ИНФОРМАЦИЯ КАК ПРОДУКТ

Как и всякий продукт информация имеет потребителей, нуждающихся в ней, и потому обладает определенными потребительскими качествами, а также имеет своих обладателей (владельцев).

С точки зрения потребителя качество используемой при управлении производством информации позволит получить дополнительный экономический или социально-моральный эффект.

С точки зрения обладателя — сохранение в тайне коммерчески важной информации позволяет успешно конкурировать на рынке производства и сбыта товаров и услуг.

Американские менеджеры утверждают:
«Бизнес — на 90% информация,
и лишь на 10% — удача».

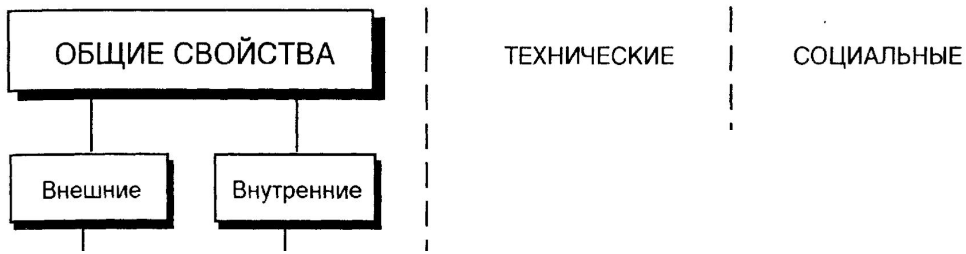


Рис. 1.3. Характеристики информации

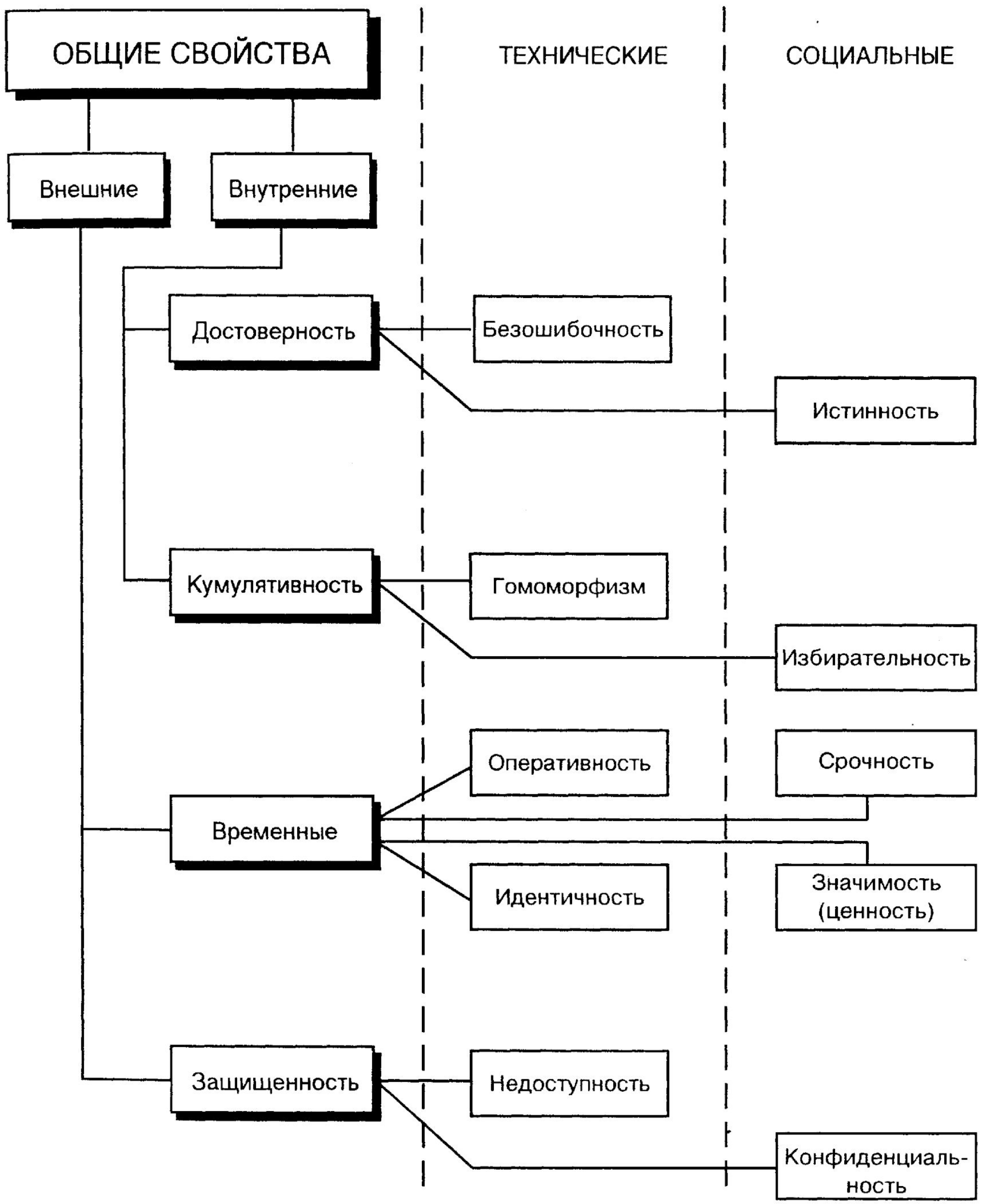


Рис. 1.3. Характеристики информации

Внешние свойства

временные свойства и свойства защищенности,

которые характерны для данных, находящихся в определенной среде

и которые исчезают **при их переносе в другую систему**.

Внутренние свойства

(достоверность и кумулятивность),

сохраняющиеся при переносе данных в другую среду (систему);

Достоверность.

В свойстве достоверности выделяются **безошибочность и истинность** данных.

Под **безошибочностью** понимается свойство данных **не иметь скрытых случайных ошибок.** Случайные ошибки в данных обусловлены, как правило, ненамеренными искажениями содержания сведений человеком или сбоями технических средств при переработке данных в ИС.

При анализе **истинности** данных рассматривают **преднамеренные искажения данных человеком** — источником сведений (в том числе и из-за неумения или непонимания сути вопроса), или искажения, вносимые средствами обработки информации.

Кумулятивность.

Кумулятивность определяет такие понятия как:

гомоморфизм - соотношение между объектами двух множеств, при котором одно множество является моделью другого;

избирательность - данные, специально отобранные для конкретного уровня пользователей.

Временные свойства.

Временные свойства определяют способность данных отображать динамику изменения ситуации.

