцо с единицей, в котором каждый элемент, отличный от нуля, обратим.

Группу U(P) = P \ {0} будем обозначать P\* и называть мультипликативной группой поля.

***Иная формулирвока из Чабан : Если алгебраическая система является абелевой группой относительно обеих операций ⊕, ⊗, и умножение дистрибутивно относительно сложения, то мы получаем поле****. Наиболее известный пример – поле действительных чисел: 〈R,+,⋅〉.*

**Определение. Подполем** F поля Р называется подкольцо в Р само являющееся полем.

Пример. ] P = R, тогда F=Q – является его подполем

Если F подполе поля, то говорят, что поле Р является **расширением** своего подполя F.

**Определение** Минимальное подполе, содержащее множество {F,a},где F – подполе Р, а а∈P  ∧ а ∉ F называется **подполем полученным присоединением** к F элемента а и обозначают F(a)

Аналогично можно говорить о подполе F(a1,a2,…,an) поля Р, полученном присоединением к F n элементов a1,a2,…,an поля Р.

**Определение. Подполем** F поля Р называется подкольцо в Р само являющееся полем.

**Определение** Минимальное подполе, содержащее множество {F,a},где F – подполе Р, а а∈P  ∧ а ∉ F называется **подполем полученным присоединением** к F элемента а и обозначают F(a)

Аналогично можно говорить о подполе F(a1,a2,…,an) поля Р, полученном присоединением к F n элементов a1,a2,…,an поля Р.

**Определение.** Поля P и P’ называются **изоморфными**, если они изоморфны как кольца.

По определению, если f: P -> P’ изоморфны, то

f(0) = 0’

f(1) = 1’

**Определение.** Говорят, что поле Р имеет характеристику нуль, если его простое подполе Ро изоморфно Q; P – поле простой (конечной характеристики) р, если P0≅ZP. Пишут charP = 0 ИЛИ charP = P >0

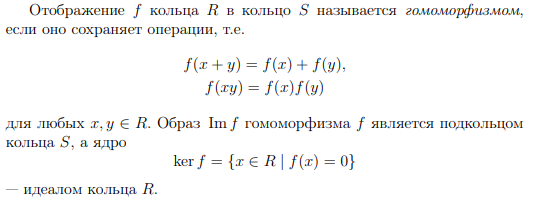
**Определение.** Поле, не обладающее никакими собственным подполем, называется **простым.**

**Определение** гомозорфизм колец

] (K, +, \*) и (K’,⊕, ⊗) – кольца. Отношение f  : K -> K’ называется гомоморфизмом, если оно сохраняет обе операции:

    f(a+b) = f(a) ⊕ f(b)

    f(a\*b) = f(a) ⊗ f(b)



Утверждение

1. f(0) = 0’
2. f(na) = n(fa), a ∈ K, n ∈ Z
3. ЕСЛИ У НАС КОЛЬЦА С ЕДИНИЦЕЙ, то f(1) = 1’, где 1’ – единица кольца K’ (этот пункт не обязателен, а вот 1 и 2 обязательны, см. начало пр эхедложения)

**Определение** Ядро гомоморфизма

Ядром гомоморфизма колец К и К’ f называется множество: Kerf = { a ∈ K | f(a)= 0’}

Утверждение Kerf является подкольцом кольца К.

Доказательство (возможно неверное/неполное)

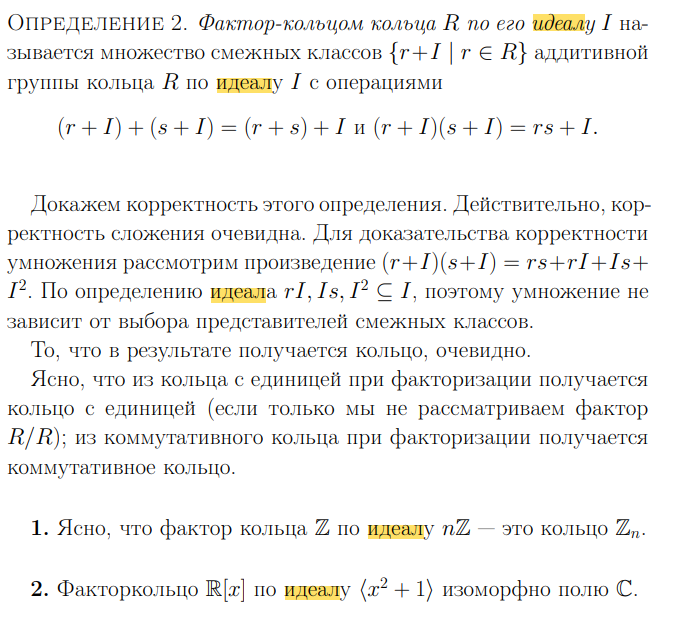
a1,a2 ∈Kerf

f(a1)=0’ и f(a2)=0’