При этом можно рассматривать или время запаздывания появления в данных соответствующих признаков объектов, или расхождение реальных признаков объекта и тех же признаков, отображаемых в данных.

Оперативность — свойство данных, состоящее в том, что время их сбора и переработки соответствует динамике изменения ситуации;

Идентичность — **свойство данных соответствовать состоянию объекта**.

Нарушение идентичности связано с техническим (по рассогласованию признаков) старением информации, при котором происходит расхождение реальных признаков объектов и тех же признаков, отображенных в информации.

Срочность — **свойство данных соответствовать сроками, определяемым социальными мотивами**;

Значимость — свойство данных сохранять ценность для потребителя с течением времени,

т. е. не подвергаться моральному старению.

Защищенность данных.

При рассмотрении защищенности можно выделить**:**

свойство недоступности - технические аспекты защиты данных от несанкционированного доступа ;

свойство конфиденциальности - социально-психологические аспекты классификации данных по степени их конфиденциальности и секретности .

Дополнительно к рассмотренным можно выделить и такие свойства информации как:

1. Общественная природа (источником информации является познавательная деятельность людей, общества).

2. Языковая природа - информация выражается с помощью языка, т. е. знаковой системы любой природы, служащей средством общения, мышления, выражения мысли.

Язык может быть естественным, используемым в повседневной жизни и служащим формой выражения мыслей и средством общения между людьми, и искусственным, созданным людьми для определенных целей (например, язык математической символики, информационно-поисковый, алгоритмический и др.).

3. Неотрывность от языка и носителя.

4. Дискретность (единицами информации как средствами выражения являются слова, предложения, отрывки текста, а в плане содержания — понятия, высказывания, описание фактов, гипотезы, теории, законы и др.).

5. Независимость от создателей.

6. Старение (основной причиной старения информации является не само время, а появление новой информации, с поступлением которой прежняя информация оказывается неверной, перестает адекватно отображать явления и закономерности материального мира, человеческого общения и мышления).

7. Рассеяние (т. е. существование в многочисленных источниках).

Математические модели открытого текста

Один из естественных подходов к моделированию открытых текстов связан с учетом их **частотных характеристик**, приближения для которых можно вычислить с нужной точностью, исследуя тексты достаточной длины.

Основанием для такого подхода является устойчивость частот *к* -грамм или целых словоформ реальных языков человеческого общения (то есть отдельных букв, слогов, слов и некоторых словосочетаний).

Основанием для такого подхода является устойчивость частот *к* -грамм или целых словоформ реальных языков человеческого общения (то есть отдельных букв, слогов, слов и некоторых словосочетаний).

Частоты букв p_i в русском языке

Пробел	0,175	р	0,040	я	0,018	х	0,009
о	0,090	в	0,038	ы	0,016	ж	0,007
е, ё	0,072	л	0,035	з	0,016	ю	0,006
а	0,062	к	0,028	ь, ъ	0,014	ш	0,006
и	0,062	м	0,026	б	0,014	ц	0,003
т	0,053	д	0,025	г	0,013	щ	0,003
н	0,053	п	0,023	ч	0,012	э	0,003
с	0,045	у	0,021	й	0,010	ф	0,002

Частоты букв русского 32-буквенного алфавита (со знаком пробела)

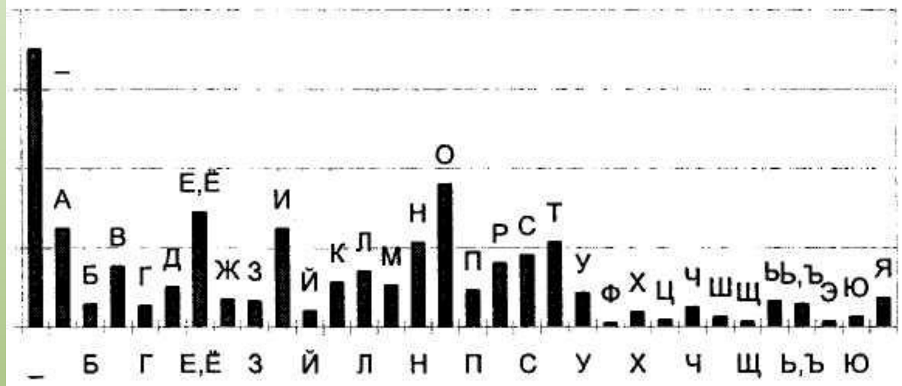


Таблица частот биграмм русского языка

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
А	2	12	35	8	14	7	6	15	7	7	19	27	19	45	5	11
Б	5					9	1		6			6		2	21	
В	35	1	5	3	3	32		2	17		7	10	3	9	58	6
Г	7				3	3			5		1	5		1	50	
Д	25		3	1	1	29	1	1	13		1	5	1	13	22	3
Е	2	9	18	11	27	7	5	10	6	15	13	35	24	63	7	16
Ж	5	1			6	12			5					6		

Учет частот ***к*** -грамм приводит к следующей модели открытого текста:

Пусть $\boldsymbol{P^{(к)}(A)}$ представляет собой массив, состоящий из приближений для вероятностей

$\boldsymbol{p}(b_1 b_2 \ldots b_k)$ появления ***к*** –грамм $b_1 b_2 \ldots b_k$ в открытом тексте.

$\boldsymbol{A}$ — $\{a_1, \ldots, a_m\}$ — алфавит открытого текста,

$b_i \in A$

$i = 1, \ldots k.$

Источник "открытого текста" генерирует последовательность c_1, $c_2,\dots,c_k,c_{k+1}$ знаков алфавита *A*,

в которой:

k - грамма $c_1,c_2,\dots,c_k$ появляется с вероятностью

$p(c_1,c_2,\dots,c_k) \in P^{(к)}(A)$,

следующая ***k***-грамма $c_2,\dots,c_k,c_{k+1}$ появляется с вероятностью $p(c_2\dots c_{k+1}) \in P^{(к)}(A)$ и т. д.

Назовем построенную модель открытого текста

вероятностной моделью ***к*** *-го приближения.*

Таким образом, простейшая модель открытого текста - ***вероятностная модель первого приближения*** –

представляет собой последовательность знаков

$\boldsymbol{c_1, c_2, \ldots}$, в которой каждый знак $\boldsymbol{c_i}$, i = 1,2,… появляется с вероятностью

$p(c_i) \in P^{(1)}(A)$, независимо от других знаков.

Эта модель также называется *позначной моделью открытого текста.*

В такой модели открытый текст $c_1 c_2 \ldots c_l$ имеет вероятность

$$p(c_1 c_2 \ldots c_l) = \prod_{i=1}^{l} p(c_i)$$

В вероятностной модели **второго приближения** первый знак c_1 имеет вероятность:

$$p(c_1) \in P^{(1)}(A),$$

а каждый следующий знак c_i , зависит от предыдущего и появляется с вероятностью:

$$p\left(c_i / c_{i-1}\right) = \frac{p\left(c_{i-1}c_i\right)}{p\left(c_{i-1}\right)}$$

где:

$$p\left(c_{i-1}c_i\right) \in P^{(2)}\left(A\right),$$

$$p\left(c_{i-1}\right) \in P^{(1)}\left(A\right)$$

В такой модели открытый текст $c_1 c_2 \ldots c_l$ имеет вероятность

$$p\left(c_1 c_2 \ldots c_l\right) = p\left(c_1\right) \cdot \prod_{i=2}^{l} p\left(c_i / c_{i-1}\right)$$

Модели открытого текста более высоких приближений учитывают зависимость каждого знака от большего числа предыдущих знаков.

Чем выше степень приближения, тем более "читаемыми" являются соответствующие модели.

Проводились эксперименты по моделированию открытых текстов с помощью ЭВМ.

1. (Позначная модель) *алисъ проситете пригнуть стречи разве возникл;*
2. (Второе приближение) *н умере данного отствии официант простояло его то;*
3. (Третье приближение) *уэт быть как ты хоть а что я спящихся фигурой куда п;*
4. (Четвертое приближение) *ество что ты и мы дохнуть перетусовались ярким сторож;*
5. (Пятое приближение) *луну него словно него словно из ты в его не полагаете помощи я д;*
6. (Шестое приближение) *о разведения которые звенел в тонкостью огнем только.*

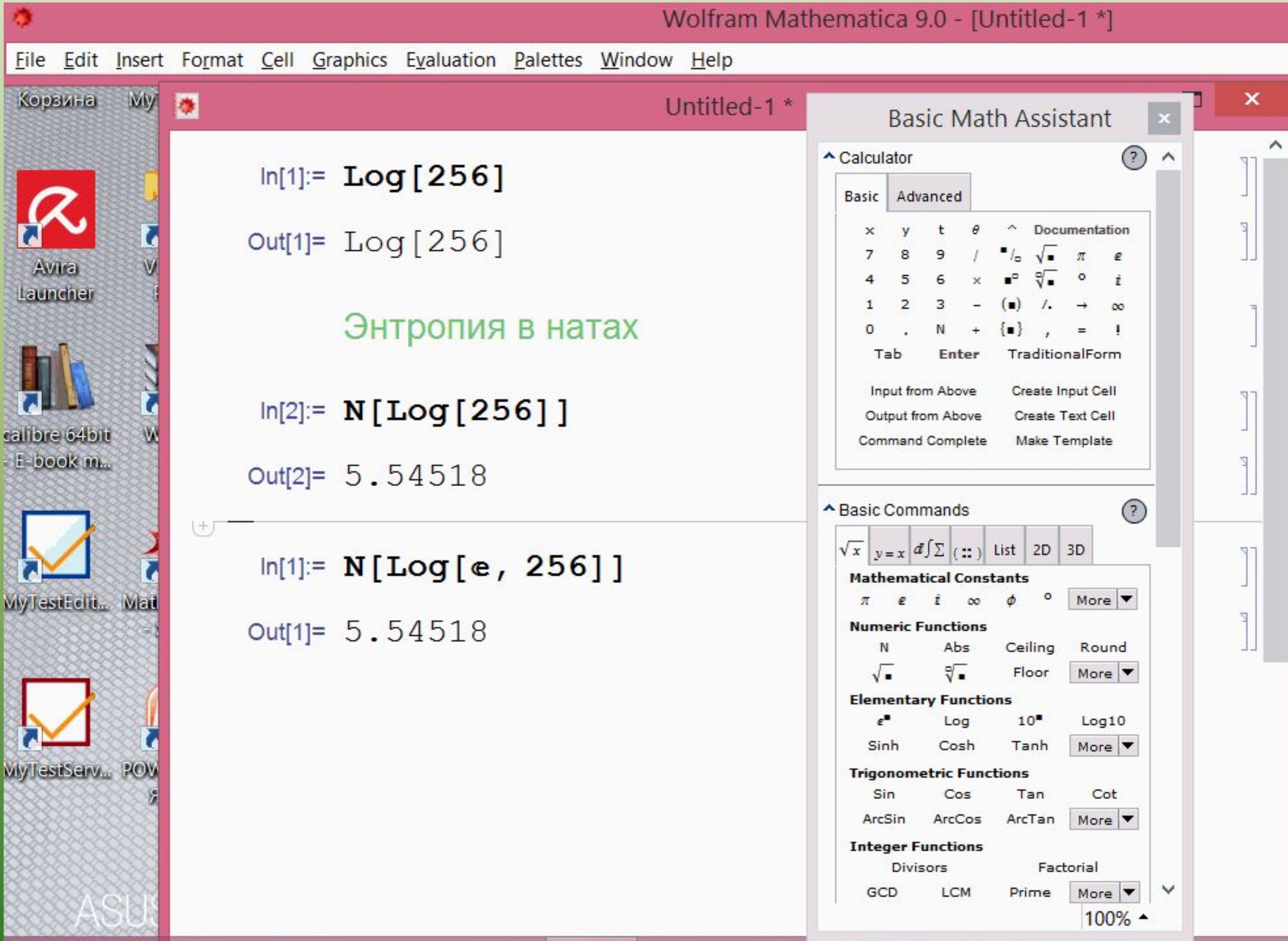
Как видим, тексты вполне "читаемы".

Преимущественно энтропия измеряется в двоичных единицах (битах), если основанием логарифма выбрано число 2;

если основание логарифма равно 10, то энтропия измеряется в десятичных логарифмических единицах (дитах);

если основанием выбрано число е, то в натуральных логарифмических единицах (натах).

Благодаря знаку минус, стоящему перед символом суммирования, энтропия всегда положительна, может принимать минимальное и максимальное значения, причем максимальна для ситуации с равновероятными исходами.


Wolfram Mathematica 9.0 - [Untitled-1 *]
File Edit Insert Format Cell Graphics Evaluation Palettes Window Help
Untitled-1 *
In[1]:= Log[256]
Out[1]= Log[256]
Энтропия в натах
In[2]:= N[Log[256]]
Out[2]= 5.54518
In[1]:= N[Log[e, 256]]
Out[1]= 5.54518
Basic Math Assistant
Calculator
Basic
Advanced
Documentation
Tab
Enter
TraditionalForm
Input from Above
Create Input Cell
Output from Above
Create Text Cell
Command Complete
Make Template
Basic Commands
Mathematical Constants
Numeric Functions
N Abs Ceiling Round
Floor
Elementary Functions
Log Log10
Sinh Cosh Tanh
Trigonometric Functions
Sin Cos Tan Cot
ArcSin ArcCos ArcTan
Integer Functions
Divisors Factorial
GCD LCM Prime
More
100%
Корзина
Avira Launcher
calibre 64bit - E-book m...
MyTestEdit...
MyTestServ...