f(a1+a2)=f(a1)⊕f(a2)=0’⊕0’=0’

f(a1\*a2)=f(a1)⊗f(a2)=0’⊗0’=0’

f(0)=0’



**Шифрование** – преобразование текста с целью скрыть его содержание от несанкционированного прочтения.

**Криптография** – наука составления шифров и шифропротоколов.

**Криптоанализ** – наука о методах и способах вскрытия шифров.

**Криптосистемой (системой шифрования)** называют известный способ шифрования, обладающий сменными элементами – **ключами**.

Обычно рассматривают **ключ шифрования** и **ключ дешифрования**. Если их необходимо хранить в секрете, то система называется **симметричной**, или **системой с секретными ключами**.

Если ключ шифрования открыт, то есть не является секретным, то такие системы называются **асимметричными**, или **системами с открытым ключом**.

Шифрируемый текст называется **исходным текстом.** Результат шифрования называется **шифртекстом**.

Система шифрования включает в себя в качестве основного элемента **функцию шифрования**. Функция шифрования преобразует исходный текст в шифровку. Эта функция зависит от ключа шифрования.

**Основное правило шифрования**

**Исходный текст должен однозначно восстанавливаться по шифртексту, то есть функция должна быть обратимой.**

**Криптостойкость** – способность криптосистемы производить шифровки, трудные для несанкционированного прочтения (взлома)

***Стойкие системы таковы, что нахождение обратной к функции шифрования в общем случае трудная задача.*** Однако при знании соотвествующего **секрета** – ключа дешифрования – это нахождение эффективно выполним

**Определение. Односторонней функцией** y = f(x) будем называть такую функцию, для которой вычисление y по x осуществляется достаточно просто, а нахождение y по x – трудная задача.

Для  шифрования используют одностороние функции y = f(x) с секретом.

1) для f существует f-1

2) f-1 можно найти эффективно, зная секрет

**В современной криптографии** используемая **киберсистема** считается **открытой**, то есть метод шифрования не является секретным. При этом её криптостойкость определяется не только качесвтом криптосистемы, но и надежностью используемых ключей.

**Алфавит**

Мы рассматриваем тексты, которые записываются в виде конечных последовательностей знаков соотсвтеующего алфавита.

Алфавит может иметь обычный смысл: 33 буквы от А до Я или 26 букв от А до Z

**Определение.** Алфавитом будем называть совокупность знаков, среди которых могут встречаться обычные буквы, цифры, знаки препинания, специальные знаки, обозначающие пробелы, и другие.

Иногда вместо алфавита используется термины **знаковая система.**

**Текстом будем называть упорядоченный набор  знаков.**

Имеется ещё одно понятие -  **единницы текста**. Самая простая единица текста  - знак. В качестве единицы текста можно считать, например, пары знаков – **диграфы** или тройки – **триграфы.**

***При k>=2 последний k-граф текста может оказаться неполным, тогда его пополняют знаками выбраннрого вида.***

Кроме этого, тексты часто разбивают на блоки. **Блок** – это некоторая конечная последовательность единиц текста. Обычна длина блока фиксирована. Одним из самых простых способов шифрования является **простая замена.**

В криптографии, как правило, **работают с оцифрованными текстами**. **Единицы текста** **заменяют на числа** различной природы. Это могут быть **обычные целые числа, элементы колец вычетов, конечных полей и т.д.**

Оцифровка текста не является шифрованием. Исходный текст в его записи в данном алфавите должен однозначно восстанавливаться по своему оцифрованному виду.

**Обозначим m∈ {0,1}\* означает m-бинарная последовательность** (последовательность из нулей и единиц)

***При использовании бинарных последовательностей удобно, чтобы алфавит содержал 2к знаков***