Untitled-1 *

Энтропия в дитах

```
In[7]:= Log[10, 256]
```

Out[7]= $\frac{\text{Log}[256]}{\text{Log}[10]}$

```
In[2]:= N[Log[10, 256]]

Out[2]= 2.40824
```

Энтропия в битах

```
In[5]:= Log[2, 256]

Out[5]= 8

In[4]:= N[Log[2, 256]]

Out[4]= 8.
```

Список

In[9]:= `p = {1 / 4, 1 / 4, 1 / 4, 1 / 4}`

Out[9]= $\left\{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\right\}$

Длина списка

In[10]:= `Length[p]`

Out[10]=

4

Элемент списка

In[11]:= `p[[3]]`

Out[11]=

$\frac{1}{4}$

200%

```
In[1]:= p = {1 / 4, 1 / 4, 1 / 4, 1 / 4}

Out[1]= {1/4, 1/4, 1/4, 1/4}

In[2]:= multiEntropy1 =
         -Sum[p[[i]] * Log[2, p[[i]]], {i, 1, Length[p]}]

Out[2]= 2
```

$$\text{In[3]:= multiEntropy2} = -\sum_{i=1}^{\text{Length[p]}} \text{p[[i]]} * \text{Log[2, p[[i]]]}$$

```
Out[3]= 2
```

```
In[6]:= s = {0, 0, 1, 1, 0, 0, 1, 1}

Out[6]= {0, 0, 1, 1, 0, 0, 1, 1}

In[7]:= Length[s]

Out[7]= 8

In[8]:= Count[s, 0]

Out[8]= 4

In[9]:= Count[s, 1]

Out[9]= 4

In[10]:= ps = {1 / 2, 1 / 2}
```

Out[10]= $\left\{\frac{1}{2}, \frac{1}{2}\right\}$

Настроить

```
s = {0, 0, 1, 1, 0, 0, 1, 1}
```

{0, 0, 1, 1, 0, 0, 1, 1}

```
ps = {1 / 2, 1 / 2}
```

$\left\{\frac{1}{2}, \frac{1}{2}\right\}$

$$\text{entropys} = -\sum_{i=1}^{\text{Length[ps]}} \text{ps[[i]]} * \text{Log[2, ps[[i]]]}$$

1

```
Entropy[2, s]
```

1

```
In[15]:= s1 = {0, 0, 1, 1, 1, 1, 1, 1}

Out[15]= {0, 0, 1, 1, 1, 1, 1, 1}

In[16]:= ps1 = {1 / 4, 3 / 4}
```

Out[16]= $\left\{\frac{1}{4}, \frac{3}{4}\right\}$

In[17]:= entropys1 = $-\sum_{i=1}^{\text{Length[ps]}}$ ps1[[i]] * Log[2, ps1[[i]]]

Out[17]= $\frac{1}{2} + \frac{3\,\text{Log}\left[\frac{4}{3}\right]}{4\,\text{Log}[2]}$

```
In[18]:= Entropy[2, s1]
```

Out[18]= $\frac{1}{2} + \frac{3\,\text{Log}\left[\frac{4}{3}\right]}{4\,\text{Log}[2]}$

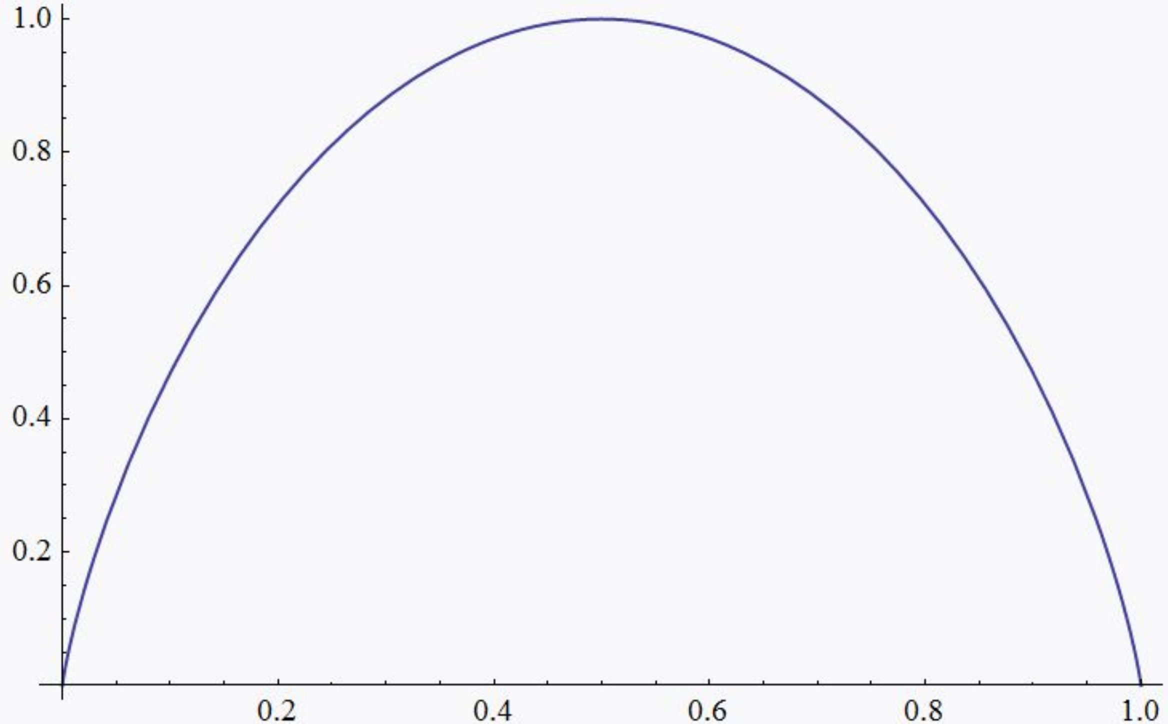
```
In[19]:= N[Entropy[2, s1]]

Out[19]= 0.811278
```

In[22]:=
```
p =. ;
ent[p_] := -p*Log[2, p] - (1 - p)*Log[2, 1 - p]
```

In[24]:=
```
Plot[ent[x], {x, 0, 1}]
```

Out[24]=



In[25]:= `str0 = "проверка расчета информационной энтропии"`

Out[25]=

проверка расчета информационной энтропии

In[26]:= `Entropy[2, str0]`

Out[26]=

$$\frac{3}{4}+\frac{3\,\text{Log}[10]}{10\,\text{Log}[2]}+\frac{3\,\text{Log}\left[\frac{40}{3}\right]}{40\,\text{Log}[2]}+\frac{3\,\text{Log}[20]}{20\,\text{Log}[2]}+\frac{9\,\text{Log}[40]}{40\,\text{Log}[2]}$$

In[27]:= `N[Entropy[2, str0]]`

Out[27]=

3.87257

МНОЖЕСТВА И ОТОБРАЖЕНИЯ

МНОЖЕСТВА

Множество – это определенная совокупность объектов.

Объекты, из которых состоит (составлено) множество, называются его элементами.

Элементы множества различны и отличимы друг от друга

Множество обозначается прописной буквой какого-либо алфавита, а его элементы – строчными буквами того же или другого алфавита.

Множества с конечным числом различных элементов могут быть описаны путем явного перечисления всех элементов. Обычно эти элементы заключаются в фигурные скобки.

Например, {16,32,64} – множество степеней двойки, заключенных между 10 и 100.

$$\mathbf{S}=\{a_1,a_2,\ldots,a_k\};$$

Множество **S**, состоящее из конечного числа элементов, называется конечным множеством, а само это число называется порядком множества **S**.
Обозначение: #**S**.

Для некоторых особо важных множеств приняты стандартные обозначения, которых следует придерживаться.
Так, буквами **N, Z, P,Q, R** обозначают соответственно:

N - множество натуральных чисел,
Z - множество целых чисел,
P - множество простых чисел,
Q - множество рациональных чисел,
R - множество вещественных чисел.

Чтобы задать множество, нужно указать, какие элементы ему принадлежат. Это можно сделать различными способами:

- перечисление элементов: $S=\{a_1,a_2,\ldots,a_k\}$;
- характеристическим предикатом: $S=\{x|P(x)\}$;
- порождающей процедурой: $S=\{x|x:=f\}$.

Характеристический предикат – это некоторое условие, выраженное в форме логического утверждения или процедуры.
Если для данного элемента условие выполнено, то он принадлежит определяемому множеству, в противном случае – не принадлежит.

Перечислением можно задать только конечное множество. Бесконечные множества задаются характеристическим предикатом или порождающей процедурой.

При заданном множестве **S** *включение* **a**$\in$**S** указывает на то, что **a** – элемент множества.
В противном случае записывают **a**$\notin$S.

Говорят, что **S** – *подмножество* **T** или **S**$\subset$**T** (**S** содержится в **T**), когда имеет место импликация:

$$\mathbf{x} \in \mathbf{S},\ \forall \mathbf{x} \Rightarrow \mathbf{x} \in \mathbf{T}$$

Два множества совпадают (или равны), если у них одни и те же элементы.
Символически это записывается в виде:

$$\mathbf{S=T \Leftrightarrow S\subset T} \text{ и } \mathbf{T\subset S}$$

Пустое множество ∅, т.е. множество, не содержащее ни одного элемента, по определению входит в число подмножеств любого множества.

Под *пересечением* двух множеств **S** и **T** понимают множество:

$$\mathbf{S\cap T=\{x|\ x\in S} \text{ и } \mathbf{x\in T\}}$$

а под их объединением – множество:

$$\mathbf{S\cup T=\{x|\ x\in S} \text{ или } \mathbf{x\in T\}}$$

Пусть **X** и **Y** – произвольные множества.

Пару (x,y) элементов $\mathbf{x \in X}$, $\mathbf{y \in Y}$, взятых в данном порядке, называют *упорядоченной парой*,
считая при этом, что $(x_1,y_1)=(x_2,y_2)$ тогда и только тогда, когда $x_1= x_2$, $y_1= y_2$.

Декартовым произведением двух множеств **X** и **Y** называется множество всех упорядоченных пар (x,y):

$$\mathbf{X \times Y = \{(x,y) | x \in X,\ y \in Y\}}$$

Пусть, **R** – множество всех вещественных чисел.
Тогда декартов квадрат $\mathbf{R}^2=\mathbf{R}\times\mathbf{R}$ есть просто множество всех декартовых координат на плоскости относительно заданных координатных осей.

Аналогично можно ввести декартово произведение трех, четырех и т.д. множеств.

При $\mathbf{X_1=X_2=X_3=\ldots=X_k=X}$ сокращенно пишут $\mathbf{X^k}$ и говорят о k-й декартовой степени множества **X**.

Элементами $\mathbf{X^k}$ являются последовательности, или строки $(x_1,x_2,\ldots x_k)$ длины k.

ОТОБРАЖЕНИЯ

Понятие ***отображения*** или ***функции*** является одним из центральных в математике.

При заданных $\boldsymbol{X}$ и $\boldsymbol{Y}$ отображение $\boldsymbol{f}$ с областью *определения* $\boldsymbol{X}$ и областью *значений* $\boldsymbol{Y}$ сопоставляет каждому элементу $\boldsymbol{x \in X}$ элемент $\boldsymbol{f(x) \in Y}$.

Символически отображение записывается в виде $\boldsymbol{f{:}X \to Y}$.

Образом при отображении $\boldsymbol{f}$ называется множество всех элементов вида $\boldsymbol{f}(\boldsymbol{x})$:

$$\mathrm{Im}\,\boldsymbol{f} = \{\, \boldsymbol{f}(\boldsymbol{x}) \mid \boldsymbol{x} \in \boldsymbol{X} \,\} = \boldsymbol{f}(\boldsymbol{X}) \subset \boldsymbol{Y}$$

Множество

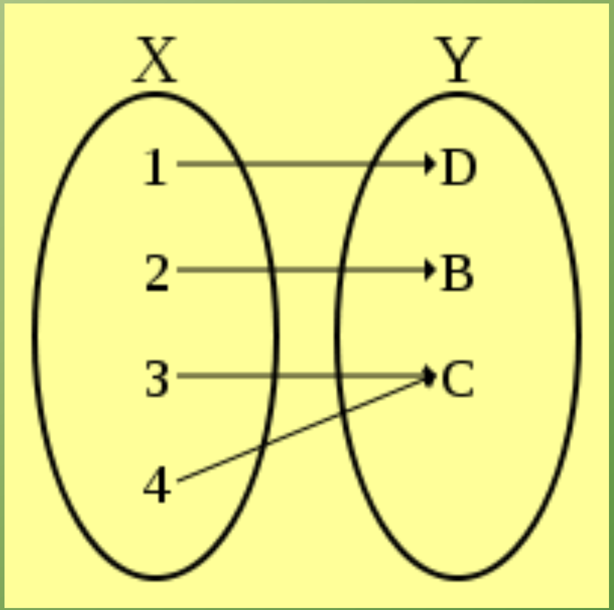
$$\boldsymbol{f}^{-1}(\boldsymbol{y}) = \{\, \boldsymbol{x} \in \boldsymbol{X} \mid \boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{y} \,\}$$

называется *прообразом* элемента $\boldsymbol{y} \in \boldsymbol{Y}$

Отображение $f : X \to Y$ называется *сюръективным,* когда $\operatorname{Im} f = Y$

Отображение f: X•Y азывается **сюръективным** (или **сюръекцией**, или **отображением на** Y), если каждый элемент множества Y является образом хотя бы одного элемента множества X, то есть .

$$\forall y \in Y \quad \exists\, x \in X \quad y = f(x)$$

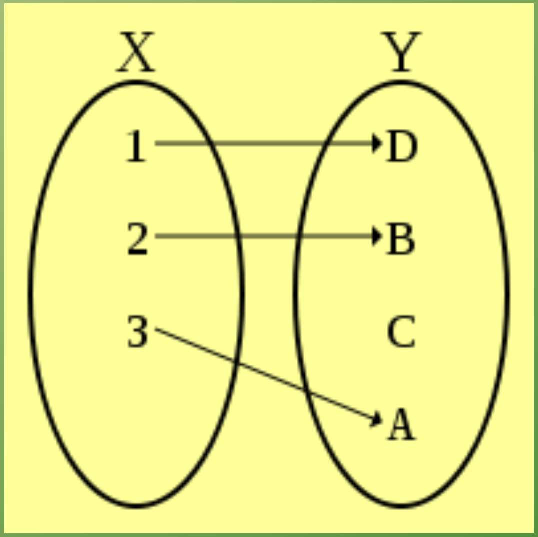


Отображение f**:X → Y** называется *инъективным,* когда из **x ≠ x' следует** f**(x) ≠** f**(x')**.

Отображение f**:X → Y** называется **инъекцией** (или **вложением в** множество ***Y***),
если разные элементы множества ***X*** переводятся в разные элементы множества ***Y***.

Формально это значит, что если два образа совпадают, то совпадают и прообразы . ***f(x) = f(y) • x = y***

Инъективность является необходимым условием биективности (достаточно вместе с сюръективностью).



Отображение $\boldsymbol{f}$**:X → Y** называется *биективным,* или взаимно однозначным, если оно одновременно сюръективно и инъективно.

Функция $\boldsymbol{f}$**:X•Y** называется **биекцией** и обозначается $\boldsymbol{f}$**:X↔Y** если она:

Переводит разные элементы множества *X* в разные элементы множества *Y* (инъективность).

$$\forall\, x_1 \in X,\ \forall\, x_2 \in X \quad f(x_1) = f(x_2) \bullet x_1 = x_2$$

.

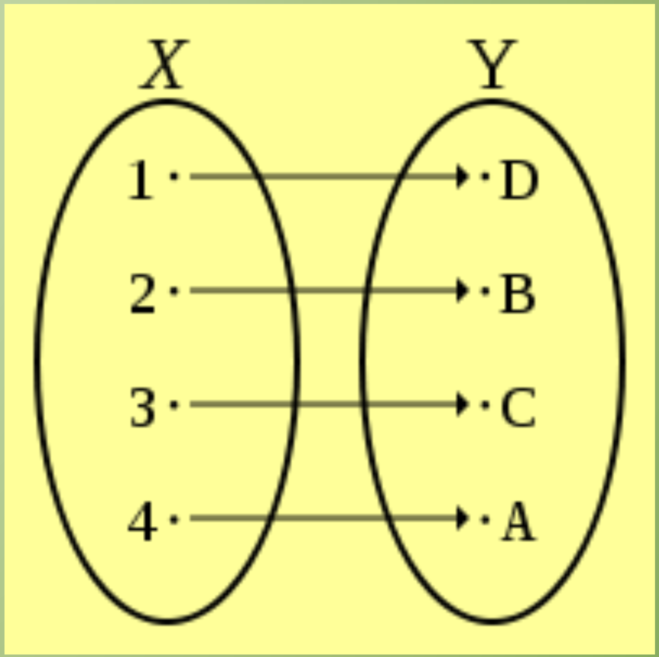
Любой элемент из *Y* имеет свой прообраз (сюръективность) :

$$\forall\, y \in Y,\ \ \exists\, x \in X \quad f(x) = y$$

Биекцию также называют

взаимно однозначным отображением или

взаимно однозначным соответствием.



Множества, для которых существует биекция, называются **равномощными**

Равенство $\boldsymbol{f=g}$ двух отображений означает по определению, что их соответствующие области совпадают

Единичным или *тождественным* отображением

$\boldsymbol{e_X : X \to X}$

называется отображение, переводящее каждый элемент $\boldsymbol{x} \in \boldsymbol{X}$ в себя .

Отображение f^{-1} является обратным к f, если $f(x) = y \Leftrightarrow f^{-1}(y) = x$

Найти обратное отображение f^{-1} для $f(x)=\dfrac{1}{\sqrt{x-5}}$.

Обратное отображение удовлетворяет условию:

$$f(f^{-1}(x))=f^{-1}(f(x))=e_X=x.$$

Следовательно:

$$\frac{1}{\sqrt{f^{-1}(x)-5}}=x$$

$$1=f^{-1}(x)\cdot x^2-5x^2$$

$$f^{-1}(x)=1/x^2+5$$

$$f(x)=\frac{1}{\sqrt{x-5}}$$

$$f^{-1}(x)=1/x^2+5$$

Проверка:

$$f(f^{-1}(x))=f(1/x^2+5)=\frac{1}{\sqrt{1/x^2+5-5}}=x$$

$$x=f^{-1}(f(x))=f^{-1}\left(\frac{1}{\sqrt{x-5}}\right)=\frac{1}{\frac{1}{x-5}}+5$$

БИНАРНЫЕ ОТНОШЕНИЯ

Для любых двух множеств **X** и **Y** всякое подмножество **O**$\subset$**X**$\times$**Y** называется *бинарным отношением* между **X** и **Y** (или просто *бинарным отношением* на **X**, если **X=Y**)

Бинарное отношение ~ на **X** называется отношением эквивалентности, если для всех $\mathbf{x}$, $\mathbf{x_1}$, $\mathbf{x_2} \in \mathbf{X}$ выполнены условия:

1. $\mathbf{x \sim x}$ (рефлексивность);

2. $\mathbf{x \sim x_1} \Rightarrow \mathbf{x_1 \sim x}$ (симметричность);

3. $\mathbf{x \sim x_1}$, $\mathbf{x_1 \sim x_2} \Rightarrow \mathbf{x_2 \sim x}$ (транзитивность).

Подмножество $H=\{x' \in X \mid x' \sim x\}$ $H \subset X$

всех элементов, эквивалентных данному **x**, называется классом эквивалентности, содержащим **x** .

Так как $x \sim x$ (условие 1),
то $x' \in H$.
Любой элемент $x' \in H$ называется ***представителем класса*** **H.**

Справедлива следующая теорема:

Теорема 1. Множество классов эквивалентности по отношению $\sim$ является разбиением множества **X** в том смысле, что **X** является объединением непересекающихся подмножеств.

МНОЖЕСТВА С АЛГЕБРАИЧЕСКИМИ ОПЕРАЦИЯМИ

БИНАРНЫЕ ОПЕРАЦИИ

Пусть **X** – произвольное множество.
Бинарной алгебраической операцией (или *законом композиции*) на **X** называется произвольное (но фиксированное) отображение
$\boldsymbol{\tau}: \mathbf{X} \times \mathbf{X} \to \mathbf{X}$ декартова квадрата $\mathbf{X}^2 = \mathbf{X} \times \mathbf{X}$ в **X**.

Таким образом, любой упорядоченной паре $(\boldsymbol{a},\boldsymbol{b})$ элементов $\boldsymbol{a},\boldsymbol{b} \in \mathbf{X}$ ставится в соответствие определенный элемент $\tau(\boldsymbol{a},\boldsymbol{b})$ того же множества **X**.
Иногда вместо $\tau(\boldsymbol{a},\boldsymbol{b})$ пишут $\boldsymbol{a}\tau\boldsymbol{b}$, а еще чаще бинарную операцию на **X** обозначают каким-нибудь специальным символом: *, · , · или +.

На **X** может быть задано, вообще говоря, много различных операций.

Желая выделить одну из них, используют скобки (**X**, *) и говорят, что операция * определяет на **X** *алгебраическую структуру* или что (**X**, *) – *алгебраическая система*.

Пример . В множестве **Z** целых чисел, помимо естественных операций +, · (сложения и умножения), легко указать получающиеся при помощи + (или -) и · "производные" операции:

$\boldsymbol{n} \cdot \boldsymbol{m} = \boldsymbol{n} + \boldsymbol{m} - \boldsymbol{n} \times \boldsymbol{m}$,

$\boldsymbol{n} * \boldsymbol{m} = -\boldsymbol{n} - \boldsymbol{m}$ и т.д.

Мы приходим к различным алгебраическим структурам (**Z**,+), (**Z**,-), (**Z**, ·) и (**Z**, *). ♦

Наряду с бинарными алгебраическими операциями не лишены интереса гораздно более общие ***n***-арные операции:

унарные при ***n***=1,

тернарные при ***n***=3 и т.д., равно как и их комбинации.
Связанные с ними алгебраические структуры составляют специальную теорию универсальных алгебр.

ПОЛУГРУППЫ И МОНОИДЫ

Бинарная операция * на множестве **X** называется ***ассоциативной***,
если $(a*b)*c=a*(b*c)$ для всех $a,b,c\in\mathbf{X}$.

Она также называется ***коммутативной***, если $a*b=b*a$.

Те же названия присваиваются и соответствующей алгебраической структуре (**X**,*).

Требования ассоциативности и коммутативности независимы.

Пример. Операция * на **Z**, заданная правилом $n*m=-n-m$, очевидно, коммутативна.

Но $(1*2)*3=(-1-2)*3=-(-1-2)-3=0 \neq 1*(2*3)= 1*(-2-3)=-1-(-5)=4$.

Так что условие ассоциативности не выполняется.

Некоторые свойства операций имеют специальные названия.

Пусть задана алгебра (M, Σ) и a,b,c ∈ M,

”•“,”*” ∈ Σ. (, т.е. бинарные операции).

Тогда:

1. ассоциативность: (a*b) *c=a* (b*c);
2. коммутативность: a*b=b*c;
3. дистрибутивность слева: a• (b*c)=a•b*a•c;
4. дистрибутивность справа: (a*b) •c=a•c*b•c;
5. поглощение: (a*b) •a=a;
6. идемпотентность: a*a=a.

Ассоциативные операции: сложение и умножение чисел, объединение и пересечение множеств, композиция отношений.

Неассоциативные операции: возведение числа в степень, вычитание множеств.

Коммутативные операции: сложение и умножение чисел, объединение и пересечение множеств.

Некоммутативные операции: умножение матриц, композиция отношений.

Дистрибутивные операции: умножение относительно сложения чисел.

Недистрибутивные операции: возведение в степень дистрибутивно относительно умножения справа, но не слева:

$$(ab)^c = a^c b^c \qquad a^{bc} \neq a^b a^c$$

Элемент $\mathbf{e} \in \mathbf{X}$ называется *единичным* (или *нейтральным*) относительно рассматриваемой бинарной операции *, если $e * x = x * e = x$ для всех $x \in \mathbf{X}$.

Если e' – еще один единичный элемент, то, как следует из определения,

$$e' = e' * e = e * e' = e.$$

Следовательно, в алгебраической структуре ($\mathbf{X}$,*) может существовать не более одного единичного элемента.

Множество **X** с заданной на нем бинарной ассоциативной операцией называется *полугруппой*.

Полугруппу с единичным (нейтральным) элементом принято называть *моноидом*.

Элемент $\boldsymbol{a}$ моноида ($\mathbf{M}$,×,$\boldsymbol{e}$) называется *обратимым*, если найдется элемент $\boldsymbol{b} \in \mathbf{M}$, для которого $\boldsymbol{a}\times\boldsymbol{b}=\boldsymbol{b}\times\boldsymbol{a}=\boldsymbol{e}$ (понятно, что элемент $\boldsymbol{b}$ тоже обратим).

Если еще и $\boldsymbol{a}\times\boldsymbol{b'} = \boldsymbol{e} = \boldsymbol{b'}\times\boldsymbol{a}$,
то $\boldsymbol{b'} = \boldsymbol{e}\times\boldsymbol{b'} = (\boldsymbol{b}\times\boldsymbol{a})\times\boldsymbol{b'} = \boldsymbol{b}\times(\boldsymbol{a}\times\boldsymbol{b'}) = \boldsymbol{b}\times\boldsymbol{e} = \boldsymbol{b}$.

Это дает основание говорить просто об *обратном элементе* $\boldsymbol{a}^{-1}$ к (обратимому) элементу $\boldsymbol{a} \in \mathbf{M}$:

$\boldsymbol{a}\cdot\boldsymbol{a}^{-1} = \boldsymbol{e} = \boldsymbol{a}^{-1}\cdot\boldsymbol{a}$.

Разумеется, $(\boldsymbol{a}^{-1})^{-1}=\boldsymbol{a}$.

Группой называется непустое множество G с бинарной операцией * на нем, для которой выполнены следующие аксиомы:

операция * ассоциативна, т.е. для любых $a,b,c \in G$ $a*(b*c)=(a*b)*c$;

В множестве имеется единичный элемент (или единица) e такой, что для любого $a*e=e*a=a$;

Для каждого $a \in G$ существует обратный элемент $a^{-1} \in G$ такой, что $a*a^{-1} = a^{-1}*a = e$;

Группа называется *абелевой* (или коммутативной), если для любых $a,b \in G$ выполняется $a*b=b*a$.

Множество Z целых чисел образует абелеву группу относительно операции сложения.
То же самое можно сказать относительно рациональных чисел Q, вещественных R и комплексных C

Группа G с мультипликативной операцией называется *циклической* , если она порождена одним элементом,
т.е. в ней имеется такой элемент a (образующий), что любой другой элемент b представим в виде $b = a^n$, $n \in Z$.

$$n < 0, a^n = (a^{-1})^{|n|}$$

Группа G обладающая конечным числом элементов называется *конечной группой*.
Число элементов конечной группы называется порядком группы и обозначается $\#G$ (или $|G|$).

Кольцом называется множество ***R*** с двумя бинарными операциями, обозначаемыми «+»и «•», такими, что:

R- абелева группа относительно операции «+»;

Операция «•» ассоциативна ,т.е. для любых выполнено (ab)c = a(bc);

Выполнены законы дистрибутивности, т.е. для всех $a, b, c \in R$ выполнено $a(b+c) = ab + ac, (b+c)a = ba + ca$

Нейтральный элемент аддитивной группы кольца называют нулем и обозначают 0.

Противоположный (обратный) к *a* элемент обозначают -*a*.

Обычно пишут вместо $a + (-b) = a - b.$

Простейшими примерами колец являются кольца целых чисел Z и многочленов R[x] с вещественными элементами.

Кольцо называется кольцом с единицей, если оно имеет мультипликативную единицу, т.е. такой элемент , что

$ea = ae = a$ для любого $a \in R$.

Кольцо называется коммутативным, если операция умножения коммутативна.

Два элемента называться делителями нуля, если :

$a \neq 0, b \neq 0$ $ab = 0$

Рассмотрим кольцо матриц размера 2×2 над полем действительных чисел.

Нулем этого кольца является матрица: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

единицей - матрица : $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Делителями нуля являются матрицы: $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ и $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$

Кольцо называется областью целостности, если оно является коммутативным кольцом с единицей и без делителя нуля.

Коммутативное кольцо называется полем, если его ненулевые элементы образуют группу относительно операции умножения.

Очевидно, что всякое поле содержит не менее двух элементов. В поле нет делителей нуля, т.к. равенство $ab=0$ при $a\neq 0$ влечет

$$a^{-1}ab=a^{-1}0=0$$

Подмножество S кольца R называется подкольцом этого кольца, если оно замкнуто относительно имеющихся операций сложения и умножения и само образует кольцо относительно этих операций.

Подкольцо H кольца R называется идеалом (двухсторонним идеалом) этого кольца ,если для всех , $a\in H$ $r\in R$ имеет место $ar\in H, ra\in H$.

Пусть область целостности ***R*** содержит единичный элемент ***e***.
Рассмотрим элемент $ne = \underbrace{e + \dots + e}_{n}, n \geq 0.$
Возможны два случая.

А) не существует такого $n \in N$, что ; $ne = 0$
Б) существует такое $n \in N$, что ; $ne = 0$

Возьмем минимальное ***n*** с таким свойством.
В первом случае говорят, что характеристика области целостности равна нулю, $charR = 0$.
Во втором случае полагают $charR = n$.

Поля

Основные понятия

Полем называется множество $\mathcal{F}$

с операциями *сложения* и *умножения,*

Примерами являются

Q - поле рациональных чисел,

R - поле действительных чисел,

C - поле комплексных чисел,

Поле $\mathcal{K}$,
такое, что $\mathcal{F} \subset \mathcal{K}$,
называется расширением поля $\mathcal{F}$,
например, поле *C* есть расширение как поля *Q*, так и поля *R*,
последнее является расширением поля *Q*.

Число *к* элементов поля называется *порядком* поля.

Различают бесконечные поля (например, множество рациональных чисел)

и

конечные поля, например, поле $\{0,1\}$ с операциями сложения по модулю два и умножения.

Конечные поля называются *полями Галуа* .

Поле Галуа порядка *к* обозначается *GF(k)* или $\mathcal{F}_k$.

Простейшим конечным полем является бинарное поле *GF{2)* с операциями $\oplus$ сложения по модулю 2 и

- умножения.

Эти операции определяются таблицами

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Отношение конгруэнтности (сравнимости) по модулю данного числа m

на расширенном (включающем число 0) множестве натуральных чисел N^+ ,

является отношением эквивалентности и разбивает

множество N^+ на классы эквивалентности, или смежные классы, по модулю m.

В качестве обозначений этих классов можно взять наименьшие числа классов.

Множество смежных классов по модулю m (или их обозначений) с операциями сложения и умножения по модулю m

на множестве обозначений этих классов

является полем тогда и только тогда,

когда m = p, где p - простое число.

Единицами по сложению и умножению этого поля GF(p) являются классы, содержащие числа 0 и 1 соответственно.

Элемент g поля называется *примитивным,* или *образующим,* если для любого другого ненулевого элемента a поля найдется неотрицательное число x, такое, что $a = g^x$.

Поле классов конгруэнтности целых чисел по модулю простого числа p $GF(p)$
(обозначается также Z/pZ или Fp) и
называется простым полем.

Если многократное сложение 1 не позволяет получить 0, то поле называется полем характеристики ноль, в этом случае оно содержит копию поля рациональных чисел.

В противном случае, если существует простое число p такое, что p-кратное сложение 1 даёт 0, число p называется характеристикой поля.

В этом случае поле содержит копию поля Z/pZ.